

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.**

Revision #2

Created 2026-03-05 04:17:07 UTC by Christian Weiß

Updated 2026-03-05 04:30:17 UTC by Christian Weiß