GnuPG VS-Desktop - Version 3.3.3 (de)

g10 Code GmbH

2025-11-06

GnuPG VS-Desktop® ist seit 2025-11-06 in der Version 3.3.3 verfügbar. Sie behebt einige Fehler und enthält ein paar kleinere neue Features. Die vorherige Version war 3.3.2.

Hinweise an die Administratorinnen

Ein Aktualisierung auf diese Version wird aufgrund der folgenden Sicherheitsfixes angeraten:

- Die Komponente *GnuPG* wurde aktualisiert, um ein Sicherheitsproblem mit externen Schlüsselsignaturen zu beheben.
- Die Komponente *Libgcrypt* wurde wegen eines Sicherheitsfixes aktualisiert.
- Die optionale Komponente *Okular* wurde wegen Sicherheitsfixes ihres internen Backends Poppler aktualisiert.

Neue Features

Engine (GnuPG)

- gpg: Es wird jetzt versucht, einen Schlüssel aus dem LDAP abzurufen, bevor er gesendet wird. Dies kann mit der Einstellung `keyserver-options no-update-before-send` deaktiviert werden. (T7730)
- scdaemon: Es kann nun auch mit Nexus Karten signiert werden. (rGe1576eee04)
- dirmngr: Das Kommando KS_DEL wurde für LDAP implementiert. (T5447)

- dirmngr: Erweiterung des Schemas für Unix-LDAP-Server, um sie wie Windows-LDS-Server ansprechen zu können. (T7742)
- gpgsm: Die "de-vs" Kennzeichnung in der trustlist.txt wird nun beachtet. (rG14383ff052)

Behobene Fehler

GUI (Kleopatra)

- Zeige die Versionsinformationen immer an. (T7639)
- Stelle das vorige Verhalten der Optionen RSAKeySizes und PGPKeyType wieder her. (T7674)
- Biete zurückgerufene UIDs nicht für verschlüsseln und signieren an. (T7678)
- Ein Workaround für eine Blockade bei der Schlüsselerzeugung wird hinzugefügt. (T7827)

GUI (Pinentry)

- Der Anzeigen/Verstecken Button ist nun per Tastatur erreichbar. (T7736)
- Pinentry-Icons sind jetzt im Hoher-Kontrast Modus erkennbar. (T7737)

Engine (GnuPG)

- gpg: Verhinderung einer möglichen Herabstufung auf SHA1 bei Beglaubigungen von öffentlichen Schlüsseln durch Dritte. (rG4329e47463)
- gpg: Zeige die VS-NfD Konformität auch mit OCB und zusätzlicher Passwortverschlüsselung korrekt an. (T7804)
- gpg: Verhinderung einer möglichen Speicherverletzung im Parser für ASCII-Daten. (rG1e929abd20)
- Die Zusatzprüfung für einen konformen RNG unter Windows funktioniert nun wieder. (rGbad0e15d87)
- gpgsm: Fehler beim Löschen und Speichern von Zertifikaten, die zu Deadlocks führen konnten, wurden behoben. (T2196)

- gpgsm: Das Caching der Flags der trustlist.txt wurde korrigiert. (T7738)
- agent,dirmngr: Behebung eines Fehlers, der beim Start auf Windows zu Blockaden führen konnte. (T7829)
- Unter Windows wird nun das nPth-freundliche gnupg_usleep statt des Standard Sleep API verwendet. (rG8491117f09)
- dirmngr: Behebung eines Assertion-Fehlers wegen falscher Pufferlänge bei bestimmten öffentlichen Schlüsseln. (rGafb0aa2674)
- scdaemon: P15-Karten mit einem leeren Label werden nun akzeptiert. (rG84229829b5)
- Libgcrypt: Globale Konfigurationsdateien unter Windows werden nun unter CSIDL_COMMON_APPDATA statt unter /etc auf dem aktuellen Laufwerk gesucht. (rC33413bf3dd)

Outlook Add-In (GgpOL)

- Fix der BRING_TO_FRONT Event-Handhabung. (rOaaf7bedef8)
- Neu angekommene verschlüsselte Mails können wieder über das Kontext Menü in Ordner verschoben werden. (T7712)
- Es wird nun sicher gestellt, dass der Name einer temporären Datei nicht zu lang ist und eine korrekte Endung hat. (T7722)
- Auch Anhänge mit langen Suffixen werden nun angezeigt. (T7813)
- Hohe CPU-Belastung bei nicht ausgewählten signierten E-Mails wird behoben. (T7771)
- Eine falsche UI Status Anzeige bei nicht-Mail Elementen wird behoben. (T7646)
- Eine falsche UI Status Anzeige bei Verwendung der Einstellung disabledAutoPreview wird behoben. (T7803)
- Ein im Read-as-Plain Modus mögliches Auftreten eines Klartext-Leaks beim allerersten Öffnen einer PGP Nachricht in Outlook wird behoben. (T7858, rO88ab93687c)

Versionen der Komponenten

Komponente	Version	Anmerkungen
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