Public Key teilen & empfangen

Damit andere Personen Dateien für dich verschlüsseln können, müssen sie deinen Public Key kennen. Diese Seite erklärt, wie du deinen Public Key weitergibst und wie du den Public Key einer anderen Person in GPG importierst.

Deinen Public Key exportieren

Windows (Kleopatra)

1. Öffne **Kleopatra**
2. Klicke mit der rechten Maustaste auf deinen Schlüssel
3. Wähle **„Exportieren"**
4. Speichere die Datei – sie hat die Endung **.asc**

Linux (Terminal)

```
gpg --export --armor deine@email.de > public_key.asc
```

Die exportierte Datei **public_key.asc** enthält deinen Public Key als lesbaren Text. Diese Datei kannst du bedenkenlos weitergeben.

Deinen Public Key teilen

Den Public Key kannst du auf verschiedene Arten teilen:

Per E-Mail: Hänge die **.asc**-Datei einfach als Anhang an eine E-Mail an.

Direkt im Text: Der Inhalt der **.asc**-Datei ist lesbarer Text und kann direkt in eine E-Mail oder ein Dokument eingefügt werden. Er beginnt immer mit:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

Im Wiki oder per Link: Du kannst deinen Public Key auch zentral ablegen, damit andere ihn jederzeit abrufen können – zum Beispiel auf einer internen Wiki-Seite des IT-Teams.

> **Hinweis:** Der Public Key ist nicht geheim und kann offen geteilt werden. **Gib niemals deinen Private Key weiter – auch nicht auf Nachfrage.**

Fingerabdruck deines Schlüssels

Jeder GPG-Schlüssel hat einen eindeutigen **Fingerabdruck** – eine Zeichenkette, anhand derer man sicherstellen kann, dass ein empfangener Public Key tatsächlich von der richtigen Person stammt und nicht ausgetauscht wurde.

Windows (Kleopatra)

Klicke auf deinen Schlüssel – der Fingerabdruck wird in der Detailansicht angezeigt.

Linux (Terminal)

```
gpg --fingerprint deine@email.de
```

Teile deinen Fingerabdruck am besten über einen zweiten Kanal – zum Beispiel persönlich oder per Telefon – damit die Empfängerin oder der Empfänger den erhaltenen Schlüssel verifizieren kann.

Public Key einer anderen Person importieren

Windows (Kleopatra)

1. Öffne **Kleopatra**
2. Klicke auf **„Importieren"**
3. Wähle die **.asc**-Datei der anderen Person aus
4. Der Schlüssel erscheint nun in deiner Schlüsselverwaltung

Linux (Terminal)

```
gpg --import public_key.asc
```

Importierten Schlüssel verifizieren

Nach dem Import solltest du den Fingerabdruck des erhaltenen Schlüssels mit dem Fingerabdruck der sendenden Person abgleichen – zum Beispiel per Telefon oder persönlich. So stellst du sicher, dass du den richtigen Schlüssel importiert hast und nicht einen gefälschten.

Windows (Kleopatra)

Klicke auf den importierten Schlüssel und prüfe den angezeigten Fingerabdruck.

Linux (Terminal)

```
gpg --fingerprint empfaenger@email.de
```

Stimmt der Fingerabdruck überein, kannst du den Schlüssel in Kleopatra als **„vertrauenswürdig"** markieren. Damit bestätigst du, dass du die Echtheit des Schlüssels geprüft hast.

> **Wichtig:** Vertraue nie blind einem erhaltenen Public Key – überprüfe immer den Fingerabdruck über einen zweiten Kanal. Ein gefälschter Schlüssel würde bedeuten, dass deine verschlüsselte Datei von einer unbefugten Person entschlüsselt werden kann.

Revision #2
Created 2026-03-05 04:16:59 UTC by Christian Weiß
Updated 2026-03-05 04:27:58 UTC by Christian Weiß