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

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

# Technical data sheet

Updated 01/2022 ▪ Changes and errors excepted.

## GnuPG Desktop

GnuPG Desktop supports 32- and 64bit Windows systems from version 7 or newer. The GpgOL Plug-in is compatible with Outlook 2010, 2013, 2016 as well as 2019 and supports mail transport via SMTP/IMAP and Exchange Server from 2010.

| GnuPG Desktop | |
|---|---|
| Data encryption | OpenPGP \| S/MIME \| Symmetric |
| Mail encryption | PGP/MIME \| S/MIME |
| Autom. key request | OpenPGP via web key directory \| S/MIME via certificate server |
| Trust models | Direct \| WoT (Web of Trust) \| TOFU+PGP (Trust on first use) |
| Authenticated encryption | Only OpenPGP |
| Compliance | de-vs \| OpenPGP \| RFC 4880bis \| PGP6 \| PGP7 \| PGP8 \| RFC 2440 |
| Smartcard / Token-Support | OpenPGP \| NetKey \| Yubikey \| NitroKey \| Gnuk \| PKCS#15 \| SC-HSM |
| ECC-Support for OpenPGP | Brainpool \| NIST-P \| Curve25519 \| Bitcoin |
| Random generators | CSPRNG (DRG.3) with Jitter-RNG [1] \| RDRAND \| Padlock |
| Algorithms | AES \| Twofish \| Camellia \| SHA-256 \| SHA-512 \| RSA (up to 8192) \| EdDSA \| ECDH \| ECDSA \| DSA (deterministically RFC 6979) |
| Webbrowser (PKCS#11) | Hardware- / Software-Token (Firefox,Thunderbird etc.) |
| Webbrowser (Web-Mail) | Firefox \| Chrome (e.g. with Mailvelope) |
| Authentication | Hardware- / Software-Token (SSH and PAM) |

| GpgOL Outlook Plug-in | |
|---|---|
| Adress book integration | Setting and distributing of keys via address book |
| Autocrypt-Support | Optional reading. Incl. encrypted subject |
| EFAIL protection | Authenticated encryption for OpenPGP \| Protection for S/MIME |
| Message board | Direct decryption without interaction |
| Inline editors | Quick reply and forwarding |
| Compatibility modes | PGP/Inline |
| Phishing protection | Via different levels of trust |
| Server | Microsoft Exchange (from version 2010) \| IMAP |
| Encrypted drafts | OpenPGP \| S/MIME |

[1] No use of the Windows random generator.