FLIPPER ZERO - Authentificator

SÉCURISATION DES ACCÈS VIA TOTP (HARDWARE TOKEN)

Cible : Flipper Zero (App Authenticator)

Contexte : Durcissement de l'authentification (MFA) pour les services critiques (Infomaniak, SSH, AWS).

Référence Normative : RFC 6238 (TOTP)

LE PROTOCOLE TOTP

Le Concept (MFA)

L'authentification repose sur trois facteurs :

1. **Ce que je sais** (Password) -> *Compromis si keylogger ou brute-force.*
2. **Ce que je possède** (Token/Flipper) -> *Nécessite un vol physique.*
3. **Ce que je suis** (Biométrie) -> *Non révocable (on ne change pas d'empreinte).*

Le Flipper agit comme facteur de **Possession**.

La Mécanique (TOTP)

Le *Time-based One-Time Password* est une danse mathématique entre le Client (Flipper) et le Serveur (Infomaniak).

- **La Graine (Seed/Secret)** : Une clé unique partagée une seule fois lors de l'enrôlement (via le QR Code).
- **Le Tempo (Time)** : Le temps Unix (Epoch) divisé par intervalle de 30 secondes.
- **L'Algorithme** : HMAC-SHA1(Secret, Temps).

> **Analogie :** C'est comme les codes d'accès à Zion dans *Matrix*. Ils changent constamment, mais le capitaine du vaisseau et la tour de contrôle ont la même horloge et le même livre de codes. Si l'horloge du vaisseau retarde, la porte reste fermée et les Sentinelles vous attrapent.

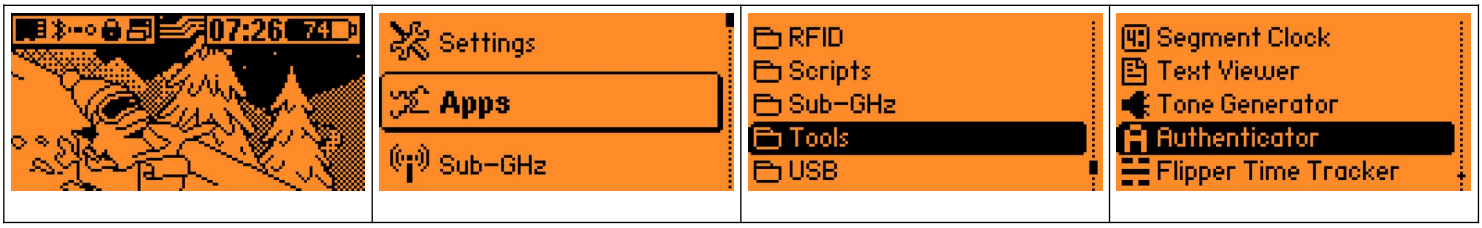
INSTALLATION RAPIDE

Pré-requis

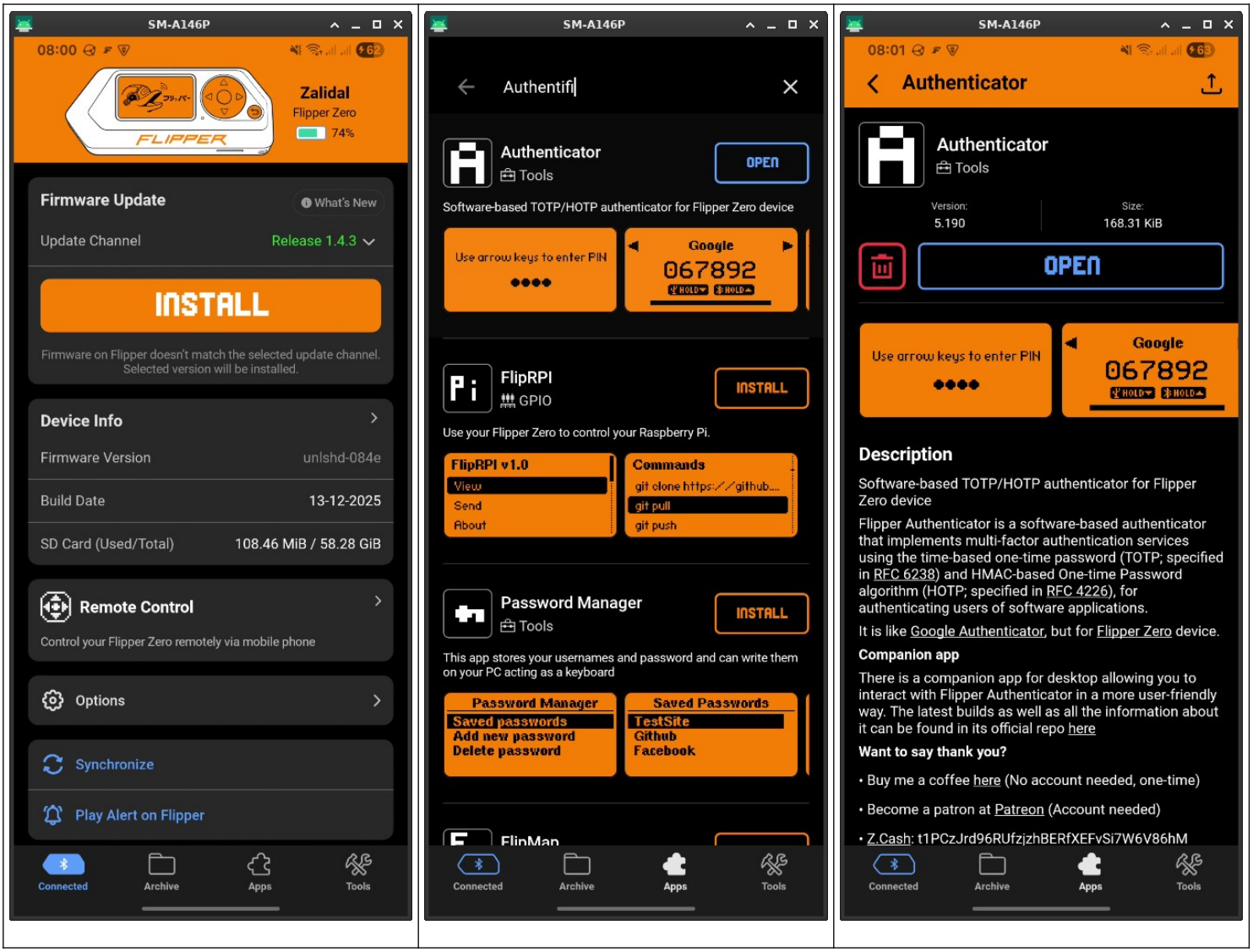
- Flipper Zero (Firmware Unleashed ou Officiel).
- Application Mobile "Flipper" (Android/iOS) pour la synchro Bluetooth.
- Carte SD insérée et montée.

Procédure

- Sur le Flipper : Menu -> Apps -> Tools -> Authenticator.



- Si absent : Installer via l'application mobile (Hub/Store).



CONFIGURATION ESSENTIELLE

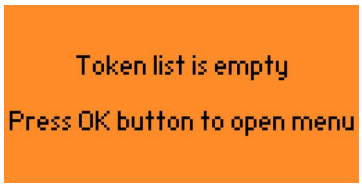
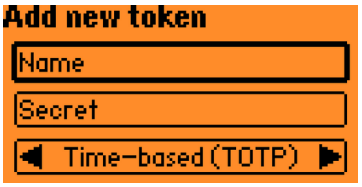
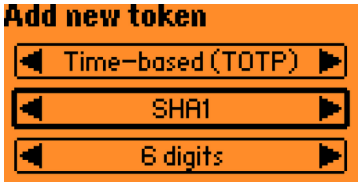
Extraction du Secret (Côté Serveur)

Sur le service à protéger (ex: Infomaniak) :

- Choisir l'option "Application Mobile" ou "Générateur de codes".
- Ne **pas** scanner le QR Code (le Flipper n'a pas de caméra).
- Chercher le lien *"Impossible de scanner"* ou *"Afficher la clé secrète"*.
- Copier la chaîne de caractères (Base32, ex: JBSWY3DPEHP...).

Injection (Côté Flipper)

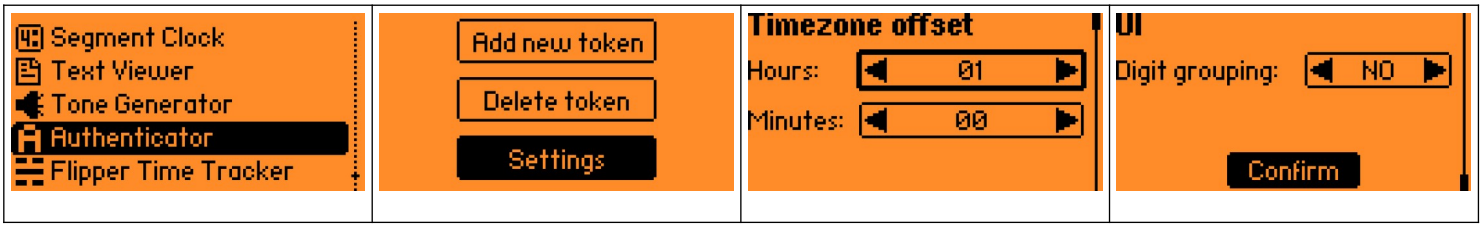
- Ouvrir l'app **Authenticator** sur le Flipper.
- Aller sur Add New -> Manually.
- **Name** : Nom explicite (ex: Infomaniak_Admin).
- **Secret** : Saisir la chaîne récupérée à l'étape précedentes.
- **Settings par défaut** :
  - Algo : SHA1 (Standard industrie).
  - Digits : 6 (Standard).
  - Time : 30 sec.

<table>
<tr>
<td> 
</td>
<td> 
</td>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td> 
</td>
<td> 
</td>
<td></td>
<td></td>
</tr>
</table>

Correction Temporelle (CRITIQUE)

Le Flipper ne gère pas les Timezones nativement.

- Dans Authenticator -> Settings.
- Régler **Timezone Offset** :
    - Hiver (France) : +01.00
    - Été (France) : +02.00
- Valider la configuration.



- **Synchronisation** : Connecter le Flipper au smartphone en Bluetooth -> App Mobile -> Options -> System -> Synchronize Date/Time.

BEST PRACTICES

- **Backup des Clés:**
    - Les clés .auth sont stockées dans SD Card/apps_data/authenticator/ ou SD Card/apps_data/authenticator/totp/ (suivant les Firmware).
    - **Action :** Copier régulièrement ce dossier sur un stockage froid (Clé USB chiffrée). Si la carte SD meurt, vous perdez vos accès.

- **Sécurité Physique :**
    - Le Flipper devient une clé de voute. Ne le laissez pas traîner sur un bureau.

- **Codes de Secours :**
    - Toujours générer et imprimer les "Recovery Codes" proposés par le service (Infomaniak) lors de l'activation. C'est votre sortie de secours si le Flipper passe à la machine à laver.