



GUIDE PAS À PAS IMPRIMABLE

Chiffrez votre clé USB sur Mac sans risquer vos fichiers

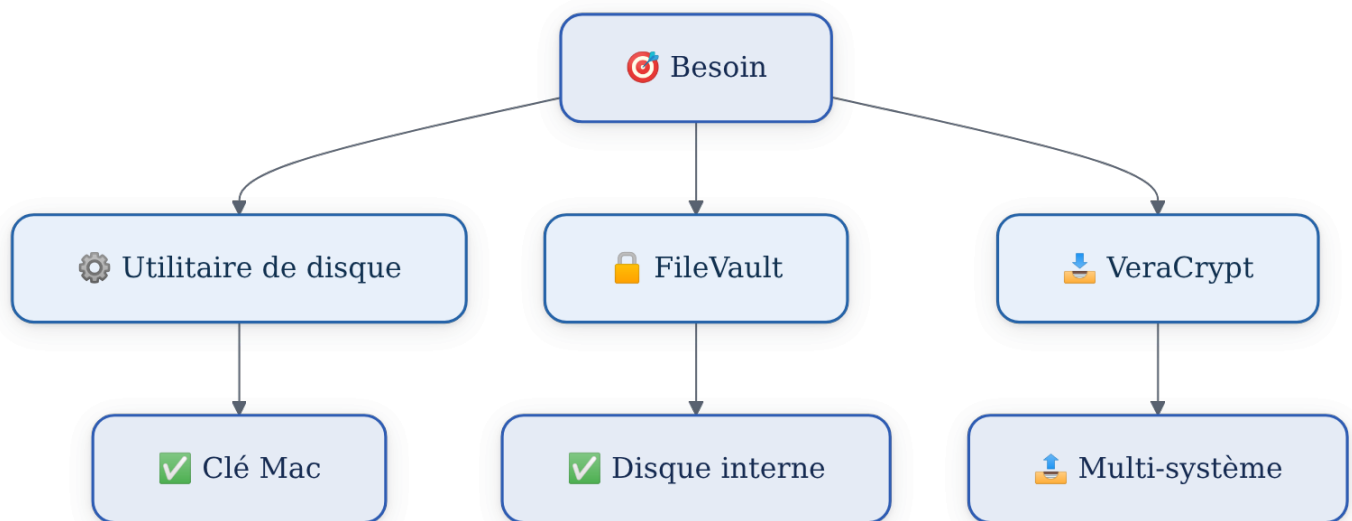
Une méthode pratique pour préparer, chiffrer et tester une clé USB avec Utilitaire de disque. Suivez les contrôles dans l'ordre : le formatage efface le contenu du support.

Au sommaire

- 1 Avant de commencer : les contrôles indispensables
- 2 Choisir la méthode adaptée
- 3 Chiffrer la clé avec Utilitaire de disque
- 4 Tester la clé juste après le chiffrement
- 5 Bon réflexe au quotidien

Avant de commencer : les contrôles indispensables

- Copier tout le contenu de la clé vers le Mac ou un autre support.**
Le chiffrement via effacement supprime les fichiers présents.
- Ouvrir plusieurs fichiers depuis la sauvegarde.**
Vérifiez par exemple un document, une photo et un fichier bureautique.
- Déterminer où la clé sera utilisée.**
La méthode native convient surtout à un usage sur Mac.
- Débrancher, si possible, les autres supports externes.**
Cela réduit le risque de sélectionner le mauvais disque.



INFOGRAPHIE Comparatif des méthodes pour chiffrer une clé USB sur Mac avec Utilitaire de disque, FileVault et VeraCrypt

CHIFFRER SON DISQUE OU SA CLÉ USB

COMPARATIF DES MÉTHODES POUR MAC ET AU-DELÀ

Le chiffrement protège vos données contre les accès non autorisés. Choisissez la méthode adaptée à votre usage et à votre environnement.

BON À SAVOIR

Le chiffrement est aussi fort que votre mot de passe. Utilisez un mot de passe long, unique et mémorable, et conservez une copie de secours sécurisée.



MÉTHODE	USAGE IDÉAL	EFFACEMENT	COMPATIBILITÉ	À RETENIR
 Mac OS étendu journalisé chiffré HFS+ (Journaled)	 Clé USB dédiée au Mac	 Oui	 Mac principalement	 Parfait pour une clé USB utilisée uniquement avec un Mac.
 APFS chiffré Apple File System	 Mac récents	 Oui	 À vérifier selon vos autres systèmes et besoins	 Optimisé pour les Mac récents, mais la compatibilité hors macOS dépend de vos usages.
 FileVault Chiffrement natif macOS	 Disque de démarrage	 Non	 Mac et compte prévu	 Intégré à macOS, idéal pour protéger votre disque de démarrage automatiquement.
 VeraCrypt Open Source	 Échange multi-système	 Selon méthode	 Mac Windows et autres	 La plus polyvalente pour sauvegarder ou transporter des données entre différents systèmes.



BONNES PRATIQUES POUR UNE SÉCURITÉ OPTIMALE



Mot de passe fort
 Au moins 12 caractères avec lettres, chiffres et symboles.



Sauvegardes régulières
 Conservez une copie de vos données chiffrées en lieu sûr.



Verrouillez toujours
 Démontez ou verrouillez vos volumes chiffrés après usage.



Ne perdez pas votre mot de passe
 Sans lui, vos données peuvent devenir définitivement inaccessibles.

Le chiffrement ne remplace pas la vigilance : restez attentif aux tentatives de phishing, malwares et pratiques à risque.

INFOGRAPHIE Comparatif des formats pour chiffrer une clé USB sur Mac selon la compatibilité.

Choisir la méthode adaptée

Pour une clé dédiée principalement au Mac, choisissez un format chiffré proposé par Utilitaire de disque, comme « Mac OS étendu (journalisé, chiffré) ».

FileVault protège principalement le disque de démarrage du Mac ; ce n'est pas l'outil destiné à chiffrer une clé USB.

APFS chiffré peut être proposé sur certains Mac récents : vérifiez que les appareils prévus pourront utiliser la clé.

Si la clé doit circuler entre Mac et Windows, envisagez une solution multi-système telle que VeraCrypt après avoir vérifié la compatibilité des appareils.



Clé sauvegardée



Ouvrir Utilitaire



Choisir la clé



Choisir format
chiffré



Créer mot de passe



Vérifier le volume

Chiffrer la clé avec Utilitaire de disque



1. Brancher et ouvrir l'outil

Branchez la clé, puis ouvrez Utilitaire de disque depuis Applications > Utilitaires. Attendez que le support apparaisse dans la barre latérale.

2. Identifier précisément le bon support

Comparez son nom, sa capacité et sa position avec votre clé. Si l'option est disponible, affichez tous les appareils afin de distinguer le périphérique physique de son volume.

3. Lancer l'effacement

Sélectionnez la clé USB, cliquez sur l'option d'effacement et donnez-lui un nom reconnaissable. Arrêtez-vous immédiatement si la sauvegarde n'a pas été vérifiée.

4. Sélectionner un format chiffré

Pour une utilisation sur Mac, sélectionnez « Mac OS étendu (journalisé, chiffré) » s'il est proposé. Ne choisissez APFS chiffré que si sa compatibilité convient à votre usage.

5. Définir et conserver le mot de passe

Créez un mot de passe distinct de celui de votre session Mac et conservez-le dans un gestionnaire de mots de passe fiable. Sans ce mot de passe, l'accès aux données peut être définitivement perdu.

6. Attendre la fin de l'opération

Confirmez l'effacement puis attendez que le nouveau volume chiffré soit créé avant de fermer Utilitaire de disque.

Tester la clé juste après le chiffrement

- ☐ Copier un ou plusieurs fichiers de test sur la clé chiffrée.

- ☐ Éjecter correctement le volume.
- ☐ Reconnecter la clé et vérifier la demande de mot de passe.
- ☐ Ouvrir les fichiers de test une fois le volume déverrouillé.
- ☐ Conserver la sauvegarde initiale jusqu'à validation complète.

! Ce que le chiffrement protège — et ce qu'il ne protège pas

Le chiffrement rend les fichiers illisibles sans le mot de passe, notamment en cas de perte ou de vol lorsque la clé est démontée. Il ne remplace ni une sauvegarde, ni la vigilance face aux logiciels malveillants, ni la protection des fichiers lorsque la clé est déjà déverrouillée.

Bon réflexe au quotidien

Utilisez la clé chiffrée uniquement sur des appareils compatibles, ne communiquez pas son mot de passe avec le support et éjectez-la après utilisation. Gardez une copie indépendante des fichiers importants : une panne, un effacement ou un mot de passe oublié peut empêcher l'accès aux données.

Attention : l'effacement d'une clé USB supprime les données qu'elle contient. Vérifiez votre sauvegarde et le support sélectionné avant de confirmer.