Dateien verschlüsseln & entschlüsseln

Diese Anleitung zeigt dir, wie du Dateien mit dem Public Key einer anderen Person verschlüsselst und wie du verschlüsselte Dateien, die für dich bestimmt sind, mit deinem Private Key entschlüsselst.

Voraussetzung

Um eine Datei für jemanden zu verschlüsseln, benötigst du den **Public Key** der Empfängerin oder des Empfängers. Wie du einen Public Key erhältst und in GPG importierst, erklärt die nächste Seite. Stelle sicher, dass der Schlüssel bereits importiert ist, bevor du fortfährst.

Datei verschlüsseln

Windows (Kleopatra)

1. Öffne **Kleopatra**
2. Klicke auf **„Dateien signieren/verschlüsseln"**
3. Wähle die zu verschlüsselnde Datei aus
4. Wähle **„Für andere verschlüsseln"**
5. Wähle den Public Key der Empfängerin oder des Empfängers aus
6. Klicke auf **„Weiter"** und anschließend auf **„Verschlüsseln"**

Es wird eine neue Datei mit der Endung **.gpg** erstellt – das ist die verschlüsselte Version. Die Originaldatei bleibt unverändert erhalten.

Linux (Terminal)

```
gpg --encrypt --recipient empfaenger@email.de dateiname.pdf
```

Ersetze **empfaenger@email.de** durch die E-Mail-Adresse, die mit dem Public Key der Empfängerin oder des Empfängers verknüpft ist. Die verschlüsselte Datei wird als **dateiname.pdf.gpg** gespeichert.

Möchtest du die Datei zusätzlich für dich selbst verschlüsseln – damit auch du sie später noch öffnen kannst – ergänze deinen eigenen Schlüssel:

```
gpg --encrypt --recipient empfaenger@email.de --recipient deine@email.de dateiname.pdf
```

Datei entschlüsseln

Windows (Kleopatra)

1. Öffne **Kleopatra**
2. Klicke auf **„Dateien entschlüsseln/prüfen"**
3. Wähle die verschlüsselte Datei (Endung **.gpg**) aus
4. Gib das Passwort deines Private Key ein
5. Wähle einen Speicherort für die entschlüsselte Datei

Linux (Terminal)

```
gpg --decrypt dateiname.pdf.gpg > dateiname.pdf
```

GPG fragt automatisch nach dem Passwort deines Private Key. Die entschlüsselte Datei wird am angegebenen Ort gespeichert.

Datei verschlüsseln und signieren

Zusätzlich zur Verschlüsselung kannst du eine Datei auch **signieren**. Eine Signatur beweist, dass die Datei tatsächlich von dir stammt und auf dem Weg nicht verändert wurde – das ist besonders bei sensiblen Dokumenten empfehlenswert.

Windows (Kleopatra)

Wähle beim Verschlüsseln zusätzlich die Option **„Signieren"** und wähle deinen eigenen Schlüssel als Signaturschlüssel aus.

Linux (Terminal)

```
gpg --encrypt --sign --recipient empfaenger@email.de dateiname.pdf
```

Wichtige Hinweise

- Verschlüsselte Dateien (**.gpg**) können nur von Personen geöffnet werden, deren Public Key beim Verschlüsseln angegeben wurde
- Ohne den passenden Private Key und das zugehörige Passwort ist eine Entschlüsselung nicht möglich
- Lösche die unverschlüsselte Originaldatei nach dem Verschlüsseln, wenn sie nicht mehr benötigt wird – insbesondere bei sensiblen Daten
- Versende ausschließlich die verschlüsselte **.gpg**-Datei, niemals das Original

---

Revision #2
Created 2026-03-05 04:16:53 UTC by Christian Weiß
Updated 2026-03-05 04:26:10 UTC by Christian Weiß