SpearID FIDO2 Suojausavaimen hallinta – Komentorivi

Versio V1.1

06/2023

Table of contents

Note: The process for MacOS using the command line interface is similar. Please install Homebrew to be able to install the correct package for your Mac. The instructions for installing Homebrew can be found from brew.sh

1.1 Installation of fido2-tools on different distributions

Monet ajan tasalla olevat Linux-jakelut sisältävät oikeat työkalut (fido2-tools) FIDO2-suojausavaimen hallintaan, mutta paketit voidaan ladata seuraavilla komennoilla:

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

1.2 Tarkistetaan järjestelmän tunnistus FIDO2-avaimelle

Aseta suojausavain USB-porttiin ja tarkista tunnistaako järjestelmä suojausavainta komennolla fido2-token -L.

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

Tuloksen alussa näkyy suojausavaimen sijainti järjestelmässä. Linuxissa sijainti on yleensä `/dev/hidraw1`. MacOS:ssa sijainti todennäköisesti on `ioreg://0123456789`.
Numero(t) *hidraw*:n ja *ioreg://*:n jälkeen voivat vaihdella.

Ohjeen esimerkeissä avaimen järjestelmäsijaintina on /dev/hidraw0.

1.3 PIN-koodin luominen FIDO2-suojausavaimelle

Jos avaimeen ei ole vielä asetettu PIN-koodia, esimerkiksi avaimen ollessa käyttämätön, aseta PIN-koodi komennolla fido2-token -S *laite*:

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

Jos suojausavaimeen on jo asetettu PIN-koodi, komento palauttaa tulokseksi `FIDO_ERR_PIN_AUTH_INVALID`. Mikäli komento ei palauta tekstiä PIN-koodin asettamisen jälkeen, PIN-koodi on asetettu onnistuneesti.

1.4 FIDO2-suojausavaimen PIN-koodin vaihtaminen

Suojausavaimen PIN-koodin vaihtamiseksi käytä komentoa fido2-token -C:

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

Mikäli komento ei palauta tekstiä PIN-koodin vaihtamisen jälkeen, PIN-koodi on asetettu onnistuneesti.

2. FIDO2-suojausavaimen nollaus

Huom! Prosessi poistaa kaiken datan tunnuksineen FIDO2-suojausavaimesta. Käytä työkalua vain, jos olet varma, että haluat palauttaa suojausavaimen tehdasasetuksiin.

2.1 Steps of resetting the FIDO2 Security Key

FIDO2-suojausavaimen nollaaminen suoritetaan komennolla fido2-token -R *laite*.

Irrota ensin suojausavain USB-liittimestä ja aseta se takaisin. Kymmenen sekunnin kuluessa takaisinasettamisesta syötä seuraava komento:

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

Komennon suorittamisen jälkeen suojausavaimen painikkeen valo alkaa vilkuttaa. Paina tässä vaiheessa suojausavaimen painiketta varmistaaksesti suojausavaimen nollauksen.
Mikäli komento ei palauta tekstiä painikkeen painamisen jälkeen, suojausavain on nollattu onnistuneesti.

2.2 Troubleshooting common errors during the reset process.

Jos prosessi ei ehtinyt alkaa kymmenen sekunnin sisällä, komento palauttaa tekstin `fido_dev_reset: FIDO_ERR_NOT_ALLOWED`. Irrota suojausavain ja aseta se uudestaan prosessin uudelleen aloittamiseksi.

MacOS:ssa *ioreg://*:n jälkeinen numerosarja vaihtuu joka kerta FIDO2-suojausavaimen asettamisen jälkeen. Tämän vuoksi suositellaan käyttämään seuraavaa yhdistelmäkomentoa sijainnin syöttämiseksi komentoon automaattisesti.

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

Asetusta -R vaihtamalla yhdistelmäkomentoa voidaan hyödyntää muissakin toiminnoissa.

Yhdistelmäkomentoa voidaan käyttää myös Linuxissa. Alla esimerkki Linuxille sovelletusta komennosta:

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

3. Tietojen näyttäminen FIDO2-suojausavaimesta

Komennolla fido2-token -I *laite* saadaan näkyville tietoja FIDO2-suojausavaimesta:

```
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
```

Esimerkissä tarkastetaan fido2-token -L -komennolla FIDO2-suojausavaimen järjestelmäsijainti ja nähdään suppeasti tietoa avaimesta. fido2-token -I *laite* -komennolla saadaan kattava lista tietoa suojausavaimesta. Esimerkissä on tiedot SpearID FIDO2 Pro USB-A -suojausavaimesta.

4. Yksittäisten tunnusten poistaminen FIDO2-suojausavaimesta

4.1 Checking stored credentials in the FIDO2 Security Key

fido2-token -L -r

Komennolla fido2-token -L -r *laite* voidaan tarkastella avaimeen tallennettuja tunnuksia.

Mikäli avaimeen on tallentunut tunnuksia, palautus voi näyttää esimerkiksi tältä:

```
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

Esimerkissä näkyy, että FIDO2-suojausavaimeen on tallentunut kahden eri tahon tunnukset. Jos suojausavaimessa on useita yhteen tahoon liitettyjä tunnuksia, niitä ei näy tässä. Jos suojausavaimessa on esimerkiksi useita Microsoftin tunnuksia, komennolla fido2-token -L -k *taho laite* voidaan tarkastella niitä yksitellen:

```
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 Deleting individual credentials using the command

fido2-token -D -i

Yllä olevassa esimerkissä on kahden eri FIDO2-suojausavaimeen tallentuneen Microsoft-tilin tunnukset. Jos halutaan poistaa joku yksittäisistä tunnuksista, käytetään komentoa fido2-token -D -i *merkkijono laite* . Komennon suorittamiseen tarvittava merkkijono on esimerkeissäkin näkyvän 00:, 01: jne. alkuisten rivien ja käyttäjätunnuksien välinen merkkijono. Sinisellä merkityissä esimerkeissä valitaan yllä oleva tunnus (example@outlook.com) poistettavaksi.

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

Mikäli komento ei palauta tekstiä suorituksen jälkeen, tunnus on poistettu onnistuneesti.
Jos komento palauttaa tekstin FIDO_ERR_MISSING_PARAMETER, merkkijono ei ole pätevä. Tarkista, että merkkijono on sama, kuin edellisen komennon palautuksessa.

fido2-token -I -c

FIDO2-suojausavaimessa on rajallinen kapasiteetti tunnuksien *(rk(s), resident keys(s))* tallentamiseen. Tallennustilan tarkastamiseksi voidaan käyttää komentoa fido2-token -I -c *laite* . Komento palauttaa tiedon, kuinka monta tunnusta on tallennettu, ja kuinka monta paikkaa uusille tunnuksille on vielä jäljellä. Alla esimerkki:

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

5. Fido2-token-työkalun käyttö Windows-järjestelmissä

1. Lataa viimeisin julkaisu alla olevalta sivulta.
    a. https://developers.yubico.com/libfido2/Releases/
    b. Windowsissa käytettävän tiedoston nimen pääte on win.zip
2. Purkaa ladattu tiedosto haluamaasi tiedostosijaintiin.
3. Avaa komentokehote järjestelmänvalvojana (tai PowerShell tai vapaavalintainen terminaali)
4. Vaihda hakemistoa sijaintiin, johon ladattu kansio on purettu, ja polku oikeaan hakemistoon, josta fido2-token.exe-sovellus löytyy. (esim. cd *C:|Downloads*\libfido2-1.13.0-win\Win64\Release\v143\dynamic)
5. Tarkista komennolla fido2-token -L näkyykö järjestelmässä FIDO2-suojausavainta
    a. PowerShelliä käyttäessä lisää merkit ./ ennen fido2-token -komentoa, jotta suoritus onnistuu (./fido2-token)
    b. FIDO2-suojausavaimen järjestelmäsijainti on Windowsissa pitkä merkkijono, esimerkkinä:

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

6. Voit käyttää ohjeessa mainittuja työkaluja FIDO2-suojausavaimen hallintaan myös Windowsilla. Lisää suojausavaimen järjestelmäsijainnin merkkijonon ympärille lainausmerkit (”), jotta komento toteutuu oikein, esim:
7.

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

Ota yhteyttä

Arvostamme palautettasi ja olemme täällä auttamassa sinua. Mikäli sinulla on kysyttävää, kommentteja tai ehdotuksia liittyen tähän asiakirjaan tai palveluihimme, ole hyvä ja ota meihin yhteyttä seuraavasti:

Sähköposti: info@spear.fi

Puhelin: +358 40 5544 380

Verkkosivusto: https://spear.fi/

Postiosoite: Eteläpuisto 17 D, 28100 Pori.

Pyrimme vastaamaan kaikkiin tiedusteluihin.
Kiitämme sinua kiinnostuksestasi ja tuestasi!