Sichere Dateiübertragung

- Was ist Verschlüsselung & Keypairs – Grundlagen verständlich erklärt
- GPG einrichten & Schlüssel erstellen – Windows & Linux
- Dateien verschlüsseln & entschlüsseln
- Public Key teilen & empfangen
- Private Key auf YubiKey sichern

Was ist Verschlüsselung & Keypairs – Grundlagen verständlich erklärt

Wenn du Dateien mit sensiblen Informationen – zum Beispiel personenbezogene Daten von Minderjährigen – sicher übermitteln oder speichern möchtest, reicht es nicht aus, sie einfach per E-Mail zu versenden oder in einem Ordner abzulegen. Verschlüsselung stellt sicher, dass nur die Person, für die eine Datei bestimmt ist, sie auch lesen kann.

Wie funktioniert Verschlüsselung?

Stell dir einen Briefkasten vor: Jeder kann einen Brief einwerfen – aber nur der Besitzer des Briefkastens hat den Schlüssel, um ihn zu öffnen. Genau so funktioniert asymmetrische Verschlüsselung.

Jede Person hat dabei zwei zusammengehörige Schlüssel:

Public Key (öffentlicher Schlüssel): Dieser Schlüssel kann und soll weitergegeben werden. Wer dir eine verschlüsselte Datei schicken möchte, verwendet deinen Public Key dafür. Mit einem fremden Public Key kann man Dateien verschlüsseln – aber nicht entschlüsseln.

Private Key (privater Schlüssel): Dieser Schlüssel bleibt ausschließlich bei dir und wird niemals weitergegeben. Nur mit dem Private Key kannst du Dateien entschlüsseln, die mit deinem Public Key verschlüsselt wurden.

Warum zwei Schlüssel?

Der entscheidende Vorteil: Du musst niemals einen geheimen Schlüssel übermitteln. Jemand, der dir eine verschlüsselte Datei schicken möchte, braucht nur deinen Public Key – den kannst du bedenkenlos öffentlich teilen. Dein Private Key verlässt dabei niemals dein Gerät.

Was ist GPG?

GPG (GNU Privacy Guard) ist ein weit verbreitetes, freies und etabliertes Programm zur Dateiverschlüsselung auf Basis dieses Verfahrens. Es gilt als sicher, ist gut dokumentiert und wird weltweit von Behörden, Organisationen und Sicherheitsexperten eingesetzt.

In diesem Kapitel verwenden wir GPG mit einer Schlüssellänge von **4096 Bit** – einem besonders hohen Sicherheitsstandard, der angesichts der Sensibilität der verarbeiteten Daten ausdrücklich empfohlen wird.

Wann sollte ich verschlüsseln?

- Bei der Übermittlung personenbezogener Daten – insbesondere von Minderjährigen
- Bei sensiblen organisatorischen Informationen
- Immer dann, wenn eine Datei über unsichere Kanäle wie E-Mail übertragen wird
- Bei der Langzeitarchivierung schützenswerter Daten

> **Wichtig:** Verschlüsselung schützt den Inhalt einer Datei – nicht die Tatsache, dass sie existiert. Sie ersetzt außerdem keine sichere Ablage und kein Zugriffskonzept, sondern ergänzt beides.

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.

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

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.

Private Key auf YubiKey sichern

Diese Seite richtet sich an fortgeschrittene Nutzer. Grundkenntnisse im Umgang mit GPG werden vorausgesetzt – stelle sicher, dass du die vorherigen Seiten dieses Kapitels gelesen und umgesetzt hast, bevor du hier weitermachst.

Was ist ein YubiKey?

Ein YubiKey ist ein Hardware-Sicherheitsschlüssel – ein kleines USB-Gerät, auf dem kryptografische Schlüssel sicher gespeichert werden können. Der Private Key verlässt dabei niemals den YubiKey. Selbst wenn dein Computer kompromittiert wird, kann der Schlüssel nicht ausgelesen oder gestohlen werden.

Für die Arbeit mit sensiblen Daten – insbesondere personenbezogenen Daten von Minderjährigen – ist ein YubiKey die sicherste Methode, den Private Key zu schützen. Mitglieder des IT-Teams der THW-Jugend verwenden YubiKeys standardmäßig für diesen Zweck.

Voraussetzungen

- Ein YubiKey (empfohlen: YubiKey 5 Series)
- GPG ist eingerichtet und ein Schlüsselpaar wurde erstellt
- Das Tool **ykman** (YubiKey Manager) ist installiert – erhältlich unter **yubico.com**

> **Wichtiger Hinweis vorab:** Das Verschieben des Private Key auf einen YubiKey ist in der Regel **nicht umkehrbar**. Stelle sicher, dass du vorher ein verschlüsseltes Backup deines Private Key erstellt und sicher aufbewahrt hast – siehe Seite „GPG einrichten & Schlüssel erstellen".

YubiKey vorbereiten

PIN und Admin-PIN setzen

Der YubiKey schützt den gespeicherten Schlüssel über zwei PINs:

PIN: Wird bei jeder Nutzung des Schlüssels abgefragt – zum Beispiel beim Entschlüsseln einer Datei. Standard-PIN: `123456`

Admin-PIN: Wird für Verwaltungsaufgaben benötigt – zum Beispiel beim Aufspielen eines Schlüssels. Standard-Admin-PIN: `12345678`

Ändere beide PINs vor der ersten Nutzung. Nach drei falschen PIN-Eingaben wird der YubiKey gesperrt. Nach drei falschen Admin-PIN-Eingaben wird er vollständig zurückgesetzt.

Windows & Linux (Terminal)

PIN ändern:

```
gpg --card-edit
```

Gib anschließend ein:

```
admin
passwd
```

Wähle Option **1** für die PIN und Option **3** für die Admin-PIN. Folge den Anweisungen auf dem Bildschirm.

Private Key auf den YubiKey verschieben

> **Nochmaliger Hinweis:** Dieser Vorgang verschiebt den Private Key auf den YubiKey. Danach ist er auf dem Computer nicht mehr vorhanden. Stelle sicher,

> dass dein Backup sicher verwahrt ist.

Windows (Kleopatra)

1. Schließe den YubiKey an
2. Öffne **Kleopatra**
3. Klicke mit der rechten Maustaste auf deinen Schlüssel
4. Wähle **„Auf Smartcard übertragen"**
5. Gib das Passwort deines Private Key ein
6. Gib die Admin-PIN des YubiKey ein
7. Bestätige die Übertragung

Linux (Terminal)

```
gpg --edit-key deine@email.de
```

Gib anschließend ein:

```
key 1
keytocard
```

Wähle den Schlüsseltyp (Signatur, Verschlüsselung oder Authentifizierung) und bestätige. Wiederhole den Vorgang für alle Unterschlüssel. Beende anschließend mit:

```
save
```

Nutzung nach der Übertragung

Nach der Übertragung funktioniert GPG wie gewohnt – mit einem Unterschied: Der YubiKey muss beim Entschlüsseln oder Signieren angeschlossen sein. GPG erkennt den YubiKey automatisch und fragt nach der PIN.

Wird der YubiKey nicht gefunden, zeigt GPG eine entsprechende Fehlermeldung. Schließe den YubiKey an und versuche es erneut.

YubiKey verloren oder defekt

Sollte der YubiKey verloren gehen oder defekt sein, kann der Private Key aus dem Backup wiederhergestellt werden:

Linux (Terminal)

```
gpg --import private_key_backup.asc
```

Windows (Kleopatra)

Klicke auf **„Importieren"** und wähle die Backup-Datei aus.

Melde den Verlust eines YubiKey umgehend beim IT-Team unter admins@thw-jugend.de, damit der zugehörige Public Key als kompromittiert markiert werden kann.

> **Sicherheitshinweis:** Ein verlorener YubiKey ohne PIN-Schutz stellt ein Sicherheitsrisiko dar. Wähle daher immer eine starke PIN und gib sie niemals weiter. **Das IT-Team wird dich niemals nach deiner YubiKey-PIN fragen.**