Technisches Datenblatt
GnuPG VS-Desktop

GnuPG VS-Desktop Installationspaket

Verschlüsselungssoftware

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)
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	CSPRNG (DRG.3) mit Jitter-RNG (2) | RDRAND | Padlock
Algorithmen	AES | Twofish | Camellia | SHA-256 | SHA-512 | RSA (bis 8192) | EdDSA | ECDH | ECDSA | DSA (deterministisch RFC6979)
Webbrowser (PKCS#11)	Hardware- und Software-Token (Firefox,Thunderbird etc.)
Webbrowser (Web-Mail)	Firefox | Chrome (z.B. mit Mailvelope)
Authentifizierung	Hardware- und Software-Token (SSH und PAM)

Outlook-PlugIn

Adressbuch-Integration	Festlegen und Verteilen der Schlüssel über das Adressbuch
Autocrypt-Unterstützung	Optional lesend. Inkl. verschlüsseltem Betreff
EFAIL-Schutz	Authenticated Encryption für OpenPGP | Absicherung für S/MIME
Nachrichtenleiste	Direktes Entschlüsseln ohne Interaktion
Inline-Editoren	Schnelles Antworten und Weiterleiten
Kompatibilitätsmodi	PGP/Inline
Phishing-Schutz	Über unterschiedliche Vertrauensstufen
Server	Microsoft Exchange (ab Version 2010) | IMAP
Verschlüsselte Entwürfe	OpenPGP | S/MIME

(1) Vorraussetzung hierfür sind zusätzliche Schutzmaßnahmen, z.B. SINA-Workstation. Siehe BSI-VSA 10412.
(2) Kein Einsatz des Windows-Zufallsgenerators.

g10 Code GmbH ▪ Gutenberg Weg 4 ▪ D-40699 Erkrath ▪ +49 2104 493 879 0 ▪ info@gnupg.com ▪ www.gnupg.com

tdb_gnupg_vs_desktop_de.pdf ▪ Rev. 01 ▪ Stand 08/2020