Datasheet: GnuPG VS-Desktop®

Stand 2025-01

The modular architecture allows GnuPG VS-Desktop® an easy integration into established applications. We only use open standards and norms to ensure interoperability across programs. All common algorithms for encryption and authentication are supported.

GnuPG VS-Desktop® consists of the following components:

- **GnuPG Core**: Crypto engine and CLI tools
- **Kleopatra**: Graphical frontend for key and smartcard management, encryption & signing
- **GpgOL**: Add-in for Microsoft Outlook
- **GpgEX**: Extension for Windows Explorer
- **Okular**: Hardened PDF viewer and editor

Component capabilities

GnuPG Core	
Data encryption	OpenPGP, S/MIME, symmetric
Data signing	OpenPGP, S/MIME
Key management	OpenPGP and S/MIME keys: generate, import, export, certify
Automatic key request	OpenPGP via LDAP server or Web Key Directory (WKD), S/MIME via certificate server
Trust models	Direct, CA trust (trusted key, trusted introducer, S/MIME), WoT (Web of Trust)
Authenticated Encryption	MDC, OCB, GCM (decrypt)
VS-NfD EU-RESTRICTED NATO-RESTRICTED	S/MIME with smartcard, OpenPGP with smartcard, OpenPGP without smartcard (Requires additional protective measures, see VSA-BSI-10867)

VS-V / EU-CONFIDENTIAL	Requires individual evaluation by the German Federal Office for Information Security (BSI)
Standards	LibrePGP, PGP6, PGP7, PGP8, OpenPGP (RFC2440, RFC4880)
Smartcard / Token	OpenPGP, NetKey, YubiKey, NitroKey, Gnuk, PKCS#15, SC-HSM
ECC support	Brainpool, NIST-P, Curve25519
Random generators	CSPRNG (DRG.3) with Jitter-RNG, RDRAND, Padlock, No use of the Windows random number generator
Algorithms	AES, Twofish, Camellia, SHA-256, SHA-384, SHA-512, RSA (bis 8192), EdDSA, ECDH, ECDSA, DSA (deterministically RFC6979)
Webbrowser (PKCS#11)	Hardware-/software token (Firefox,Thunderbird etc.)
Webbrowser (WebMail)	Firefox, Chrome (e.g. with Mailvelope)
Authentication	Hardware-/software token (SSH and PAM)
Operating systems	Windows (x86-64) version 10 or 11, Linux (x86-64)

GpgOL Outlook Add-In	
Mail encryption & signing	PGP/MIME, PGP inline, S/MIME
Key discovery	GnuPG Keyring, LDAP, WKD, Autocrypt
EFAIL protection	Authenticated encryption for OpenPGP, protection for S/MIME
Message preview	Direct decryption without interaction
Phishing protection	Via different levels of trust
Mail Transport / MTA	Microsoft Exchange version 2010 or greater; IMAP + SMTP
Security and compliance measures	Encrypted drafts (OpenPGP & S/MIME); Visual indicators of encryption compliance
Address book integration	Setting and distributing of keys via address book
Compatibility	Outlook 2010, 2013, 2016, 2019, Office 365 (classic); 32 bit or 64 bit, x86

Kleopatra Graphical Crypto Frontend	
Key management	OpenPGP and X.509 keys: generate, import, export, certify
Files and folders	Sign & encrypt, decrypt & verify files or folders (For multiple files and folders gpgtar is used.)
Notepad	Sign & encrypt, decrypt & verify texts
Directorys	Fetch from LDAP or WKD, send to LDAP-Server
Smartcards	Supported; also setup of OpenPGP cards
Security and compliance measures	Compliance self test and indicator; Visual indicators about (non) compliant certificates and encryption
Operating systems	Windows (x86-64) version 10 or 11, Linux (x86-64)

Okular PDF viewer - GnuPG Edition	
Hardening	Only standard PDF support, support for active components is disabled, no JavaScript
Signing	Embeded qualified electronic signatures (QES, X.509)
Editing	Highlighting, text annotation, insert text, fill in forms, insert notes
Operating systems	Windows (x86-64) version 10 or 11, Linux (x86-64)