

ID–software ver. 3.10.3 (released 15.04.2015 <https://installer.id.ee>)

- Supported operating systems:
 - Windows 7 SP1 32bit and 64bit,
 - Windows 8 32bit and 64bit,
 - Windows 8.1 32bit and 64bit,
 - Mac OS X 10.8, 10.9, 10.10 (only Intel),
 - Windows Server 2008 R2
 - Windows Server 2012
- [Source Code](#)
- Browsers: the latest browsers supported by the operation systems are supported.
 - Windows: Internet Explorer, Mozilla Firefox, Google Chrome
 - Mac OSX: Mozilla Firefox, Safari, Google Chrome
 - Linux: Mozilla Firefox, Google Chrome
- Packaging release notes
- Running windows installer with ENABLENPAPI=OFF key disables enabling NPAPI support in Chrome. Windows installer doesn't check if chrome is running and updater is not executed. This makes it possible to run windows installer quietly. The ENABLENPAPI=OFF key does not work when upgrading from 3.10.2 to 3.10.3.

ID–software ver. 3.10.2 (released 06.04.2015 <https://installer.id.ee>)

- Supported operating systems:
 - Windows 7 SP1 32bit and 64bit,
 - Windows 8 32bit and 64bit,
 - Windows 8.1 32bit and 64bit,
 - Mac OS X 10.8, 10.9, 10.10 (only Intel),
 - Ubuntu 14.04 32bit and 64bit, Ubuntu 14.10 32bit and 64bit,
 - Windows Server 2008 R2
 - Windows Server 2012
- [Additional info](#)
- [Source Code ja source distribution packages](#)
- Browsers: the latest browsers supported by the operation systems are supported.
 - Windows: Internet Explorer, Mozilla Firefox, Google Chrome
 - Mac OSX: Mozilla Firefox, Safari, Google Chrome
 - Linux: Mozilla Firefox, Google Chrome
- Packaging release notes
- Added functionality for enabling NPAPI support in Chrome. Windows installer checks if Chrome is running and executes Updater. The `-chrome-npapi` flag is set by Updater.
- Added functionality for enabling NPAPI support in Chrome. OSX installer checks if Chrome is running and executes Updater. The `-chrome-npapi` flag is set by Updater.

- ID-updater release notes
- Added functionality to OSX and Windows ID-Updaters for enabling NPAPI support in Chrome browser, the `-chrome-npapi` flag is set.
- Added `chrome-token-signing` component's version number information to the OSX ID-Updater's diagnostics GUI.
- Added functionality for identifying Windows 10 operating system in Windows ID-Updater.
- Added the external server's URL value to debugging view.
- Implemented usage of the operating system's proxy settings via QT in case of Windows platform.
- Added diagnostics GUI view for OSX ID-Updater that enables to view information about the web components that are updated.
- Chrome Token Signing release notes
- Changed native messaging API <https://github.com/open-eid/chrome-token-signing/wiki/NativeMessagingAPI>
- Added native messaging hosts for OSX and Windows
- Changed linux native messaging host UI from using GTK to QT
- Native messaging hosts changed to being stateful
- to maintain certificate selection binding (only user-confirmed certificate can be used for signing)
- to check for same origin in all messages after first technically valid CERT request containing origin
- Added python test suite for native messaging hosts
- Improved logging
- Changed error codes to use string constants instead of numbers
- Changed extension API
- Moved extension to Chrome Web Store
- Added branding to extension
- Changed versioning – starting from 1.0.0

ID-software browser integration package ver. 3.10.1 (released 19.03.2015 (Mac OS X <https://installer.id.ee>))

- Supported operating systems:
 - Mac OS X 10.8, 10.9, 10.10 (only Intel)
- Fixed 3.5 card version ID-card and digi-ID problem which occurred when a Mac OS X browser plugin was used with a card reader supporting extended APDU.
- Software development can now be monitored in GitHub environment:
- <https://github.com/open-eid/esteid-pkcs11>

- <https://github.com/open-eid/esteid-tokenid>
- [Source Code](#)

ID–software ver. 3.10 (released 05.03.2015 (Windows) and 06.03.15 (Linux) <https://installer.id.ee>)

- Supported operating systems:
 - Windows 7 SP1 32bit and 64bit,
 - Windows 8 32bit and 64bit,
 - Windows 8.1 32bit and 64bit,
 - Mac OS X 10.8, 10.9, 10.10 (only Intel),
 - Ubuntu 14.04 LTS 32bit and 64bit, Ubuntu 14.10 32bit and 64bit,
 - Windows Server 2008 R2
 - Windows Server 2012
- [Additional info](#)
- [Source Code](#)
- Source distribution package
- Browsers: the latest browsers supported by the operation systems are supported.
 - Windows: Internet Explorer, Mozilla Firefox, Google Chrome
 - Mac OSX: Mozilla Firefox, Safari, Google Chrome
 - Linux: Mozilla Firefox, Google Chrome

DigiDoc3 client release notes (OS X version released in AppStore 05.03.2015)

- Started using BDOC as the default digital signature container format instead of DIGIDOC–XML 1.3.
- Added information about BDOC format to signing introduction window.
- Added support for creating ASiC–E signatures (BDOC with time–stamps).
- Updated options for selecting the default digital signature container format in the "Settings" menu's "Signing" tab. Added option for ASiC–E format.
- Implemented functionality of using the appropriate signature format in case of adding signatures to existing BDOC and ASiC–E containers. By default, the format of the existing signature is used for new signatures.
- Implemented TSL Trust service Status list functionality for BDOC and ASiC–E formats. TSL is used for checking the trustworthiness of trust–services (CA, OCSP, time–stamping services) during signature creation and validation. The European Commission's (EC) TSL list (https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml) is used for finding the trusted national TSL lists.
- Certificates of all the EU member states' trust services that are registered in national TSL lists are supported.
- By default, the Estonian national TSL list (<http://sr.riik.ee/tsl/estonian-tsl.xml>) is used.
- Added the European Commission's TSL URL value to the signature details view.

- Implemented TSL progress bar that indicates the progress of loading the TSL data during the application's startup.
- Implemented automatic checking for new TSL versions. Added possibility to deactivate the automatic version check with the "Online TSL digest check" checkbox under "Settings" menu's "General" tab.
- Added pop-up notification to the user if the TSL version check was unsuccessful.
- Started using older version of esteid-pkcs11 driver in case of OSX 10.9 and earlier OSX versions.
- Fixed problem with "Send container to email" functionality with Thunderbird e-mail client. Added identification of the user's default e-mail client and implemented Thunderbird workaround for attachments
- Fixed problem with "Send container to email" functionality that appeared in OSX in case of Outlook e-mail client. Added Outlook to sandbox exception list.
- Software development can now be monitored in GitHub environment:
<https://github.com/open-eid/qdigidoc>
- DigiDoc3 crypto release notes
- Changed the usage of intermediate DDOC containers during encryption
- By default, intermediate DDOC container is not used when encrypting a single data file. Note that such encrypted document cannot be decrypted with DigiDoc3 Crypto versions 3.8 and earlier.
- Added checkbox to "Settings" menu's "General" view that enables to always use intermediate DDOC containers for interoperability with DigiDoc3 Crypto versions 3.8 and earlier.
- Fixed format error in the intermediate DDOC container's <DataFile> element's Size attribute. The value is now generated in bytes with no suffix.
- Improved memory usage with large files
- Added functionality to display information of the new E-resident Digi-ID certificate in the main window's "Keys" section
- Improved displaying of the encrypted document's name in the container content view. Previously the encrypted document's name was not displayed in case of minor format errors (e.g. in case of encrypted penalty documents).
- Improved handling of non latin1 characters in CDOC documents
- Improved handling of data files to avoid reading an incorrect file from the user's file system when the file name contains slash characters.
- Fixed the translation of some buttons that on OSX platform appeared in English even if the chosen language was Russian or Estonian.
- Software development can now be monitored in GitHub environment::
<https://github.com/open-eid/qdigidoc>
- ID-card Utility release notes
- Added "Clean certs" button to "Settings" menu that enables to remove old certificates from Windows Certificate Store.
- Created separate installation package for Windows environment
- Fixed crash that occurred when using RDP session

- Improved visual representation of long e-mail and name values
- Improved representation of the certificates' validity date in the ID-card utility's main window. When the end of validity is at 00:00 then the date of the following day is shown (instead of the previous day).
- Software development can now be monitored in GitHub environment::
<https://github.com/open-eid/qesteidutil>
- Packaging release notes
- Changed Windows and OSX installation packages, SK's certificates are no longer installed to the certificate store, previously installed SK certificates are removed. The SK CA certificates are distributed through the operating system's native update mechanism.
- Fixed packaging of Latvian and Lithuanian CA certificates , the certificates are no longer included in the Estonian DigiDoc3 Client's distribution for Linux platform.
- 2010 C++ Runtime is now installed only when msvcp100.dll file is not found in System32 folder to resolve problem with ID-software installation in Windows Server 2012.
- Upgraded signing of OSX distribution packages, v2 signature is now used.
- Removed Safari browser signing plug-in from OSX installation package, Firefox NPAPI plug-in is used instead.
- esteid-tokenend and esteid-pkcs11 drivers
- Fixed problem with version 3.5 ID-card and Digi-ID that occurred with smart card readers that support extended APDUs when using browser plug-in in OS X 10.10.
- Software development can now be monitored in GitHub environment: <https://github.com/open-eid/esteid-pkcs11> and <https://github.com/open-eid/esteid-tokenend>

DigiDoc3 Client ver 3.9.2 for Mac OS X (released 14.01.2015 [App Store](#))

- Supported op. systems:
 - Mac OS X 10.7, 10.8, 10.9, 10.10 (only Intel),
- [Additional info](#)
- [Source code](#)
- Fixes
- Added support for Mac OS X 10.10
- BDOC as the default digital signature container (only for new installations, do not apply for updates)

ID-card Utility ver. 3.10 for Mac OS X (released 15.12.2014 [App Store](#))

- Supported op. systems:
 - Mac OS X 10.8, 10.9, 10.10 (only Intel),
- [Additional info](#)
- [Source code](#)
- Added support for Mac OS X 10.10

ID–software ver. 3.9 SP1 (released 08.10.2014 <https://installer.id.ee>)

- Supported operating systems:
 - Windows 7 SP1 32bit and 64bit,
 - Windows 8 32bit and 64bit,
 - Windows 8.1 32bit and 64bit,
 - Mac OS X 10.7, 10.8, 10.9 (only Intel),
 - Ubuntu 14.04 32bit and 64bit, Ubuntu 13.10 32bit and 64bit,
 - Windows Server 2008 R2
 - Windows Server 2012
- [Additional info](#)
- [Source Code](#)
- [Source distribution package](#)
- Browsers: the latest browsers supported by the operation systems are supported.
 - Windows: Internet Explorer, Mozilla Firefox, Google Chrome
 - Mac OSX: Mozilla Firefox, Safari, Google Chrome
 - Linux: Mozilla Firefox, Google Chrome
- C library DDOC security fixes
- Improved XML structure validation for DDOC files. This is a highly relevant security fix having an effect on the validation of DDOC files. The unfixed library can mistakenly give positive results on validation of invalid DDOC files with incorrect XML elements ordering.
- esteid–plugin
- Added 64–bit browser signing plug–in for 64–bit Chrome browser in Windows environment.
- DigiDoc3 client release notes
- Fixed problems with DDOC and BDOC file extensions in OSX. Previously, in some cases the .ddoc or .bdoc file extensions were not set according to the document's format when saving the document to file system.
- Upgraded OSX DigiDoc3 Client and Crypto distribution package signing, v2 signature is now used.
- DigiDoc3 crypto release notes
- Fixed decryption of CDOC documents that were encrypted with DigiDoc Crypto version 2.7. Previously, decryption did not succeed in Linux environment.
- Upgraded signing of DigiDoc3 Client and Crypto OSX distribution package, v2 signature is now used.
- Packaging release notes
- Fixed Windows installation package parameter that can be used by administrators to avoid installing the default certificates that are included in the package. Otherwise, the default certificates are re–installed and existing certificates are overwritten.
- Started using QT version 5.3.1 in OSX environment.
- Fixed KLASS3–SK 2010 certificate's installation problem in Windows.
- Removed test certificates from DigiDoc3 Client packaging in OSX.

- New Minidriver release
- Fixed RDP problem with WUDF driver.
- Added functionality of reading card owner's personal code, first name and surname from AUTH certificate in case of Digi-ID cards.
- Added SMARTCARDPP_NOPINPAD environment variable support for all platforms.
- Fixed PINPAD detection bug that occurred when two or more readers were connected.

ID-software ver. 3.9 (released 01.07.2014 <https://installer.id.ee>)

- Supported operating systems:
 - Windows 7 SP1 32bit and 64bit,
 - Windows 8 32bit and 64bit,
 - Windows 8.1 32bit and 64bit,
 - Mac OS X 10.7, 10.8, 10.9 (only Intel),
 - Ubuntu 14.04 32bit and 64bit, Ubuntu 13.10 32bit and 64bit,
 - Windows Server 2008 R2
 - Windows Server 2012
- [Additional info](#)
- [Source Code](#)
- [Source distribution package](#)
- Browsers: the latest browsers supported by the operation systems are supported.
 - Windows: Internet Explorer, Mozilla Firefox, Google Chrome
 - Mac OSX: Mozilla Firefox, Safari, Google Chrome
 - Linux: Mozilla Firefox, Google Chrome
- DigiDoc3 client release notes
- Changed OCSP validity confirmation server access certificate usage for private persons. A default access certificate is installed along with the software's installation. The same default server access certificate is used in case of all private persons, the private person does not have to manage the access certificate's installation anymore.
- Added monthly signature counter functionality, signatures that are created during one month are counted.
- Added OCSP validity service usage conditions' confirmation to signing intro view.
- Added warning message that is displayed when trying to create a new signature but the monthly signature counter value is over limit.
- If the default access certificate has expired then signing is no longer possible with the current version of the software, the software must be updated.
- Changed the OCSP server access certificate related notification messages for business users. No other changes were made for business users regarding server access certificates.
- Implemented automated ID-software version check that periodically checks from server if the currently installed ID-software version is up-to-date and officially supported.

- Added warning message that is displayed if the software version check has not succeeded after 7 or more consecutive days. Added possibility to prevent the message from appearing consecutively.
- Implemented Kill Switch functionality that is executed if the currently installed ID–software version is not supported or if the automated software version check has not succeeded during 12 months' period.
- Added restriction so that the ID–software cannot be used if the Kill Switch has been executed. Information in a pop–up window about required update of the software is displayed, the ID–software window is closed after the user clicks OK and the current software version cannot be used.
- Added support for validating BDOC signatures with time–stamps (BDOC–TS profile).
- Implemented changes to "Signature" tab ("Show details" view):
- BDOC–TS signature's format is displayed as "BES/time–stamp" in the "Signature format" data field.
- Added button "Show TSA certificate". The Time–Stamping Authority's certificate is displayed when clicking on the button.
- Added data fields "TSA time", "TSA time (UTC)", "TSA certificate issuer".
- The signature creation time of BDOC–TS signature is the time–stamp's creation time (in case of a signature with time–stamp, the OCSP validity confirmation's creation time is the signing time). The value is displayed in "Signed on" field in the main window, "TSA time" field in "Signature" tab ("Show details" view), "Time" field in Validity Confirmation Sheet ("Print Summary" window).
- Default time–stamping service is not set
- Fixed problem with extracting data files from DDOC container if the data file's name contains special characters.
- Implemented changes for using new DigiDocService web service's API during M–ID signing. The data file's mimetype value is now also set to the service.
- Added error message "Invalid phone number! Please include country code" that occurs during M–ID signing when the user has not inserted mobile number's country code or the country code is incorrect.
- Fixed error with M–ID signing in OSX. The problem occurred when the data file's name contained special characters, an erroneous signature was created as a result.
- Fixed problem with M–ID signing in OSX, added check that PKCS#11 driver is called out only when PC/SC process is running. Previously, M–ID signing was occasionally not successful and produced libdigidoc error 16 if there was no ID–card reader connected to the computer during signing.
- Fixed „Send container to e–mail“ functionality. Previously, the BDOC or DDOC container was not added as an attachment to the e–mail in OSX platform.
- Changed the signed document's signing time display format in "Time" field of the Validity Confirmation Sheet (Print Summary window). The signing time is now displayed in the local time instead of UTC time.
- Changed the text that is displayed in case of signature that is valid with warnings.

- Added text "NB! WARNINGS" to the Validity Confirmation Sheet ("Print Summary" window) in case of signatures that are valid with warnings.
- Added text "NB! TEST SIGNATURE" to the Validity Confirmation Sheet ("Print Summary" window) in case of signatures that are created by using test-certificates.
- Removed "Help" button from the error message pop-up window.
- Conducted code review, removed obsolete code.
- DigiDoc3 crypto release notes
- Implemented automated DigiDoc3 Crypto version check that periodically checks from server if the currently installed software version is up-to-date and officially supported.
- Added warning message that is displayed if the software version check has not succeeded after 7 or more consecutive days. Added possibility to prevent the message from appearing consecutively.
- Implemented Kill Switch functionality that is executed if the currently installed software version is not supported or if the automated software version check has not succeeded during 12 months' period.
- Added restriction so that the software cannot be used if the Kill Switch has been executed. Information in a pop-up window about required update of the software is displayed, the DigiDoc3 Crypto window is closed after the user clicks OK and the current software version cannot be used.
- Added support for efficient BDOC decryption. Decrypting CDOC document that contains a directly encrypted BDOC file (that has not been added to additional DDOC container before encryption).
- Removed Libdigidoc library's dependency. Added functionality that enables creating and parsing CDOC and DDOC files during encryption and decryption operations.
- Fixed encryption error in OSX. Previously, the encrypted data was not actually added to CDOC container if there was no ID-card reader connected to the computer during encryption.
- Fixed error that occurred when trying to encrypt or decrypt data file with the size of 0 bytes. Previously, the file could not be opened from the main window before encryption nor after decryption.
- Improved recipient search settings in "Add recipient" view when searching for recipient according to company's name or registration number. Now, SSL/TLS certificates are not displayed, only Digital Stamp certificates are shown.
- Removed "Settings" menu.
- Removed "Help" button from the error message pop-up window.

ID-software ver. 3.8.2 (released 07.03.2014 <https://installer.id.ee>)

- Supported op. systems and browsers are the same as ver. 3.8. [Additional info.](#)
- [Source Code](#)
- [Source distribution package](#)
- Packaging release notes

- Added Microsoft Visual C++ 2008 SP1 run-time library for Windows XP SP3 users to fix authentication with smart card in Internet Explorer browser.
- Fixed the removal of smart card ATR entries during Minidriver installation, existing ATR entries which have been created during installing Minidriver from MS Update are not removed when installing ID-card software package which supports the same Minidriver version.
- Changed ID-card software installation in Windows environment to improve EstEID plugin usage in Internet Explorer browsers. During ID-card software installation, the user's group policy settings are altered so that EstEID plugin usage is automatically allowed in Internet Explorer, additional confirmation is no longer asked from the user in the browser. As a result, the EstEID plugin can not be manually disabled in Internet Explorer settings, the user has to uninstall ID-card software package to remove the plugin.

ID-software ver. 3.8.1 (released 29.01.2014 <https://installer.id.ee>)

- Supported op. systems and browsers are the same as ver. 3.8. [Additional info.](#)
- [Source Code](#)
- [Source distribution package](#)
- DigiDoc3 client release notes
- Removed the modification restriction (adding and removing signatures) for the DDOC files whose X509IssuerName and X509SerialNumber elements are in the wrong namespace.
- Server access certificate import to OSX keychain has been improved to not display the private key export notification during DigiDoc3 client signing.
- Server access certificates are no longer displayed in Safari web browser during authentication.
- Packaging release notes
- Minidriver component installation was improved for DELL and HP computers as some users were getting "Please insert a smart card ... Unknown Card" error while authenticating to e-services and DigiDoc3 client could not find an ID-card.
- For specific DELL computers the EnableScPnP parameter was changed to Windows default.
- For specific HP computers the overlapping ActivIdentity ProtectTools ATR records with ID-card were removed.
- Separate package release for Windows XP users that are using specific outdated graphic card drivers that cause DigiDoc3 client and ID-card utility crashes. Users with this problem should contact abi@id.ee
- Mac OS X ID-software installation process no longer tries to remove OpenSC package.
- Other
- Authenticating with ID-card in Firefox web browser for Mac OS X has been improved by adding the *one-pin* module.

ID-software ver. 3.8 (released 10.12.2013 <https://installer.id.ee>)

- Supported operating systems:
 - Windows XP SP3 32bit,
 - Windows 7 SP1 32bit and 64bit,
 - Windows 8 32bit and 64bit,
 - Windows 8.1 32bit and 64bit,
 - Mac OS X 10.7, 10.8, 10.9 (only Intel),
 - Ubuntu 12.04 32bit and 64bit, Ubuntu 13.10 32bit and 64bit,
 - Windows Server 2008 R2
 - [Additional info](#).
- Browsers: the latest browsers supported by the operation systems are supported.
 - Windows: Internet Explorer, Mozilla Firefox, Google Chrome
 - Mac OSX: Mozilla Firefox, Safari, Google Chrome
 - Linux: Mozilla Firefox, Google Chrome
 - [Source Code](#)
 - [Source distribution package](#)
 - DigiDoc3 Client release notes
 - Added BDOC 2.1 document format support.
 - Added Elliptic Curve Cryptography (ECC) based certificates support for BDOC 2.1 format.
 - Changed the distribution of DigiDoc3 Client for OSX platform. DigiDoc3 Client (common application for Client and Crypto) and Utility program are now available only from Apple App Store.
 - Added signature status "valid (with warnings)"
 - Added support for validation of signatures that are created with Finnish ID-card. The certificate files have to be installed with separate packages.
 - Improved the user's notification in case of altering old and not supported DigiDoc file formats (SK-XML 1.0, DIGIDOC-XML 1.1, 1.2).
 - Moved signature and OCSP confirmation information to a single Signature tab (in "Show details" window), optimized the information that is displayed.
 - Improved of displaying the signature creation time in case of daylight saving time.
 - Added field of OCSP validity confirmation time in UTC format to Signature tab in "Show details" window.
 - Changed the name of the field "Signing time" to "Signer's computer time (UTC)" in Signature tab ("Show details" window). The time is shown in UTC format.
 - Fixed the problem of not showing the time of the day in the signer certificate's validity period fields in Signature tab (in "Show details" window).
 - Replaced the field "Hash value of validity confirmation (OCSP response)" with "Hash value of signature" in Validity Confirmation Sheet (Print Summary view).
 - Added "Generate certificate" button to Server Access Certificate tab (under "Settings" window). The button enables to generate a new server access certificate if the previous one is expired or about to expire.

- Changed the name of the field “Hash value of issuer’s public key” to “Authority key identifier” in Validity Confirmation Sheet (Print Summary view).
- Added notification to the user when trying to view Validity Confirmation Sheet if there is no printer installed in the user’s system.
- It is now allowed for a person to give more than one signature to a single DigiDoc document. Notification is displayed to the user before adding a complementary signature to a document that he/she has previously signed.
- Changed the displaying of Digital signing intro, the intro is shown to the user when signing the first document instead of running the application for the first time.
- Fixed the problem of the application not responding in specific situations when signing two documents in parallel in two DigiDoc3 Client application windows with ID-card.
- Fixed the problem in OSX platform that caused the application to open multiple overlapping windows when signing from context menu or opening a DigiDoc file with double click.
- Fixed the problem in Windows with using \ characters as folder separators in digidocpp.conf configuration file’s OCSP server access certificate’s file name (parameter "pkcs12.cert"). Now, both / and \ characters are supported as folder separators in the parameter value.
- Fixed the problem of mistakenly overwriting an existing data file with the same name when saving data files to disk and not choosing to overwrite the file.
- Fixed the problem of not being able to concurrently open two data files that have the same name but are in different DigiDoc containers.
- Fixed the problem with updating the notification “This container is signed by you” which shows if the current DigiDoc container is signed by the owner of the ID-card which is inserted into card reader.
- Fixed the problem with crash reports in OSX platform in case of application that was installed from Apple App Store. Improved the crash report system.
- Started using coverity.com static analysis tool to find source code defects and vulnerabilities. Fixed the defects that were discovered.
- Optimized sending status requests to DigiDocService web service during signature creation with Mobile-ID.
- Qt framework has been updated to version 5.2 in OSX, version 5.1.1 in Windows environments, version 5.0.2 in Ubuntu 13.10, version 4.8 in Ubuntu 12.04.
- Security fix. Client side verification for DigiDocService web site certificates added (while creating a TLS connection to DigiDocService website). The missing verification step was discovered analytically. No attacks or malware are known to take advantage of the missed control.
- DigiDoc3 Crypto release notes
- DigiDoc3 Crypto and DigiDoc3 Client are now run with a single executable file.

- Changed the distribution of DigiDoc3 Crypto for OSX platform. DigiDoc3 Client (common application for Client and Crypto) and Utility program are now available only from Apple App Store.
 - Added functionality to the Used Certificates and SK certificates tabs (in Add Recipient window), it is now possible to sort the previously used certificates list by owner, type, issuer and expiry date.
 - Added functionality to search for the recipient's certificate by company's registry number (in Add recipient view). Can be used when searching for certificates issued to legal entities.
 - Fixed the error situation which occurred when using special characters when searching for recipient's certificate by company name.
 - ID-card Utility release notes
-
- Changed the distribution of DigiDoc Utility program for OSX platform. DigiDoc Utility program and DigiDoc3 Client (common application for Client and Crypto) are now available only from Apple App Store.
 - Added warning message which is displayed if the inserted ID-card is issued in 2011 and the card's electronic component has not been renewed.
 - Fixed problems with Apple App Store version of ID-card utility, including crash report system.
 - Changed the default format in which the card owner's certificates are saved into the user's computer, PEM format is now used.
 - Changed the public key size calculation method to show the exact size of the key in a certificate's "public key" field.
 - Fixed the problem that did not enable manual updating of the ID-card software in the Settings window before the automatic software updater's execution is on.
 - Added "Run Task Scheduler" button to the Settings window to see the schedule when the next ID-card software update is executed.
 - Started using coverity.com static analysis tool to find source code defects and vulnerabilities. Fixed the defects that were discovered.
 - Qt framework has been updated to version 5.2 in OSX, version 5.1.1 in Windows environments, version 5.0.2 in Ubuntu 13.10, version 4.8 in Ubuntu 12.04.
 - Id-Updater release notes
-
- Created new ID-card software updater for OSX platform by using the platform's own tools. The ID-Updater application can be managed from System Preferences.
 - Improved Updater's execution in Windows platform, the updater is run on laptops regardless of whether the user is on battery power or AC power.
 - Improved Updater system to distribute the server's load when necessary.
 - Changed the user-agent data that is sent to the server with Windows Updater, the version number of the whole .msi package is now sent instead of only the version number of the Updater.

- Packaging release notes
- Created browser integration package for OSX platform that installs the components which are not accessible from Apple App Store and are needed to use ID-card. Added the ID-card software uninstalling script into OSX package. Discontinued packaging of the general ID-software package for OSX platform, the ID-software components are now distributed separately via Apple App Store and the browser integration package.
- Changed the process of distributing SK root certificates in case of Linux environment. The certificates are now distributed via Firefox CA certificates package.
- Fixed Ubuntu Debian packaging errors that were discovered by using Lintian tool.
- Improved Windows installer: added translation to Estonian language and implemented new design.
- Other
- Ended support for CSP
- SmartCardRemoval service has been removed from main ID-software package.
- Stopped using onepin-opensc-pkcs11.so module in Windows and Linux environments as the module is no longer distributed with OpenSC package.
- Started using esteid-pkcs11 and esteid-token drivers in OSX (instead of OpenSC).
- Bug fixes in version 3.8.0.1430, released 16.12.2013.
- Fixed the problem which requested for an additional accept to install Windows Minidriver during installation of Windows package.
- Bug fixes in version 3.8.0.1435, released 19.12.2013.
- Fixed the problem which caused Firefox browser to request PIN2 during authentication. Error occurred during initial activation of Firefox after installing the ID-software and ID-card was not in reader.

ID-software ver. 3.7.2 (released 22.08.2013 <https://installer.id.ee>)

- Supported op. systems and browsers are the same as ver. 3.7
- [Source Code](#)
- [Source distribution package](#)
- Removed support for BDOC 1.0 format. It's not possible to create or verify BDOC files.
- Fixed one critical bug in the DDOC parsing routines. By persuading a victim to open a specially-crafted DDOC file, a remote attacker could exploit this vulnerability to overwrite arbitrary files on the system with the privileges of the victim.

ID-software ver. 3.7.1 (released 09.04.2013 <https://installer.id.ee>)

- Supported op. systems and browsers are the same as ver. 3.7
- [Source Code](#)
- [Source distribution package](#)
- Changed the handling of DigiDoc container which has no xmlns attribute in the <DataFile> element. [Additional info.](#)
- Added Windows registry cleanup of old ID–software 2.x.x entries before software installation.
- The phone number format has changed in DigiDoc3 client software, the new format is 372xxx (previously +372xxx). Symbols, for example +, are not allowed any more.
- **Bug fixes compared to 3.7.1 version 3.7.1.1204 released on 09.04.2013**
- Improved Windows registry cleanup of old ID–software 2.x.x entries before software installation.

ID–software ver. 3.7 (released 22.01.2013 <https://installer.id.ee>)

- Supported operating systems:
 - Windows XP SP3 32bit
 - Windows Vista SP2 32bit and 64bit
 - Windows 7 SP1 32bit and 64bit
 - Windows 8 32bit and 64bit
 - Mac OS X 10.6, 10.7, 10.8 (only Intel)
 - Ubuntu 12.04 32bit and 64bit, Ubuntu 12.10 32bit and 64bit
 - Fedora 17 32bit and 64bit
 - openSuse 12.2 32bit and 64bit
 - Windows Server 2008 R2
- Browsers: the latest browsers supported by the operation systems are supported.
 - Windows: Internet Explorer, Mozilla Firefox, Google Chrome
 - Mac OSX: Mozilla Firefox, Safari
 - Linux: Firefox
- [Source Code](#)
- [Source distribution package](#)
- ID–card utility meets the requirements of Apple and is separately downloadable from Apple App Store.
- Windows Minidriver component meets the requirements of Microsoft and will be automatically installed from Windows Update under Windows 7 and 8. Read more [here](#).
- Web browser authentication PIN–dialogue has been unified for Windows Vista, 7 ja 8 (except for Mozilla Firefox web browser). Identical PIN–dialogue window is also used in DigiDoc3 client and crypto.
- Instead of CSP component a Windows Minidriver component is used for Windows XP, this ensures better reliability for notebook users and also changes the PIN–dialogue window. As a side effect it's not possible to use ID–card authentication over RDP connection to Windows XP server with Internet Explorer and Chrome web browsers.

- Certificate registration dialogue window in ID-card utility has been replaced with automatic certificate registration on every ID-card utility launch.
- Under Windows the ID-card utility will be launched after ID-card software installation.
- Java Applet digital signing component support has been removed from web browsers. This means that it is not possible to digitally sign in web services that use Java Applet. ID-card software package no longer installs the PKCS11Wrapper.dll Applet module and when upgrading from older ID-card software it will be deleted from the computer.
- Active-X digital signing component support has been removed from web browsers in Windows XP. This means that it is not possible to digitally sign in web services that use Active-X.
- Digital stamps on USB crypto tokens can be used in DigiDoc3 client in Windows operating systems (except XP) without additional configuration changes (*-capi* parameter).
- Changes to DigiDoc3 client Settings menu regarding Server Access Certificate installation, removal and information display.
- Added hint about new ID-card chip location to the DigiDoc3 client and crypto when no card can be found in the reader.
- ID-card utility diagnostics now displays the card reader driver name and both ATR's.
- DigiDoc3 client and crypto info menu now has the ability to view and save diagnostics.
- ID-card utility, DigiDoc3 client and crypto info menu now has a licence information of the sub libraries used for software creation.
- Under Mac OSX the DigiDoc3 crypto is not a separate application any more and can be opened through DigiDoc3 client only (choice - I want to: encrypt files for secure transfer).
- In DigiDoc3 client it is no longer possible to add signatures or create the containers in old Digidoc 1.0, 1.1 and 1.2 formats. It's still possible to verify signatures and open contained documents in these old Digidoc containers.
- The documentation of the [jdigidoc](#), [libdigidoc](#) and [COM](#) libraries has been updated.
- The following bugs have been fixed:
 - Russian version of DigiDoc3 client signature confirmation sheet has a translation error, which causes for a valid signature to be shown as invalid on signature confirmation sheet.
 - Digital signing with Mobile-ID in DigiDoc3 client fails when a proxy server has been configured.
 - When DigiDoc3 client server access certificate settings have both IP based access and expired access certificate configured then digital signing with Mobile-ID fails.
 - DigiDoc3 crypto will crash if before encrypting the document in the container is saved, opened with a doubleclick or drag'n'dropped from the container.
 - DigiDoc3 crypto will crash if before encrypting the addressee is removed.
 - DigiDoc3 crypto displays file path along with file name for encrypted documents.
 - In some cases ID-card utility displays birth date with 1 day difference.
 - Entering a wrong PIN in Internet Explorer under Windows XP (or if CSP is used) will display a misleading error message.

- Improvements to Mozilla Firefox 18 authentication module, which caused involuntary browser restarting after software installation.
- Added the check of the nonce field of the signature for DDOC signing and verification. This is a highly relevant security fix having an effect on the verification of DDOC files. The unfixed library can mistakenly give positive results on verification of invalid DDOC container with the wrong nonce field value on the signature.
- .ddoc security updates. Please find more detailed info at [jdigidoc](#), [libdigidoc](#) pages.
- **Bug fixes compared to 3.7 beta version released on 14.12.2012**
- Fixed a bug that caused digital signing to fail in digidoc.sk.ee portal using Firefox and Chrome under Windows.
- **Bug fixes compared to 3.7 version 3.7.0.1110 released on 22.01.2013**
- Fixed a bug that prevented launching DigiDoc3 client and ID-card utility under Windows XP. Users got a following error: "This application has failed to start because the application configuration is incorrect. Reinstalling the application may fix this problem."
- Fixed a bug that caused digital signing failure in e-services under Windows XP with an error "Please insert a smart card".
- **Bug fixes compared to 3.7 version 3.7.0.1114 released on 31.01.2013**
- Fixed a bug that prevented launching Firefox web browser. More information about this bug can be found at: <http://sander85.com/2013/02/01/id-tarkvara-3-7-firefox-ei-kaivitu/>

ID-software ver. 3.6 (released 27/06/2012 at <http://installer.id.ee>).

- Supported OS:
 - Windows XP SP3, 32-bit and 64-bit
 - Windows Vista SP2, 32-bit and 64-bit
 - Windows 7 SP1
 - Mac OS X 10.6 and 10.7 (both Intel)
 - Ubuntu 12.04 32-bit and 64-bit
 - Fedora 16 32-bit and 64-bit
 - openSuse 12.1 32-bit and 64-bit
- Browsers: the latest browsers supported by the operation systems are supported.
 - Windows: Internet Explorer, Mozilla Firefox, Google Chrome.
 - Mac OSX: Mozilla Firefox, Safari.
 - Linux: Firefox.
- [Source Code](#).
- Support for visually impaired users has been added and tested with the NonVisual Desktop Access screen reader (NVDA).
- Support for Gemalto Ezio Shield PinPAD card reader has been added.
- Support for the Windows 2008 R2 server has been added.
- Support for the generation of automatic error report (the crash report system) when the software stops working has been added.

- An update has been made for the functionality of automatic certificate deletion to be set up manually (Windows); by default software certificates are not deleted from the Windows Certificate Store automatically.
- Added key usage check in certificate on verification of a signature.
- Text has been added to explain that the filling of the role and resolution fields in the DigiDoc3 client is not obligatory for signing.
- When opened, the DigiDoc3 client automatically displays the option chosen last time when a signature was successfully provided (it used to display “Use the ID-card” at all times before).
- The display of the error message in case of a failure to update automatically has been updated.
- The text displayed in the “Settings” menu of the DigiDoc3 client if the BDOC format is selected has been changed. The BDOC format is being updated to comply with the new ASiC signature container standards ([ETSI TS 102 918](#), [ETSI TS 103 171](#), [ETSI TS 103 174](#)), so the BDOC format supported at the moment will undergo further modifications. Visit www.id.ee/bdoc for more information.
- The text of the ID-card utility saying that the card is not in the reader has been supplemented to hint that the contact chip is located on the back side of new ID-cards.
- A button has been added to the ID-card utility for the Mac OSX to delete the user’s old ID-card certificates from the computer Keychain when the user has updated his or her certificates. It should be used in case of a failure to use the ID-card after the certificates have been updated.
- Support for the TEST of KLASS3-SK 2010 test certificate has been added.
- The documentation of the [jdigidoc](#), [libdigidoc](#) and [COM](#) libraries has been updated.
- The following bugs have been fixed.
- The ID-card utility displays the message “This document is invalid” if the certificates of the ID-card are outdated.
- Files without a name or extension sometimes appear in the Applications directory under Mac OSX 10.6 operation system when the DigiDoc3 client is launched.
- Digital signing fails if there is no access certificate and you press “No” in certificate installation dialogue when using the ID-card to sign a document digitally with DigiDoc3 software.
- The bug that displayed that a signature was valid in a .ddoc file where the content has been deleted, i.e. a detached file has been fixed.
- The bug where the ID-card utility displayed the status of Mobiil-ID certificates incorrectly when the status of user’s ID-card certificates showed it was suspended or marked.
- The detection of menu choices in the ID-card utility under Mac OS X has been fixed.
- The bug where the ID-card utility showed the certificate expiry time according to the wrong time zone has been fixed.
- .ddoc security updates. Please find more detailed info at [jdigidoc](#), [libdigidoc](#) pages.
- **Bug fixes compared to the 3.6 beta version released on 25/05/2012.**

- The bug where faulty .ddoc files were regarded as correct has been fixed.
- The plugin crash of digital signing under Ubuntu 12.04 has been fixed.
- Mobiil-ID verification code support for the screen reader has been updated (using the Tab key for moving).
- After installation, Smartcard removal is by default manual under 32-bit Windows as well.
- The bug that blocked the encryption of several documents in a row without shutting down the software in between.
- The display of the information from qdigidoc diagnostics files under Windows has been fixed.
- **Bug fixes compared to the 3.6 beta version released on 11/06/2012.**
- The bug under Ubuntu 12.04 64bit that caused authentication problems with Firefox has been fixed. The problem was with PKCS11 loader module which was not loaded.
- The bug under Ubuntu 12.04 where DDOC/CDOC/BDOC files were associated with Firefox not DigiDoc3 client and crypto has been fixed

ID software version. 3.5 SP1 (3.5.6034) (published 03/04/2012)

- Supported operating systems:
 - Windows XP 32bit
 - Vista 32bit and 64bit
 - Windows 7 32bit and 64bit
 - Mac OS X 10.6 and 10.7 (both Intel)
 - Ubuntu 4.11 32 bit and 64bit
 - Fedora 15 32bit and 64bit
- Supported web browsers are the newest available and supported by those operating systems
 - Windows: Internet Explorer, Mozilla Firefox, Google Chrome
 - Mac OSX: Mozilla Firefox, Safari
 - Linux: Firefox
- [Source code](#)
- Realized the following bug fixes:
 - Corrected the Firefox browser to use the signature component
 - Corrected automatic renewal errors
 - Safety Improvements

ID-software version 3.5 (released on 10.11.2011)

- Supported operating systems:
 - Windows XP 32bit
 - Windows Vista 32bit and 64bit
 - Windows 7 32bit and 64bit
 - Mac OS X 10.6 and 10.7 (both Intel)

- Ubuntu 11.04 32bit and 64bit
 - Fedora 15 32bit and 64bit
 - openSuse 11.4 32bit and 64bit
- Supported web browsers are the newest available and supported by those operating systems
 - Windows: Internet Explorer, Mozilla Firefox, Google Chrome
 - Mac OSX: Mozilla Firefox, Safari
 - Linux: Mozilla Firefox
- added functionality for software automatic updates (Windows, Mac OSX)
- Windows 7 and Vista have a new Minidriver (new authentication and digital signature PIN dialogues)
- added BDOC file format functionality (possibility to choose the format of digitally signed documents)
- added functionality for certificate automatic removal under Windows
- DigiDoc3 client digital signing using authentication proxy is now possible. Squid software was used for testing and all other solutions work "as is".
- one software package for all supported Mac OS X's
- added support for digital stamping in DigiDoc3 client and crypto using crypto token
- certificate automatic registering requires a restart to finalize software installation (this happens when the computer had ID–software version 3.4 or earlier)
- [Source code](#)
- this release contains following bug fixes:
- Server access certificate installation fails if user profile has special characters like äöü (for example c:\users\tõnis).
- After installing new server access certificate Mac OS X users will get an error 92 (Failed to sign document, libdigidoc code: 92, message: PKCS#12 certificate has expired).
- Sertifitseerija ESTEID–SK 2011 alt välja antud sertifikaatide puhul ei mahu seerianumber korrektselt kinnituselehele ära.
- During 3.4 version installation the Generic USB CCID driver will be removed, this causes a situation under Windows XP where card/card reader can not be found and authentication doesn't work in Firefox, Internet Explorer and also Chrome web browser.
- Fixed certificate automatic registering in Windows.
- During certificate renewal using ID–card utility under Windows, the old certificates were not removed.
- Software installation for computers in a domain fails with an error: 26352.

ID software version 3.4 (released on 09.05.2011)

- support for operating systems: Windows XP 32 bit, Windows Vista 32 bit and 64 bit, Windows 7 32 bit and 64 bit, support for web browsers: Internet Explorer from version 7, Firefox from version 4, Google Chrome version 10.0; support for operating systems: Mac OS X 10.5 and 10.6 (both Intel), support for web browsers: Safari 5 and Firefox from

version 4; support for operating systems: Ubuntu 10.10 32 bit and 64 bit, Fedora 14 32 bit and 64 bit, openSuse 11.4 32 bit and 64 bit, support for web browsers: Firefox from version 4

- added support for PinPad readers
- added support for several card readers
- added new SK root certificate and support for new lower certifiers

[Source code](#)

ID–software ver. 3.3 (published 09.02.2011)

- supported operating systems Windows XP 32bit, Windows Vista 32bit and 64bit, Windows 7 32bit and 64bit, supported web browsers starting from Internet Explorer 7 ,Firefox 3.6 , Google Chrome 8.0. Mac OS 10.5 ja 10.6 (both intel), supported web browsers Safari 5 and Firefox ver 3.6 or newer. Ubuntu 10.04, 10.10 32bit and 64bit, Fedora 13, 14 32bit and 64bit, openSuse 11.3 32bit and 64bit, supported web browser Firefox ver 3.6 or newer.
- added 2011 ID–card and residence card support
- digi–ID card support for all operating systems
- this release contains following bug fixes:
- Windows 64 bit users have to remove old ID–card software for Firefox before installing new software.
- Under Windows 7 and Windows Vista, launching software installation directly from web browser is not possible, software packages should be downloaded and then run.
- Sometimes file associations for .cdoc and .ddoc files will not be created for DigiDoc client/crypto and they should be manually configured.
- PIN confirmation window in Internet Explorer and Google Chrome do not display whether they ask for PIN1 or PIN2. Yellow padlock icon represents PIN1 and envelope PIN2.
- [Source code](#)

ID–software ver. 3.2 (published 19.01.2011)

- supported operating systems Windows XP 32bit, Windows Vista 32bit and 64bit, Windows 7 32bit and 64bit, supported web browsers starting from Internet Explorer 7 ,Firefox 3.6 , Google Chrome 8.0
- missing 2011 ID–card support
- BDOC file format is not supported
- [Source code](#)

ID–software ver. 3.1 (published 29.10.2010)

- first public version

- supported Mac OS 10.5 ja 10.6, supported web browsers Safari 5 and Firefox ver 3.6 or newer
- supported Linux distros: Ubuntu 10.04 32bit and 64bit, Fedora 13 32bit and 64bit, openSuse 11.3 32bit and 64bit, supported web browser Firefox ver 3.6 or newer
- missing digi-ID support
- missing 2011 ID-card support
- BDOC file format is not supported
- [Source code](#)