GnuPG VS-Desktop - Version 3.3.3 (en)

g10 Code GmbH

2025-11-06

GnuPG VS-Desktop® version 3.3.3 is available since 2025-11-06. It fixes a couple of bugs and introduces a few minor features. The previous version was 3.3.2.

Notes to Admins

An update to this version is suggested due to these security fixes:

- The component *GnuPG* has been updated to fix a security issue with 3rd party key signatures.
- The component *Libgcrypt* has been updated to fix a security issue.
- The optional *Okular* component has been updated with security fixes for it's backend Poppler.

New Features

Engine (GnuPG)

- gpg: Try to retrieve a key from LDAP before sending it. This can be disabled using `keyserver-options no-update-before-send` (T7730)
- scdaemon: Make signing work for Nexus cards. (rGe1576eee04)
- dirmngr: Implement command KS_DEL for LDAP. (T5447)
- dirmgr: Support Unix LDAP servers using a schema like the one used on Windows LDS servers. (T7742)
- gpgsm: Make use of the de-vs flag in the trustlist.txt. (rG14383ff052)

Solved Bugs

GUI (Kleopatra)

- Show version information always. (T7639)
- Restore behavior of configuration options RSAKeySizes and PGPKeyType. (T7674)
- Do not offer revoked UIDs for sign/encrypt. (T7678)
- Add workaround for locking issue on key generation. (T7827)

GUI (Pinentry)

- Show/Hide button is now accessible via keyboard. (T7736)
- Fix issue with pinentry icons in high contrast mode. (T7737)

Engine (GnuPG)

- gpg: Avoid potential downgrade to SHA1 in 3rd party key signatures. (rG4329e47463)
- gpg: Fix de-vs compliance with OCB and additional password. (T7804)
- gpg: Fix possible memory corruption in the armor parser. (rG1e929abd20)
- Make the extra check for a compliant RNG on Windows actually work again. (rGbad0e15d87)
- gpgsm: Fix delete and store certificate locking glitches. (T2196)
- gpgsm: Fix caching of the trustlist's flags. (T7738)
- agent,dirmngr: Fix possible races on startup under Windows. (T7829)
- On Windows use the nPth friendly gnupg_usleep instead of the standard Sleep API in the sharing violation retry code. (rG8491117f09)
- dirmngr: Fix assertion failure due to wrong buffer length for certain public keys. (rGafb0aa2674)
- scdaemon: Accept P15 cards with a zero-length label. (rG84229829b5)
- Libgcrypt: Global configuration files on Windows are now expected below CSIDL_COMMON_APPDATA instead of /etc on the current drive. (rC33413bf3dd)

Outlook Add-In (GgpOL)

- Fix BRING_TO_FRONT event handling. (rOaaf7bedef8)
- Fix moving new encrypted emails to folder via context menu. (T7712)
- Make sure that a temp file name does not get too long and has a proper suffix. (T7722)
- Show attachments with long suffixes. (T7813)
- Fix high CPU load for not selected signed mails. (T7771)
- Fix invalid UI Status with non mail items. (T7646)
- Fix invalid UI Status with disabledAutoPreview. (T7803)
- Prevent possible plaintext leak of the very first opened PGP message if Outlook is in read-as-plain mode. (T7858, rO88ab93687c)

Versions of the Components

Component	Version	Remarks
GnuPG	2.2.51	
Kleopatra	3.3.3	
GpgOL	2.6.9	
GpgEX	1.0.11	
Libgcrypt	1.8.12	T7887
Libksba	1.6.7	T7173