GnuPG for Windows - Version 5.0.0

g10 Code GmbH

2026-01-14

Gpg4win version 5.0.0 is available since 2026-01-14. This is a major release with many new features andimprovements:

Notes to Users

An update to this version is strongly recommended due to a couple of security fixes and to address the close end-of-life of some components:

- The *GnuPG* component fixes a minor security issue related to third-party key signatures (T7904) and a minor memory access violation (T7904).
- The *Okular* component has been improved and updated with security fixes for its Poppler backend.

New Features

GUI

Upgrade to Qt 6.10.1 and KDE Frameworks 6.20. This upgrade from Qt 5 brings many improvements, including better dark mode support.

GUI (Kleopatra)

- Move Qt configuration files to new locations. (T6799,T7575,T7700,T7717)
- Use Breeze style icons on Windows. (T7415)
- Reorder menu items. (T7579)
- Reduce the number of actions in the context menus. (T7515,T7231)

- Support Kyber (FIPS-203) key generation. (T7397)
- Improved support for V5 fingerprints. (T7297)
- Format fingerprints everywhere. (T7707)
- Sign/encrypt window improvements. (T7556)
- Change logic for option to always show the result window. (T7553)
- Check box "Encrypt to Others" is functional now. (T6485)
- Improved verification results messages. (T6869)
- Notepad:
  - Opens now in separate window. (T7361)
  - Recipient information are now on the side of the input field. (T5957)
  - Buttons are now below the input field. (T7760)
  - Improved notepad result messages. (T7341)
  - Close message notification on revert. (T7762)
- Remove imported certificates tabs. (T7630)
- Show certificate's comment field in certification dialog. (T7558)
- Show more information for publish on keyserver in certifications dialog. (T6663)
- Add option to hide 3rd party certifications in dialog. (T6627)
- Add pinentry counters to smart card management view. (T6787)
- Look up missing OpenPGP certificates for card keys. (T7272)
- Do ask for confirmation only twice when deleting a secret key. (T7538)
- Show designated revoker in details window. (T7095)
- Add audit log link for missing subkey error. (T7886)
- Use filter in certificate selection for encryption. (T7236)
- Display the same tooltip for keys in different fields. (T7473)

- Display keys in the same way in different contexts. (T7474)
- For update via WKD show if the certificate was unchanged. (T7513)
- Show progress window when updating a certificate. (T7655)
- Add search function to configuration overview. (T7552)
- Restore last window location on next start. (T7554)
- Add a dialog window to the disable/enable certificate action. (T7580)
- Update custom colored UI elements when colors change. (T7610)
- Add option to start Kleopatra as additional process. (T7704)
- Remember last used file system locations when saving or opening files. (T7802)
- Improved success message on keyserver upload. (T7495)
- Improved crypto operations on clipboard. (T7455)
- Improved UX of subkey expiry change window. (T7215)
- Improved "About data". (T7329)
- Accessibility improvements:
  - Improved the certificate signing request dialog. (T6117)
  - High contrast mode. (T7588,T6921)
  - Navigation issues. (T7751,T7770, T7859,T7879,T7890, T7935,T6825,T7355)
  - Screenreader related. (T7878,T7862, T7854,T7850,T7739, T7937,T7826)

GUI (Okular/GnuPG-edition)

- OpenPGP signature support.
- Improved signature workflow.
- Improved visual representation of signatures.
- Improved zoom.
- QES certificates are marked as such (if they are properly configured in the backend).

Outlook-New Add-In (GpgOL/Web)

Introduction of the new GpgOL/Web add-in, still EXPERIMENTAL.

It was designed and implemented from scratch to support the new, web-based Outlook. This add-in uses a locally running service to fetch and send encrypted messages from/to Outlook. I.e. unencrypted content does not leave the local operating system and is not synced to the cloud.

This add-in is still in development and missing features. Currently only standard Microsoft-365 accounts are supported.

Engine (GnuPG)

- `gpg`: Support for composite Kyber+ECC public key algorithms according to the FIPS-203 and the LibrePGP specifications. (T6815)
- `gpg`: New commands `--add-recipients` and `--change-recipients`. (T1825)
- `gpg`: New command `--quick-tsign-key` to create a trust signature. (rGd90b290f97)
- `gpg`: New options `--[no-]auto-key-upload`. (T7333)
- `gpg`: New option `--show-only-session-key`. (rG1695cf267e)
- `gpg`: New option –proc-all-sigs. (T7261)
- `gpg`: New option `--disable-pqc-encryption`. (rG00c31f8b04)
- `gpg`: New list option "show-trustsig" to be used in with-colons listings. (rG41d6ae8f41)
- `gpg`: New import option "force-update". (T7892,rGf6237ccd31)
- `gpg`: Try to retrieve a key from LDAP before sending it. This can be disabled using `keyserver-options no-update-before-send` (T7730)
- `gpg`: Do not present a default when asking for another output filename. (T7908)
- `gpg`: Include ADSK keys in key listings specified by fingerprints. (T7892)
- `gpg`: New "pfc" record for key preferences in with-colons key listings. (T7897)

- `gpg`: Keys send to an LDAP server are now first updated from that server. New keyserver option "no-update-before-send" to disable this feature. (T7730)
- `gpg`: Add a notation with version information to signatures. See doc/DETAILS for, well, details. (rG11d3a83b04)
- `gpg`: Show revocation reason with a standard key listing. Emit a revocation reason as comment in a "pub" record. (T7083)
- `gpg`: Add a flag to the filter expressions for left anchored substring match. (rGc12b7d047e)
- `gpg`: Emit status error for an invalid ADSK. (T7322)
- `gpg`: New keygen parameter "User-Id". (rGcfd597c603)
- `gpgv`: New option `--print-notation`. (rGe3cc410003)
- `gpgsm`: Nearly fourfold speedup of validated certificate listings. (T7308)
- `gpgsm`: New option –assert-signer. (T7286)
- `gpgsm`: Add option `--no-qes-note` and new trustlist flag "noconsent". (T7713)
- `gpgsm`: Extend `--learn-card` by an optional s/n argument. (T7379)
- `gpgsm`: Allow unattended PKCS#12 export without passphrase. (rG159e801043)
- `gpgsm`: Allow CSR generation with an unprotected key. (rG89055f24f4)
- `agent`: New option `--change-std-env-name`. (T7522)
- `agent`: Allow OpenSSH to sign data larger than the Assuan line length. (T7436)
- `scdaemon`: Make newer TCOS signature cards work. (rG17596e830f)
- `scdaemon`: Make signing work with Nexus cards. (rGe1576eee04)
- `scdaemon`: Support Yubikey attestation generation for the OpenPGP app. (rG5ddfedf24a)
- `dirmngr`: Implement command `KS_DEL` to delete keys from an LDAP keyserver. (T5447)

- `dirmngr`: Support Unix LDAP servers using a schema similar to the one used on Windows LDS servers. (T7742)
- `dirmngr`: New LDAP keyserver flag "upload". (T7866)
- `dirmngr`: New option `--user-agent` and use "GnuPG/2.6" as default User-Agent header of for all HTTP requests. (T7715)
- `dirmngr`: A list of used URLs for loaded CRLs is printed first in the output of the LISTCRL command. (T7337)
- `gpg-wks-server`: Support templates for mail content. (T7381)
- `gpg-card`:: New command "ll" as an alias for "list –cards". (rGd6ee7adebe)
- `gpg-mail-tube`: Support templates for mail content. (T7381)
- `gpg-mail-tube`: Make sure GNUPGHOME is set in vsd mode. New option `--as-attach`. (rG4511997e9e1b)
- Add `GNUPG_ASSUME_COMPLIANCE` environment variable and a registry key for testing de-vs compliance mode. [rGb287fb5775,rG7b0be541a9]

Solved Bugs

GUI (Kleopatra)

- Fix for issues with delayed or failing initial keylistings. (T7332)
- PIN reset now possible with Admin-PIN. (T7134)
- Fix jumping cursor issue in certificate view search field. (T7510)
- Fix issue with decryption of archives located at very long file paths. (T7532)
- Always show dialog when setting trust in root certificates. (T7349)
- "Show Audit Log" is now a button and opens after first click. (T7644), (T7782)
- Upper case file extensions of encrypted files work now. (T7780)
- Not functional configuration for AllowMarkTrusted is removed. (T7868)

- Fix deletion of public key URL on ZeitControl OpenPGP v3.4 card. (T7881)
- Group creation is not reset any more on opening certificate details window. (T7963)
- Fix language settings for the filter names. (T7612)
- RSA-1024 is not shown as unknown algorithm any more. (T7394)
- The title of certify dialog works now for email-only user IDs. (T7816)
- Command line options `--help` etc now work even if Kleopatra is already running. (T7686)
- Main certificate view does now keep selected column width even if screen settings change. (T5304)

GUI (Pinentry)

- The *Show/Hide* button is now accessible via keyboard. (T7736)
- Fix an issue with pinentry icons in high-contrast mode. (T7737,T7230)

Engine (GnuPG)

- `gpg`: Prevent a possible memory violation in the ASCII armor parser. (T7906,rG1e929abd20)
- `gpg`: Prevent a potential downgrade to SHA1 when handling third-party key signatures. (T7904,rGdb9705ef59)
- `gpg`: Fix a validation bug when using keyboxd. (T7983)
- `gpg`: Take care about the prefix for cv25519 encryption. (T7649)
- `gpg`: Error out on unverified output for non-detached signatures. [T7903,rG8abc320f2a]
- `gpg`: Avoid a second Pinentry pop-up for a configured ADSK during key generation. (T7491)
- `gpg`: Fix regression in using the secp256k1 curve. (T7698)
- `gpg`: Make combination of show-only-fpr-mbox and show-unusable-uid work. (rGd5a4a2dc89)

- `gpg`: Fix a double free of internal data in no-sig-cache mode. (T7547)
- `gpg`: Fix a verification DoS due to a malicious subkey in the keyring. (T7527)
- `gpg`: Fix `--quick-add-key` for Weierstrass EC keys with usage given. (T7506)
- `gpg`: Fix handling of ascii armor without a CRC. (T7071)
- `gpg`: Fix an import problem with keys having another primary key as a subkey. (T7527)
- `gpg`: Print a warning if the card backup key could not be written. (T2169)
- `gpg`: Validate the trustdb after the import of a trusted key. (T7200)
- `gpg`: Exclude expired trusted keys from the key validation process. (T7200)
- `gpg`: Fix a wrong decryption failed status for signed and OCB encrypted messages without a signature verification key. (T7042)
- `gpg`: Fix `--quick-set-expire` for V5 subkey fingerprints. (T7298)
- `gpg`: Fix curve "cv25519" v5 export regression. (T7316)
- `gpg`: Fix getting key by IPGP record (RFC-4398). (T7288)
- `gpg`: Print designated revokers also in non-colon listing mode. (rG9d618d1273)
- `gpg`: Make `--with-sig-check` work with `--show-key` in non-colon listing mode. (rG0c34edc443)
- `gpgsm`: Allow an empty subject DN also during import. (T7171)
- `gpgsm`: Correct caching of trustlist.txt flags. (T7738)
- `gpgsm`: Fix output of card serial number in colon listing. (T7914)
- `gpgsm`: Fix delete and store certificate locking glitches. (T7855)
- `gpgsm`: Skip expired certificates when selection a certificate by subject. (rG4cf83273e8)
- `gpgsm`: Terminate key listing on output write error. (T6185)

- `gpgsm`: More improvements to PKCS#12 parsing to cope with latest IVBB changes. (T7213)
- `gpg,gpgsm`: Run keybox compression only when there are no other users. Improve keybox closing and locking order on read and write. (T7855)
- `gpgtar`: Fix regression in end-of-archive detection. (T7757)
- `keyboxd`: Fix schema of the fingerprint table. (T7892,rG81bb949755)
- `keyboxd`: Use case-insensitive search for mail addresses. (T7576)
- `keyboxd`: Fix a race condition on the database handle. (T7294)
- `gpg-agent`, `dirmngr`: Fix a startup issue on Windows that could lead to blocking conditions. (T7829)
- `agent`: Retry private key deletion in case of sharing violations for up to 400ms. (T7863)
- `agent`: Fix a crash on Windows in the Putty support. (T7799)
- `agent`: Fix for smartcard decryption with Brainpool keys. (T7709)
- `scdaemon`: Accept P15 cards with an empty label. (rGdb25aa9887)
- `scdaemon`: Fix an oddity in changing the PIN. (T7840)
- `scdaemon`: Fix a harmless read buffer over-read in a function used by PKCS#15 cards. (T7662)
- `scdaemon`: Fix posssible lockup due to a lost select result. (rGa7ec3792c5)
- `agent`: Fix RSA signature handling for newer ssh specs. (T7882)
- `agent`: Fix KEYTOCARD command when used with a loopback pinentry. (T7283)
- `dirmngr`: Fix OCSP next-update check. (rG9ef87bcdb0)
- `dirmngr`: Do not require a keyserver for "gpg –fetch-key". (T7693)
- `dirmngr`: Fix a problem in libdns related to an address change from 127.0.0.1. (T4021)
- `dirmngr`: Fix possible hangs due to blocking connection requests. (T6606,T7434)

- `gpgconf`: Fix reload and kill of keyboxd. (T7569)
- Fix a glitch in socket handling in case of a nonce mismatch. (rG645cf7d8fc)
- Fix a race condition in creating the socket directory. (T7332)
- Fix logic for certain recsel conditions. (rG8968e84903)
- Global configuration files for Libgcrypt are now located under `CSIDL_COMMON_APPDATA` instead of `/etc` on the current drive. (rC995b870fd2)

Outlook Classic Add-In (GgpOL)

- Fix handling of the `BRING_TO_FRONT` event. (rOaaf7bedef8)
- Newly received encrypted emails can again be moved to folders via the context menu. (T7712)
- Ensure that the name of a temporary file does not become too long and has a proper suffix. (T7722)
- Also show attachments with long suffixes. (T7813)
- Fix high CPU load for unsigned mails that are not selected. (T7771)
- Fix incorrect UI status display for non-mail items. (T7646)
- Fix incorrect UI status display when the disabledAutoPreview setting is used. (T7803)
- Fix a possible plaintext leak when opening the very first PGP message in Outlook if Outlook is operating in read-as-plain mode. (T7858, rO88ab93687c)

Other Changes

Engine (GnuPG)

- `gpg`: Escape characters with the high bit set in NOTATION status lines. (T7896)
- `gpg`: Disable default compression for 7z compressed input. (rG53252628de)
- `gpg`: Change the ADSK key binding time to use the current time. (T6882)

- `gpg`: Do not show the non-standard secp256k1 curve in the menu to select the curve. It can however be specified using its name. (rG49a9171f63)
- `gpg`: Allow updating a SHA-1 key certification w/o using the `--force-sign-key` option. (T7663)
- `gpg`: The group key flag has now been fully implemented. (rG8833a34bf0)
- `gpg`: Do not allow compressed key packets on import. (T7014)
- `gpg`: Allow for signature subpackets of up to 30000 octets. (rG36dbca3e69)
- `gpg`: Silence expired trusted-key diagnostics in quiet mode. (T7351)
- `gpg`: Improve detection of input data read errors. (T6528)
- `dirmngr`: New compatibility flag `ocsp-sha256-certid` to work with forthcoming libksba versions. (rG674aa54242)
- `agent`: Accept a trustlist with a missing LF at the end. (rG1b4ac98de7)
- `agent`: Enable "relax" in the trustlist by default and add flag "norelax". (rG7b133027ae)
- `agent`: Recover the old behavior with "max-cache-ttl=0". (T6681)
- `gpgtar`: Use `log-file` from common.conf only in `--batch` mode. (rGb389e04ef5)
- Use a synchronous spawning method for the daemon processes. (T7716)
- Improve file renaming in case of a sharing violation error. (T7829)
- Use the KEM interface of Libgcrypt for encryption/decryption. (T7649,T7811,T7845)
- Enable additional runtime protections in Speedo builds for Windows. (rG39aa206dc5)

Incompatible Changes

- `gpg`: Deprecate the option `--not-dash-escaped` and ignore the `NotDashEscaped` armor header. (T7901)
- The `--supervised` options of gpg-agent and dirmngr have been renamed to `--deprecated-supervised` as preparation for their removal. (rGa019a0fcd8)

- There is no more default for an OpenPGP keyserver.
- The Windows version will now be build for 64-Bit Windows and with the corresponding changes to the installation directory and Registry keys.

Known Issues

- When using the keyboxd the export of multiple X.509 S/MIME certificates exports only the first. (T8026)

Versions of the Components

Component	Version	Remarks
GnuPG	2.5.16	T7642
Kleopatra	gpg4win-5.0.0	
GpgOL	2.7.0	
GpgEX	1.1.0	
Libgcrypt	1.11.2	T7642
Libksba	1.6.7	T7173