

Bilan après 1 an d'utilisation d'une Nitrokey 3A Mini

Gauthier Catteau

Contexte

- L'authentification multi-facteur est devenu incontournable pour obtenir un niveau satisfaisant de sécurité.
- Nous connaissons tous les applications TOTP à installer sur son téléphone, mais ce n'est pas la panacée en terme d'usage.

Mes interrogations ?

- Peut-on faire confiance à son téléphone pour stocker une clef OTP ?
- Où stocker le mot de passe du gestionnaire de mot de passe ?
- Comment faire pour s'authentifier sur un poste sur lequel on ne peut pas avoir totalement confiance ?
- Comment signer ou déchiffrer un mail sans laisser sa clef gpg sur le poste ?
- Comment alléger la procédure d'authentification MFA ?

Besoins

- Support Fido2
- Gestionnaire de mot de passe sécurisé
- Stockage clef gpg
- Prix abordable
- Bonne documentation

Solutions clef USB

- Yubikey (USA-Suède)
- Feitian BioPass (Chine)
- Thales SafeNet eToken
- Nitrokey (Allemagne)

Choix

Nitrokey 3A Mini

- Prix ~50€
- + de fonctionnalités qu'une Yubikey
- Firmware opensource écrit en rust
- Outils opensource écrit en Python
- Produit en Allemagne

À quoi ça ressemble ?



Mes usages

- Stockage des mots de passes les + importants - 50 max
- Stockage OTP
- MFA avec FIDO2
- Stockage clefs GPG (Curve25519) - 3 max
- Tous ses usages sont protégés par différents codes PIN et un contact physique de la clef USB.

Autres usages à développer

Bientôt

- Déchiffrement des disques *LUKS/dm-crypt*
- Utilisation de la clef *gpg* pour les connexions *ssh*
- U2F pour l'authentification sous linux *libpam-u2f*

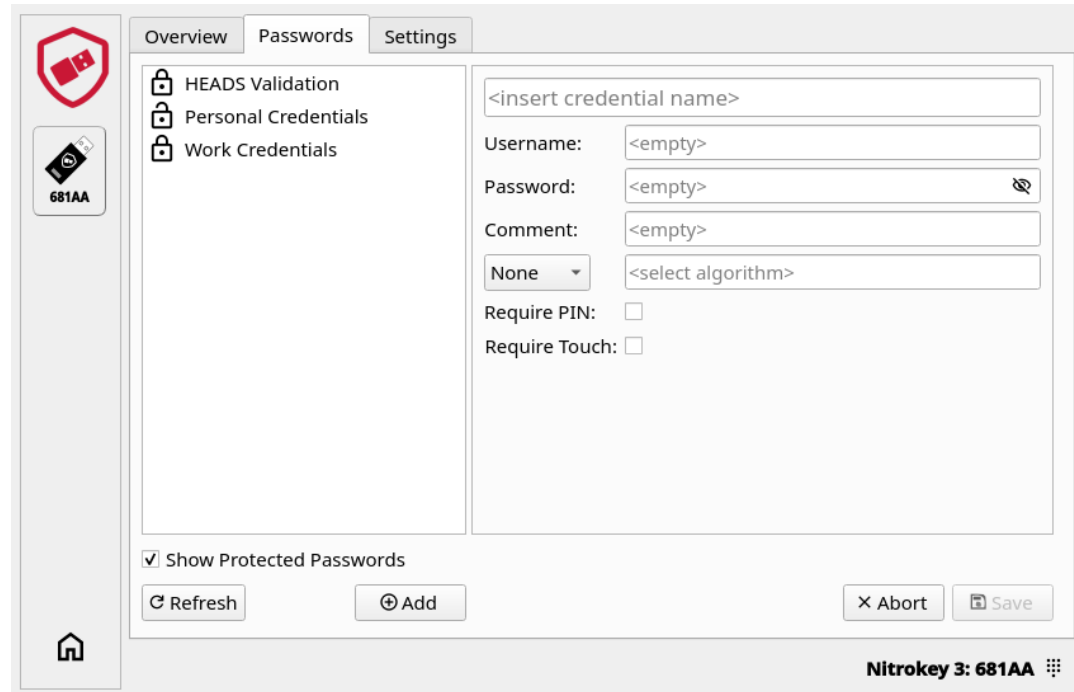
Peu probable

- NIST PIV (Authentication Windows)

Outils Nitrokey

- NitrokeyApp - Application desktop
- nitropy - cli pour les scripts
- Nitrokey Python SDK

NitrokeyApp2



The screenshot displays the NitrokeyApp2 interface. On the left, a sidebar contains a red shield icon with a white 'X', a USB icon labeled '681AA', and a home icon at the bottom. The main window has three tabs: 'Overview', 'Passwords', and 'Settings'. The 'Passwords' tab is active, showing a list of credential categories: 'HEADS Validation', 'Personal Credentials', and 'Work Credentials'. To the right of this list are input fields for adding a new credential: a text field for '<insert credential name>', 'Username:' with '<empty>', 'Password:' with '<empty>' and a toggle icon, 'Comment:' with '<empty>', a dropdown menu set to 'None' next to '<select algorithm>', and checkboxes for 'Require PIN:' and 'Require Touch:'. At the bottom left, there is a checked checkbox for 'Show Protected Passwords' and 'Refresh' and 'Add' buttons. At the bottom right, there are 'Abort' and 'Save' buttons. The footer shows 'Nitrokey 3: 681AA' with a small icon.

Overview Passwords Settings

HEADS Validation
Personal Credentials
Work Credentials

<insert credential name>
Username: <empty>
Password: <empty>
Comment: <empty>
None <select algorithm>
Require PIN: ☐
Require Touch: ☐

☒ Show Protected Passwords

Refresh Add Abort Save

Nitrokey 3: 681AA

nitropy



```
> nitropy nk3 secrets get-password pihole
Command line tool to interact with Nitrokey devices 0.10.0
Please touch the device if it blinks
Credential not found. Please provide PIN below to search in the PIN-protected database.
Current PIN (8 attempts left):
Please touch the device if it blinks
login          : pihole
password       : .....
metadata       : ---
properties     : f1
name           : pihole
```

nitropy



```
> nitropy nk3 secrets add-otp --digits-str 6 --kind TOTP --hash SHA256 --touch-button --protect-with-pin
```

```
> nitropy nk3 secrets get-otp "TOTP Mattermost"
```

Command line tool to interact with Nitrokey devices 0.10.0

Please touch the device if it blinks

Credential not found. Please provide PIN below to search in the PIN-protected database.

Current PIN (8 attempts left):

Please touch the device if it blinks

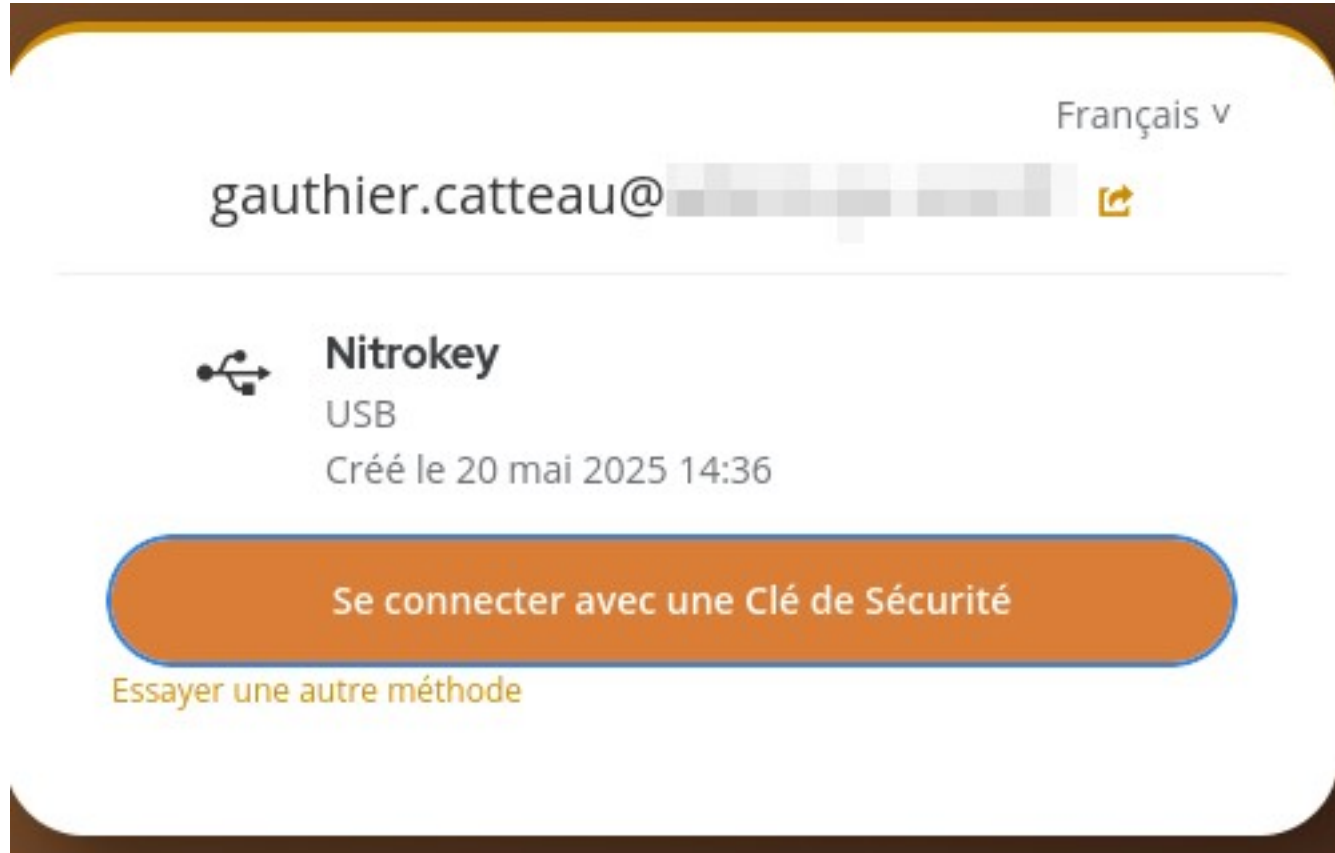
Timestamp: 2025-11-23T14:20:20 (1763904020), period: 30

123456

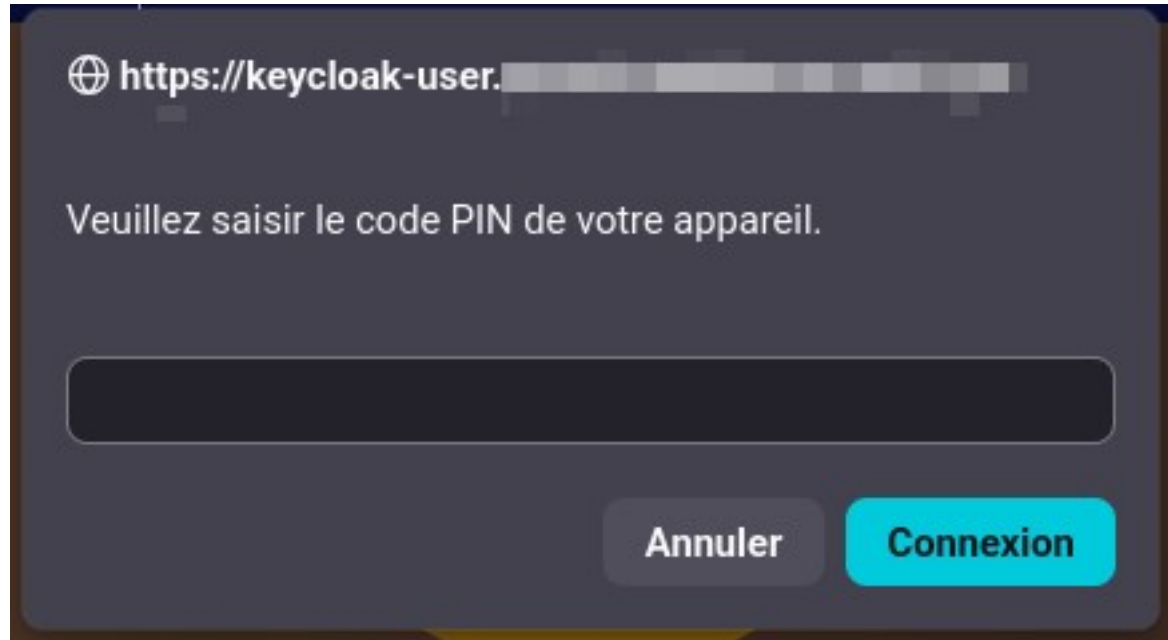
Applications compatibles FIDO2 utilisées

- Keycloak
- Discourse
- OVH
- VaultWarden
- Gandi
- Codeberg
- GitHub
- GitLab
- Wikipedia
- ...

Exemple d'intégration avec Keycloak dans Firefox



Exemple d'intégration avec Keycloak dans Firefox



A screenshot of a Firefox mobile interface for Keycloak integration. The address bar shows a URL starting with 'https://keycloak-user.' followed by a blurred domain. Below the address bar, the text 'Veuillez saisir le code PIN de votre appareil.' (Please enter the PIN code of your device.) is displayed. A large, empty, rounded rectangular input field is provided for the PIN. At the bottom right, there are two buttons: 'Annuler' (Cancel) in a light gray button and 'Connexion' (Connect) in a bright blue button.

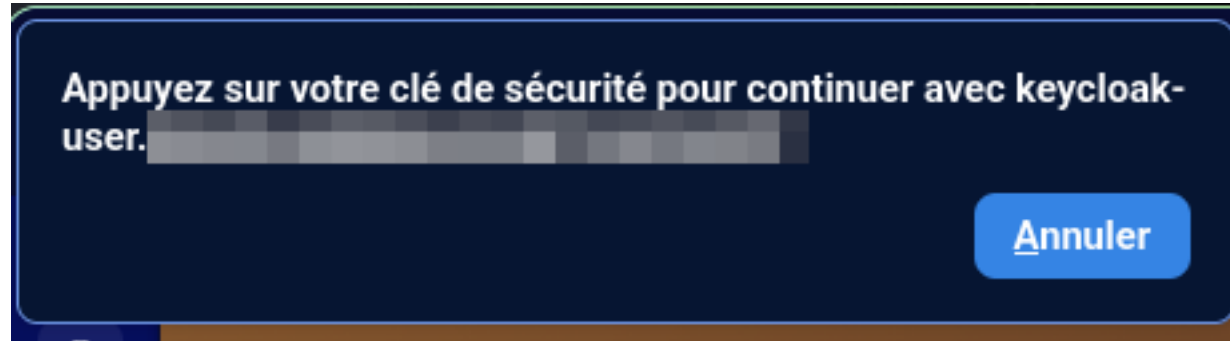
https://keycloak-user. [blurred domain]

Veuillez saisir le code PIN de votre appareil.

[Empty PIN input field]

Annuler Connexion

Exemple d'intégration avec Keycloak dans Firefox



Points importants

- Prévoir une solution de secours en cas de perte, destruction ou vol de la clef.
- Le but de cette présentation est plus de montrer l'intérêt de ce type de clef plutôt que de faire de la publicité pour cette clef.

Conclusions

- Le gestionnaire de mot de passe est intuitif
- Facilement scriptable grâce à l'outil cli nitropy
- Le remplacement du code OTP sur le téléphone par FIDO2 est vraiment appréciable
- L'utilisation de ce type d'équipement pour les autres usages reste complexe
- Quelques interrogations sur la fiabilité à long terme de ce type d'équipement

Questions ?