

GnuPG VS-Desktop - Version 3.4.0 (de)

g10 Code GmbH

2026-09-16

GnuPG VS-Desktop[®] Version 3.4.0.0 ist seit dem 2026-09-16 verfügbar. Die vorherige Version war 3.3.7.

Hinweise für Administrator:innen

Diese Version behebt das Problem aus 3.3.7, bei dem die Entschlüsselung von S/MIME-Mails fehlschlug, wenn das Zertifikat abgelaufen war. (T8282)

Geänderte Voreinstellungen

Der GnuPG-Registry-Schlüssel `GpgsmCompatibility` ist jetzt undefiniert; zuvor war er auf `de-vs-trustlist` gesetzt. Dadurch werden nur noch S/MIME-Zertifikate als VS-NfD-konform angezeigt, deren Root-CAs in der globalen `trustlist.txt` mit `de-vs` markiert sind. Falls für ein X.509-Zertifikat, das VS-NfD-konform sein sollte, keine VS-Konformität angezeigt wird, prüfen Sie den entsprechenden CA-Eintrag in `%ALLUSERSPROFILE%\GNU\etc\gnupg\trustlist.txt` oder in Ihrer individuellen globalen Trustlist-Datei, z. B. `mytrustlist.txt`.

Die Kleopatra-Konfigurationsdatei `kleopatrarc` liegt jetzt nicht mehr unter `%LOCALAPPDATA%`, sondern am besser geeigneten Ort `%APPDATA%\GnuPG VS-Desktop`. (T7717)

Neue Einstellungen

Neu in GnuPG VS-Desktop[®] 3.4 sind die folgenden Registry-Werte für Kleopatra:

Subkey: Welcome, Wert: welcome-text[\$i] Legt den Text fest, der bei leerer Zertifikatsliste angezeigt wird. (T7967)

Subkey: Export, Wert: AllowPublicKeyUpload Steht er auf false, dürfen Anwender:innen nur ihre eigenen OpenPGP-Zertifikate hochladen; der geheime Schlüssel muss also vorhanden sein. Standard: true. (T7772)

Subkey: CertificateCreationWizard, mehrere neue Werte für den CSR-Dialog

Der überarbeitete Dialog zum Erstellen von Zertifikatsanforderungen (CSR) bietet für alle Attribute nun zusätzliche Werte. Näheres dazu finden Sie auf der Seite mit den Kleopatra (Registry-)Einstellungen. Der Wert `CN_placeholder` ist jetzt veraltet und verhält sich nun wie der neue Wert `CN_hint`: Der angegebene Text erscheint als Hinweis über dem Feld für den Common Name (CN) von S/MIME-CSRs. (T6117)

Linux-AppImage

Ab Version 3.4 verfügt das AppImage über eine Installationsoption. Wenn Sie es nun installieren oder auf eine neue Version aktualisieren, machen Sie zunächst das heruntergeladene AppImage ausführbar und rufen es dann mit `--install` auf:

```
./gnupg-vs-desktop-3.4.0.0-x86_64.AppImage --install
```

Dafür sind Root-Rechte erforderlich. Falls Sie den Befehl nicht in einer Root-Shell ausführen, werden Sie nach dem sudo-Passwort gefragt.

Hinweise für Anwender:innen

Neues Handbuch

GnuPG VS-Desktop[®] enthält jetzt ein Benutzerhandbuch, das Sie über das Hilfe-Menü von Kleopatra erreichen. Es ersetzt die meisten der bisherigen Hilfedokumente und wird künftig weiter ausgebaut und verbessert.

GpgOL-Workaround für verschlüsselte Mails im Anhang

Wir haben die Behandlung von Anhängen in GpgOL geändert, damit der Inhalt angehängter Krypto-Mails zuverlässig angezeigt wird (T7806). Es ist aktuell jedoch ein Workaround nötig: Speichern Sie die angehängte, S/MIME-verschlüsselte Mail im Dateisystem (ziehen Sie sie z. B. auf den Desktop) und öffnen Sie sie von dort (etwa per Doppelklick).

Neue Features

Engine (GnuPG)

- **gpg**: Neue Optionen `--show-session-hash` und `--show-only-session-hash`. (rGfaa571fbff)
- **gpgconf, w32**: Anzeige von mehr Registry-Schlüssel von GpgOL. (rGa570827330)
- **gpgconf**: Inhalt von `versioninfo.txt` mit `-vV` ausgeben. (rGa1f08f40d7)

Kleopatra

- Ausführen von Kleopatra als Administrator wird nun verhindert. (T8210)
- Der Text der Willkommenseite ist jetzt konfigurierbar. (T7967)
- Neue Option `--standalone`, um Kleopatra als zusätzlichen Prozess zu starten. (T7704)
- Es wird nun angeboten, eine S/MIME-Verschlüsselung mit niedrigeren Sicherheitseinstellungen zu wiederholen, falls diese mit `not trusted` fehlgeschlagen ist. (T6702)
- Überarbeitung des Dialogs zum Erstellen von S/MIME-Zertifikatsanforderungen (CSR): Er ähnelt jetzt dem Dialog zur OpenPGP-Schlüsselerzeugung und sollte barrierefrei sein. (T6117)
- Ein `tar.gpg`-Archiv mit einem einzelnen Ordner wird in eindeutigen Fällen nun direkt in das angegebene Verzeichnis entpackt. (T8022), (T8154)
- Filter für gültige Zertifikate hinzugefügt. (T7950)
- Zertifikate für qualifizierte Signaturen werden nicht mehr fett angezeigt. (T8077)
- Der VSD-Konformitätshinweis wird nur noch bei erfolgreicher Überprüfung angezeigt. (T8413)
- Status `abgelaufen` oder `"widerrufen"` wird jetzt in den LDAP-Suchergebnissen angezeigt. (T8042)
- Erfolgsmeldung beim Hochladen auf den Schlüsselserver verbessert. (T7495)

- Neue Konfigurationsoption, um nur das Hochladen eigener Zertifikate auf einen LDAP-Schlüsselserver zu erlauben. (T7772)
- Rückfrage beim Import eines geheimen Schlüssels verbessert. (T7637)
- Beim Import eines geheimen Team-Schlüssels fällt jetzt die Rückfrage nach dem eigenen Schlüssel weg. (T8098)
- Neues Standard-Tastenkürzel für die Zertifikatsdetails hinzugefügt. (T7752)
- Suchfunktion in der "Konfigurationsübersicht" hinzugefügt. (T7552)
- Leer- und Sonderzeichen werden nun im vorgeschlagenen Exportdateinamen ersetzt. (T7848)
- Zertifikate werden in verschiedenen Kontexten einheitlich dargestellt. (T7474)
- Verständlichkeit des Dialogs Ablaufdatum ändern für Unterschlüssel verbessert. (T7215)
- Beim Übertragen eines Schlüssels auf eine Smartcard entfällt das .gpgsk-Backup. (T8327)

Behobene Fehler

Engine (GnuPG)

- **gpg**: Lösche die lokale Kopie des geheimen Schlüssels nach bkuptocard. (T8312)
- **gpg**: Beim TOFU-Vertrauensmodell werden jetzt tatsächlich die UTK-Signaturen geprüft. (T8404)
- **gpgsm**: Mögliches Double-free im CMS-Parser behoben. (T8240)
- **gpgsm**: Regression in `gpgsm_verify` bei abgelaufenen Zertifikaten behoben. (T8282), (T8188)
- **gpgsm**, **gpgme**: Ausgabe des de-vs-Konformitätsstatus nur noch im de-vs-Konformitätsmodus. (T8333)
- **gpgsm**: Verlange eine Mindest-Tag-Länge für die GCM-Entschlüsselung. (rGab2395daeb)

- **dirmngr**: Fix für Problem bei LDAP-Upload-Flags. (T7866)
- **gpg**: Fix für Problem bei LDAP-AKL-Mechanismus. (T7133)

GUI (Kleopatra)

- Anzeige von Ablaufdaten bei S/MIME-Zertifikaten jenseits von 2038 korrigiert. (T8088)
- Aktualisierung der Zertifikatsliste nach dem Löschen geheimer Schlüssel ist nun zuverlässiger. (T7863)
- Neue Reiter in der Zertifikatsliste übernehmen jetzt das Spaltenlayout des aktuellen Reiters. (T7008), (T8415)
- Verbesserte Fehlermeldung, wenn ein abgelaufenes Zertifikat zum Verschlüsseln gewählt wird. (T7789)
- Das Kommentarfeld eines Zertifikats wird jetzt im Beglaubigungsdialog angezeigt. (T7558)
- Die Algorithmusnamen von RSA-1024- und Kyber-Schlüssel werden jetzt angezeigt. (T7394)
- Migration der Konfigurationsdateien der Qt-Anwendungen von %LOCALAPPDATA% nach %APPDATA%. (Kleopatra + Okular) (T7717)
- Zertifikatsdetails: Deaktivierung der Unterschlüssel-Backup-Aktion bei Hauptschlüsseln. (T8321)
- Problem bei Konformitätsanzeige behoben. (T8245)
- Roter Hintergrund für den Status Fehlerhafte Installation ergänzt. (T8310)
- Zurücksetzen auf das voreingestellte Erscheinungsbild funktioniert nun. (T7212)
- Anzeigereihenfolge von Filtern mit eigener ID im Einstellungsdialog korrigiert. (T8079)
- Anwendungsreihenfolge der Formatierung von Zertifikatskategorien korrigiert. (T8279)
- Das Zurücksetzen der Gruppenkonfiguration, wenn Zertifikatsdetails geöffnet werden, erfolgt nun nicht mehr. (T7963)

- Veraltete AllowMarkTrusted-Checkbox aus dem Konfigurationsdialog entfernt. (T7868)
- Vervollständigung von Befehlen in der GnuPG-Konfigurationsübersicht beachtet jetzt die Groß- und Kleinschreibung. (T7615)
- Alle Filternamen folgen jetzt denselben Spracheinstellungen. (T7612)
- Zeilenumbruch des Tooltips "Add ADSK" korrigiert. (T7602)
- Verwendung des neuen Codes auch zum Prüfen abgetrennter OpenPGP-Signaturen. (T8337)
- Der Notizblock zeigt den signiertenText nicht mehr an, falls die Signatur ungültig ist. (T8020)
- Beim Ergebnis der Signaturprüfung unnötige Angabe eines Pfades entfernt. (T8332)
- Fingerabdrücke sind jetzt überall formatiert. (T7707)

Barrierefreiheit

- Der Fokus kehrt nun nach dem Schließen des Detaildialogs zur Zertifikatsliste zurück. (T8410)
- Tab-Reihenfolge im Entschlüsselungsergebnis für E-Mail-Dateien korrigiert. (T8125)
- Tab-Reihenfolge in der Smartcard-Tabelle korrigiert. (T8051)
- Fokus- und Tab-Reihenfolge in den Einstellungen zu Verzeichnisdiensten korrigiert. (T7846)
- Barrierefreie Bezeichnung für die Symbolleiste im Konfigurationsdialog ergänzt. (T7890)
- Einige Listen und Tabellen barrierefreier gestaltet. (T7859)
- Notizblock: Links in der Ergebnisliste in Schaltflächen umgewandelt und Tab-Reihenfolge korrigiert. (T7784)
- Notizblock: Tastaturnavigation im Texteditor korrigiert. (T7355)
- Prüfprotokoll anzeigen in der Signaturprüfung öffnet jetzt beim ersten Klick. (T7644)

- Barrierefreie Bezeichnung für das Textfeld des Notizblocks ergänzt. (T7751)
- Ausblenden versteckter Reiter in Ordnung gebracht. (T8422)
- Farbe einiger Schaltflächentexte in der Einstellung "Hoher Kontrast, Weiß" korrigiert. (T7585)
- Tabellenspalten-Überschriften barrierefrei gemacht. (T6568)
- Kontrast der Ergebnisliste bei Dateioperationen verbessert. (T5846)
- Rückmeldung "Es wurden keine Zertifikate gefunden" bei der Serverabfrage für Screenreader zugänglich gemacht. (T7862)
- Screenreader können jetzt eine leere Liste der Verzeichnisdienste rückmelden. (T7860)
- Doppeltes Vorlesen mehrerer Einträge durch Screenreader behoben. (T7854), (T7850), (T7739)

Outlook-Add-in (GpgOL)

- Ribbon-Symbol und Tooltip spiegeln jetzt die gewählten Sicherheitseinstellungen einer neuen Mail wider. (T7098)
- Der Inhalt reiner OpenPGP-HTML-Mails wird jetzt auch mit aktivierter Option "Als Klartext lesen" angezeigt. (T7843)
- Die Handhabung angehängter Krypto-Mails wurde verbessert. (T7806, rO06e35e5)
- Multipart-Anhangstyp bei fehlender CID korrigiert. (T8161)
- p7m-Anhänge brechen die Anhangsverarbeitung nicht mehr ab. (T8113)
- Einfrieren von Outlook beim Speichern eines S/MIME-verschlüsselten Entwurfs behoben. (T7837)
- Das Overlay wird nun auch in einem Fehlerfall nach dem Senden geschlossen. (rO0d36b54)
- gpg4win-tools: Kodierung der Statusinformationen korrigiert. (T8362)
- Gpgolconfig: Anzeige unveränderlicher Einstellungen korrigiert. (T8254)

- Memory Leaks behoben. (rO5b52c25, rOc18e33a, rO4330c1736f)
- Bestimmte MIME-Anhänge (CSV-Dateien) werden jetzt als Anhang statt eingebettet angezeigt, auch wenn der Content-Disposition-Header fehlt. (T8411)
- Bei der Mail-Verarbeitung beim Wechseln zwischen Mails sind nun weniger interne Aufrufe nötig. (T8418)
- Beim Schließen einer S/MIME-Nachrichtendatei wird keine leere Mail mehr im Posteingang gespeichert. (T8438)

Okular

- Die aktualisierte Poppler-Version behebt ein Problem mit Zertifikaten, deren Ablaufdatum im Jahr 2038 oder später liegt. (T8274)

Versionen der Komponenten

Komponente	Version	Anmerkungen
GnuPG	2.2.56	T8450
Kleopatra	3.4.0	
GpgOL	2.7.6	
GpgEX	1.0.11	
Libgcrypt	1.8.14	T8225
Libksba	1.8.0	T8253