GPG einrichten & Schlüssel erstellen – Windows & Linux

Diese Anleitung zeigt dir, wie du GPG auf deinem Computer einrichtest und dein erstes Schlüsselpaar erstellst. Du brauchst dafür keine Vorkenntnisse – folge einfach den Schritten für dein Betriebssystem.

Installation

Windows

Unter Windows empfehlen wir **Gpg4win** (Empfehlung des BSI LINK) , das GPG zusammen mit einer grafischen Oberfläche (Kleopatra) installiert.

1. Lade Gpg4win unter **gpg4win.org** herunter
2. Starte den Installer und folge den Anweisungen
3. Stelle sicher, dass **Kleopatra** als Komponente ausgewählt ist
4. Schließe die Installation ab

Linux

Unter den meisten Linux-Distributionen ist GPG bereits vorinstalliert. Falls nicht, installiere es über den Paketmanager:

Ubuntu / Debian:

```
sudo apt install gnupg
```

Fedora:

```
sudo dnf install gnupg2
```

Arch:

```
sudo pacman -S gnupg
```

Schlüsselpaar erstellen

Windows (Kleopatra)

1. Öffne **Kleopatra**
2. Klicke auf **„Neues Schlüsselpaar"**
3. Wähle **„Persönliches OpenPGP-Schlüsselpaar erstellen"**
4. Gib deinen Namen und deine THW-Jugend-E-Mail-Adresse ein
5. Klicke auf **„Erweiterte Einstellungen"** und stelle folgendes ein:
   - Algorithmus: **RSA**
   - Schlüssellänge: **4096 Bit**
   - Ablaufdatum: empfohlen, z. B. **2 Jahre**
6. Klicke auf **„Erstellen"**
7. Vergib ein starkes **Passwort** für deinen Private Key – dieses schützt deinen Schlüssel zusätzlich

Linux (Terminal)

Führe folgenden Befehl aus:

```
gpg --full-generate-key
```

Du wirst durch mehrere Schritte geführt:

1. Wähle **„RSA and RSA"** (Option 1)
2. Gib als Schlüssellänge **4096** ein
3. Lege ein Ablaufdatum fest – empfohlen: **2y** (2 Jahre)
4. Gib deinen Namen und deine THW-Jugend-E-Mail-Adresse ein
5. Bestätige mit **„O"** (Okay)
6. Vergib ein starkes Passwort für deinen Private Key

Schlüssel überprüfen

Windows (Kleopatra)

Dein neuer Schlüssel erscheint nach der Erstellung in der Übersicht von Kleopatra. Du siehst dort Name, E-Mail-Adresse, Schlüssel-ID und Ablaufdatum.

Linux (Terminal)

Liste deine vorhandenen Schlüssel mit folgendem Befehl auf:

```
gpg --list-secret-keys --keyid-format LONG
```

Backup des Private Key

Erstelle unmittelbar nach der Schlüsselerstellung ein Backup deines Private Key und speichere es sicher – am besten verschlüsselt und offline. Ohne dieses Backup ist eine Wiederherstellung nicht möglich.

Windows (Kleopatra)

Klicke mit der rechten Maustaste auf deinen Schlüssel und wähle **„Sichern von geheimen Schlüsseln"**. Speichere die Datei an einem sicheren Ort.

Linux (Terminal)

```
gpg --export-secret-keys --armor deine@email.de > private_key_backup.asc
```

> **Wichtig:** Der Private Key darf niemals per E-Mail, Chat oder Cloud übertragen werden. Bewahre das Backup offline auf – zum Beispiel auf einem verschlüsselten USB-Stick.

Revision #2
Created 2026-03-05 04:16:44 UTC by Christian Weiß
Updated 2026-03-05 04:23:21 UTC by Christian Weiß