GnuPG und OpenPGP

Einordnung

OpenPGP ist ein Standard zur Verschlüsselung und digitalen Signatur von Dateien und E-Mails. GnuPG (gpg) ist eine freie Implementierung dieses Standards.

Bei der **asymmetrischen Verschlüsselung** verschlüsselt der Absender mit dem öffentlichen Schlüssel des Empfängers. Zum Entschlüsseln wird der zugehörige geheime Schlüssel benötigt. Daneben unterstützt GnuPG die **symmetrische Verschlüsselung** mit einer Passphrase.

Ein OpenPGP-Schlüssel kann aus einem Hauptschlüssel und mehreren Unterschlüsseln bestehen, die unterschiedliche Aufgaben übernehmen, beispielsweise Signieren oder Entschlüsseln.

GnuPG = GNU Privacy Guard
PGP = Pretty Good Privacy

Quellen:

- Projekt GnuPG
- GnuPG Befehle
- GnuPG bei Ubuntuusers
- GnuPG-Software (auch für Windows-Systeme)

Installation unter Debian

Paketlisten aktualisieren:

```
sudo apt update
```

GnuPG installieren:

```
sudo apt install gnupg
```

Installation prüfen:

```
gpg --version
```

Der GnuPG-Schlüsselbund

Als **Schlüsselbund** bezeichnet man den lokal von GnuPG verwalteten Bestand an öffentlichen und geheimen Schlüsseln. Er ist keine einzelne Datei, sondern besteht bei aktuellen GnuPG-Versionen aus mehreren Dateien und Verzeichnissen.

Standardmäßig liegen diese Daten unter `~/.gnupg/` im Home-Verzeichnis des jeweiligen Linux-Benutzers. Der öffentliche Schlüsselbestand wird beispielsweise in `pubring.kbx` verwaltet; geheime Schlüssel liegen normalerweise im Unterverzeichnis `private-keys-v1.d/`. Der genaue Aufbau kann je nach Version und Konfiguration abweichen.

Den verwendeten GnuPG-Datenordner anzeigen:

```
gpgconf --list-dirs homedir
```

Öffentliche Schlüssel anzeigen:

```
gpg --list-keys
```

Geheime Schlüssel anzeigen:

```
gpg --list-secret-keys
```

Fingerprints anzeigen:

```
gpg --fingerprint
```

Ein neu erzeugtes Schlüsselpaar wird automatisch im eigenen GnuPG-Schlüsselbestand abgelegt. Der öffentliche Schlüssel eines anderen Empfängers muss vor der Verschlüsselung für diesen Empfänger importiert werden. Auf dem Rechner, auf dem entschlüsselt werden soll, muss der passende geheime Schlüssel verfügbar sein.

Wichtig: Der öffentliche Schlüssel eines Empfängers allein reicht nicht zum Entschlüsseln. Ein Import eines öffentlichen Schlüssels erzeugt auch keinen dazugehörigen geheimen Schlüssel.

Hinweis: In Thunderbird erzeugte und verwaltete OpenPGP-Schlüssel werden von GnuPG (gpg –list-keys) normalerweise nicht angezeigt, da Thunderbird einen eigenen Schlüsselbund verwendet.

Eigenes Schlüsselpaar erzeugen

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

Der Dialog führt durch Schlüsseltyp, Gültigkeitsdauer und Benutzerkennung. Für den geheimen Schlüssel sollte bei interaktiver Nutzung eine geeignete Passphrase vergeben werden.

Danach kann der eigene Schlüsselbestand überprüft werden:

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

Die Benutzerkennung (beispielsweise eine E-Mail-Adresse) ist eine Kennzeichnung des Schlüssels. Sie beweist für sich allein keine Identität.

Öffentlichen Schlüssel exportieren und importieren

Eigenen öffentlichen Schlüssel exportieren

```
gpg --armor --export beispiel@wiki.bluegnu.de > public.asc
```

`public.asc` enthält den öffentlichen Schlüssel. Diese Datei darf weitergegeben werden.

Öffentlichen Schlüssel eines Empfängers importieren

```
gpg --import public.asc
```

Anschließend den Fingerprint anzeigen:

```
gpg --fingerprint beispiel@wiki.bluegnu.de
```

Der Fingerprint muss vor einer vertraulichen Verwendung über einen unabhängigen, vertrauenswürdigen Kanal mit dem Empfänger abgeglichen werden. Der Import allein bestätigt die Identität nicht.

GnuPG kann bei nicht ausreichend bestätigter Schlüsselvertrauenswürdigkeit vor der Verschlüsselung nachfragen. Solche Warnungen sollten nicht ungeprüft übergangen werden.

Datei asymmetrisch verschlüsseln

Voraussetzung: Der geprüfte öffentliche Schlüssel des Empfängers ist im lokalen Schlüsselbund vorhanden.

```
gpg --encrypt --recipient beispiel@wiki.bluegnu.de --output dokument.gpg
dokument.txt
```

Die Datei `dokument.gpg` enthält den verschlüsselten Inhalt. Die ursprüngliche Datei `dokument.txt` wird dadurch nicht automatisch gelöscht.

Datei asymmetrisch entschlüsseln

Auf dem empfangenden Rechner muss der zum Empfängerschlüssel gehörende geheime Entschlüsselungsschlüssel im GnuPG-Schlüsselbestand verfügbar sein. Falls dieser durch eine Passphrase geschützt ist, kann GnuPG sie abfragen.

```
gpg --decrypt --output dokument-entschluesselt.txt dokument.gpg
```

Die entschlüsselte Datei wird unter dem angegebenen Namen gespeichert. Ein bereits vorhandenes Ausgabeziel wird von GnuPG nicht ohne entsprechende Rückfrage überschrieben.

Datei symmetrisch verschlüsseln

Bei der symmetrischen Verschlüsselung ist kein OpenPGP-Schlüsselpaar erforderlich. GnuPG fragt eine Passphrase ab und leitet daraus das benötigte Schlüsselmaterial ab.

```
gpg --symmetric --output dokument-symmetrisch.gpg dokument.txt
```

Datei symmetrisch entschlüsseln

Hier wird die bei der Verschlüsselung verwendete Passphrase benötigt.

```
gpg --decrypt --output dokument-symmetrisch-entschluesselt.txt dokument-
symmetrisch.gpg
```

Dateien signieren und Signaturen prüfen

Abgetrennte Signatur erstellen

```
gpg --armor --detach-sign dokument.txt
```

Dadurch entsteht üblicherweise `dokument.txt.asc` mit der Signatur. Die Originaldatei bleibt unverändert.

Signatur überprüfen

```
gpg --verify dokument.txt.asc dokument.txt
```

Die Prüfung erfordert den öffentlichen Signaturschlüssel. Eine gültige kryptografische Signatur beweist nicht automatisch, dass die zugehörige Benutzerkennung tatsächlich zur behaupteten Person gehört. Hierfür ist zusätzlich die Identität beziehungsweise der Fingerprint des Schlüssels zu prüfen.

Eine Signatur verschlüsselt die Datei nicht.

Geheimen Schlüssel sichern und wiederherstellen

Ein geheimer Entschlüsselungsschlüssel kann erforderlich sein, um ältere verschlüsselte Dateien später wieder zu lesen. Deshalb sind sichere, getrennt aufbewahrte Sicherungen wichtig.

Geheimen Schlüssel exportieren

Sicherheitshinweis: Ein Export des geheimen Schlüssels ist hochsensibel. Die Exportdatei darf nicht

öffentlich zugänglich sein. Die folgenden Befehle sollten nur in einem geschützten Verzeichnis auf einem vertrauenswürdigen System ausgeführt werden.

Vor dem Erstellen einer neuen Exportdatei die Zugriffsrechte neu angelegter Dateien beschränken:

```
umask 077
```

Geheimen Schlüssel exportieren:

```
gpg --export-secret-keys --output geheimschluessel-backup.gpg
beispiel@wiki.bluegnu.de
```

Der Export kann passphrasengeschützte Schlüssel enthalten; die Datei muss trotzdem wie ein Geheimnis behandelt und sicher gesichert werden. Bei Smartcards oder Hardware-Token sind geheime Schlüssel möglicherweise nicht exportierbar.

Geheimen Schlüssel wieder importieren

Den gesicherten Schlüssel auf einem vertrauenswürdigen System importieren:

```
gpg --import geheimschluessel-backup.gpg
```

Anschließend prüfen, ob der geheime Schlüssel verfügbar ist:

```
gpg --list-secret-keys
```

Ein Import ist keine Garantie für die erfolgreiche Wiederherstellung aller Funktionen: Bei Hardware-Schlüsseln, Unterschlüsseln oder abweichenden Vertrauenseinstellungen können weitere Schritte nötig sein. Eine Sicherung sollte deshalb durch einen kontrollierten Wiederherstellungstest überprüft werden.

Schlüsselverlust, Widerruf und Kompromittierung

Geht ein geheimer Entschlüsselungsschlüssel ohne verwendbare Sicherung verloren, können damit verschlüsselte Daten dauerhaft unlesbar werden.

Bei Verdacht auf Kompromittierung muss geprüft werden, ob der Schlüssel widerrufen und ersetzt werden muss. Bereits offengelegte Daten werden durch einen Widerruf nicht nachträglich geschützt.

GnuPG kann bei der Schlüsselerstellung ein Widerrufszertifikat im Verzeichnis `~/.gnupg/openpgp-revocs.d/` ablegen. Dieses muss vor unbefugtem Zugriff geschützt werden, da damit ein Schlüssel widerrufen werden kann.

Weitere Hinweise: Schlüsselverwaltung und Sicherung.

Weiterführende Informationen

- Kryptografische Grundlagen
- Fingerprints und digitale Signaturen
- Schlüsselverwaltung

Zurück zur Übersicht

From:
https://wiki.bluegnu.de/ - **wiki**

Permanent link:
https://wiki.bluegnu.de/doku.php/open:it:secure:gpg_openpgp

Last update: **2026/11/15 20:51**