-----BEGIN PGP MESSAGE-----

hQGMA4zJmb2qRccfAQv+PP0ICikBlEraqIREjf67wz1aG44Fcsi/0nZpzq53cn1b
dy0OIcziXtKXI27PNK0hmYN8mBcjo5Pc2ZFgnacnVR/gVMk00GoWkHf9TCZ/ExmQ
XK4CGR7ETkRY7NdBVTct+NsMQA9UJynCf0TlZFWvJcSwLKlDHn/qK6kF9YkH7Ebi
tAJk63Xkkh76iqzx+ohAGAvxc8w/7N/cCdSclZ+xswpSB7EP0tSc37i1FbDtzGAm
vcTHYbuMlbs9ieANOxv/zWP1+PmAYV/FKmR41j33Sor1oAXmTukb0H9hYw01bOPP

GnuPG.com

Datenblatt: GnuPG VS-Desktop®

Stand 2025-01

Aufgrund seiner modulare Architektur kann GnuPG VS Desktop® leicht in alle etablierten Anwendungen integriert werden. Wir nutzen ausschließlich offene Standards und Normen und ermöglichen damit eine programmübergreifende Interoperabilität. Alle gängigen Algorithmen zur Verschlüsselung und Authentifizierung werden unterstützt.

GnuPG VS-Desktop® besteht aus den folgenden Komponenten:

- **GnuPG Core**: Krypto-Engine und Kommandozeilen-Tools
- **Kleopatra**: Grafische Benutzeroberfläche für Schlüssel- und Smartcardverwaltung, Verschlüsselung & Signatur
- **GpgOL**: Add-In für Microsoft Outlook
- **GpgEX**: Erweiterung für Windows Explorer
- **Okular**: Gehärteter PDF-Viewer und -Editor

Komponenten Eigenschaften

GnuPG Core	
Datenverschlüsselung	OpenPGP, S/MIME, symmetrisch
Datensignierung	OpenPGP, S/MIME
Schlüsselverwaltung	OpenPGP und S/MIME Schlüssel: erzeugen, importieren, exportieren, beglaubigen
Automatischer Schlüsselabruf	OpenPGP via LDAP-Server oder Web Key Directory (WKD), S/MIME via Zertifikatsserver
Vertrauensmodelle	Direkt, CA Vertrauen (Trusted Key, Trusted Introducer, S/MIME), WoT (Web of Trust)
Authenticated Encryption	MDC, OCB, GCM (entschlüsseln)
VS-NfD EU-RESTRICTED NATO-RESTRICTED	S/MIME mit Smartcard, OpenPGP mit Smartcard, OpenPGP ohne Smartcard (Voraussetzung hierfür sind zusätzliche Schutzmaßnahmen, siehe VSA-BSI-10867)

VS-V / EU-CONFIDENTIAL	Nach Bewertung durch das BSI
Standards	LibrePGP, PGP6, PGP7, PGP8, OpenPGP (RFC2440, RFC4880)
Smartcards / Token	OpenPGP, NetKey, Yubikey, NitroKey, Gnuk, PKCS#15, SC-HSM
ECC-Unterstützung	Brainpool, NIST-P, Curve25519
Zufallsgeneratoren	CSPRNG (DRG.3) mit Jitter-RNG, RDRAND, Padlock, Kein Einsatz des Windows-Zufallsgenerators
Algorithmen	AES, Twofish, Camellia, SHA-256, SHA-384, SHA-512, RSA (bis 8192), EdDSA, ECDH, ECDSA, DSA (deterministisch RFC6979)
Webbrowser (PKCS#11)	Hardware- / Software-Token (Firefox,Thunderbird etc.)
Webbrowser (WebMail)	Firefox, Chrome (z.B. mit Mailvelope)
Authentifizierung	Hardware- / Software-Token (SSH und PAM)
Betriebssysteme	Windows (x86-64) Version 10 oder 11, Linux (x86-64)

GpgOL Outlook Add-In

Mailverschlüsselung & Signieren	PGP/MIME, PGP-inline, S/MIME
Schlüsselsuche	GnuPG Keyring, LDAP, WKD, Autocrypt
EFAIL-Schutz	Authenticated Encryption für OpenPGP, spezielle Absicherung von S/MIME
Nachrichtenvorschau	Direktes entschlüsseln ohne Interaktion
Phishing-Schutz	Durch unterschiedliche Vertrauensstufen
Mail Transport / MTA	Microsoft Exchange ab Version 2010; IMAP + SMTP
Sicherheit und Compliance	Verschlüsselte Entwürfe (OpenPGP & S/MIME); Visuelle Indikatoren Anzeige der Verschlüsselungskonformität
Adressbuch-Integration	Festlegen und Verteilen der Schlüssel über das Adressbuch
Kompatibilität	Outlook 2010, 2013, 2016, 2019, Office 365 (klassisch); 32 bit or 64 bit, x86

Kleopatra Grafisches Crypto Frontend

Schlüsselverwaltung	OpenPGP und X.509 Schlüssel: erzeugen, import, export, beglaubigen
Dateien und Verzeichnisse	Signieren & verschlüsseln, entschlüsseln & überprüfen von Dateien und Verzeichnissen (Bei mehrere Dateien und Ordner wird gpgtar verwendet)
Notizblock	Signieren & verschlüsseln, entschlüsseln & überprüfen von Texten
Verzeichnisse	Abrufen von LDAP Server oder WKD, senden an LDAP-Server
Smartcards	Werden unterstützt, auch die Einrichtung von OpenPGP Karten
Sicherheit und Compliance	Selbsttest und Indikator für die Einhaltung der Konformität; visuelle Indikatoren für (nicht) konforme Zertifikate und Verschlüsselung
Betriebssysteme	Windows (x86-64) Version 10 oder 11, Linux (x86-64)

Okular PDF viewer - GnuPG Edition

Härtung	Nur Standard-PDF-Unterstützung, Unterstützung für aktive Komponenten ist deaktiviert, kein JavaScript
Signieren	Eingebettete qualifizierte elektronische Signaturen (QES, X.509)
Bearbeiten	Hervorheben, Textanmerkungen, Text einfügen, Formulare ausfüllen, Notizen einfügen
Betriebssysteme	Windows (x86-64) Version 10 oder 11, Linux (x86-64)