GnuPG VS-Desktop - Version 3.2.0 (en)

g10 Code GmbH

2023-12-04

GnuPG VS-Desktop® version 3.2.0 is available since 2023-12-04. The previous version was 3.1.26.

New Features

PDF Reader

GnuPG VS-Desktop® has been extended with the popular *Okular* PDF Viewer. Aside of showing and editing documents Okular also provides the ability to sign and verify documents using a qualified electronic signature (QES) as long as the respective smart card is supported by GnuPG.

This *GnuPG Edition* of Okular is optimized to be lightweight and to provide as little attack surface as possible. It does not support any active content like JavaScript or media files in PDF documents. It should therefore be more suitable in high security environments than common PDF readers.

This feature is not installed by default. It can be selected in the advanced installer dialog or bei providing the parameter `INST_OKULAR=true` when installing the package.

GUI (Kleopatra)

- A new mail viewer mode has been added, allowing crypto mails received by mail clients without PGP/MIME or S/MIME support to be decrypted. This means that you can open an SMIME.p7m file or openpgp-encrypted-message.asc attachment with Kleopatra and it will be displayed as a mail. (T6199)
- It is now possible to certify multiple certificates at once using the group interface. (T6469)

- Folder encryption and decryption (gpgtar) has been completely reworked so that it now has roughly the same performance as on the command line. The new architecture also allows for further performance improvements in the future and is much more robust. And solves several other issues. (T5478,T6488}}}, et.al.)

- The start time of Kleopatra has been drastically improved on throttled systems with third-party software installed, which manipulates system calls. The number of system calls to start Kleopatra has been roughly halved. (T6259)

- Windows dark mode is now fully supported. (T4066)

- The support for Telesec signature cards has been improved. (T6830)

- When exporting or publishing certificates, the user is now informed if there are uncertified certificates in the export. This is especially useful when exporting groups. (T6766)

- The dialog to extend OpenPGP certificates has been improved and redundant options removed. (T6621)

- It is now possible to rename the output file, if a file with the same name already exists, instead of just overwriting or canceling. (T6372)

- It is now offered to delete the secret key on the computer after it was successfully transferred to a smartcard. (T5836)

- Added warnings when your certificate or other certificates in your keyring are about to expire. The warnings are configurable and should allow a smoother switch to a new or extended certificate. (T6452)

- The Notepad now also uses the last chosen certificates for signing and self-encryption as default. The values are shared with file encryption. (T6415)

- The certificate selection input and dropdown fields are now alphabetically sorted. (T6492,T6514)

- Backed up subkeys can now be restored through the UI even when they were used from a smartcard in between. (T3456,T3391)

- For certifications of public keys it is now possible to configure a default validity period. (T6452)

- The default validity of new certificates is now three years instead of two. This can be changed through configuration. (T2701)

- When extending the validity period of a certificate, the default for new ones is now preset. (T6479)

Outlook Add-In (GgpOL)

- Added support for RFC2231 encoded attachment filenames, which increases compatibility with Apple Mail. (T6604)

- Draft encryption with S/MIME certificates now skips CRL checks and is much faster and reliable. (T6827)

- The error handling was improved if a preference for S/MIME is set and signing selected but no signing certificate can be found. See the Registry Setting page under “smimeNoCertSigErr" on how to add a custom message to instruct users what to do in this case. (T6683)

- It is now possible to encrypt to S/MIME certificates that are untrusted or cannot be validated because of CRL errors. In this case a warning dialog is shown, allowing the user to override the errors. This is not VS-NfD compliant but can be used for unrestricted encryption. (T6701)

- Mails without the correct MIME type but which still look like crypto mails are now decrypted. This improves compatibility with Apple Mail and various mail gateways that modify the structure of crypto mails in transit. (T6701)

- The internal attachments are now called `GpgOL_MIME_structure.mime` instead of `GpgOL_MIME_structure.txt` to make it easier to link them to Kleopatra. This is, for example, visible for users when using the Outlook web interface. (T6656)

- The security approval dialog has been improved to better show problems with the available certificates in case a compliant encryption is not possible. (T6742,T6743,T6744)

- The security approval dialog now increases its size based on the number of recipients to avoid having to use a scroll bar. (T6837)

Engine (GnuPG)

- Elliptic-curve cryptography (ECC) has been implemented for S/MIME, and the approval documentation has been adapted accordingly. Currently, only Brainpool curves are VS-NfD compliant, but other curves can be used. (T6253,T6802)
- OCB has been added as a new encryption mode and the approval documentation has been updated accordingly. According to the updated approval this is compliant for restricted communication. (T6263)
- The default for keyservers is now the value "none". This avoids unnecessary queries agsinst the Active Directory which might slow down operations. (T6708)
- Automatic proxy detection has been improved. (T5768)
- Detection of already compressed data has been improved. This can significantly increase performance when encrypting already compressed data. (T6332)
- The listing of certificates has been sped up. This is in particular noticeable with S/MIME certificates. (rG08ff55bd44)
- The new "ADSK" feature is now supported. ADSK signals the intention to encrypted messages to multiple subkeys. (T6395, Description)

Solved Bugs

GUI (Kleopatra)

- Some invalid operations, such as signing with an expired certificate, which would have resulted in errors, can no longer be triggered. The reason for this is indicated, too. (T6742,T6788)
- Expiry dates after 18.01.2038 (year 2038 bug) are now possible. (T6736)
- When creating archives, they are now written out as a ".part" file to improve error handling and canceling the operation without leaving a broken archive in the file system. (T6584)
- Updating certificates now also looks for updates in a Web Key Directory if one exists for the mail address. (T5951)

- Progress bars are now also properly shown for S/MIME file operations and work correctly for very large files. (T6534)
- The startup time of Kleopatra has been greatly improved. (T6259)
- Handling of permission and write errors has been improved across the board. (T6528)
- An accidental timeout when creating checksum files has been removed. This could result in empty or incomplete checksum files. (T6573)
- The validity period of all subkeys is now extended even if the primary key was already expired. This fixes the case where seemingly extended keys were no longer usable for encryption. (T6473)
- A rare occurrence, where encryption only keys would be offered as signing keys, has been fixed. (T6456)
- Canceling file operations now reliably cancels the underlying backend operations, too. (T6524)
- A number of encoding problems when displaying output from the backend have been solved. (T5960)
- Selecting cancel when exporting a secret subkey now properly cancels instead of creating a file without the secret part. (T5755)
- When importing secret keys you do not want to mark as your own, it is no longer asked multiple times if it is your own key. (T6474)
- The state of Kleopatra is now properly stored in configuration files when Kleopatra is shut down on user log out. (T6667)
- Importing a certificate with Kleopatra will now open the main window of Kleopatra. (T6671)
- No longer unnecessarily watches the clipboard for changes; this could have caused issues with password managers that would empty the clipboard as soon as a third-party application tried to access it. (T6531)
- It is no longer possible to set expiry dates to the past. (T6519)
- Importing multiple certificates at once can no longer cause Kleopatra to lock up. (T6323)

- When generating keys on a smartcard in compliance mode, only compliant algorithms are offered. (T6750)
- Several additional encoding problems when showing GnuPG output have been fixed. (T5960)
- Fixed an issue where certificate tags would not be displayed correctly after reloading certificates. (T6768)

Outlook Add-In (GgpOL)

- The initialization has been moved to avoid the incorrect message that GpgOL is causing a slow start of Outlook. This message might still be shown, since Outlook shows this sometimes regardless of actual timings, but the delay should be 0ms. (T6856)
- A crash has been fixed that happened reliably when sending crypto mails with attachments without a filename. This occurred for some signatures that included an image. (T6546)
- Category and flag changes now work again if the mail is not displayed in a decrypted state when they are made. (T4127)
- Fixed a crash that occurred when encrypting a mail with an attachment without a file name. (T6546)
- The security approval dialog now correctly updates the compliance status after switching protocols. (T6600)
- The security approval is now always shown if encryption is to a group which contains uncertified or otherwise non-compliant certificates. (T6401)
- Fixed an issue with S/MIME opaque signed mails where the contents of invalid signed mails would not be shown. (T6624)
- When generating a key through the security approval dialog, the configured default algorithms from GnuPG are now used. (T6805)
- Generating keys through the security approval dialog now works as intended. (T6813,T6823,T6566)
- An issue has been fixed where crypto mails would show up empty if text/plain display was preferred. (T6357)
- Added safeguards against a plain text leak back to the server in a specific unusual configuration. (rOdd3ff839)

Engine (GnuPG)

- The PKCS#12 parser has been improved to allow for more formats. This should fix several issues when trying to import p12 files with Kleopatra. (T6536)

Installer

- The installer now properly terminates running background processes, eliminating the need to restart the computer after upgrading to a new GnuPG VS-Desktop version. (T6567)

Versions of the Components

Component	Version	Remarks
GnuPG	2.2.42	T6307
Kleopatra	3.2.0	
GpgOL	2.5.11	
GpgEX	1.0.10	
Libgcrypt	1.8.11	
Libksba	1.6.5	T6822