

08_Claude et la sécurité digitale du jux's univers

- [1 - la prise en main sur Bitwarden](#)
- [2 - sauvegarde et récupération de l'accès au coffre](#)

1 - la prise en main sur Bitwarden

Relevé et suivi des passkeys du Jux's univers. Cette page a deux fonctions : conserver l'état du **coffre Bitwarden**, et servir de **fiche de relevé** pour ce que chaque service a réellement enregistré de son côté. C'est la confrontation des deux qui fait apparaître les *credentials orphelins*.

“ **Pourquoi les deux moitiés sont nécessaires.** Il n'existe aucun registre central des passkeys. Le coffre ne connaît que ce qu'il stocke lui-même ; la liste qui fait autorité est détenue par chaque service. Supprimer une passkey dans Bitwarden ne la révoque pas côté serveur, et l'inverse est vrai aussi.

1. État du coffre — relevé du 2026-08-25

14 passkeys, obtenues par `bw list items` (voir § 4).

Domaine (rpId)	Élément	Identifiant	Créée le
amazon.fr	amazon.fr	jubertrand@gmail.com	2025-02-14
auth.monidentifiant.sncf	monidentifiant.sncf	nexte@ik.me	2026-01-15
aws.amazon.com	signin.aws.amazon.com	arn:aws:iam::712353451166:root	2024-12-17
google.com	accounts.google.com	bertrand.dadone@gmail.com	2024-07-07
google.com	accounts.google.com	jubertrand@gmail.com	2024-03-15
google.com	accounts.google.com	nexte.urbanisme@gmail.com	2024-02-01
juxjux.synology.me	juxjux.synology.me	juxjux	2026-01-09
login.eau.veolia.fr	login.eau.veolia.fr	jubertrand@gmail.com	2024-09-18
login.microsoft.com	outlook.live.com	julien.bertrand@live.fr	2025-07-29

Domaine (rpId)	Élément	Identifiant	Créée le
login.nvgs.nvidia.com	login.nvgs.nvidia.com	juxjux@yahoo.com	2026-08-19
nextcloud.juxjux.ovh	nextcloud.juxjux.ovh	julien	2025-12-10
vault.bitwarden.com	vault.bitwarden.com	julien.bertrand@ik.me	2024-01-16
www.dropbox.com	dropbox.com	nexte@ik.me	2026-01-16
www.paypal.com	paypal.com	julien.bertrand@laposte.net	2026-04-04

10 identités distinctes pour 14 passkeys. Les trois lignes `google.com` ne sont **pas** des doublons : ce sont trois comptes Google différents — le script les signale comme doublons, c'est un faux positif connu.

2. Fiche de relevé côté services

Tableau à compléter au fil des visites. Une ligne par domaine. La colonne **Identifiants côté service** se remplit avec ce que la page de sécurité du service affiche réellement, séparé par des virgules — c'est elle que le script compare au coffre. Laisser `Relevé le` vide tant que la vérification n'a pas été faite.

#	Domaine (rpId)	URL de vérification	Identifiants côté service	Relevé le	Action
1	login.microsoft.com	account.microsoft.com → Sécurité → Options de connexion avancées			
2	aws.amazon.com	Console AWS → IAM → Identifiants de sécurité (compte racine)			
3	google.com	passwords.google.com → Passkeys (les 3 comptes)			
4	www.paypal.com	paypal.com → Paramètres → Sécurité			
5	www.dropbox.com	dropbox.com → Paramètres → Sécurité			

#	Domaine (rpId)	URL de vérification	Identifiants côté service	Relevé le	Action
6	juxjux.synology.me	DSM → Personnel → Compte → Sécurité			
7	amazon.fr	amazon.fr → Connexion et sécurité			
8	auth.monidentifiant.sncf	monidentifiant.sncf → Sécurité			
9	login.eau.veolia.fr	eau.veolia.fr → Mon compte			
10	login.nvgs.nvidia.com	nvidia.com → Mon compte → Sécurité			
11	vault.bitwarden.com	vault.bitwarden.com → Paramètres → Sécurité			
12	nextcloud.juxjux.ovh	service démonté — voir § 3	—	2026-08-25	Supprimer du coffre

Sources hors coffre, à ne pas oublier

Ces emplacements peuvent contenir des passkeys **absentes du coffre** — typiquement celles créées directement sur le téléphone.

Emplacement	Où regarder	Relevé le
Google Password Manager	passwords.google.com → Passkeys (par compte)	
Android — S23 / Xiaomi	myaccount.google.com → Sécurité → Vos appareils	
Windows Hello	<i>néant sur ce poste : aucun TPM, voir § 3</i>	2026-08-25
Clés USB FIDO2	Windows → Paramètres → Comptes → Clés de sécurité	

3. Points d'attention

Compte racine AWS — le plus critique. `arn:aws:iam::712353451166:root`, passkey du 17/12/2024. Un compte racine AWS peut tout faire, y compris fermer le compte et changer le

moyen de paiement. Deux questions ouvertes : le compte est-il encore utilisé, et cette passkey est-elle son **seul** facteur MFA ? Si oui, sa perte coupe l'accès à un compte susceptible d'accumuler de la facturation. C'est le seul cas de la liste justifiant une **clé USB FIDO2 de secours**.

Dépendance circulaire Bitwarden. La passkey `vault.bitwarden.com` est stockée dans Bitwarden : elle sert à ouvrir le coffre qui la contient. Sans conséquence tant que la connexion par mot de passe maître reste active — mais un passage du coffre en « passkey uniquement » enfermerait dehors. À laisser en l'état en le sachant, ou à déplacer sur le téléphone.

`nextcloud.juxjux.ovh` — **orphelin confirmé le 2026-08-25**. Le vhost subsiste dans `/etc/nginx/sites-enabled/` mais répond **502**, et aucun container Nextcloud ne tourne sur le VPS. La passkey date du 10/12/2025 : le service a été démonté depuis. Sans usage possible, à supprimer du coffre. Le vhost mort est par ailleurs déjà listé au nettoyage, avec `agendav` et `infcloud` — mais **pas radicale**, qui sert en réalité Readeck.

Compte Microsoft et Mobile connecté. La passkey `login.microsoft.com` sur `julien.bertrand@live.fr` existe depuis le 29/07/2025. Un compte Microsoft doté d'une passkey bascule souvent en mode sans mot de passe : lors de l'appairage du téléphone du 2026-08-25, le mot de passe saisi n'était probablement pas « incorrect », il n'était simplement plus le facteur attendu.

Aucun service auto-hébergé ne figure au coffre, hormis le Nextcloud défunt. BookStack, Immich, Readeck, Komga, Gitea restent en mot de passe ou TOTP — le support WebAuthn demeure inégal côté logiciels self-hosted.

Ce poste ne peut pas créer de passkey localement. Aucun TPM détecté (MSI A320M-A PRO, BIOS 1.40 de 2020, Ryzen 5 2600X) : Windows Hello n'a nulle part où protéger une clé. Le fTPM AMD serait activable au BIOS, mais **déconseillé ici** — BIOS antérieur aux AGESA corrigeant les micro-freezes fTPM, sur une machine à l'historique d'instabilité chargé. Passer par le téléphone ou le coffre.

4. Mode opératoire

Prérequis : Node (présent) et la CLI Bitwarden. Le dossier des binaires npm globaux **n'était pas dans le PATH** — correctif du 2026-08-25 :

```
[Environment]::SetEnvironmentVariable('Path',  
[Environment]::GetEnvironmentVariable('Path','User') + ";$env:APPDATA\npm", 'User')
```

Relevé du coffre :

```
npm install -g @bitwarden/cli  
bw login
```

```
$env:BW_SESSION = bw unlock --raw  
bw list items | py -3.12 "D:\Syncthing\Jux_univers\Jux-  
scripts\Passkeys\inventaire_passkeys.py"
```

Le mot de passe maître se tape directement dans la console. Le script n'affiche **aucun secret** : seuls le nom de l'élément, le domaine, l'identifiant et la date de création.

5. Rapprochement automatique

```
bw list items | py -3.12 inventaire_passkeys.py --confronter
```

Le script relit le tableau du § 2 **depuis cette page** (via l'API BookStack) et le compare à la sortie du coffre. Il signale :

- les **orphelins côté service** — enregistrés chez le fournisseur, absents du coffre (typiquement créés sur le téléphone) ;
- les **orphelins côté coffre** — présents dans Bitwarden, plus reconnus par le service (cas `nextcloud.juxjux.ovh`) ;
- les **domaines jamais relevés** — colonne `Relevé le` vide.

Comme pour la veille FreshRSS, le script parse le **HTML** de la page et non son markdown : la configuration continue de fonctionner si la page est un jour rééditée en WYSIWYG.

Script : `Jux-scripts/Passkeys/inventaire_passkeys.py` — *stdlib seule, utilisable sur Windows, Ubuntu et le VPS.*

2 - sauvegarde et récupération de l'accès au coffre

Procédure de sauvegarde de l'accès au coffre Bitwarden. Complète la fiche de relevé des passkeys (page « 1 - la prise en main sur Bitwarden »). **Aucun secret ne figure sur cette page, et aucun ne doit y être ajouté** — voir § 5.

1. Ce qu'il faut sauvegarder, et pourquoi ce n'est pas la passkey

Une passkey stockée dans Bitwarden n'est pas sur un appareil : elle est **dans le coffre**, donc déjà répliquée sur chaque machine connectée et présente dans les sauvegardes serveur de Bitwarden. Elle n'est pas le maillon fragile.

Le maillon fragile est **l'accès au coffre**. Le scénario qui coupe l'accès à Bitwarden coupe aussi l'accès à une passkey Bitwarden, où qu'elle soit dupliquée. Sauvegarder la passkey elle-même ne protégerait donc de rien — et n'est de toute façon pas possible : les passkeys ne figurent pas dans les exports de coffre.

Corollaire : on ne duplique jamais une passkey, **on en enregistre une seconde**. Chaque authenticateur génère sa propre paire de clés, le service en tient la liste. La redondance se joue côté service, pas côté fichier.

À sauvegarder	Où le récupérer	Rôle
Code de récupération	<code>vault.bitwarden.com</code> → Paramètres → Sécurité → Connexion en deux étapes → Voir le code de récupération	Désactive tous les facteurs 2FA. Le document qui rouvre le coffre
Export chiffré du coffre	<code>bw export --format encrypted_json --password <phrase></code>	Les identifiants survivent à une disparition de Bitwarden en tant que service

À sauvegarder	Où le récupérer	Rôle
Graines TOTP	Selon les comptes	Non incluses dans les passkeys, régulièrement oubliées
Inventaire des passkeys	Page 1 du chapitre, ou <code>inventaire_passkeys.py --csv</code>	Savoir quoi reconstruire, compte par compte

2. Le code de récupération ne tourne pas tout seul

Point vérifié dans la documentation Bitwarden le 2026-08-25, et contre-intuitif : **ni le changement de mot de passe maître, ni l'ajout ou le retrait de méthodes de connexion en deux étapes ne modifient le code de récupération**. Il est permanent tant qu'il n'a pas servi.

Le seul mécanisme de rotation documenté est de **l'utiliser** : après usage, un nouveau code est généré. L'opération désactive au passage les méthodes de connexion en deux étapes, qu'il faut ensuite ré-enrôler — et vérifier si la passkey `vault.bitwarden.com` en fait partie, ou si elle relève de la connexion par passkey, qui est un mécanisme distinct.

Conséquence pratique : **ce code se traite comme un document permanent**, pas comme un jeton qu'on pourra régénérer à peu de frais s'il fuit. Sa compromission se répare, mais au prix d'un ré-enrôlement complet du 2FA.

3. Emplacements de conservation

Le vault **Cryptomator** est le bon réceptacle : chiffrement côté client, présent sur le PC `julie` et sur le PC Nexte, avec une copie sur kDrive. Infomaniak ne voit qu'un blob chiffré.

Support	Contenu	Remarque
Papier, rangé physiquement	Code de récupération	Le seul support qui résiste simultanément à la panne de disque, au rançongiciel et à la perte du téléphone
Vault Cryptomator (PC julie, PC Nexte)	Code, export chiffré, graines TOTP, inventaire	Second exemplaire, hors ligne au repos
Copie kDrive du vault	Idem	Exemplaire hors site. La phrase de passe est le seul rempart

Les deux dépendances circulaires à éviter

1. **La phrase de passe Cryptomator ne doit pas être dans Bitwarden.** Sinon la sauvegarde devient inutilisable précisément le jour où elle servirait. Elle doit être mémorisée, ou écrite sur papier hors ligne.
2. **L'accès kDrive ne doit pas dépendre uniquement du coffre,** pour la même raison.

Même logique que la passkey `vault.bitwarden.com` stockée dans Bitwarden, signalée en page 1 : une sauvegarde qui a besoin de ce qu'elle sauvegarde n'est pas une sauvegarde.

4. Si le code est noté sous forme masquée

Un code partiellement substitué — segments remplacés par des références mnémotechniques (dates, numéros de département, lieux liés à des personnes connues) — appelle deux précautions.

Sur la robustesse : masquer deux groupes sur huit laisse les trois quarts du code lisible, et l'espace résiduel se compte en milliers de combinaisons. Le procédé ralentit une lecture opportuniste, il ne résiste pas à quelqu'un qui cible et connaît l'entourage. Ne pas lui prêter plus de solidité qu'il n'en a.

Sur la récupérabilité — le point qui compte le plus : la règle de décodage devient un second secret à ne pas perdre. Le code servira probablement dans plusieurs années, en situation dégradée. Il faudra alors se rappeler quelles personnes, quels lieux, dans quel ordre, et quelle parenthèse est une date plutôt qu'un département. **Un code de récupération qu'on ne sait plus décoder équivaut à ne pas en avoir.**

D'où le principe à respecter : **séparer le code masqué de sa règle de décodage.** Le papier ne porte que la version masquée, la règle vit dans le vault Cryptomator. Les deux ensemble reconstituent, chacun seul ne dit rien — et aucune perte unique n'est fatale.

5. Où ne jamais écrire ces secrets

Pas dans BookStack, ni dans aucun service auto-hébergé. Une page BookStack finit dans la base MariaDB du VPS, dans la sauvegarde nocturne de 2 h, puis dans l'archive 7z uploadée sur kDrive : trois copies supplémentaires, sur des systèmes que le code de récupération est justement censé pouvoir contourner.

Attention aux formats d'export. N'utiliser que `encrypted_json` avec `--password` :

- `csv` et `json` écrivent **tous les mots de passe en clair** — y compris dans les fichiers temporaires de Syncthing et l'historique kDrive si le vault Cryptomator est ouvert au moment de la synchronisation ;
- `encrypted_json` **sans** `--password` chiffre avec la clé de compte Bitwarden : l'archive n'est alors restaurable que sur ce même compte, ce qui la rend inutile dans le scénario où l'on perd le compte. La phrase passée en `--password` doit être distincte du mot de passe maître.

Transcripts Claude Code : ils résident dans `C:\Users\julie\claudio\projects\D--Syncthing-Jux-univers-Claude-pcelio-jux--claudio\*.jsonl`, soit **hors de l'arbre Syncthing** — ils ne se propagent donc ni vers le VPS, ni vers le téléphone, ni vers kDrive. Ils restent néanmoins en clair sur le disque local : ne pas y coller de secret exploitable.

6. Ordre d'exécution

1. Récupérer le **code de récupération** dans l'interface Bitwarden, le porter sur papier, en déposer un second exemplaire dans le vault Cryptomator. (*Fait le 2026-08-25.*)
2. Enregistrer une **seconde passkey Bitwarden sur le téléphone** (Google Password Manager) — casse au passage la dépendance circulaire de la page 1.
3. Produire l'**export chiffré** avec une phrase de passe distincte, le déposer dans le vault.
4. Vérifier que la **phrase Cryptomator n'est pas uniquement dans Bitwarden**.

Seul le point 1 est urgent. Les trois autres peuvent être étalés.

Voir aussi : page 1 du chapitre pour l'inventaire des passkeys et la fiche de relevé côté services.
Script : `Jux-scripts/Passkeys/inventaire_passkeys.py`.