# Kommandozeilenverwaltung für SpearID FIDO2 Hardware Security Key

**Version 1.1**

**06/2023**

# Inhaltsübersicht

# 1. Hinzufügen und Ändern der PIN für den FIDO2-Sicherheitsschlüssel unter Linux

*Hinweis: Der Prozess für MacOS unter Verwendung der Befehlszeilenschnittstelle ist ähnlich. Bitte installieren Sie Homebrew, damit Sie das richtige Paket für Ihren Mac installieren können. Die Anweisungen für die Installation von Homebrew finden Sie unter brew.sh*

## 1.1 Installation von fido2-tools auf verschiedenen Distributionen

Mehrere aktuelle Distributionen enthalten fido2-tools. Wenn das Werkzeug nicht installiert ist, kann das Paket, das das Werkzeug enthält, z.B. durch installiert werden:

| | |
|---|---|
| Debian & Ubuntu | `sudo apt install fido2-tools` |
| OpenSUSE | `sudo zypper install libfido2-utils` |
| MacOS | `brew install libfido2` |

## 1.2 Überprüfung der Systemerkennung des FIDO2-Schlüssels

Um zu überprüfen, ob das System den FIDO2-Schlüssel und den Systempfad zum Schlüssel erkennt, geben Sie den Befehl fido2-token -L ein. Die Rückgabe sollte wie folgt aussehen:

```
fido2-token -L
/dev/hidraw0: vendor=0x00ff, product=0xff00 ( FIDO2
Security Key
```

Der Systempfad unter Linux zum FIDO2-Schlüssel lautet normalerweise /dev/hidraw1. Unter MacOS sollte der Pfad wie folgt aussehen `ioreg://0123456789`.

**Die Nummer(n) nach *hidraw* oder *ioreg://* können variieren.**

In den Beispielen dieses Handbuchs lautet der Pfad zum Schlüssel **/dev/hidraw0**.

## 1.3 Erstellen einer PIN für FIDO2-Sicherheitsschlüssel

Wenn für den Schlüssel noch keine PIN festgelegt wurde, z. B. weil Sie den FIDO2-Schlüssel zum ersten Mal verwenden, legen Sie die PIN mit dem Befehl **fido2-token -S** *device* :

```
fido2-token -S /dev/hidraw0
Enter new PIN for /dev/hidraw0:
Enter the same PIN again:
```

Wenn der Schlüssel bereits eine PIN gesetzt hat, wird FIDO_ERR_PIN_AUTH_INVALID zurückgegeben. Erfolgt nach der zweiten PIN-Eingabe keine Rückgabe, ist die Einstellung der PIN erfolgreich abgeschlossen.

## 1.4 Ändern der PIN für FIDO2-Sicherheitsschlüssel

Um die PIN zu ändern, verwenden Sie den Befehl **fido2-token -C** *device* :

```
fido2-token -C /dev/hidraw0
Enter current PIN for /dev/hidraw0:
Enter new PIN for /dev/hidraw0:
Enter the same PIN again:
```

Wenn nach Abschluss der erforderlichen Schritte keine Rückmeldung erfolgt, ist die Änderung der PIN erfolgreich abgeschlossen.

# 2. Zurücksetzen des FIDO2-Sicherheitsschlüssels

*Hinweis! Der Prozess löscht alle Daten und Berechtigungsnachweise auf dem FIDO2-Schlüssel. Verwenden Sie das Tool nur, wenn Sie sicher sind, dass Sie den FIDO2-Schlüssel auf die Werkseinstellungen zurücksetzen möchten.*

## 2.1 Schritte zum Zurücksetzen des FIDO2-Sicherheitsschlüssels

Es ist möglich, den FIDO2-Schlüssel mit dem Befehl **fido2-token -R** *device*. Entfernen Sie zunächst den FIDO2-Schlüssel aus dem USB-Anschluss und stecken Sie ihn wieder ein. Geben Sie den folgenden Befehl innerhalb von zehn Sekunden nach dem Wiedereinstecken des FIDO2-Schlüssels ein.

```
fido2-token -R /dev/hidraw0
```

Die Taste des FIDO2-Schlüssels sollte blinken. Drücken Sie die blinkende Taste. Wenn der Befehl nichts zurückgibt, ist der FIDO2-Schlüssel korrekt zurückgesetzt.

## 2.2 Fehlerbehebung bei häufigen Fehlern während des Rücksetzvorgangs.

Häufiger Fehler `fido_dev_reset: FIDO_ERR_NOT_ALLOWED` wird zurückgegeben, wenn die Rückstellung nicht innerhalb der vorgeschriebenen Zeit erfolgt ist. Ziehen Sie den Schlüssel ab und stecken Sie ihn wieder ein, um es erneut zu versuchen.

Unter MacOS wird die Zahl nach *ioreg*:// wird sich nach dem erneuten Einsetzen des FIDO2-Sicherheitsschlüssels ändern. Es wird empfohlen, den folgenden kombinierten Befehl zu verwenden, um den Systempfad für den Schlüssel automatisch zu erfassen:

```
fido2-token -R $(fido2-token -L | grep -o 'ioreg://[0-9]\{1,10\}')
```

Es ist auch möglich, diesen kombinierten Befehl für andere Funktionen zu verwenden, indem man die Option **-R** in etwas anderes ändert.
Diese kombinierten Befehle können auch unter Linux verwendet werden. Der Systempfad im untenstehenden Beispiel wird auf einen für Linux-Systeme korrigiert:

```
fido2-token -I $(fido2-token -L | grep -o '/dev/hidraw[0-9]')
```

# 3. Show detailed information of the FIDO2 Security Key

Befehl **fido2-token -I** *device* zeigt die Informationen des FIDO2-Sicherheitsschlüssels an:

```
FIDO2@SpearID:~> fido2-token -L
/dev/hidraw0: vendor=0x1ea8, product=0xfc25 (FIDO2 Security Key)
FIDO2@SpearID:~> fido2-token -I /dev/hidraw0
proto: 0x02
major: 0x02
minor: 0x01
build: 0x00
caps: 0x05 (wink, cbor, msg)
version strings: U2F_V2, FIDO_2_0, FIDO_2_1_PRE
extension strings: credProtect, hmac-secret
transport strings: usb, nfc, ble
algorithms: es256 (public-key)
aaguid: bbf4b6a7679df6fcc4f28ac0ddf9015a
options: rk, up, noplat, noclientPin, credentialMgmtPreview
fwversion: 0x0
maxmsgsiz: 2048
maxcredcntlst: 8
maxcredlen: 96
maxlargeblob: 0
pin protocols: 1
pin retries: undefined
pin change required: false
uv retries: undefined
```

Im obigen Beispiel wird der Befehl **fido2-token -L** wird verwendet, um den Systempfad zu und eine kurze Zusammenfassung des FIDO2-Sicherheitsschlüssels anzuzeigen. Die detaillierten Informationen werden mit dem Befehl **fido2-token -I** *device*.
Die Rückgabe zeigt die Informationen für SpearID FIDO2 Pro USB-A.

## 4.1 Überprüfen der gespeicherten Anmeldeinformationen im FIDO2-Sicherheitsschlüssel

### fido2-token -L -r

Um die im FIDO2-Sicherheitsschlüssel gespeicherten Anmeldeinformationen zu überprüfen, verwenden Sie zunächst den Befehl **fido2-token -L -r** *device* .

Wenn der FIDO2-Sicherheitsschlüssel gespeicherte Anmeldeinformationen enthält, sollte die Rückgabe beispielsweise so aussehen:

```
fido2-token -L -r /dev/hidraw0
Enter PIN for /dev/hidraw0:
00: QomM+rcC3l/jteVhHvGWphK/sJxPNghDAHTw8Z273Eg=
login.microsoft.com
01: oI4oLhMQpFmx8us54YL+EiTSUibtPEGQnyxifkhJNFA= apple.com
```

### fido2-token -L -k

Hier können wir sehen, dass der FIDO2-Sicherheitsschlüssel Anmeldeinformationen von zwei verschiedenen vertrauenden Parteien gespeichert hat. Wenn einige der vertrauenden Parteien mehrere Berechtigungsnachweise im Schlüssel gespeichert haben, wird dies hier nicht angezeigt. Daher können wir den Befehl **fido2-token -L -k** verwenden *relying_party device* um die gespeicherten Anmeldeinformationen für eine bestimmte vertrauenswürdige Partei, z. B. Microsoft, zu prüfen:

```
fido2-token -L -k login.microsoft.com /dev/hidraw0
Enter PIN for /dev/hidraw0:
00: kgG5VJ7L4LAeGnPbuHtRHVrxW1WNV0SOYSK5Rihmjbw=
example@outlook.com
WzixCJ81GDeJuYdDHiuX3ERESG352y9wqak1JBs8B7g= es256 uvopt
01: a59iQ1x8Z0G/Zp0BTFEcIKFGUm7zGkNerhTCpzW6Bps= John Doe
dQ4+aB47QU03THfrl1zzc1UKOUqY2HNzr10lboY1H+A= es256 uvopt
```

## 4.2 Löschen einzelner Berechtigungsnachweise mit dem Befehl

### fido2-token -D -i

Im obigen Beispiel haben wir Anmeldeinformationen für zwei verschiedene Microsoft-Konten im FIDO2-Sicherheitsschlüssel gespeichert. Wenn wir z. B. die Anmeldeinformationen für example@outlook.com löschen möchten, müssen wir im nächsten Schritt die Zeichenkette zwischen der 00: und dem Benutzernamen (example@outlook.com) verwenden. Die Zeichenkette ist in diesem Beispiel blau markiert.
Das Löschen eines einzelnen Berechtigungsnachweises ist mit dem **Befehl fido2-token -D -i** möglich. *character_string device* . Mit der Zeichenkette aus der Rückgabe des Befehls **-L -k** funktioniert das Entfernen des Credentials wie folgt:

```
fido2-token -D -i kgG5VJ7L4LAeGnPbuHtRHVrxW1WNV0SOYSK5Rihmjbw=
/dev/hidraw0
Enter PIN for /dev/hidraw0:
```

Wenn der Befehl nichts zurückgibt, wurde der Berechtigungsnachweis erfolgreich gelöscht.
Wenn der Befehl FIDO_ERR_MISSING_PARAMETER zurückgibt, ist die Zeichenkette ungültig. Bitte prüfen Sie, ob die Zeichenkette mit der vom vorherigen Befehl zurückgegebenen identisch ist.

### fido2-token -I -c

Die FIDO2-Sicherheitsschlüssel haben einen begrenzten Speicherplatz für gespeicherte Berechtigungsnachweise (rk(s), residente(r) Schlüssel). Um zu überprüfen, wie viele Berechtigungsnachweise gespeichert sind und wie viele Slots für neue Berechtigungsnachweise noch zur Verfügung stehen, verwenden Sie den Befehl **fido2-token -I -c** device . Die Rückgabe sollte wie im folgenden Beispiel aussehen:

```
fido2-token -I -c /dev/hidraw0
Enter PIN for /dev/hidraw0:
existing rk(s): 7
remaining rk(s): 43
```

# 5. Using fido2-token in Windows systems

1. Laden Sie die neueste Softwareversion von der unten verlinkten Website herunter.
    a. https://developers.yubico.com/libfido2/Releases/
    b. Die richtige Version für Windows-Systeme ist diejenige, die mit win.zip endet
2. Entpacken Sie den heruntergeladenen Ordner an einen Ort Ihrer Wahl
3. Öffnen Sie die Eingabeaufforderung als Administrator (oder PowerShell oder ein Terminal Ihrer Wahl)
    a. Das Tool erkennt keine externen Security Keys, wenn es als Standardbenutzer ausgeführt wird.
4. Wechseln Sie in das Verzeichnis des extrahierten Ordners und zum richtigen Speicherort für die Anwendung fido2-token.exe. (z. B. cd C:\Downloads\libfido2-1.13.0-win\Win64\Release\v143\dynamic)

5. Mit dem Befehl **fido2-token -L** werden die im System gefundenen Security Keys aufgelistet.
    a. Wenn Sie PowerShell verwenden, denken Sie daran, ./ vor den fido2-token-Befehlen zu verwenden (./fido2-token)
    b. Der Systemstandort des FIDO2-Sicherheitsschlüssels in Windows kann eine lange Zeichenkette sein, z. B.

```
fido2-token -L
\\?\hid#vid_^F2AwWs1_ZLg9Wu!_QndEdREE7VKhg*ZG27RW#{4d1e55b2-f16f-11cf-88cb-001111000030}: vendor=0x1ea8, product=0xfc25 (FIDO2 Security Key)
```

6. Use the tools mentioned in other steps in this manual, remember to put quotation marks before and after the character string for the shell to recognize the path correctly, f. e.

```
fido2-token -I "\\?\hid#vid_^F2AwWs1_ZLg9Wu!_QndEdREE7VKhg*ZG27RW#{4d1e55b2-f16f-11cf-88cb-001111000030}"
```

## Kontaktieren Sie uns

Wir schätzen Ihr Feedback und sind für Sie da. Wenn Sie Fragen, Kommentare oder Vorschläge zu diesem Dokument oder zu unseren Dienstleistungen haben, können Sie uns gerne kontaktieren:


E-Mail: info@spear.fi

Telefon: +358  40 5544 380

Website: https://spear.fi/

Postanschrift: Eteläpuisto 17 D, 28100 Pori.