Produktdatenblatt

GnuPG Desktop

DIE UNIVERSELLE KRYPTO-LÖSUNG

GnuPG Desktop ist eine für den Einsatz in Unternehmen maßgeschneiderte Version von Gpg4win, einer Software zum Verschlüsseln und Signieren von E-Mails, Dateien und Ordnern unter Windows.

Qualitätsgesicherte GnuPG-Desktop-Pakete mit GnuPG und allen Gpg4win-Komponenten erhalten Sie direkt vom Hersteller. Die Firma g10 Code bietet außerdem professionellen Support, garantierte Reaktionszeiten und Service made in Germany – persönlich und individuell auf Ihr Unternehmen abgestimmt.

Freiheit

Alle unsere Programme sind Open Source. Wir veröffentlichen also den Quelltext unserer Software, und jeder kann diesen überprüfen. Dadurch ist sichergestellt, dass Sie nicht von einem einzigen Hersteller abhängig sind und auch nach Jahrzehnten noch Ihre Daten entschlüsseln können.

Flexibilität

GnuPG setzt auf eine modulare Architektur: ein Kryptokern und mehrere Anwendungen, die diesen Kern nutzen. Dadurch ist es leicht, GnuPG in etablierte Prozesse und Programme zu integrieren. Automatisierung ist unser Designziel – der Einsatz offener Standards garantiert Interoperabilität. GnuPG unterstützt nahezu alle gängigen Algorithmen zur Verschlüsselung und Authentifizierung.

Zuverlässigkeit

Seit 1997 funktioniert GnuPG und verschlüsselt. Und funktioniert. Und verschlüsselt. GnuPG ist die Standardlösung, um Netze und Dienste abzusichern, und nahezu jeder Linux-Server setzt auf unsere Software, um die Integrität des Systems abzusichern.

Unsere Leistungen:

- Gut abgestimmtes Product Lifecycle Management (PLM)
- Regelmäßige Sicherheitsupdates (Bereitstellung von Patches und Fixes innerhalb einer Woche maximal)
- Einfaches Deployment dank MSI-Paketierung
- Direkter Zugang zu den Entwicklern (professioneller Support in Deutsch und Englisch)

Features der Software:

- Integration in Microsoft Outlook (GpgOL)
- Dateien verschlüsseln im Windows Explorer
- Schlüssel und Zertifikate verwalten in Kleopatra
- SSH-Authentifizierung mit PuTTY-Integration

Technische Details

Verschlüsseln von Dateien	OpenPGP, S/MIME, symmetrisch
Verschlüsseln von E-Mails	PGP/MIME, S/MIME
Automatisches Abrufen der Schlüssel	Web Key Directory (WKD) für OpenPGP, X.509-Zertifikatsserver für S/MIME
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 mit weiteren Schutzmaßnahmen, 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-Token, PKCS#15, SC-HSM
ECC-Unterstützung (Elliptic Curve Cryptography) für OpenPGP	Brainpool, NIST-P, Curve25519, Bitcoin
Zufallsgeneratoren	CSPRNG (DRG.3) mit Jitter-RNG, RDRAND, Padlock **Kein Einsatz des Windows-Zufallsgenerators**
Algorithmen	AES, Twofish, Camellia, SHA-256, SHA-512, RSA (bis 8192), EdDSA, ECDH, ECDSA, DSA (deterministisch RFC6979)
Webbrowser (PKCS#11)	Mit Hardware- und Software-Token (Firefox, Thunderbird usw.)
Webbrowser (Web-Mail)	Firefox, Chrome (z.B. mit Mailvelope)
Authentifizierung	Mit Hardware- und Software-Token (SSH und PAM)

Outlook Integration

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