

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.*

Revision #2

Created 2026-08-25 08:03:41 UTC by Julien

Updated 2026-08-25 08:09:27 UTC by Julien