

# SpearID

## Manuel d'utilisation de la clé de sécurité SpearID FID02



Version 1.3

05/2025

AUCUNE GARANTIE DE QUELQUE NATURE QUE CE SOIT N'EST ACCORDÉE PAR CE DOCUMENT.

Tout produit et matériel connexe divulgué dans le présent document n'est fourni que conformément et sous réserve des conditions d'une licence de produit ou d'un accord d'achat ou de location d'équipement dûment exécuté. Les seules garanties accordées par Spear Innovations Oy, le cas échéant, concernant les produits décrits dans ce document sont énoncées dans cette licence ou cet accord. Spear Innovations Oy ne peut accepter aucune responsabilité financière ou autre qui pourrait résulter de votre utilisation des informations ou du matériel logiciel, y compris des dommages directs, indirects, spéciaux ou consécutifs.

Vous devez veiller à ce que l'utilisation de ces informations et/ou du matériel logiciel soit conforme aux lois, règles et réglementations des juridictions dans lesquelles il est utilisé. Tous droits réservés.

Copyright © 2025 Spear Innovations Oy.

## Table des matières

1	Vue d'ensemble	4
2	Présentation du produit	4
3	Fonctionnement de base	6
4	Authentification multifactorielle	7
5	Gestionnaire FIDO et OTP	9
6	Questions fréquentes	9
7	Caractéristiques techniques	10

## 1. Vue d'ensemble

La clé de sécurité SpearID FIDO2 NFC est un dispositif d'authentification matériel compatible avec les normes FIDO2 et FIDO U2F, offrant des interfaces de communication NFC et USB. Elle permet de sécuriser vos comptes grâce à l'authentification à deux facteurs, l'authentification multifactorielle ou l'authentification sans mot de passe sur les services et applications compatibles FIDO2 ou U2F. Ses multiples interfaces facilitent l'authentification sur différents appareils, qu'il s'agisse d'ordinateurs ou d'appareils mobiles.

## 2. Présentation du produit



SpearID FIDO2 Pro (USB-C & NFC)

Le bouton de la SpearID FIDO2 Pro (USB-C & NFC) présente deux états lumineux différents lors de l'utilisation de la connexion USB :

État lumineux	Description
Lumière blanche fixe	La clé de sécurité est branchée à un appareil
Lumière blanche clignotante	La clé de sécurité reçoit une demande d'authentification



SpearID FID02 Pro (USB-A, NFC & BLE)

Le bouton de la SpearID FID02 Pro (USB-A, NFC & BLE) présente les états lumineux suivants :

État lumineux	Description
Lumière blanche fixe	La clé de sécurité est connectée à un appareil
Lumière blanche clignotante	La clé de sécurité reçoit une demande d'authentification
Lumière bleue fixe	La clé n'est pas encore appairée avec l'appareil - maintenez le bouton enfoncé pendant 5 secondes pour activer le mode d'appairage Bluetooth. Une fois l'appairage réussi, l'indicateur passera à une lumière bleue clignotante
Lumière bleue clignotante	Appuyez sur le bouton pour activer le mode d'authentification Bluetooth
Lumière rouge clignotante	Batterie faible - rechargez l'appareil via USB

## 3. Fonctionnement de base

### 3.1 Enregistrement

1. Connectez-vous à un service compatible avec le protocole FIDO2 ou FIDO U2F
2. Branchez la clé de sécurité à votre appareil
3. Enregistrez la clé de sécurité sur votre compte
4. Une fois la clé enregistrée, le service web vous la demandera lors de vos connexions futures. Selon le service, le code PIN de la clé pourra être exigé.

#### ① REMARQUE:

Si vous branchez la clé via USB-C à votre téléphone, la fonction NFC sera désactivée et l'authentification se fera uniquement via USB-C. Le code PIN peut contenir des chiffres, des lettres minuscules et majuscules ainsi que des caractères spéciaux.

### 3.2 NFC

2. Assurez-vous que la fonction NFC de votre appareil mobile est activée
3. Approchez la clé de sécurité de l'antenne NFC de l'appareil après réception d'une demande d'autorisation
4. Selon le processus de connexion, votre appareil mobile pourra vous demander de saisir le code PIN de la clé

#### ① NOTE:

Le connecteur USB doit être exposé, car le couvercle métallique bloque le signal NFC.

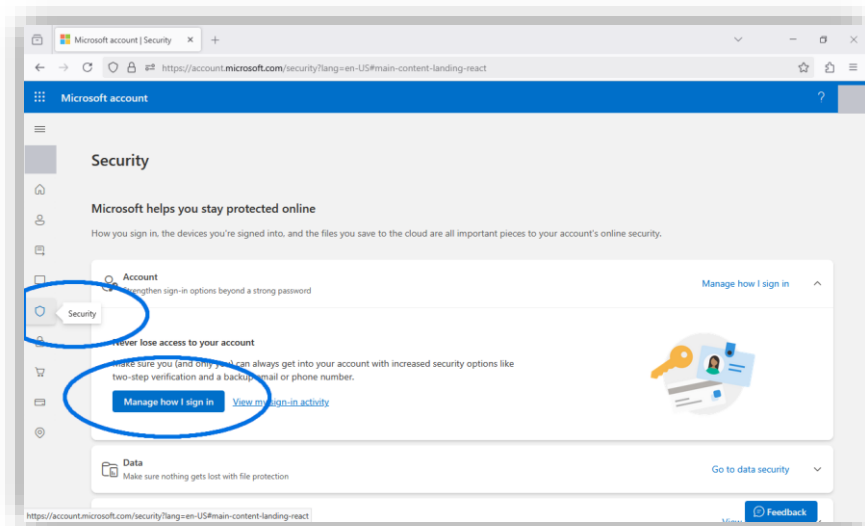
## 4. Une clé de sécurité FIDO2 pour l'authentification multifactorielle

### 4.1 Enregistrement

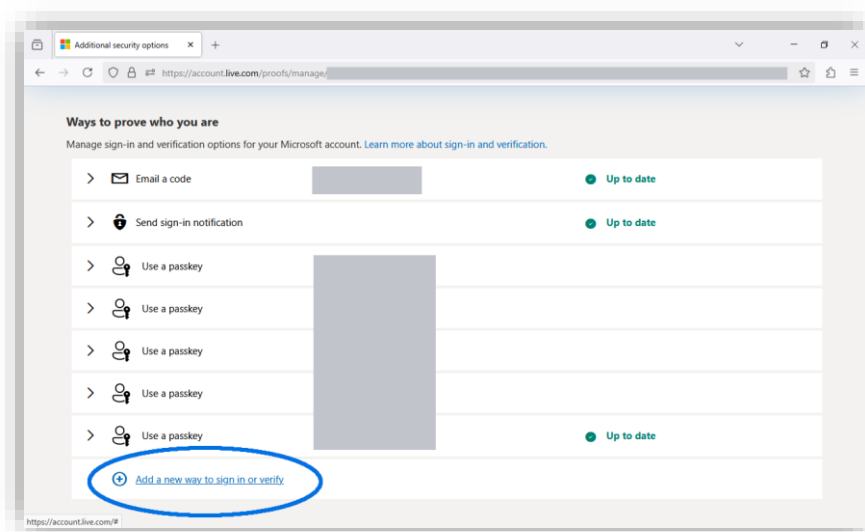
Associez votre clé de sécurité FIDO2 à votre compte Google pour en faire votre second facteur d'authentification.

Dans l'exemple suivant, nous enregistrons la clé de sécurité FIDO2 sur un compte Microsoft personnel depuis un appareil Windows 11 :

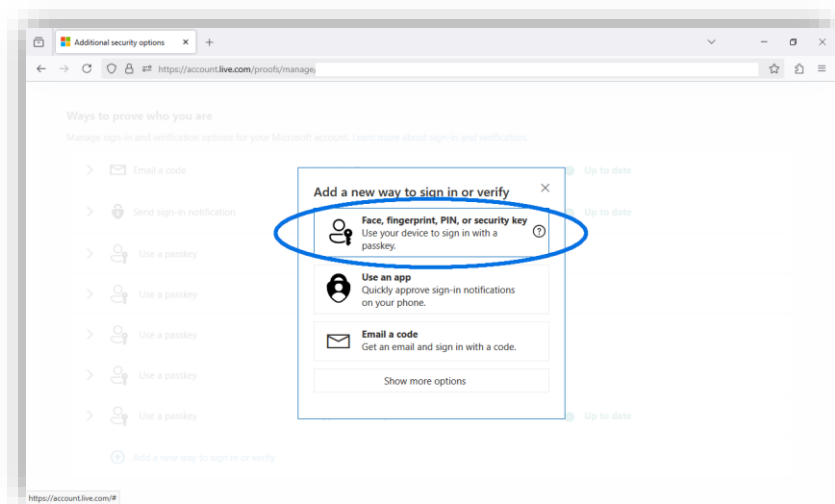
1. Connectez-vous à l'interface de gestion de votre compte Microsoft à l'adresse <https://account.microsoft.com>
2. Dans les paramètres de sécurité, choisissez *Gérer mes méthodes de connexion*.



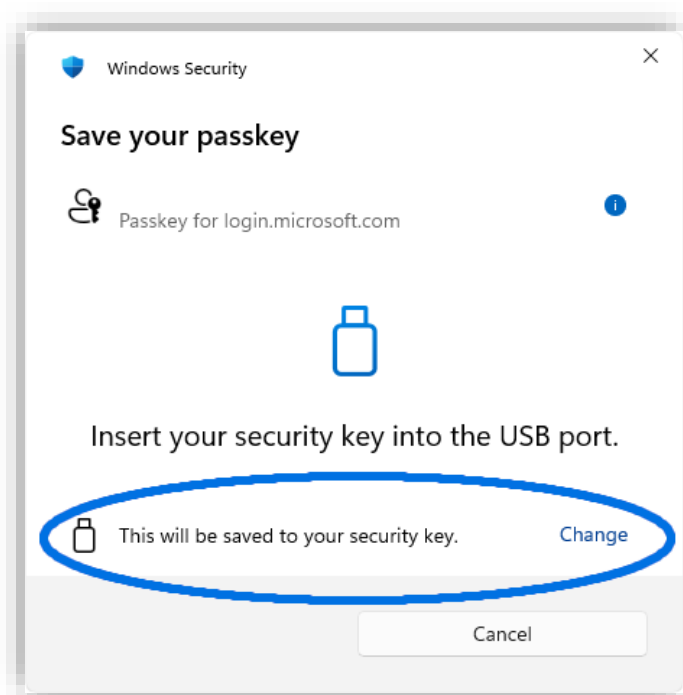
3. Sélectionnez *Ajouter une nouvelle méthode de connexion ou de vérification*.



4. Choisissez *Visage, empreinte digitale, code PIN ou clé de sécurité*.



5. Suivez les instructions du système. Veillez à bien enregistrer la clé de sécurité, et non une autre méthode comme Windows Hello.



6. Une fois l'enregistrement terminé, votre clé de sécurité apparaîtra dans la liste des méthodes d'authentification.

① NOTE:

Chaque service web dispose de sa propre méthode pour enregistrer les dispositifs FIDO2. En général, cette option se trouve dans les paramètres de sécurité du service.

## 5. Utilisation du gestionnaire FIDO et OTP

Le logiciel SpearID FIDO2 Manager vous permet de gérer vos identifiants FIDO2 et de créer et utiliser des codes TOTP et HOTP. Vous pouvez télécharger ce logiciel pour votre système d'exploitation sur <https://fido2.fi> (en bas de page).

## 6. FAQ

*J'ai deux comptes Gmail. De combien de clés de sécurité ai-je besoin pour les protéger tous les deux ? Me faut-il une clé supplémentaire pour mon second compte Gmail ?*

Vous pouvez utiliser une seule clé de sécurité FIDO2 NFC avec plusieurs comptes, bien que ce ne soit pas l'idéal. Que vous protégiez un ou plusieurs comptes Gmail, nous vous recommandons d'enregistrer plusieurs clés (si le service le permet). Ainsi, en cas de perte, de dommage ou de vol de votre clé principale, vous disposerez toujours d'une clé de secours opérationnelle.

*Que faire en cas de perte de ma clé de sécurité FIDO2 NFC ?*

Rendez-vous sur les sites où votre clé est enregistrée. Dans les paramètres de sécurité ou de vérification en deux étapes, supprimez l'appareil perdu. Nous recommandons de posséder deux clés de sécurité FIDO2 NFC : une pour l'usage quotidien et une autre comme sauvegarde.

*Pourquoi GitHub affiche-t-il "ce navigateur ne prend pas en charge les clés de sécurité" sur mon iPhone ?*

Assurez-vous que votre iPhone est mis à jour vers iOS 13.3 minimum et utilisez Safari pour vous connecter.

*Quelles applications sont compatibles avec la clé de sécurité FIDO2 NFC ?*

Les applications prenant en charge FIDO U2F/FIDO2 incluent, sans s'y limiter : Google, Facebook, Dropbox, GitHub, Dashlane, DUO, StrongAuth, etc.

*Puis-je enregistrer une clé de sécurité FIDO2 NFC depuis mon smartphone ?*

*Non. Bien que vous puissiez utiliser la clé de sécurité FIDO2 NFC pour vous authentifier depuis vos appareils mobiles, l'enregistrement initial doit être effectué depuis un ordinateur.*

## 7. Product Specs

<b>Produit</b>	<b>Clé de sécurité SpearID FIDO2 NFC (FD202)</b>
<b>Systèmes compatibles</b>	Windows, macOS, Linux
<b>Navigateurs compatibles</b>	Edge, Chrome, Firefox, Opera, Safari
<b>Fonctions</b>	FIDO U2F, FIDO2, HOTP, TOTP
<b>Algorithmes</b>	SHA256, AES, HMAC, ECDH, ECDSA
<b>Dimensions</b>	44,9 x 16,0 x 9,2 mm
<b>Interfaces</b>	USB-C, NFC
<b>Conservation des données</b>	≥ 10 ans
<b>Cycles de réécriture</b>	≥ 100 000
<b>Tension de fonctionnement</b>	5V ± 10%

<b>Tension de fonctionnement</b>	<b>5V ± 10%</b>
<b>Courant de fonctionnement</b>	Max < 40mA
<b>Bouton</b>	Unique
<b>Durabilité du bouton</b>	≥ 100 000 pressions
<b>Température de fonctionnement</b>	-10 ~ 60°C
<b>Température de stockage</b>	-20 ~ 60°C
<b>Indicateur lumineux</b>	Blanc
<b>Matériaux</b>	Aluminium, Polycarbonate