Stratégie de configuration d'OnlyKey Duo

Table des matières

Aperçu général

Ce document décrit une stratégie de sécurité complète pour l'utilisation d'une clé de sécurité matérielle OnlyKey Duo afin de protéger deux gestionnaires de mots de passe (Bitwarden et KeePassXC), l'accès SSH à GitHub et le chiffrement des courriels par GPG. L'objectif est de garantir qu'un ordinateur portable ou un appareil mobile perdu ou volé reste sécurisé, à condition que l'OnlyKey Duo lui-même ne soit pas compromis.

Capacités de l'OnlyKey Duo

L'OnlyKey Duo offre les fonctionnalités suivantes :

- **2 profils** : Profil 1 (principal) et Profil 2 (déni plausible)
- **12 emplacements par profil** : 6 emplacements par page, 2 pages
- **Emplacements de clés ECC/RSA** : Pour les clés privées SSH et les sous-clés GPG
- **Support FIDO2/WebAuthn** : Sécurisé par matériel, prend en charge un nombre illimité d'enregistrements de sites
- **Défi-réponse HMAC-SHA1** : Compatible avec KeePassXC et des outils similaires
- **PIN d'autodestruction** : Efface l'appareil après un nombre configurable de tentatives de PIN incorrectes

---

Correspondance des exigences aux fonctionnalités OnlyKey

Bitwarden

Bitwarden prend en charge **FIDO2/WebAuthn** nativement, ce qui en fait l'intégration la plus simple.

Étapes de configuration :

1. Enregistrer l'OnlyKey Duo comme clé de sécurité FIDO2 dans les paramètres de *Connexion en deux étapes* de Bitwarden.
2. Conserver le mot de passe maître Bitwarden en mémoire (ne jamais le stocker sur l'appareil).
3. Le Duo devient le second facteur obligatoire à chaque connexion.

Résultat sur le plan de la sécurité :

Sur un ordinateur portable ou un téléphone volé, un attaquant ne dispose ni du mot de passe maître ni du Duo physique. L'accès est totalement bloqué.

> Warning
>
> Enregistrer une **clé FIDO2 de secours** (un second OnlyKey ou un autre appareil FIDO2) pour Bitwarden et la conserver hors ligne en lieu sûr. Sans cela, la perte du Duo vous exclut définitivement de Bitwarden.

KeePassXC

KeePassXC prend en charge le **défi-réponse HMAC-SHA1**, que l'OnlyKey Duo fournit en mode compatible YubiKey.

Étapes de configuration :

1. Dans l'application de configuration OnlyKey, affecter un emplacement au **défi-réponse HMAC-SHA1**.
2. Dans KeePassXC, activer *Défi-Réponse* comme facteur de protection supplémentaire de la base de données (dans *Base de données > Sécurité de la base de données*).
3. L'ouverture de la base de données nécessitera désormais à la fois le mot de passe maître et une pression physique sur le Duo.

Résultat sur le plan de la sécurité :

Un ordinateur portable volé contenant le fichier de base de données KeePassXC ne peut pas être ouvert sans la présence du Duo.

> Warning
>
> Le secret de défi-réponse HMAC-SHA1 est stocké sur le Duo et est inclus dans la **sauvegarde chiffrée OnlyKey**. Si le Duo est perdu et qu'aucune sauvegarde n'existe, la base de données KeePassXC devient définitivement inaccessible. Maintenez toujours une sauvegarde à jour.

Accès SSH à GitHub

Deux options sont disponibles. L'option B est recommandée pour GitHub en particulier.

Option A — Stocker la clé privée SSH sur l'OnlyKey

- Charger une clé privée Ed25519 ou NIST P-256 dans l'un des **emplacements de clé ECC** de l'OnlyKey.
- La clé privée n'existe jamais sous forme utilisable dans le système de fichiers de l'ordinateur portable.
- Les opérations SSH sont effectuées par l'OnlyKey ; la clé privée ne peut pas être extraite.
- Configurer `~/.ssh/config` pour utiliser `onlykey-agent` ou l'interface PKCS#11.

Option B — Clé SSH résidente FIDO2 (Recommandée)

- GitHub prend en charge nativement les clés SSH FIDO2 utilisant le type de clé `sk-ssh-ed25519`.
- Générer une clé SSH résidente FIDO2 stockée directement sur le Duo

```
ssh-keygen -t ed25519-sk -O resident -C "github-onlykey"
```

- Téléverser la clé publique résultante sur GitHub comme d'habitude.
- Aucune gestion de clé séparée n'est nécessaire ; le Duo conserve les identifiants.
- La présence physique (pression) est requise pour chaque authentification SSH.

Résultat sur le plan de la sécurité :

Un ordinateur portable volé ne contient aucune clé privée utilisable pour GitHub. L'authentification exige le Duo physique.

GPG / Chiffrement des courriels

L'OnlyKey Duo agit comme une **carte à puce OpenPGP**, contenant les sous-clés GPG pour la signature, le chiffrement et l'authentification.

Étapes de configuration :

1. Générer une clé maître GPG sur une **machine déconnectée d'internet** (jamais sur l'ordinateur portable ou le Duo).
2. Générer trois sous-clés GPG à partir de la clé maître :
    - **[S]** Sous-clé de signature
    - **[E]** Sous-clé de chiffrement
    - **[A]** Sous-clé d'authentification
3. Charger chaque sous-clé dans un **emplacement de clé ECC** sur l'OnlyKey Duo.
4. Exporter et téléverser la clé publique sur un serveur de clés ou la partager directement.
5. Les opérations GPG (signature, déchiffrement) nécessitent désormais la présence et la pression du Duo.

> Important
>
> La **clé de certification maître GPG** doit rester en stockage froid (machine déconnectée, sauvegarde hors ligne chiffrée ou clé papier imprimée). Elle ne doit **jamais** être stockée sur le Duo ou sur un

appareil connecté à Internet. La clé maître est nécessaire pour ajouter des sous-clés, révoquer des clés ou prolonger leur expiration — la perdre signifie perdre le contrôle de votre identité GPG.

Résultat sur le plan de la sécurité :

Le déchiffrement et la signature des courriels nécessitent la possession physique du Duo. Un appareil volé ne peut pas usurper l'identité du propriétaire ni déchiffrer le courrier reçu.

Plan d'allocation des emplacements (Profil 1)

Le tableau suivant présente une affectation d'emplacements recommandée pour le profil principal :

Emplacement	Utilisation
Emplacement ECC 1	Clé privée SSH (GitHub) ou clé SSH résidente FIDO2
Emplacement ECC 2	Sous-clé de chiffrement GPG [E]
Emplacement ECC 3	Sous-clé de signature GPG [S]
Emplacement ECC 4	Sous-clé d'authentification GPG [A]
Emplacement HMAC	Défi-réponse KeePassXC
FIDO2	Bitwarden + tous les autres sites WebAuthn/FIDO2
Emplacements 1–3	OTP / mots de passe statiques pour des comptes supplémentaires si nécessaire

Le Profil 2 peut être réservé à un ensemble d'identifiants de déni plausible ou laissé vide.

Analyse du scénario de vol d'appareil

Avec cette configuration, les protections suivantes s'appliquent si un ordinateur portable ou un appareil mobile est perdu ou volé :

Bitwarden
: Bloqué. Le second facteur FIDO2 exige le Duo physique.

KeePassXC
: Bloqué. La base de données ne peut pas être ouverte sans pression sur le Duo.

GitHub SSH
: Bloqué. La clé privée réside sur le Duo ; la copie dans le système de fichiers est inutilisable.

GPG / Courriel
: Bloqué. Les sous-clés sont sur le Duo ; le déchiffrement et la signature nécessitent une pression physique.

La surface d'attaque restante est le **PIN de l'OnlyKey Duo** lui-même. Atténuez ce risque en :

- Utilisant un PIN fort (6 chiffres ou plus).
- Activant la fonctionnalité **PIN d'autodestruction** pour effacer l'appareil après un nombre configuré de mauvaises tentatives.
- Ne jamais partager ni enregistrer le PIN à proximité de l'appareil.

Stratégie de sauvegarde critique

> !DANGER!
>
> Négliger les sauvegardes est l'erreur la plus courante et la plus catastrophique. Perdre le Duo sans sauvegarde peut vous bloquer définitivement hors de tous les services et données protégés.

Les sauvegardes suivantes doivent être maintenues :

1. **Sauvegarde chiffrée OnlyKey** Exporter une sauvegarde chiffrée complète du Duo via l'application OnlyKey. La stocker dans un endroit hors ligne sécurisé (ex. : clé USB chiffrée dans un coffre-fort physique, ou code QR imprimé conservé en sécurité). Cela préserve les secrets HMAC, les emplacements de clés ECC et la configuration OTP.
2. **Seconde clé FIDO2 pour Bitwarden (et autres sites WebAuthn)** Enregistrer une clé matérielle FIDO2 de secours pour chaque service protégé par FIDO2. Conserver la clé de secours séparément du Duo principal.
3. **Sauvegarde de la base de données KeePassXC** Maintenir une copie séparément stockée de la base de données accessible avec le seul mot de passe maître (sans défi-réponse) pour la récupération d'urgence. Conserver cette copie dans un endroit lui-même bien protégé.
4. **Stockage froid de la clé maître GPG** La clé de certification maître GPG doit être stockée sur une machine déconnectée d'internet ou un support hors ligne chiffré. Sans elle, il est impossible d'émettre des certificats de révocation ou de prolonger l'expiration des sous-clés.
5. **Documentation de l'affectation des emplacements** Documenter les affectations d'emplacements du Duo et conserver l'enregistrement dans votre coffre Bitwarden (une fois configuré) ou dans un autre endroit sécurisé.

Ordre de configuration recommandé

Suivre cette séquence pour garantir un accès fonctionnel aux identifiants avant d'ajouter des couches de protection supplémentaires :

1. **Définir le PIN de l'OnlyKey Duo et la phrase secrète de sauvegarde** en premier. Sans cela, rien d'autre ne peut être récupéré.
2. **Configurer l'emplacement HMAC** et paramétrer le défi-réponse KeePassXC. Vérifier que la base de données s'ouvre correctement, puis exporter une sauvegarde OnlyKey.
3. **Générer les clés GPG** sur une machine déconnectée d'internet. Charger les sous-clés dans les emplacements ECC du Duo. Vérifier que la signature et le déchiffrement fonctionnent via GPG. Stocker la clé maître hors ligne.
4. **Générer une clé SSH FIDO2** pour GitHub (`ssh-keygen -t ed25519-sk`). Ajouter la clé publique à votre compte GitHub. Tester l'accès SSH.
5. **Enregistrer le Duo auprès de Bitwarden** comme clé FIDO2. Enregistrer également une clé FIDO2 de secours lors de la même session. Tester la connexion sur un second appareil.

6. **Exporter et stocker une sauvegarde chiffrée OnlyKey finale** maintenant que tous les emplacements sont entièrement configurés.

Cet ordre garantit que l'accès aux mots de passe est sécurisé avant que le durcissement SSH et GPG ne commence, minimisant le risque de verrouillage lors de la configuration.

Résumé

L'OnlyKey Duo convient parfaitement à ce cas d'usage. En combinant FIDO2 pour Bitwarden, le défi-réponse HMAC pour KeePassXC, les emplacements de clés ECC pour les sous-clés GPG, et soit les clés résidentes FIDO2, soit les emplacements ECC pour SSH, tous les secrets principaux sont retirés des systèmes de fichiers de l'ordinateur portable et du téléphone. La possession physique du Duo (et la connaissance de son PIN) devient le facteur de contrôle unique pour l'accès à l'ensemble de l'écosystème d'identifiants.

Le point faible de toute stratégie de clé matérielle est la procédure de sauvegarde. Investissez du temps dans l'établissement et le test des sauvegardes avant de finaliser la configuration.

Document généré en avril 2026. Le micrologiciel et les logiciels de l'OnlyKey Duo peuvent évoluer ; vérifiez le nombre d'emplacements actuel et les fonctionnalités dans la documentation officielle OnlyKey à l'adresse https://docs.onlykey.io