Command line management for SpearID FIDO2 Hardware Security Key

Version 1.1

06/2023

Table of contents

1. Adding and changing the PIN for the FIDO2 Security Key in Linux

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

Several up-to-date distributions include fido2-tools. If the tool is not installed, the package containing the tool can be installed by for example:

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

1.2 Checking system recognition of the FIDO2 key

To check if the system recognizes the FIDO2 key and the system path to the key enter command fido2-token -L. The return should look like:

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

The system path in Linux to the FIDO2 key is usually /dev/hidraw1. In MacOS the path should look like `ioreg://0123456789`.
The number(s) following ***hidraw*** or ***ioreg://*** can vary.

In examples of this manual the path to the key is /dev/hidraw0.

1.3 Creating a PIN for FIDO2 Security Key

If the key does not have a PIN set, for example it is the first time using the FIDO2 key, set the PIN using command fido2-token -S *device* :

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

If the key already has a PIN set, FIDO_ERR_PIN_AUTH_INVALID is returned. If there is no return after entering the PIN second time, the setting of the PIN is completed successfully.

1.4 Changing the PIN for FIDO2 Security Key

For changing the PIN, use command 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:
```

If there is no return after completing the required steps, the changing of the PIN is completed successfully.

2. Resetting the FIDO2 Security Key

Note! Process removes all data and credentials on the FIDO2 key. Only use the tool if you are sure you want to reset the FIDO2 key to factory settings.

2.1 Steps of resetting the FIDO2 Security Key

It is possible to reset your FIDO2 key using the command fido2-token -R *device*.

First remove the FIDO2 key from the USB port and reinsert it. Enter the following command in ten seconds after reinserting the FIDO2 key.

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

The button of the FIDO2 key should flash. Press the flashing button. If the command returns nothing, the FIDO2 key is reset correctly.

2.2 Troubleshooting common errors during the reset process.

Common error `fido_dev_reset: FIDO_ERR_NOT_ALLOWED` is returned if the reset did not meet the time requirement. Remove and reinsert the key to try again.

In MacOS the number after *ioreg://* will change after reinserting the FIDO2 Security Key. It is recommended to use the following combined command to automatically acquire the system path for the key:

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

It is also possible to use this combined command for other functions modifying the -R option to something else.

These combined commands can also be used in Linux. The system path in the example below is corrected to one for Linux systems:

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

3. Show detailed information of the FIDO2 Security Key

Command fido2-token -I *device* shows the information of the FIDO2 Security Key:

```
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
```

In the example above, the command fido2-token -L is used to show the system path to, and a brief summary of the FIDO2 Security Key. The detailed information is shown by command fido2-token -I *device*. The return shows the information for SpearID FIDO2 Pro USB-A.

4. Remove individual credentials from FIDO2 Security Key

4.1 Checking stored credentials in the FIDO2 Security Key

fido2-token -L -r

To check the credentials that are stored into the FIDO2 Security Key, first use command fido2-token -L -r *device* .

If the FIDO2 Security Key has any stored credentials, the return should look like for example:

```
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

Here we can see the FIDO2 Security Key has credentials stored by two different relying parties. If some of the relying parties have several credentials stored into the key, it is not seen here. Therefore, we can use the command fido2-token -L -k *relying_party device* to examine the stored credentials for a certain relying party, for example Microsoft:

```
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

In the example above, we have credentials for two different Microsoft accounts stored in the FIDO2 Security Key. If we would like to delete for example the credentials for *example@outlook.com*, we need to use the character string between the 00: and the username (example@outlook.com) for the next step. The character string is marked in blue for this example.
Deleting an individual credential is possible by command fido2-token -D -i. *character_string device* . Using the character string from the return of the command -L -k , the removal of the credential works as follows:

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

If the command returns nothing, the credential is deleted successfully.
If the command returns FIDO_ERR_MISSING_PARAMETER, the character string is invalid. Please check if the character string is identical to that returned from the previous command.

fido2-token -I -c

The FIDO2 Security Keys have limited storage for stored credentials *(rk(s), resident key(s))*. To check how many credentials are stored and how many slots for new credentials are remaining, use command fido2-token -I -c *device* . The return should look like example below:

```
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. Download the latest software release from the site linked below.
    a. https://developers.yubico.com/libfido2/Releases/
    b. The correct release for Windows systems is the one ending with win.zip file name
2. Extract the downloaded folder to a destination of your choice
3. Open Command Prompt as and Administrator (or PowerShell or terminal of your choice)
    a. The tool won't recognize external Security Keys if run as a standard user
4. Change Directory into the extracted folder and to the correct location for the fido2-token.exe application. (f.e. cd *C:*|*Downloads*\libfido2-1.13.0-win\Win64\Release\v143\dynamic)

5. Using the command fido2-token -L lists the Security Keys found in the system.
    a. If using PowerShell, remember to use ./ before the fido2-token commands (./fido2-token)
    b. The system location of the FIDO2 Security Key in windows can be a lengthy character string, f. e.

```
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}"
```

SPEAR
innovations oy ltd

Contact Us

We value your feedback and are here to assist you.
If you have any questions, comments, or suggestions related to this document or our services, please feel free to contact us through:

Email: info@spear.fi

Phone: +358 40 5544 380

Website: https://spear.fi/

Mailing Address: Eteläpuisto 17 D, 28100 Pori.

We strive to respond to all inquiries.

Thank you for your interest and support!