Guide complet de gestion des mots de passe

Windows – macOS – Linux

Rédigé par **Alferann**

Ce guide accompagne pas à pas la mise en place d'une gestion de mots de passe structurée en 3 couches, de la création du coffre local KeePassXC au déploiement de Vaultwarden sur VPS.

Sommaire

- Pré-requis 4
- Estimation des coûts 4
- Versions des logiciels 4

Phase A – Stratégie et fondations 5
- A.1 Niveaux de protection 5
- A.2 Arbre de décision – où stocker ce secret ? 5

Checklist 6
- Couche 2 – KeePassXC (coffre local) 6
- Couche 1 – Vaultwarden / Bitwarden 6
- Migration et sécurisation 6
- Couche 3 – Sauvegarde physique 6

Phase B – KeePassXC (coffre local) 7
- B.1 Installation 7
  - Méthode via interface graphique 7
- B.2 Génération du mot de passe maître 7
  - Méthode diceware (recommandée) – via l'interface graphique 7
  - Méthode caractères aléatoires (alternative) 8
  - Critères d'un bon mot de passe maître 8
  - Étapes critiques avant de continuer 8
- B.3 Création de la base 9
  - Via l'interface graphique 9
  - Permissions sur le fichier 9
  - Réglages recommandés (interface graphique) 10
- B.4 Arborescence des groupes 11
- B.5 Premières entrées 11
  - Entrée 1 : VPS root 11
  - Entrée 2 : clé SSH 11
  - Entrée 3 : mot de passe maître Bitwarden 11
- B.6 Préparer une clé USB chiffrée 11
  - Méthode via interface graphique 12
  - Utilisation quotidienne 13
- B.7 Sauvegarde KeePassXC sur clé USB 13
  - Méthode via interface graphique 13
- B.8 Test de la sauvegarde 14

Phase C – Bitwarden / Vaultwarden (coffre du quotidien) 15
- Option A : Bitwarden.com (débutant, 5 minutes) 15
- Option B : Vaultwarden auto-hébergé (avancé) 15
  - C.1 Présentation et pré-requis 15
  - C.2 Installer Docker sur le VPS (Ubuntu) 16
  - C.3 Lancer Vaultwarden 16
  - C.4 Configurer le DNS (sous-domaine) 16
  - C.5 Ouvrir les ports du pare-feu 17
  - C.6 Nginx proxy inverse + HTTPS 17
  - C.7 Créer le compte et désactiver les inscriptions 18
  - C.8 Stocker le mot de passe maître Bitwarden dans KeePassXC 19
  - C.9 Activer le 2FA sur Vaultwarden 19
  - C.10 Sauvegardes automatiques 19

C.11 Mise à jour de Vaultwarden 20
Phase D – Configuration des clients Bitwarden 21
D.1 Extension navigateur 21
D.2 Réglages recommandés 21
D.3 Structure des dossiers Bitwarden 22
D.4 Fiches de référence des entrées 22
Conventions de nommage 22
Tableau de référence non exhaustif 22
Phase E – Migration des secrets 23
E.1 Migrer les mots de passe dans Bitwarden 23
E.2 Migrer codes de récupération et clés dans KeePassXC 23
Suppression sécurisée 24
Cas particulier : seeds crypto en clair sur le disque 24
Phase F – Couche physique 25
F.1 OneKey KeyTag – présentation 25
F.2 Encodage BIP-39 en binaire 25
Principe 25
Exemples 25
Procédure de gravure 26
F.3 Stockage physique – séparation des lieux 26
F.4 Split de seed (optionnel, gros patrimoines crypto) 26
Shamir's Secret Sharing (SSS) 27
Découpage manuel (alternative simple) 27
Phase G – Bonnes pratiques 28
G.1 Mots de passe générés 28
G.2 2FA (double authentification) 28
G.3 Vérification des fuites 28
G.4 Politique de rotation 29
G.5 Seeds crypto – pourquoi les séparer 29
G.6 Scénario « J'ai perdu mon PC » 29
Annexe A – YubiKey : authentification matérielle (optionnel) 30
A.1 Installation de YubiKey Manager 30
A.2 Configuration avec Vaultwarden 31
A.3 Configuration avec KeePassXC 31
A.4 Autres services compatibles 31
A.5 Procédure en cas de perte 31
Annexe B – Dépannage 32
Problèmes communs (tous OS) 32
Problèmes spécifiques par OS 32
Docker après reboot du VPS 33

Pré-requis

Élément	Description
Système	Windows 10/11, macOS 12+ (Monterey) ou Linux (toute distribution)
Outils	Terminal / PowerShell, navigateur web
Logiciels	KeePassXC (installé au fil du guide)
Couche avancée	VPS (serveur privé virtuel) + nom de domaine
Sauvegarde locale	Clé USB dédiée
Sauvegarde physique	Plaque métal type OneKey KeyTag

Temps estimé : 1 à 2 heures pour les couches 1 et 2. La couche 3 se fait à part, à votre rythme.

Estimation des coûts

Élément	Coût	Fréquence
KeePassXC	Gratuit (open-source)	–
Bitwarden.com (gratuit)	0 EUR	–
Vaultwarden (auto-hébergé)	0 EUR (open-source)	–
VPS (ex : Hetzner, Hostinger)	4–10 EUR/mois	Mensuel
Nom de domaine	10–15 EUR/an	Annuel
Clé USB (16+ Go)	8–15 EUR	Unique
YubiKey 5 NFC (x2)	50–70 EUR x2	Unique
Plaque métal (OneKey, Cryptosteel)	30–60 EUR	Unique
Extension navigateur Bitwarden	Gratuit	–
Aegis / ente Auth	Gratuit	–

Total annualisé (estimation) :
- **Configuration minimale** (Bitwarden.com gratuit, sans VPS, sans YubiKey) : 50–80 EUR (clé USB + plaque)
- **Configuration complète** (VPS + domaine + YubiKey) : 250–350 EUR la première année, puis 60–135 EUR/an

Versions des logiciels

Logiciel	Version	Site officiel
KeePassXC	2.7.x	keepassxc.org
Vaultwarden	1.32.x	github.com/dani-garcia/vaultwarden
Docker Engine	27.x	docs.docker.com
Nginx	1.26.x	nginx.org
Certbot	3.x	certbot.eff.org
Bitwarden (extension)	2024.x	bitwarden.com
YubiKey Manager	1.2.x	yubico.com

Note : vérifier les versions courantes au moment de l'utilisation.

Phase A – Stratégie et fondations

A.1 Niveaux de protection

Trois niveaux de protection pour trois types de secrets :

Niveau	Outil	Usage et exemples
Quotidien	Bitwarden (Vaultwarden auto-hébergé)	Mots de passe web, identifiants, notes. Synchro : cloud personnel (VPS). *Ex : GitHub, Google, banques, achats en ligne.*
Critique	KeePassXC (local, pas de synchro)	Codes de récupération, clés, root VPS, mot de passe maître Bitwarden. *Ex : clé SSH, root VPS, codes 2FA.*
Physique	Plaque métal / papier (aucune synchro)	Seeds crypto, passphrase maître KeePassXC (mémorisée). *Ex : seeds crypto sur plaque métal (cf. Phase F).*

Pourquoi cette étape ? En séparant tes secrets en trois niveaux, tu limites les dégâts en cas de compromission d'un des niveaux. Un mot de passe de forum n'a pas la même valeur qu'une seed crypto.

A.2 Arbre de décision – où stocker ce secret ?

```
Ce secret est-il une seed crypto ?
+-- OUI
|   +-- Support physique UNIQUEMENT (plaque métal, cf. Phase F)
+-- C'est un code de récupération ou une clé privée ?
|   +-- KeePassXC (codes 2FA, clés SSH, etc.)
+-- C'est la fondation d'un service critique ? (root VPS, mot de passe maître Bitwarden)
|   +-- KeePassXC (c'est ce qui protège tout le reste)
+-- NON (mot de passe classique, identifiant web)
    +-- Bitwarden
```

Principe fondamental : le mot de passe root du VPS va dans KeePassXC car c'est la fondation de tout – c'est lui qui protège le serveur qui héberge Vaultwarden. De même, le mot de passe maître Bitwarden est stocké dans KeePassXC comme copie de secours.

En résumé – Bitwarden pour le quotidien, KeePassXC pour les secrets critiques (codes, clés), plaque métal pour les seeds crypto.

Checklist

Couche 2 – KeePassXC (coffre local)

- [ ] Installer KeePassXC (B.1)
- [ ] Générer et mémoriser la passphrase maître diceware, 6+ mots (B.2)
- [ ] Créer la base AES-256/Argon2id et restreindre les permissions (B.3)
- [ ] Créer les 6 groupes et ajouter les premières entrées : VPS root, clé SSH, mot de passe maître Bitwarden (B.4–B.5)
- [ ] Chiffrer la clé USB de sauvegarde (B.6)
- [ ] Sauvegarder la base sur la clé USB et vérifier l'intégrité (B.7)
- [ ] Tester la restauration sur un autre appareil (B.8)

Couche 1 – Vaultwarden / Bitwarden

- [ ] Créer un compte Bitwarden (bitwarden.com ou auto-hébergé)
- [ ] Installer l'extension navigateur et configurer les réglages (D.1–D.2)
- [ ] Créer les 13 dossiers (D.3)
- [ ] Migrer les comptes dans Bitwarden (E.1)

Si auto-hébergé (Option B) :

- [ ] Déployer Vaultwarden : Docker, DNS, Nginx + HTTPS (C.2–C.6)
- [ ] Créer le compte, désactiver les inscriptions, activer le 2FA (C.7–C.9)
- [ ] Configurer les sauvegardes automatiques (C.10)

Migration et sécurisation

- [ ] Migrer codes de récupération et clés dans KeePassXC (E.2)
- [ ] Installer Aegis/ente Auth et activer le 2FA sur tous les comptes possibles (G.2)
- [ ] Stocker les codes de récupération 2FA dans KeePassXC (G.2)

Couche 3 – Sauvegarde physique

- [ ] Se procurer une plaque métal OneKey KeyTag ou équivalent (F.1)
- [ ] Encoder les seeds en binaire BIP-39, graver et vérifier le décodage (F.2)
- [ ] Stocker la plaque dans un lieu sécurisé hors du domicile (F.4)

Phase B – KeePassXC (coffre local)

KeePassXC est un gestionnaire de mots de passe local, open-source et multiplateforme. Il ne synchronise rien : le fichier `.kdbx` reste sur votre machine.

B.1 Installation

Méthode via interface graphique

Windows

1. Aller sur keepassxc.org > Télécharger > **Windows**
2. Télécharger l'installeur `.msi`
3. Lancer l'installeur et suivre l'assistant
4. KeePassXC apparaît dans le menu Démarrer

macOS

1. Aller sur keepassxc.org > Télécharger > **macOS**
2. Télécharger le fichier `.dmg`
3. Ouvrir le `.dmg`, glisser KeePassXC dans Applications
4. Première ouverture : clic droit > **Ouvrir** (contourner Gatekeeper)

Linux

1. Ouvrir le magasin de logiciels (Discover, GNOME Logiciels, pamac)
2. Rechercher **KeePassXC**
3. Cliquer sur **Installer**

Sous Arch Linux, KeePassXC est aussi disponible via le gestionnaire de paquets graphique pamac.

Alternative CLI

Windows

```
winget install KeePassXCTeam.KeePassXC
```

macOS

```
brew install --cask keepassxc
```

Linux

```
# Arch Linux
sudo pacman -S keepassxc

# Debian / Ubuntu
sudo apt install keepassxc
```

Vérifier l'installation : ouvrir KeePassXC depuis le menu ou le lanceur d'applications. L'écran d'accueil s'affiche.

B.2 Génération du mot de passe maître

Le mot de passe maître protège l'intégralité de la base KeePassXC. Il doit être **mémorisable**, **résistant au bruteforce** et **unique**.

Méthode diceware (recommandée) – via l'interface graphique

1. Ouvrir KeePassXC > **Outils** > **Générateur de mot de passe**
2. Sélectionner l'onglet **Phrase de passe**
3. Nombre de mots : **6** (minimum)
4. Séparateur : `-`, `*` ou `+`
5. Cliquer sur **Générer**
6. Copier la phrase de passe obtenue

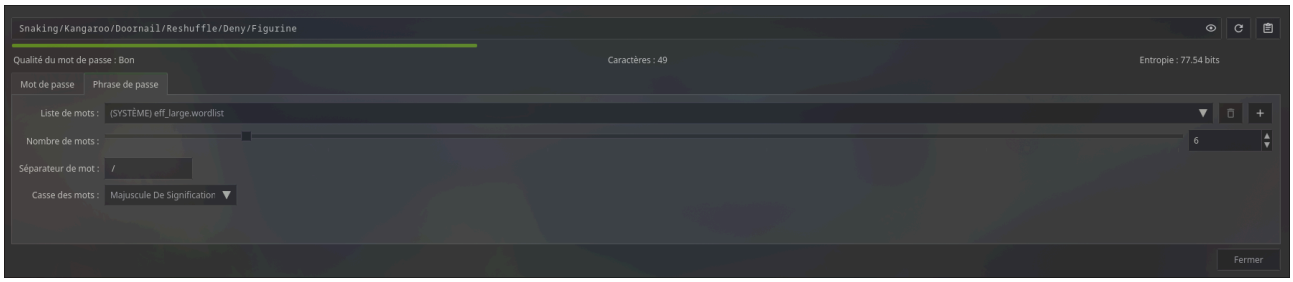


Fig. 1. – KeePassXC – générateur, onglet « Phrase de passe »

Alternative CLI

```
# Generate a diceware passphrase with 6 random words
keepassxc-cli diceware --words 6

# Example output: voltage-tramway-shelter-fungal-rooftop-kindle
```

Méthode caractères aléatoires (alternative)

1. Dans le générateur, rester sur l'onglet **Mot de passe**
2. Longueur : **32 caractères**
3. Cocher : majuscules, minuscules, chiffres, symboles
4. Cliquer sur **Générer**

Alternative CLI

```
# Generate a 32-character random password
keepassxc-cli generate --length 32 --lower --upper --numeric --special
```

Critères d'un bon mot de passe maître

- **Longueur** : 6+ mots diceware ou 32+ caractères aléatoires
- **Entropie** : minimum 77 bits (6 mots diceware = 77,5 bits)
- **Mémorisable** : une passphrase diceware se retient en quelques jours
- **Unique** : ne doit être utilisé pour aucun autre service

Étapes critiques avant de continuer

1. Générer le mot de passe maître avec une des méthodes ci-dessus
2. Le noter sur papier (écriture manuscrite)
3. Stocker le papier en lieu sûr (coffre-fort, enveloppe scellée)
4. Le mémoriser en le tapant plusieurs fois par jour pendant une semaine
5. Ne passer à l'étape suivante qu'une fois le mot de passe mémorisé

Attention – Si tu perds ce mot de passe maître, il n'existe **aucun moyen de récupérer** le contenu de ta base KeePassXC. Le papier est ton filet de sécurité.

B.3 Création de la base

Via l'interface graphique

1. Lancer KeePassXC > **Base de données** > **Nouvelle base de données**
2. Nom : `secrets` – Description : `Base locale de secrets critiques`

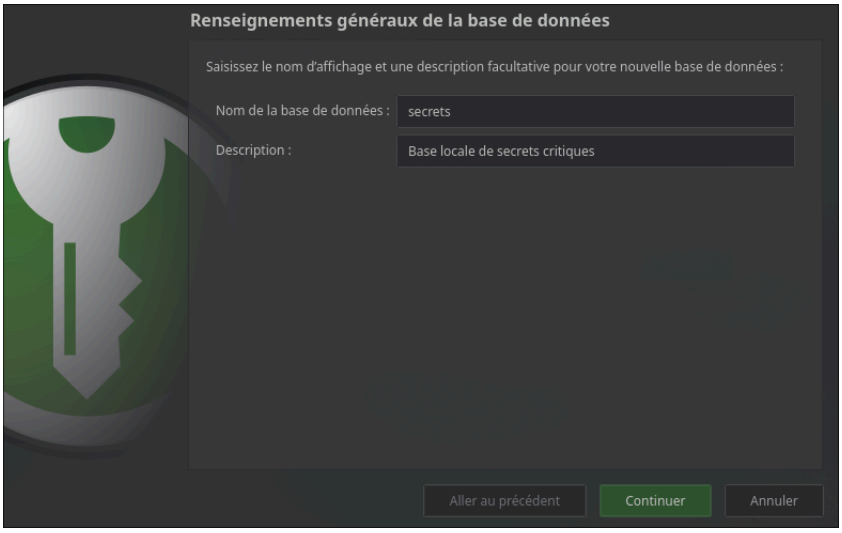


Fig. 2. – KeePassXC – écran de création d'une nouvelle base de données

3. Paramètres de chiffrement (rend les données illisibles sans le mot de passe) :
   - **Algorithme** : AES-256
   - **Fonction de dérivation** : Argon2id
   - Cliquer sur **Calibrer 1 seconde** (viser 1 à 2 secondes de délai)

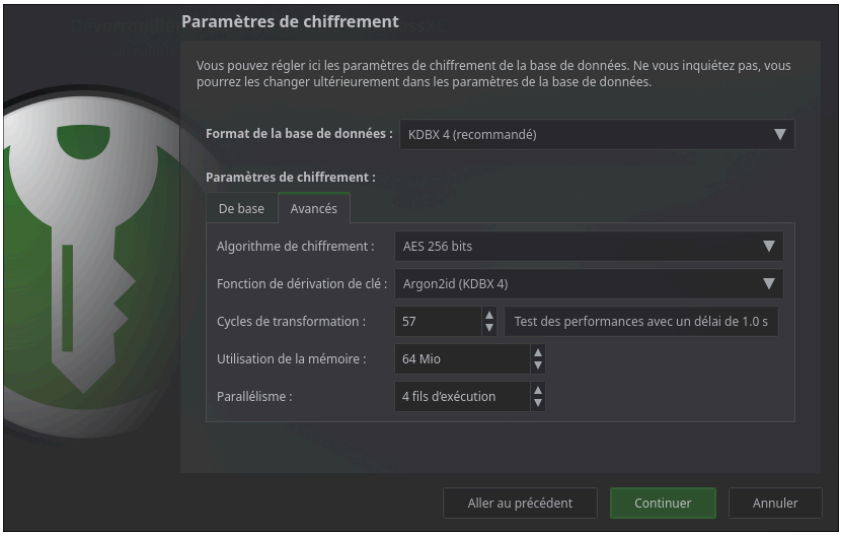


Fig. 3. – KeePassXC – paramètres de chiffrement Argon2id

4. Entrer le mot de passe maître généré à l'étape précédente
5. (Optionnel) Ajouter un **fichier clé** stocké sur une clé USB séparée
6. Enregistrer le fichier : choisir un emplacement sécurisé sur votre disque

Permissions sur le fichier

Restreindre les permissions du fichier `.kdbx` limite la surface d'attaque.

Windows

1. Clic droit sur `secrets.kdbx` > **Propriétés** > onglet **Sécurité**
2. Cliquer sur **Avancé** > **Désactiver l'héritage**
3. Choisir **Convertir les autorisations héritées en autorisations explicites**
4. Supprimer « Utilisateurs » et « Tout le monde »
5. Ne garder que votre propre compte utilisateur (Contrôle total)
6. Valider

macOS

macOS est un système Unix : les commandes `chmod` fonctionnent comme sous Linux.

- Ouvrir le **Terminal** (Applications > Utilitaires)

```
chmod 600 ~/
secrets.kdbx
chmod 700 ~/
dossier_securite/
```

Alternative GUI : Finder > clic droit sur le fichier > **Lire les informations** > section **Partage et permissions** > restreindre l'accès.

Linux

```
# Restrict database
file: owner read/write
only
chmod 600 ~/chemin/
vers/secrets.kdbx

# Restrict security
directory: owner only
chmod 700 ~/chemin/
vers/dossier_securite/

# Restrict key file if
used
chmod 600 /media/usb/
keyfile.keyx
```

Pourquoi cette étape ? Sans ces permissions, n'importe quel programme de votre machine pourrait copier la base chiffrée et tenter un bruteforce hors ligne. Les restrictions d'accès empêchent cette copie.

Réglages recommandés (interface graphique)

Dans KeePassXC > **Outils** > **Paramètres** :

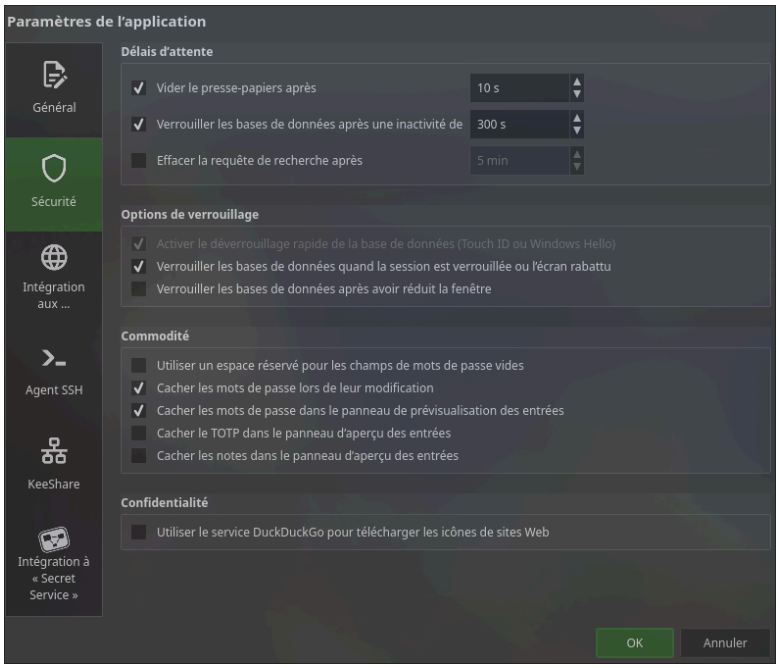


Fig. 4. – KeePassXC – paramètres de sécurité

Aucune synchronisation : pas de Syncthing, pas de Git, pas de cloud.

B.4 Arborescence des groupes

Créer les groupes suivants dans la base KeePassXC (clic droit sur la racine > **Nouveau groupe**) :

```
secrets.kdbx
+-- Infrastructure critique
+-- Seeds et clés crypto
+-- Codes de récupération
+-- Certificats et clés
+-- Codes de secours 2FA
+-- Notes sensibles
```

B.5 Premières entrées

Entrée 1 : VPS root

Champ	Valeur
Titre	VPS nomHébergeur – root
Nom d'utilisateur	root
Mot de passe	(le mot de passe root du VPS)
URL	ssh://IP_DU_VPS:22
Notes	Centre de données, IP : x.x.x.x, OS : Ubuntu
Groupe	Infrastructure critique

Entrée 2 : clé SSH

SSH (Secure Shell) est un protocole sécurisé pour se connecter à distance à un serveur.

Champ	Valeur
Titre	Clé SSH – VPS
Mot de passe	(passphrase de la clé SSH si applicable)
Notes	Clé publique : ~/.ssh/id_ed25519.pub, Empreinte : SHA256:…
Pièces jointes	Joindre la clé privée `id_ed25519` en sauvegarde
Groupe	Infrastructure critique

Entrée 3 : mot de passe maître Bitwarden

Champ	Valeur
Titre	Vaultwarden – mot de passe maître
Nom d'utilisateur	(adresse courriel du compte Bitwarden)
Mot de passe	(généré via KeePassXC : phrase de passe de 7 mots)
URL	https://vault.tondomaine.fr
Groupe	Infrastructure critique

B.6 Préparer une clé USB chiffrée

La clé USB chiffrée servira de sauvegarde physique de la base KeePassXC. Le chiffrement garantit que même en cas de perte ou de vol de la clé, les données restent inaccessibles sans le mot de passe.

Méthode via interface graphique

Windows

BitLocker To Go (Windows 10/11 Pro, Enterprise, Education)

1. Brancher la clé USB
2. Ouvrir l'**Explorateur de fichiers**
3. Clic droit sur la clé USB > **Activer BitLocker**
4. Cocher **Utiliser un mot de passe pour déverrouiller le lecteur**
5. Entrer le mot de passe (même mot de passe maître que KeePassXC)
6. Sauvegarder la clé de récupération > **Enregistrer dans un fichier** (temporaire, à supprimer ensuite)
7. Choisir **Chiffrer l'espace disque utilisé uniquement**
8. Mode de chiffrement : **Mode compatible** (pour utiliser sur d'autres PC)
9. Cliquer sur **Démarrer le chiffrement**

macOS

Utilitaire de disque

1. Brancher la clé USB
2. Ouvrir **Utilitaire de disque** (Applications > Utilitaires)
3. Sélectionner la clé USB dans le panneau gauche
4. Cliquer sur **Effacer**
5. Format : **APFS (chiffré)** ou **Mac OS étendu (journalisé, chiffré)**
6. Entrer le mot de passe (même mot de passe maître que KeePassXC)
7. Cliquer sur **Effacer**

Linux

GNOME Disques

1. Installer GNOME Disques si nécessaire (souvent préinstallé)
2. Lancer **Disques** depuis le lanceur d'applications
3. Sélectionner la clé USB dans le panneau gauche
4. Menu (...) > **Formater le disque** > Schéma : MBR > **Formater**
5. Cliquer sur le + pour créer une nouvelle partition
6. Taille : tout l'espace > **Suivant**
7. Nom du volume : `backup_keepassxc`
8. Type : **Ext4** et cocher **Volume protégé par mot de passe (LUKS)**
9. Entrer le mot de passe (même mot de passe maître que KeePassXC)

Alternative CLI

Sous Linux, le chiffrement complet via la ligne de commande :

```
# Install disk encryption tools (Arch Linux)
sudo pacman -S cryptsetup

# Identify the USB drive
lsblk

# Wipe partition table and create a single partition
sudo wipefs -a /dev/sdb
echo -e "o\nn\np\n1\n\n\nw" | sudo fdisk /dev/sdb

# Encrypt the partition with LUKS2
sudo cryptsetup luksFormat --type luks2 /dev/sdb1

# Open, format, mount
```

```
sudo cryptsetup open /dev/sdb1 usb_chiffree
sudo mkfs.ext4 -L backup_keepassxc /dev/mapper/usb_chiffree
sudo mkdir -p /mnt/usb
sudo mount /dev/mapper/usb_chiffree /mnt/usb
sudo chown "$USER":"$USER" /mnt/usb

# Unmount and close
sudo umount /mnt/usb
sudo cryptsetup close usb_chiffree
```

Utilisation quotidienne

Windows

1. Brancher la clé USB
2. Windows demande le mot de passe BitLocker
3. Entrer le mot de passe > la clé apparaît dans l'Explorateur
4. Après utilisation : clic droit sur la clé > **Éjecter**

macOS

1. Brancher la clé USB
2. macOS demande le mot de passe du volume chiffré
3. Entrer le mot de passe > la clé apparaît dans le Finder
4. Après utilisation : clic droit > **Éjecter**

Linux

1. Brancher la clé USB
2. Le gestionnaire de fichiers demande le mot de passe LUKS
3. Entrer le mot de passe > la clé est montée automatiquement
4. Après utilisation : clic droit > **Démonter** puis **Éjecter**

Alternative CLI
Sous Linux, les commandes manuelles sont :

```
# Open and mount
sudo cryptsetup open /dev/sdb1 usb_chiffree
sudo mount /dev/mapper/usb_chiffree /mnt/usb

# ... copy files ...

# Unmount and close
sudo umount /mnt/usb
sudo cryptsetup close usb_chiffree
```

B.7 Sauvegarde KeePassXC sur clé USB

- **Support** : clé USB chiffrée (cf. B.6), jamais de cloud
- **Fréquence** : après chaque modification de la base
- **Test** : ouvrir la sauvegarde sur un autre PC une fois par trimestre

Méthode via interface graphique

Windows

macOS

1. Ouvrir le **Finder**

Linux

1. Ouvrir l'**Explorateur de fichiers**
2. Copier `secrets.kdbx` vers la clé USB (glisser-déposer ou Ctrl+C / Ctrl+V)
3. Vérifier la copie :

Vérification d'intégrité (PowerShell) :

```
certutil -hashfile C:
\chemin\secrets.kdbx
SHA256
certutil -hashfile E:
\secrets.kdbx SHA256
```

Les deux empreintes doivent être identiques.

2. Copier `secrets.kdbx` vers la clé USB (glisser-déposer avec la touche Option enfoncée pour copier)
3. Vérifier la copie :

Vérification d'intégrité (Terminal) :

```
shasum -a 256 ~/chemin/
secrets.kdbx
shasum -a 256 /Volumes/
usb/secrets.kdbx
```

Les deux empreintes doivent être identiques.

1. Ouvrir le gestionnaire de fichiers
2. Copier `secrets.kdbx` vers la clé USB (glisser-déposer ou Ctrl+C / Ctrl+V)
3. Vérifier la copie :

Vérification d'intégrité (terminal) :

```
sha256sum ~/chemin/
secrets.kdbx
sha256sum /mnt/usb/
secrets.kdbx
```

Les deux empreintes doivent être identiques.

Alternative CLI
Sous Linux :

```
cp ~/chemin/secrets.kdbx /mnt/usb/
sync
sha256sum ~/chemin/secrets.kdbx /mnt/usb/secrets.kdbx
```

B.8 Test de la sauvegarde

1. Brancher la clé USB, déchiffrer le volume
2. Ouvrir le fichier `.kdbx` avec KeePassXC sur un autre PC
3. Vérifier que toutes les entrées sont présentes et lisibles
4. Répéter au moins une fois par trimestre

Attention – Une sauvegarde non testée est une sauvegarde qui n'existe pas.

Phase C – Bitwarden / Vaultwarden (coffre du quotidien)

Deux options s'offrent à vous pour la couche 1 (coffre du quotidien). Choisissez l'option qui correspond à votre niveau.

Option A : Bitwarden.com (débutant, 5 minutes)

Si vous débutez ou ne disposez pas d'un VPS, commencez ici :

1. Aller sur **bitwarden.com** et créer un compte gratuit
2. Choisir un mot de passe maître solide (généré via KeePassXC, cf. B.2)
3. Installer l'extension navigateur Bitwarden
4. Passer directement à la **Phase D** (configuration de l'extension navigateur)

Vous pourrez migrer vers l'auto-hébergement (Option B) plus tard sans perdre vos données (export/import depuis le coffre web Bitwarden).

Option B : Vaultwarden auto-hébergé (avancé)

La suite de cette phase nécessite un VPS et un nom de domaine.

C.1 Présentation et pré-requis

Vaultwarden (anciennement bitwarden_rs) est une implémentation alternative du serveur Bitwarden, écrite en Rust. Léger, compatible avec tous les clients Bitwarden, open-source, et inclut les fonctionnalités premium gratuitement.

Pré-requis

- VPS sous Ubuntu ou Debian (Hostinger, OVH, Hetzner, etc.)
- Un sous-domaine (ex : `vault.tondomaine.fr`) pointant vers l'IP du VPS
- Le mot de passe root du VPS (stocké dans KeePassXC, cf. B.5)
- Accès SSH au VPS

Connexion au VPS

Windows

Depuis Windows 10, OpenSSH est intégré. Ouvrir **Windows Terminal** ou **PowerShell** :

```
ssh root@IP_DU_VPS
```

Alternative GUI : PuTTY pour une interface graphique de connexion SSH.

macOS

Ouvrir le **Terminal** (Applications > Utilitaires) :

```
ssh root@IP_DU_VPS
```

macOS inclut nativement un client SSH.

Linux

Ouvrir un terminal :

```
ssh root@IP_DU_VPS
```

Le client SSH est préinstallé sur toutes les distributions.

Toutes les commandes de la Phase C (à partir de C.2) sont exécutées **sur le VPS**.

C.2 Installer Docker sur le VPS (Ubuntu)

```
# Install dependencies
sudo apt update && sudo apt install -y ca-certificates curl gnupg

# Add Docker official GPG key
sudo install -m 0755 -d /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/ubuntu/gpg \
  | sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg
sudo chmod a+r /etc/apt/keyrings/docker.gpg

# Add Docker repository (Ubuntu)
echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg] \
  https://download.docker.com/linux/ubuntu \
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

# Install Docker
sudo apt update && sudo apt install -y \
  docker-ce docker-ce-cli containerd.io docker-compose-plugin

# Add current user to docker group
sudo usermod -aG docker $USER
```

Attention – Après `usermod`, fermez la session SSH (`exit`) et reconnectez-vous, ou tapez `newgrp docker`.

Vérifier : `docker --version && docker compose version`

C.3 Lancer Vaultwarden

```
# Create data directory
sudo mkdir -p /vw-data

# Launch Vaultwarden container
docker run -d --name vaultwarden \
  -e SIGNUPS_ALLOWED=true \
  -v /vw-data/:/data/ \
  -p 127.0.0.1:8080:80 \
  --restart unless-stopped \
  vaultwarden/server:latest
```

Pourquoi cette étape ? `127.0.0.1:8080` signifie que le conteneur n'écoute qu'en local. Nginx (étape C.6) servira de point d'entrée HTTPS sécurisé vers l'extérieur.

Vérifier : `docker ps`

C.4 Configurer le DNS (sous-domaine)

Dans le panneau de votre hébergeur (Hostinger, OVH...) :

1. Aller dans **DNS / Zone DNS** du domaine
2. Ajouter un enregistrement **A** :
   - **Nom** : `vault`

- **Type** : A
- **Valeur** : IP du VPS
- **TTL** : 3600

Vérifier : `dig +short vault.tondomaine.fr`

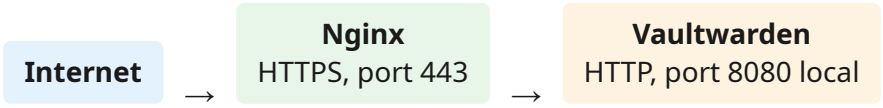
C.5 Ouvrir les ports du pare-feu

```
sudo ufw allow OpenSSH       # port 22
sudo ufw allow 80            # HTTP (Certbot)
sudo ufw allow 443           # HTTPS
sudo ufw enable
sudo ufw status
```

Si `ufw` est absent : vérifiez le pare-feu dans le panneau de l'hébergeur (ports 80 et 443 en entrée).

C.6 Nginx proxy inverse + HTTPS

Nginx (« engine-x ») sert de proxy inverse : il reçoit les requêtes internet et les transmet à Vaultwarden. **Certbot** obtient les certificats SSL gratuits (Let's Encrypt) pour le HTTPS.



Installer et configurer

```
sudo apt install -y nginx certbot python3-certbot-nginx
sudo nano /etc/nginx/sites-available/vaultwarden
```

Contenu du fichier (remplacer `vault.tondomaine.fr`) :

```
server {
    listen 80;
    server_name vault.tondomaine.fr;

    location / {
        proxy_pass http://127.0.0.1:8080;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}
```

```
sudo ln -s /etc/nginx/sites-available/vaultwarden /etc/nginx/sites-enabled/
sudo nginx -t && sudo systemctl reload nginx
```

Obtenir le certificat HTTPS

```
sudo certbot --nginx -d vault.tondomaine.fr
```

Attention – Erreur « délai dépassé » ? Le port 80 est bloqué. Revenez à l'étape C.5.

Configuration Nginx finale (référence)

```
server {
    listen 443 ssl http2;
    server_name vault.tondomaine.fr;

    ssl_certificate /etc/letsencrypt/live/vault.tondomaine.fr/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/vault.tondomaine.fr/privkey.pem;

    add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
    add_header X-Frame-Options "SAMEORIGIN" always;
    add_header X-Content-Type-Options "nosniff" always;

    # WebSocket support (Bitwarden real-time notifications)
    location /notifications/hub {
        proxy_pass http://127.0.0.1:8080;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
        proxy_set_header Host $host;
    }

    location / {
        proxy_pass http://127.0.0.1:8080;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        client_max_body_size 128M;
    }
}

server {
    listen 80;
    server_name vault.tondomaine.fr;
    return 301 https://$host$request_uri;
}
```

C.7 Créer le compte et désactiver les inscriptions

1. Ouvrir `https://vault.tondomaine.fr` dans le navigateur
2. Cliquer sur **Créer un compte** et remplir les champs

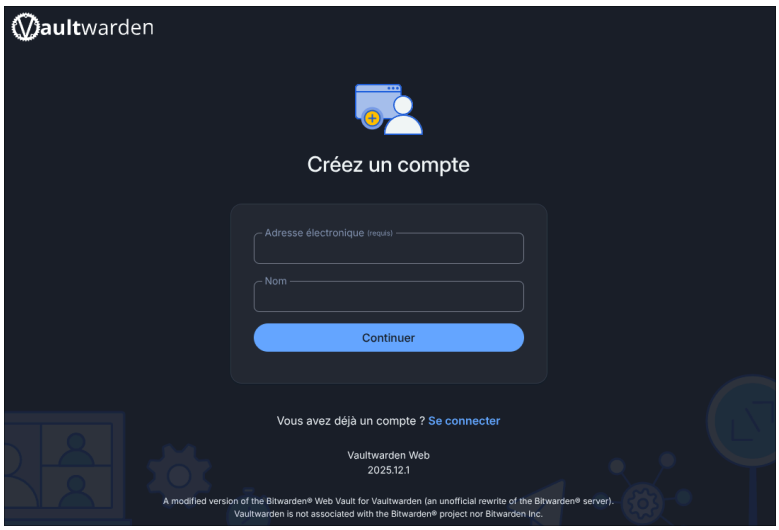


Fig. 5. – Vaultwarden – page de création de compte

3. Choisir un **mot de passe maître solide** (généré via KeePassXC, cf. B.2)

Puis **sur le VPS**, désactiver les inscriptions :

```
docker stop vaultwarden && docker rm vaultwarden

docker run -d --name vaultwarden \
  -e SIGNUPS_ALLOWED=false \
  -v /vw-data/:/data/ \
  -p 127.0.0.1:8080:80 \
  --restart unless-stopped \
  vaultwarden/server:latest
```

`docker rm` supprime le conteneur, pas les données (`/vw-data/`).

C.8 Stocker le mot de passe maître Bitwarden dans KeePassXC

Champ	Valeur
Groupe	Infrastructure critique
Titre	Vaultwarden – mot de passe maître
Nom d'utilisateur	(adresse courriel du compte)
Mot de passe	(le mot de passe maître Bitwarden)
URL	https://vault.tondomaine.fr

C.9 Activer le 2FA sur Vaultwarden

1. Se connecter à `https://vault.tondomaine.fr`
2. **Paramètres** > **Sécurité** > **Authentification à deux facteurs**
3. Choisir **Application d'authentification**
4. Scanner le QR code avec Aegis ou ente Auth
5. Entrer le code à 6 chiffres pour confirmer
6. Copier le **code de récupération**

Stocker le code de récupération dans KeePassXC (groupe « Codes de secours 2FA », entrée dédiée séparée du mot de passe maître).

C.10 Sauvegardes automatiques

```
sudo apt install -y sqlite3
sudo mkdir -p /opt/vaultwarden
sudo nano /opt/vaultwarden/backup_vaultwarden.sh
```

Contenu du script :

```
#!/usr/bin/env bash
set -euo pipefail

BACKUP_DIR="/opt/vaultwarden/backups"
DATA_DIR="/vw-data"
DATE=$(date +%Y%m%d_%H%M%S)

mkdir -p "$BACKUP_DIR"

# Backup SQLite database (with lock)
```

```
sqlite3 "$DATA_DIR/db.sqlite3" ".backup '$BACKUP_DIR/db_$DATE.sqlite3'"

# Backup attachments and configuration
tar czf "$BACKUP_DIR/data_$DATE.tar.gz" \
  -C "$DATA_DIR" \
  attachments/ sends/ config.json rsa_key* 2>/dev/null || true

# Keep only the 7 most recent backups
ls -t "$BACKUP_DIR"/db_*.sqlite3 | tail -n +8 | xargs rm -f
ls -t "$BACKUP_DIR"/data_*.tar.gz | tail -n +8 | xargs rm -f

echo "Backup completed: $DATE"
```

```
sudo chmod 755 /opt/vaultwarden/backup_vaultwarden.sh

# Add to crontab (daily at 3 AM):
sudo crontab -e
# 0 3 * * * /opt/vaultwarden/backup_vaultwarden.sh >> /var/log/vaultwarden-backup.log 2>&1
```

C.11 Mise à jour de Vaultwarden

```
# 1. Backup before update
/opt/vaultwarden/backup_vaultwarden.sh

# 2. Pull latest image
docker pull vaultwarden/server:latest

# 3. Stop and remove container
docker stop vaultwarden && docker rm vaultwarden

# 4. Relaunch with updated image
docker run -d --name vaultwarden \
  -e SIGNUPS_ALLOWED=false \
  -v /vw-data/:/data/ \
  -p 127.0.0.1:8080:80 \
  --restart unless-stopped \
  vaultwarden/server:latest

# 5. Verify
docker ps | grep vaultwarden
curl -s https://vault.tondomaine.fr/alive
```

Phase D – Configuration des clients Bitwarden

D.1 Extension navigateur

1. Installer l'extension **Bitwarden** depuis le magasin d'extensions de votre navigateur (Chrome Web Store, Firefox Add-ons, etc.)
2. Cliquer sur l'icône Bitwarden > engrenage (paramètres)
3. Si auto-hébergé : renseigner l'**URL du serveur** : `https://vault.tondomaine.fr`
4. Enregistrer et se connecter

Client	Configuration
Application bureau	Champ « URL du serveur » sur l'écran de connexion
Mobile	Paramètres > URL du serveur avant de se connecter

D.2 Réglages recommandés

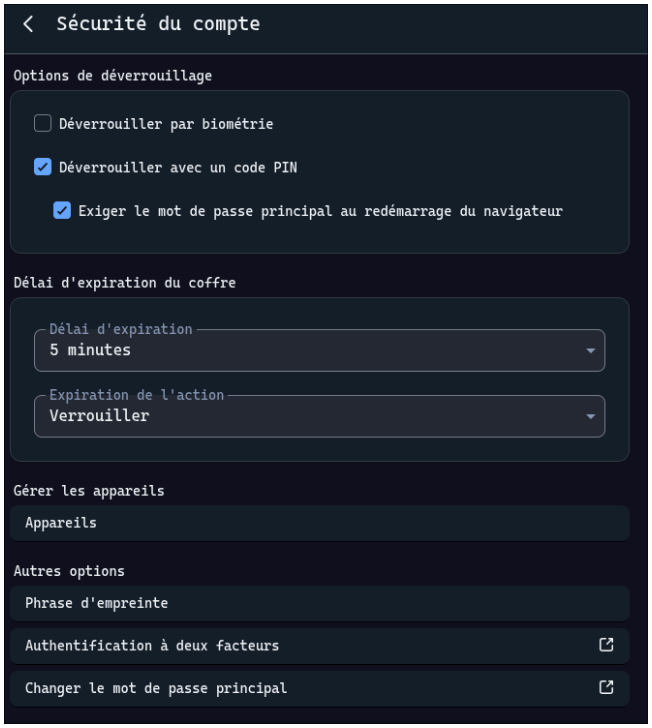


Fig. 6. – Bitwarden – sécurité du compte et options de déverrouillage

Pourquoi cette étape ? On est pas des terroristes, le déverrouillage par biométrie (empreinte digitale, Face ID) ou par code PIN est acceptable pour Bitwarden au quotidien, à condition que le code PIN ait une entropie suffisante (6+ chiffres) et soit unique à cet usage. Le coffre est déjà protégé par le mot de passe maître au premier déverrouillage de la session ; le PIN ou la biométrie ne servent qu'à le déverrouiller ensuite sans le retaper. On n'est pas dans un modèle de menace extrême – il s'agit de trouver un équilibre entre sécurité et ergonomie au quotidien.

D.3 Structure des dossiers Bitwarden

Dossier	Entrées typiques
Infrastructure	Hébergeur VPS, GitHub…
Courriel et identité	Google Perso, Proton Mail…
Travail	Outils pro
Dev et IA	Claude/Anthropic, OpenAI…
Finance et banque	Banques, PayPal, TradingView…
Crypto / Web3	Hyperliquid, Rabby Wallet, Keplr, Phantom…
Achats en ligne	Leboncoin, Vinted, Amazon…
Réseaux sociaux	X/Twitter, Discord, Telegram, Meta…
Voyage et transport	SNCF Connect, Air France, Airbnb…
Santé et sport	Mutuelle, Garmin, Strava…
Énergie et services	Engie, EDF…
Divertissement	TV Time, PSN, Netflix, Amazon Prime…
VPN (pas de mdp)	Mullvad – numéro de compte uniquement

D.4 Fiches de référence des entrées

Conventions de nommage

- **Format du titre** : `Service -- Précision` (ex : `Google -- Perso`)
- **URL** : toujours la page de connexion, pas la page d'accueil
- **Mot de passe** : unique par entrée, généré via Bitwarden (20+ caractères)
- **Champs personnalisés** : numéros de compte, codes client

Tableau de référence non exhaustif

Pour chaque entrée, le mot de passe est généré par Bitwarden et le dossier correspond à la catégorie indiquée. Ces champs ne sont pas répétés.

Dossier	Titre	ID	URL	Notes
Infra.	Hostinger – Panneau	courriel	hostinger.fr/cpanel-login	Offre : KVM2
Infra.	GitHub	pseudo	github.com/login	2FA activé
Courriel	Google – Perso	courriel	accounts.google.com/signin	Compte principal
Dev / IA	Claude – Anthropic	courriel	console.anthropic.com/login	–
Finance	Société Générale	n. client	particuliers.sg.fr	Champ perso.
Finance	PayPal	courriel	paypal.com/signin	2FA activé
Crypto	Rabby Wallet	(vide)	rabby.io	Mdp extension
VPN	Mullvad	(vide)	mullvad.net/account	Champ perso.

Le mot de passe root du VPS n'est **pas** dans Bitwarden – il est dans KeePassXC (cf. B.5). Mullvad n'utilise pas de mot de passe (numéro de compte uniquement).

Phase E – Migration des secrets

E.1 Migrer les mots de passe dans Bitwarden

Pour chaque compte web :

1. Se connecter au service
2. Changer le mot de passe pour un nouveau généré par Bitwarden (20+ caractères) – passez de préférence par l'extension plutôt que l'auto-remplissage
3. Bitwarden propose automatiquement de sauvegarder l'identifiant
4. Classer dans le bon dossier (cf. D.3)
5. Activer le 2FA si disponible (code de récupération dans KeePassXC)

Commencez par les 5 comptes les plus importants : courriel principal, banque, réseaux sociaux. Puis migrez les autres au fil de vos connexions.

E.2 Migrer codes de récupération et clés dans KeePassXC

> **Attention** – Les **seeds crypto** ne vont PAS dans KeePassXC. Ils sont exclusivement stockés sur support physique (plaque métal ou papier). Cf. Phase F pour la procédure de sauvegarde physique.

Seuls les **codes de récupération** et les **clés** (SSH, certificats) sont migrés dans KeePassXC.

Pour chaque code de récupération ou clé en clair sur le disque :

1. Copier dans KeePassXC (dans le groupe correspondant)
2. Si le fichier traînait en clair, ajouter dans les notes :
   `COMPROMIS - à regénérer - trouvé en clair le YYYY-MM-DD`
3. Supprimer le fichier source de manière sécurisée (voir ci-dessous)

Suppression sécurisée

Windows

Méthode GUI : Eraser

1. Télécharger **Eraser** depuis eraser.heidi.ie
2. Installer et lancer
3. Clic droit sur le fichier sensible dans l'Explorateur > **Eraser** > **Erase**
4. Eraser écrase le fichier plusieurs fois avant de le supprimer

Méthode CLI : SDelete

Télécharger **SDelete** depuis Sysinternals (Microsoft) :

```
sdelete -p 3 fichier_sensible.txt
```

Cas des SSD

Les SSD gèrent la suppression différemment (nivellement d'usure). Après suppression, exécuter dans un PowerShell administrateur :

```
Optimize-Volume -DriveLetter C -ReTrim
```

macOS

Depuis macOS Catalina, la commande `srm` a été supprimée car APFS rend la suppression sécurisée peu fiable sur SSD.

Alternative GUI : Permanent Eraser

Télécharger **Permanent Eraser** (application gratuite) et glisser les fichiers sensibles dessus.

Recommandation

Pour les fichiers sensibles sur macOS, la meilleure approche est d'utiliser un volume chiffré dès le départ (FileVault ou volume APFS chiffré). La gestion TRIM est automatique sur macOS.

Linux

```
# Securely overwrite and delete (3 passes + zero fill)
shred -vfz -n 3 fichier_sensible.txt
```

Options : `-v` verbeux, `-f` force, `-z` remplit de zéros, `-n 3` trois passes.

Cas des SSD

`shred` fonctionne sur ext4 mais n'est **pas garanti** sur les SSD (nivellement d'usure). Après `shred` sur SSD :

```
sudo fstrim -v /
```

Cas particulier : seeds crypto en clair sur le disque

Si vous trouvez une seed en clair sur le disque :

1. Le transcrire **directement sur support physique** (plaque métal ou papier, cf. Phase F)
2. Supprimer le fichier numérique avec la méthode de suppression sécurisée de votre OS
3. Considérer la seed comme potentiellement compromise (créer un nouveau portefeuille et transférer les fonds si le montant le justifie)

Phase F – Couche physique

La couche physique est la sauvegarde ultime : elle ne dépend d'aucun appareil électronique et résiste au feu, à l'eau et au temps. Elle concerne exclusivement les **seeds crypto** et la **passphrase maître KeePassXC**.

La préparation de la clé USB chiffrée et les sauvegardes KeePassXC sont traitées en Phase B (cf. B.6, B.7, B.8).

F.1 OneKey KeyTag – présentation

Le OneKey KeyTag est une plaque en acier inoxydable conçue pour sauvegarder des seeds crypto. Elle est composée de cases correspondant aux mots de la liste BIP-39.

Des alternatives existent : **Cryptosteel Capsule**, **Billfodl**, ou tout support en acier inoxydable compatible BIP-39.

Propriétés :

- Acier inoxydable (résiste au feu jusqu'à 1500 °C)
- Résistant à l'eau et à la corrosion
- Aucune dépendance électronique
- Compact et discret

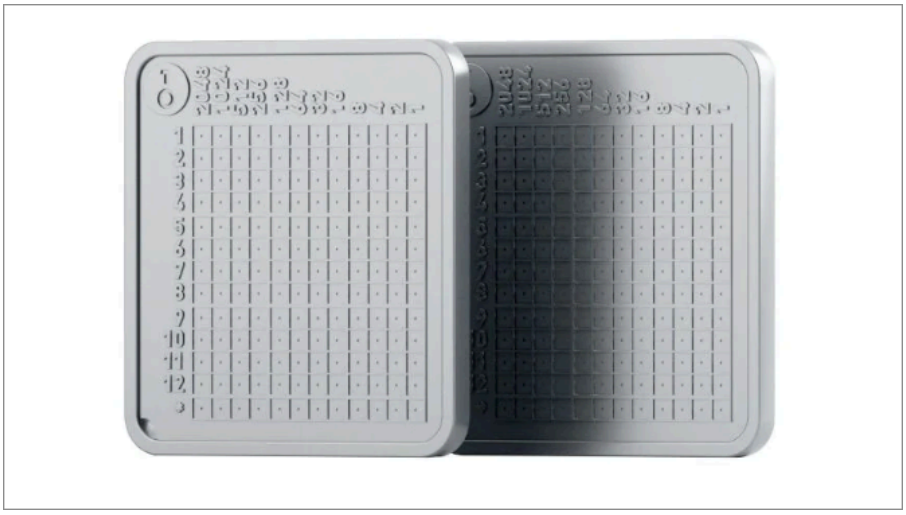


Fig. 7. – OneKey KeyTag – plaque vierge

F.2 Encodage BIP-39 en binaire

La liste BIP-39 contient 2048 mots, numérotés de 0 à 2047. Chaque mot correspond à un nombre représentable en 11 bits ($2^{11} = 2048$).

Principe

1. Trouver le numéro du mot dans la liste BIP-39 (disponible sur github.com/bitcoin/bips)
2. Convertir ce numéro en binaire sur 11 bits
3. Poinçonner les cases correspondantes sur la plaque (1 = poinçon, 0 = vide)

Exemples

Mot	Numéro BIP-39	Binaire (11 bits)
abandon	0	000 0000 0000

Mot	Numéro BIP-39	Binaire (11 bits)
ability	1	000 0000 0001
voltage	1934	111 1000 1110
zoo	2047	111 1111 1111

Procédure de gravure

1. Noter votre seed sur papier (en clair, temporairement)
2. Pour chaque mot, trouver son numéro dans la liste BIP-39
3. Convertir en binaire sur 11 bits
4. Poinçonner les cases correspondantes sur la plaque
5. **Vérifier** en décodant la plaque pour retrouver les mots originaux
6. Détruire le papier intermédiaire de manière sécurisée

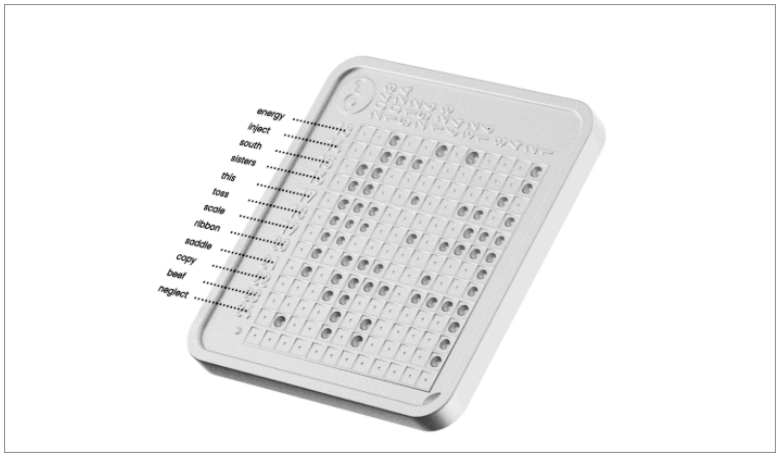


Fig. 8. – OneKey KeyTag – plaque poinçonnée (valeurs fictives)

Attention – Décodez la plaque immédiatement après la gravure pour confirmer que chaque mot est correct. Une erreur de poinçon est irréversible.

F.3 Stockage physique – séparation des lieux

- La plaque métal est conservée dans un **lieu différent du domicile** (coffre bancaire, domicile d'un proche de confiance, etc.)
- Ne jamais photographier la plaque
- Ne jamais la stocker au même endroit que l'ordinateur ou la clé USB

Pourquoi cette étape ? Si un cambrioleur accède à votre domicile, il peut trouver l'ordinateur et la clé USB, mais pas la plaque métal. Chaque couche est physiquement séparée.

F.4 Split de seed (optionnel, gros patrimoines crypto)

Pour ceux qui détiennent des montants significatifs en crypto, le stockage d'un seed complet dans un seul lieu représente un risque : vol, coercition (on vous force à révéler la seed), catastrophe naturelle.

Shamir’s Secret Sharing (SSS)

Le principe : diviser la seed en N parts, dont M sont nécessaires pour la reconstituer (schéma M-sur-N).

Exemple : 3 parts, 2 nécessaires. Chaque part est stockée dans un lieu différent. Aucune part seule ne permet de reconstituer la seed.

Découpage manuel (alternative simple)

Pour une seed de 24 mots :

- Part A : mots 1 à 16
- Part B : mots 9 à 24
- Part C : mots 1 à 8 + mots 17 à 24

Chaque part couvre 16 mots. Il en faut 2 sur 3 pour reconstituer les 24 mots.

Ce niveau de protection est réservé aux patrimoines crypto significatifs. Pour la plupart des utilisateurs, une seule plaque métal dans un lieu sécurisé suffit.

Phase G – Bonnes pratiques

G.1 Mots de passe générés

- Longueur minimum : **20 caractères**
- Inclure : majuscules, minuscules, chiffres, symboles
- Un mot de passe unique par service, sans exception
- Pour les mots de passe principaux : méthode diceware (cf. B.2)

G.2 2FA (double authentification)

- Activer sur **tous** les comptes qui le proposent
- Application TOTP recommandée : **Aegis** (Android) ou **ente Auth**
- Codes de récupération dans KeePassXC (groupe « Codes de secours 2FA »)
- **Éviter les SMS** (vulnérable à l'échange de carte SIM)
- Ne pas stocker les TOTP dans Bitwarden (séparation des facteurs)

G.3 Vérification des fuites

- Vérifier régulièrement sur Have I Been Pwned
- Bitwarden : coffre web > Outils > Rapports (exposés, réutilisés, faibles)
- Changer immédiatement tout mot de passe compromis

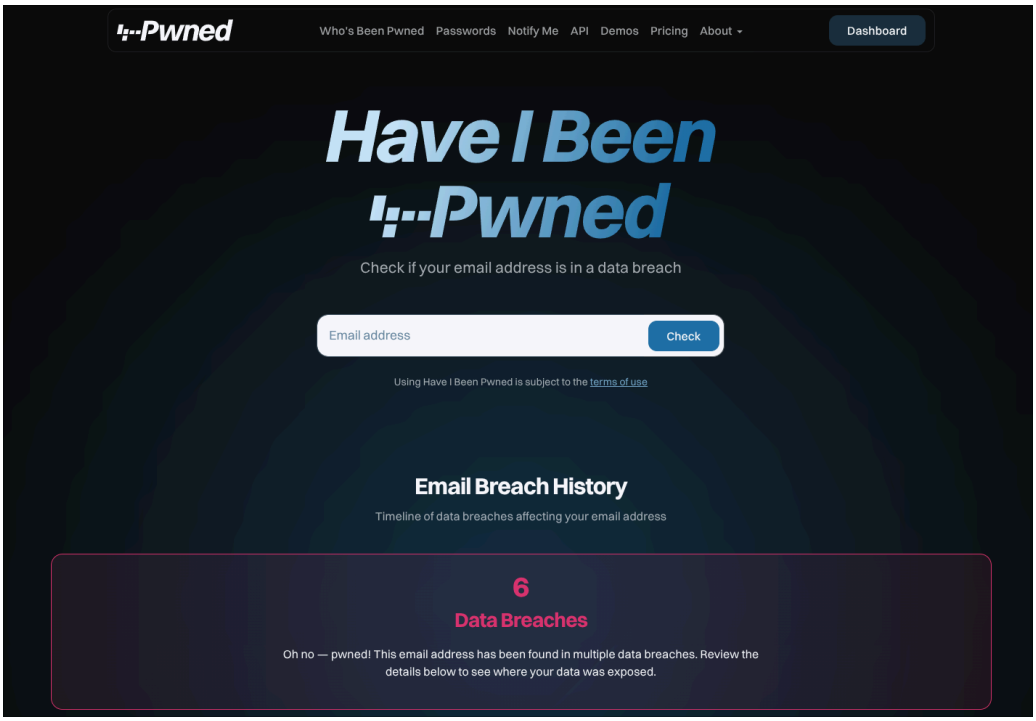


Fig. 9. – Have I Been Pwned – Exemple des fuites de données de mon ancienne adresse mail

G.4 Politique de rotation

Type de secret	Fréquence de rotation
Mots de passe web compromis	Immédiatement
Mot de passe principal Bitwarden	Annuellement ou si suspicion
Mot de passe principal KeePassXC	Annuellement ou si suspicion
Mot de passe root VPS	Annuellement
Clés SSH	Tous les 2 ans ou si compromission
Seeds crypto	Jamais (créer un nouveau portefeuille et transférer)

G.5 Seeds crypto – pourquoi les séparer

Les seeds crypto sont **irréversibles**. Une seed compromise = fonds perdus définitivement. Aucun support client, aucun recours.

Règles :

- **Jamais en cloud** (pas dans Bitwarden, pas dans Google Drive, pas dans un courriel)
- **Jamais en photo** (pas de capture d'écran, pas de numérisation)
- **Jamais dans KeePassXC** – les seeds vont exclusivement sur support physique (plaque métal, cf. Phase F)
- KeePassXC ne stocke que les **codes de récupération** et **clés** associés aux comptes crypto

> **En résumé** – Les seeds ne doivent exister que sur un support physique (plaque métal ou papier) stocké hors du domicile. Consultez la Phase F pour la procédure complète de sauvegarde physique.

G.6 Scénario « J'ai perdu mon PC »

1. **Bitwarden** : se connecter depuis n'importe quel appareil sur `https://vault.tondomaine.fr`
2. **KeePassXC** : brancher la clé USB chiffrée, déchiffrer (même mot de passe maître), ouvrir le `.kdbx`
3. **Seeds crypto** : récupérer depuis la sauvegarde physique (plaque métal, cf. Phase F)
4. **VPS** : SSH depuis n'importe quel terminal (mot de passe root dans KeePassXC)
5. **Ordre de récupération** : KeePassXC (clé USB) > VPS (root) > Vaultwarden > tous les autres comptes

Annexe A – YubiKey : authentification matérielle (optionnel)

Une **YubiKey** est une clé USB physique d'authentification qui remplace ou complète les codes TOTP comme second facteur (2FA).

Fig. 10. – YubiKey 5 NFC

Avantages : résistant à l'hameçonnage, pas de code à taper, pas de batterie, secret cryptographique non copiable.
Inconvénients : coût (50-70 EUR), il faut deux clés, pas universel.

Modèle	Port	NFC	Usage
YubiKey 5 NFC	USB-A	Oui	Bureau + téléphone
YubiKey 5C NFC	USB-C	Oui	Portable + téléphone
YubiKey 5Ci	USB-C + Lightning	Non	Apple

Acheter **2 clés identiques** : une au quotidien, une de secours.

A.1 Installation de YubiKey Manager

Windows

1. Aller sur yubico.com/support/download
2. Télécharger **YubiKey Manager** pour Windows
3. Installer et lancer
4. L'interface graphique est identique sur les 3 OS

macOS

1. `brew install ykman` (via Homebrew)
2. Ou télécharger depuis yubico.com
3. L'interface graphique est identique sur les 3 OS

Linux

```
# Arch Linux
sudo pacman -S yubikey-manager

# Debian / Ubuntu
sudo apt install yubikey-manager
```

Vérifier : `ykman info`

A.2 Configuration avec Vaultwarden

1. Se connecter à `https://vault.tondomaine.fr`
2. **Paramètres** > **Sécurité** > **Authentification à deux facteurs**
3. Choisir **WebAuthn** (pas « Yubico OTP »)
4. Insérer la YubiKey, toucher le bouton quand demandé
5. Nommer la clé, **répéter avec la deuxième clé**
6. **Sauvegarder le code de récupération** dans KeePassXC

A.3 Configuration avec KeePassXC

KeePassXC supporte les YubiKey en mode **défi-réponse** (challenge-response).

1. Ouvrir **YubiKey Manager** > onglet **OTP** > **Configure** slot 2
2. Choisir **HMAC-SHA1 Challenge-Response**
3. Cocher **Require touch**
4. Cliquer sur **Generate** puis **Finish**
5. Dans KeePassXC : **Base de données** > **Paramètres** > **Sécurité** > **Ajouter une protection supplémentaire** > **Défi-réponse** > sélectionner emplacement 2

Alternative CLI

```
# Verify the key is detected
ykman info

# Configure slot 2 for HMAC-SHA1 challenge-response
ykman otp chalresp --touch --generate 2
```

Attention – Configurez la deuxième clé avec le même secret HMAC-SHA1 : `ykman otp chalresp --touch 2 <secret_hex>`

A.4 Autres services compatibles

Service	Configuration
Google	Paramètres > Sécurité > Vérification en 2 étapes > Clé de sécurité
GitHub	Paramètres > Authentification > Clés de sécurité
Proton Mail	Paramètres > Sécurité > Clé de sécurité
Microsoft	Sécurité > Options de sécurité avancées
X/Twitter	Paramètres > Sécurité > 2FA

A.5 Procédure en cas de perte

1. Utiliser la **clé de secours** pour se connecter
2. Supprimer la clé perdue de tous les services
3. Acheter une nouvelle clé, l'enregistrer partout
4. La nouvelle clé devient la clé de secours

Si les deux clés sont perdues : utiliser les **codes de récupération** stockés dans KeePassXC.

Annexe B – Dépannage

Problèmes communs (tous OS)

Problème	Solution
`permission denied` avec `mkdir` sur le VPS	Utiliser `sudo`
`docker: command not found`	Refaire l'étape C.2
`docker ps` sans `sudo` ne fonctionne pas	`newgrp docker` ou se reconnecter en SSH
Page Vaultwarden inaccessible	`sudo systemctl status nginx`
Erreur HTTPS / pas de cadenas	`sudo certbot certificates`
Certbot « délai dépassé »	Port 80 bloqué – vérifier ufw + pare-feu hébergeur (cf. C.5)
Impossible de créer un compte	`SIGNUPS_ALLOWED` est `false` (cf. C.7)
Connexion Bitwarden échoue en HTTP	HTTPS obligatoire – configurer Nginx + Certbot (cf. C.6)
Certbot échoue à vérifier le domaine	`dig +short vault.tondomaine.fr` (cf. C.4)
Extension Bitwarden ne se connecte pas	Vérifier URL (avec `https://`), `docker ps`, `nginx -t`
YubiKey non détectée	Vérifier `lsusb` ou Gestionnaire de périphériques, installer les pilotes

Problèmes spécifiques par OS

Windows

KeePassXC ne démarre pas
Vérifier que **Visual C++ Redistributable** est installé (télécharger depuis microsoft.com).

BitLocker non disponible
BitLocker n'est pas inclus dans Windows Home. Utiliser **VeraCrypt** comme alternative (veracrypt.fr).

SSH « command not found »
OpenSSH n'est pas activé par défaut sur certaines installations :

1. **Paramètres** > **Applications** > **Fonctionnalités facultatives**

macOS

KeePassXC bloqué par Gatekeeper
Clic droit sur KeePassXC.app > **Ouvrir** (et non double-clic). macOS demande confirmation, cliquer sur **Ouvrir**.

« Operation not permitted »

1. **Préférences Système** > **Confidentialité et sécurité** > **Accès complet au disque**
2. Ajouter le Terminal ou KeePassXC

Volume chiffré non monté
Ouvrir **Utilitaire de disque** > sélectionner le volume > **Monter**. Si le mot de passe

Linux

KeePassXC sous Wayland (Hyprland, Sway…)
Si KeePassXC refuse de démarrer ou affiche des artefacts :

```
# Option 1: force native Wayland
QT_QPA_PLATFORM=wayland keepassxc

# Option 2: force XWayland
QT_QPA_PLATFORM=xcb keepassxc
```

Rendre permanent via une règle `windowrulev2` dans la configuration Hyprland.

2. Cliquer sur **Ajouter une fonctionnalité**
3. Rechercher **Client OpenSSH** > **Installer**

Docker Desktop ne démarre pas
Vérifier que la virtualisation (Hyper-V ou WSL 2) est activée dans le BIOS/UEFI.

est demandé, l'entrer manuellement.

Homebrew non installé
Installer Homebrew :

```
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

Erreur « The name is not activatable » (LUKS via Nautilus)
Cause : Nautilus tente de sauvegarder la passphrase LUKS dans le trousseau GNOME, absent sous Hyprland.

Impact : aucun. La clé se déverrouille correctement malgré le message.

Recommandation : ignorer l'erreur. Ne pas installer `gnome-keyring` – cela évite que la passphrase LUKS soit sauvegardée en clair dans le trousseau.

Clé USB LUKS non détectée

```
lsblk
dmesg | tail -20
sudo cryptsetup open /dev/sdb1 usb_chiffree
```

Si « No key available » : vérifier le mot de passe et le périphérique (`/dev/sdb1` vs `/dev/sdb`).

Docker après reboot du VPS

```
sudo systemctl status docker
sudo systemctl start docker && sudo systemctl enable docker
docker ps -a | grep vaultwarden   # If "Exited": docker start vaultwarden
```

En résumé – La plupart des problèmes se résolvent en vérifiant : permissions, services (`systemctl` / Gestionnaire de services), connectivité (ports/pare-feu) et chemins. Consultez `docker logs`, `journalctl` ou l'Observateur d'événements Windows pour les détails.