GnuPG VS-Desktop - Version 3.2.0 (de)

g10 Code GmbH

2023-12-04

GnuPG VS-Desktop® ist seit 2023-12-04 in der Version 3.2.0 verfügbar. Die vorherige Version war 3.1.26.

Neue Features

PDF Reader

GnuPG VS-Desktop® wurde um den beliebten PDF Reader *Okular* ergänzt. Neben dem Anzeigen von Dokumenten können diese jetzt auch mit einer qualifizierten elektronischen Signatur (QES) versehen werden. Voraussetzung ist eine von GnuPG unterstützte Smartcard.

Diese *GnuPG Edition* von Okular ist zudem darauf optimiert, leichtgewichtig zu sein und eine möglichst geringe Angriffsfläche zu bieten. So werden beispielsweise keine aktiven Inhalte wie Mediendateien oder JavaScript unterstützt. Diese Edition sollte daher in Umgebungen mit hohen Sicherheitsanforderungen geeigneter sein als übliche PDF Reader.

Okular wird noch nicht per Standard installiert. Die Installation von Okular kann unter „Erweitert“ im Installer ausgewählt werden oder durch `INST_OKULAR=true` als Parameter übergeben werden.

GUI (Kleopatra)

- Ein neuer Anzeigemodus für Maildateien wurde hinzugefügt, damit Krypto-Mails, die von Mail-Clients ohne PGP/MIME- oder S/MIME-Unterstützung empfangen wurden, komfortabel entschlüsselt werden können. Dies bedeutet, dass Sie eine p7m Datei oder eine openpgp-encrypted-message.asc Anlage mit Kleopatra öffnen können, und sie wird wie eine Mail angezeigt. (T6199)

- Es ist nun möglich, mehrere Zertifikate gleichzeitig über die Gruppen-Verwaltung zu beglaubigen. (T6469)
- Das Ver- und Entschlüsseln von Dateiordnern wurde komplett überarbeitet, so dass es nun in Kleopatra etwa genau so schnell ist wie auf der Kommandozeile. Die neue Architektur ist zudem deutlich robuster und ermöglicht auch zukünftige Leistungsverbesserungen. Auch wurden dadurch mehrere Probleme behoben. (T5478,T6488,T6499 et.al.)
- Die Startzeit von Kleopatra wurde drastisch verbessert, insbesondere auf gedrosselten Systemen mit installierter Drittanbieter-Software, die Systemaufrufe manipuliert. Die Anzahl der Systemaufrufe zum Starten von Kleopatra wurde etwa halbiert. (T6259)
- Der Windows Dark Mode wird nun vollständig unterstützt. (T4066)
- Die Unterstützung von Telesec Signaturkarten wurde verbessert. (T6830)
- Es wird nun eine Information angezeigt, wenn Zertifikate ohne Beglaubigung exportiert werden sollen. Dies ist besonders beim Exportieren von Gruppen hilfreich. (T6766)
- Der Dialog um OpenPGP-Zertifikate zu verlängern wurde verbessert und überflüssige Optionen entfernt. (T6621)
- Es ist nun möglich, die Ausgabedateien von Kleopatra umzubenennen, wenn eine Datei mit dem gleichen Namen bereits existiert, statt nur überschreiben oder abbrechen zu können. (T6372)
- Es wird nun angeboten, den geheimen Schlüssel auf dem Computer zu löschen, wenn er erfolgreich auf eine Smartcard verschoben wurde. (T5836)
- Es wird nun gemeldet, wenn das eigene Zertifikat oder Zertifikate von Kommunikationspartnern bald ablaufen. Dies ist konfigurierbar und soll helfen, einen Austausch von neuen bzw. verlängerten Zertifikaten frühzeitig durchzuführen. (T6452)
- Der Notizblock verwendet nun auch das letztgewählte Signatur- sowie eigene Verschlüsselungs-Zertifikat als Standard. Die Werte werden mit der Dateiverschlüsselung geteilt. (T6415)
- Die vorgeschlagenen Zertifikate in den Eingabefeldern und in der Dropdown Auswahl werden nun alphabetisch sortiert. (T6492,T6514)

- Gesicherte Unterschlüssel können nun über die Benutzeroberfläche wiederhergestellt werden, auch wenn sie zwischenzeitlich über eine Smartcard genutzt wurden. (T3456,T3391)

- Für Beglaubigungen von Zertifikaten kann nun eine Standard Gültigkeitsdauer konfiguriert werden. (T6452)

- Die Standard Gültigkeitsdauer für neue Zertifikate wurde von zwei auf drei Jahre erhöht. Dies kann in den Einstellungen geändert werden. (T2701)

- Beim Verlängern der Gültigkeitsdauer von Zertifikaten wird nun der gleiche Zeitraum vorbelegt wie bei der Neuerstellung. (T6479)

Outlook Add-In (GgpOL)

- Unterstützung für RFC2231-kodierte Anhangsdateinamen wurde hinzugefügt, was die Kompatibilität mit Apple Mail erhöht. (T6604)

- Die Entwurfsverschlüsselung mit S/MIME-Zertifikaten wurde massiv verbessert und funktioniert nun zuverlässig. Es werden hierbei z.B. keine CRL-Prüfungen mehr durchgeführt. (T6827)

- Die Fehlerbehandlung wurde stark verbessert für den Fall, dass S/MIME aktiviert und bevorzugt sowie Signieren ausgewählt ist, ohne dass ein Signaturzertifikat verfügbar ist. In den Registry Settings unter „smimeNoCertSigErr“ ist beschrieben, wie Sie eine benutzerdefinierte Anweisung für diesen Fall hinzufügen können. (T6683)

- Es ist nun möglich, an S/MIME-Zertifikate zu verschlüsseln, die nicht vertrauenswürdig sind oder aufgrund von CRL-Fehlern nicht validiert werden können. In diesem Fall wird ein Warnhinweis angezeigt, der es dem Benutzer ermöglicht, die Fehler zu ignorieren. Dies ist nicht VS-NfD konform, kann aber für nicht eingestufte Kommunikation verwendet werden. (T6701)

- Mails ohne den korrekten MIME-Typ, die jedoch immer noch wie Krypto-Mails aussehen, werden nun entschlüsselt. Dies verbessert die Kompatibilität mit Apple Mail und verschiedenen Mail-Gateways, die die Struktur von Krypto-Mails im Transit ändern. (T6701)

- Die internen Anhänge werden nun `GpgOL_MIME_structure.mime` und nicht mehr `GpgOL_MIME_structure.txt` genannt, um es einfacher zu

machen, sie mit Kleopatra zu verknüpfen. Dies ist beispielsweise für Benutzer sichtbar, die die Outlook-Web Schnittstelle verwenden. (T6656)

- Der Sicherheitsbestätigungsdialog wurde verbessert, um Probleme mit den verfügbaren Zertifikaten besser anzuzeigen, falls eine konforme Verschlüsselung nicht möglich ist. (T6742,T6743,T6744)

- Der Sicherheitsbestätigungsdialog verändert nun seine Größe basierend auf der Anzahl der Empfänger, um so Scrollbalken zu vermeiden. (T6837)

Engine (GnuPG)

- Die elliptische Kurvenkryptografie (ECC) wurde für S/MIME implementiert, und die Zulassungsunterlagen wurden entsprechend angepasst. Derzeit sind nur Brainpool-Kurven VS-NfD-konform, aber technisch können auch andere Kurven verwendet werden. (T6253,T6802)

- OCB wurde als neuer Verschlüsselungsmodus hinzugefügt und ist gemäß den aktualisierten Zulassungsunterlagen VS-NfD konform. (T6263)

- Als Schlüsselserver ist jetzt der Wert `none` voreingestellt. Damit werde unnötige Abfragen gegen das Active Directory vermieden, die Operationen verlangsamen könnten. (T6708)

- Einstellungen für Proxyserver können jetzt automatisch von Windows übernommen werden. (T5768)

- Die Erkennung bereits komprimierter Daten wurde verbessert. Dies kann die Verschlüsselungsgeschwindigkeit bereits komprimierter Daten erheblich verbessern. (T6332)

- Das Anzeigen von Zertifikaten wurden beschleunigt. Dies trifft insbesondere auf S/MIME Zertifikate zu. (rG08ff55bd44]

- Das neue „ADSK“ Feature wird unterstützt. Dieses signalisiert, dass an mehrere Unterschlüssel gleichzeitig verschlüsselt werden sollte. (T6395, Beschreibung)

Behobene Fehler

GUI (Kleopatra)

- Verschiedene ungültige Operationen, z. B. das Signieren mit einem abgelaufenen Zertifikat, die zu Fehlern geführt hätten, können nicht

mehr ausgelöst werden. Mit Anzeige, warum dies der Fall ist. (T6742,T6788)

- Ablaufdaten nach dem 18.01.2038 (Jahr 2038 Fehler) sind nun möglich. (T6736)
- Beim Erstellen von Archiven werden diese nun zunächst als „.part" Datei geschrieben, um so die Fehlerbehandlung zu verbessern und den Vorgang abbrechen zu können, ohne ein defektes Archiv im Dateisystem zu hinterlassen. (T6584)
- Das Aktualisieren von Zertifikaten berücksichtigt nun auch ein eventuell vorhandenes Web Key Directory für die entsprechende Mailadresse. (T5951)
- Fortschrittsbalken werden nun auch korrekt für S/MIME Dateioperationen angezeigt und funktionieren jetzt auch für sehr große Dateien. (T6534)
- Die Startzeit von Kleopatra wurde deutlich verbessert. (T6259)
- Die Fehlerbehandlung von Dateiberechtigungs- und Schreibfehlern wurde grundsätzlich verbessert. (T6528)
- Ein unbeabsichtigter Timeout bei der Erstellung von Prüfsummendateien wurde entfernt. Dieser konnte zu unvollständigen oder leeren Prüfsummendateien führen. (T6573)
- Die Gültigkeitsdauer von Unterschlüsseln wird nun auch mit verlängert, wenn der Primärschlüssel bereits abgelaufen ist. Dies behebt das Problem, dass augenscheinlich verlängerte Schlüssel nicht mehr zum Verschlüsseln verwendet werden konnten. (T6473)
- Ein seltener Fall, bei dem Schlüssel ohne Signaturfunktion zum Signieren angeboten wurden, wurde behoben. (T6456)
- Das Abbrechen von Dateioperationen sorgt nun zuverlässig dafür, dass auch die entsprechenden Hintergrundoperationen abgebrochen werden. (T6524)
- Eine Reihe von Zeichensatzproblemen bei der Anzeige wurde behoben, z.B. bei Umlauten aus der GnuPG Ausgabe. (T5960)
- Beim Exportieren eines geheimen Unterschlüssels wird nun bei einem Abbruch korrekt abgebrochen und keine Datei ohne den geheimen Anteil erstellt. (T5755)

- Beim Importieren geheimer Schlüssel, die nicht als eigene markiert werden sollen, wird nun nicht mehr mehrfach nachgefragt, ob es der eigene Schlüssel ist. (T6474)

- Der Zustand von Kleopatra wird nun ordnungsgemäß in Konfigurationsdateien gespeichert, wenn Kleopatra beim Ausloggen des Benutzers geschlossen wird. (T6667)

- Das Importieren einer Zertifikatsdatei öffnet nun auch das Hauptfenster von Kleopatra. (T6671)

- Es wird nun nicht mehr unnötigerweise die Zwischenablage überwacht. Dies könnte Probleme mit Passwortmanagern verursacht haben, die die Zwischenablage leeren, sobald eine Fremdanwendung darauf zugreifen will. (T6531)

- Es ist nun nicht mehr möglich, das Ablaufdatum eines Zertifikats in die Vergangenheit zu legen. (T6519)

- Beim gleichzeitigen Importieren mehrerer Zertifikate kann es nicht mehr vorkommen, dass Kleopatra einfriert. (T6323)

- Beim Erstellen von Schlüsselmaterial auf Smartcards werden im konformen Modus auch nur konforme Algorithmen angeboten. (T6750)

- Verschiedene weitere Probleme bei der Darstellung von Sonderzeichen aus GnuPG-Ausgaben wurden behoben. (T5960)

- Ein Problem wurde behoben, bei dem „Tags“ bzw. Anmerkungen an Zertifikaten nicht korrekt angezeigt wurden, nachdem die Zertifikate neu geladen wurden. (T6768)

Outlook Add-In (GgpOL)

- Die Initialisierung des Plugins wurde nun verschoben, um die falsche Meldung zu vermeiden, dass GpgOL einen langsamen Start von Outlook verursacht. Allerdings kann diese Meldung immer noch angezeigt werden, da Outlook dies manchmal unabhängig von den tatsächlichen Zeitabläufen zeigt, aber die Verzögerung sollte 0ms betragen. (T6856)

- Ein Absturz wurde behoben der auftrat, wenn eine Mail mit einem Anhang ohne Dateinamen verschlüsselt werden sollte. (T6546)

- Änderungen an Kategorien und Flaggen werden nun korrekt übernommen, wenn diese durchgeführt werden ohne dass die Mail dabei entschlüsselt angezeigt wird. (T4127)
- Ein Absturz wurde behoben, der dann auftrat, wenn Anhänge ohne Dateinamen verschickt wurden. Dies trat z.B. bei einigen Signaturen auf, die ein Bild enthielten. (T6546)
- Der Sicherheitsbestätigungsdialog aktualisiert nun korrekterweise die Anzeige der Konformität, wenn man zwischen Protokollen wechselt. (T6600)
- Der Sicherheitsbestätigungsdialog wird nun immer angezeigt, wenn an Gruppen verschlüsselt wird, die nicht beglaubigte oder anderweitig nicht konforme Zertifikate enthalten. (T6401)
- Ein Problem wurde behoben, bei dem S/MIME „opak“" signierte Mails mit ungültiger Signatur ohne Inhalt angezeigt wurden. (T6624)
- Beim Erstellen von Schlüsseln über den Sicherheitsbestätigungsdialog von GpgOL werden nun die Einstellungen zur Schlüsselerstellung von GnuPG berücksichtigt. (T6805)
- Das Erstellen von Schlüsseln über den Sicherheitsbestätigungsdialog funktioniert nun wie vorgesehen. (T6813,T6823,T6566)
- Ein Fehler wurde behoben bei dem Krypto Mails als Leer angezeigt wurden, wenn Textdarstellung als bevorzugt eingestellt war. (T6357)
- Es wurden zusätzliche Schutzmaßnahmen eingefügt, um zu verhindern, das Klartext in einer ganz bestimmten ungewöhnlichen Konfiguration zurück zum Server übertragen wird. (rOdd3ff839)

Engine (GnuPG)

- Der Parser für das PKCS#12 Dateiformat wurde erweitert, um mehr Formate zu unterstützen. Dies sollte Probleme beim Import von p12 Dateien in Kleopatra beheben. (T6536)

Installer

- Installer: Das Installationspaket beendet nun laufende Hintergrundprozesse ordnungsgemäß, wodurch ein Neustart nach einem Update von GnuPG VS-Desktop nicht mehr erforderlich ist. (T6567)

Versionen der Komponenten

Komponente	Version	Anmerkungen
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