



Gestion en ligne de commande pour la clé de sécurité matérielle SpearID FIDO2.



Version 1.1

06/2023

Table des matières

1	Ajout et modification du code PIN pour la clé de sécurité FIDO2 sous Linux	3
1.1	Installation de fido2-tools sur différentes distributions	3
1.2	Vérification de la reconnaissance du système pour la clé FIDO2	3
1.3	Création d'un code PIN pour la clé de sécurité FIDO2	4
1.4	Modification du code PIN pour la clé de sécurité FIDO2	4
2	Réinitialisation de la clé de sécurité FIDO2	5
2.1	Processus de réinitialisation de la clé FIDO2	5
2.2	Résolution des erreurs courantes lors du processus de réinitialisation	5
3	Affichage des informations détaillées de la clé de sécurité FIDO2	6
4	Suppression des informations d'identification individuelles de la clé de sécurité FIDO2	7
4.1	Vérification des informations d'identification stockées dans la clé FIDO2	7
4.2	Suppression des informations d'identification individuelles à l'aide de la commande	8
5	Utilisation de fido2-token sur les systèmes Windows	9
5.1	Téléchargement de la version du logiciel pour Windows	9
5.2	Extraction du dossier téléchargé	9
5.3	Ouverture de l'invite de commandes en tant qu'administrateur	9
5.4	Changement du répertoire vers l'emplacement de fido2-token.exe	9
5.5	Utilisation des commandes fido2-token sur les systèmes Windows	9
6	Contacteur	10

1. Ajout et modification du code PIN pour la clé de sécurité FIDO2 sous Linux

Remarque : Le processus pour MacOS en utilisant l'interface en ligne de commande est similaire. Veuillez installer Homebrew pour pouvoir installer le package correct pour votre Mac. Les instructions d'installation de Homebrew se trouvent sur brew.sh.

1.1 Installation de fido2-tools sur différentes distributions

Plusieurs distributions à jour incluent fido2-tools. Si l'outil n'est pas installé, le package contenant l'outil peut être installé de la manière suivante:

Debian & Ubuntu	<code>sudo apt install fido2-tools</code>
OpenSUSE	<code>sudo zypper install libfido2-utils</code>
MacOS	<code>brew install libfido2</code>

1.2 Vérification de la reconnaissance du système pour la clé FIDO2

Pour vérifier si le système reconnaît la clé FIDO2 et le chemin système vers la clé, saisissez la commande `fido2-token -L`. Le résultat devrait ressembler à ceci :

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

Le chemin système vers la clé FIDO2 sous Linux est généralement `/dev/hidraw1`. Sous MacOS, le chemin devrait ressembler à : `ioreg://0123456789`. Le(s) numéro(s) suivant `hidraw` ou `ioreg://` peuvent varier.

Dans les exemples de ce manuel, le chemin vers la clé est `/dev/hidraw0`.

1.3 Création d'un code PIN pour la clé de sécurité FIDO2

Si la clé n'a pas de code PIN défini, par exemple si c'est la première utilisation de la clé FIDO2, définissez le code PIN en utilisant la commande `fido2-token -S device` :

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

Si la clé a déjà un code PIN défini, `FIDO_ERR_PIN_AUTH_INVALID` est renvoyé. S'il n'y a pas de retour après avoir saisi le code PIN une deuxième fois, la configuration du code PIN est effectuée avec succès.

1.4 Modification du code PIN pour la clé de sécurité FIDO2

Pour modifier le code PIN, utilisez la commande `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:
```

S'il n'y a pas de retour après avoir terminé les étapes requises, la modification du code PIN est effectuée avec succès.

2. Réinitialisation de la clé de sécurité FIDO2

Remarque ! Ce processus supprime toutes les données et informations d'identification de la clé FIDO2. Utilisez l'outil uniquement si vous êtes sûr de vouloir réinitialiser la clé FIDO2 aux paramètres d'usine.

2.1 Étapes de réinitialisation de la clé de sécurité FIDO2

Il est possible de réinitialiser votre clé FIDO2 en utilisant la commande `fido2-token -R device`.

Retirez d'abord la clé FIDO2 du port USB et réinsérez-la. Saisissez la commande suivante dans les dix secondes suivant la réinsertion de

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

Le bouton de la clé FIDO2 devrait clignoter. Appuyez sur le bouton clignotant. Si la commande ne renvoie rien, la clé FIDO2 a été réinitialisée correctement.

2.2 Résolution des erreurs courantes lors du processus de réinitialisation.

L'erreur courante `fido_dev_reset: FIDO_ERR_NOT_ALLOWED` est renvoyée si la réinitialisation ne respecte pas les exigences de temps. Retirez et réinsérez la clé pour réessayer.

Sous MacOS, le nombre après `ioreg://` changera après la réinsertion de la clé de sécurité FIDO2. Il est recommandé d'utiliser la commande combinée suivante pour obtenir automatiquement le chemin système de la clé :

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

Il est également possible d'utiliser cette commande combinée pour d'autres fonctions en modifiant l'option `-R` en autre chose.

Ces commandes combinées peuvent également être utilisées sous Linux. Le chemin système dans l'exemple ci-dessous est corrigé pour les systèmes Linux :

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

3. Show detailed information of the FIDO2 Security Key

La commande `fido2-token -l device` affiche les informations de la clé de sécurité FIDO2 :

```
FIDO2@SpearID:~> fido2-token -L
/dev/hidraw0: vendor=0x1lea8, 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
```

Dans l'exemple ci-dessus, la commande `fido2-token -L` est utilisée pour afficher le chemin système et un bref résumé de la clé de sécurité FIDO2. Les informations détaillées sont affichées par la commande `fido2-token -l device`.

Le retour affiche les informations pour la clé FIDO2 Pro USB-A de SpearID.

4. Supprimer des identifiants individuels de la clé de sécurité FIDO2

4.1 Vérification des identifiants stockés dans la clé de sécurité FIDO2

fido2-token -L -r

Utilisez la commande suivante pour vérifier les identifiants stockés dans la clé de sécurité FIDO2: `fido2-token -L -r device` .

Si la clé de sécurité FIDO2 contient des identifiants stockés, le retour ressemblera par exemple à ceci :

```
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

Ici, nous pouvons voir que la clé de sécurité FIDO2 contient des identifiants stockés pour deux parties tierces différentes. Si certaines parties tierces ont plusieurs identifiants stockés dans la clé, cela ne sera pas visible ici. Par conséquent, nous pouvons utiliser la commande `fido2-token -L -k relying_party device` pour examiner les identifiants stockés pour une certaine partie tierce, par exemple 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 Suppression d'identifiants individuels à l'aide de la commande

fido2-token -D -i

Dans l'exemple ci-dessus, nous avons des identifiants pour deux comptes Microsoft différents stockés dans la clé de sécurité FIDO2. Si nous voulons supprimer par exemple les identifiants pour *example@outlook.com*, nous devons utiliser la chaîne de caractères entre "00:" et le nom d'utilisateur (*example@outlook.com*) pour l'étape suivante. La chaîne de caractères est marquée en bleu pour cet exemple. La suppression d'un identifiant individuel est possible avec la commande suivante: *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:
```

Si la commande ne renvoie rien, l'identifiant est supprimé avec succès. Si la commande renvoie FIDO_ERR_MISSING_PARAMETER, la chaîne de caractères est invalide. Veuillez vérifier si la chaîne de caractères est identique à celle

fido2-token -I -c

Les clés de sécurité FIDO2 ont une capacité de stockage limitée pour les identifiants enregistrés *credentials (rk(s), resident key(s))*. Pour vérifier combien d'identifiants sont stockés et combien d'emplacements restent disponibles pour de nouveaux identifiants, utilisez la commande *fido2-token -I -c* La sortie devrait ressembler à l'exemple ci-dessous .:

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

5. Utilisation de fido2-token sur les systèmes Windows

1. Téléchargez la dernière version du logiciel à partir du site lié ci-dessous :
 - a. <https://developers.yubico.com/libfido2/Releases/>
2. La version appropriée pour les systèmes Windows est celle se terminant par le nom de fichier win.zip.
3. Extrayez le dossier téléchargé vers une destination de votre choix.
4. Ouvrez l'invite de commandes en tant qu'administrateur (ou PowerShell ou terminal de votre choix).

L'outil ne reconnaîtra pas les clés de sécurité externes s'il est exécuté en tant qu'utilisateur standard.

Accédez au répertoire extrait et à l'emplacement correct de l'application fido2-token.exe (par exemple, 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. Si vous utilisez PowerShell, n'oubliez pas d'utiliser ./ avant les commandes fido2-token (./fido2-token).
 - b. L'emplacement système de la clé de sécurité FIDO2 sur Windows peut être une longue chaîne de caractères, par exemple

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

6. Utilisez les outils mentionnés dans les autres étapes de ce manuel, n'oubliez pas de mettre des guillemets avant et après la chaîne de caractères pour que l'interpréteur de commandes reconnaisse correctement le chemin, par exemple:

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



SPEAR
innovations oy ltd

Nous sommes à votre écoute

Nous accordons une grande importance à vos retours et nous sommes là pour vous aider. Si vous avez des questions, des commentaires ou des suggestions concernant ce document ou nos services, n'hésitez pas à nous contacter. Nous nous engageons à répondre à toutes les demandes dans les meilleurs délais.

Email: info@spear.fi

Téléphone: +358 40 5544 380

Site web: <https://spear.fi/>

Adresse postale: Eteläpuisto 17 D, 28100 Pori.

Nous vous remercions de votre intérêt et de votre soutien!