Datenblatt: GnuPG VS-Desktop®

Stand 2024-10

Durch die 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 mit uns unterstützt:

GnuPG VS-Desktop®	
Datenverschlüsselung	OpenPGP, S/MIME, symmetrisch
Mailverschlüsselung	PGP/MIME, S/MIME
Autom. Schlüsselabruf	OpenPGP über Web Key Directory, S/MIME über Zertifikatsserver
Vertrauensmodelle	Direkt, WoT (Web of Trust), TOFU+PGP (Trust on first use)
Authenticated Encryption	Nur in OpenPGP
VS-NfD (EU-RESTRICTED)	S/MIME mit Smartcard, OpenPGP und S/MIME ohne Smartcard [1] OpenPGP symmetrisch (nur mit Passwort)
VS-V (EU-CONFIDENTIAL)	Nach Bewertung durch das BSI
Compliance	de-vs, OpenPGP, RFC4880bis, PGP6, PGP7, PGP8, RFC2440
Unterstützte Smartcards	OpenPGP, NetKey, Yubikey, NitroKey, Gnuk, PKCS#15, SC-HSM
ECC-Unterstützung für OpenPGP	Brainpool, NIST-P, Curve25519, Bitcoin
Zufallsgeneratoren [2]	CSPRNG (DRG.3) mit Jitter-RNG, RDRAND, Padlock
Algorithmen	AES, Twofish, Camellia, SHA-256, 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)

GnuPG VS-Desktop® unterstützt 32- und 64bit-Windows-Systeme ab Version 7 oder neuer.

[1] Voraussetzung hierfür sind zusätzliche Schutzmaßnahmen, siehe VSA-BSI-10573.
[2] Kein Einsatz des Windows-Zufallsgenerators.

GpgOL Outlook Add-In	
Adressbuch-Integration	Festlegen und Verteilen der Schlüssel über das Adressbuch
Autocrypt-Unterstützung	Optional lesend. Inkl. verschlüsseltem Betreff
EFAIL-Schutz	Authenticated Encryption für OpenPGP, spezielle Absicherung von S/MIME
Nachrichtenleiste	Direktes entschlüsseln ohne Interaktion
Inline-Editoren	Schnelles Antworten und Weiterleiten
Kompatibilitätsmodi	PGP/Inline
Phishing-Schutz	Unterschiedliche Vertrauensstufen
Server	Microsoft Exchange ab Version 2010, IMAP
Verschlüsselte Entwürfe	OpenPGP, S/MIME

Das GpgOL Outlook Add-In ist kompatibel mit Outlook 2010, 2013, 2016 und 2019 und unterstützt Mailtransport per SMTP/IMAP und Exchange Server ab 2010.