



KryptKey

J'AIME

Chiffrement/déchiffrement très rapide; lecture directe des fichiers depuis la clé; utilitaire polyvalent; faible encombrement; utilisation des fichiers chiffrés conjointement sur un Mac et un PC Windows.

J'AIME MOINS

Le démontage n'est pas automatique quand on quitte l'utilitaire; le format RTFD n'est que partiellement géré.

MACOS 10.10+ (ET WINDOWS 7+)
PRIX : 60 €

Fabricant: MDK Solutions
(voir Bottin VVMac)

Une « vraie » clé de chiffrement

macOS propose plusieurs fonctions de chiffrement, via Filevault, sur le disque interne ou un disque externe (en entier), ou via Utilitaire de disque, qui crée des images disques protégées. KryptKey est une approche différente, pratique, très sécurisée et « mobile », qui permet en plus d'échanger des fichiers chiffrés de Mac à PC.

KryptKey est une petite clé USB en métal, de 16 Go, livrée dans une petite boîte avec un manuel. La première étape est de créer un compte chez le fabricant, en indiquant nom et prénom, ainsi qu'une phrase secrète et sa réponse (qui, en cas de problème, permettra de réinitialiser le mot de passe ou de recevoir une copie de la phrase secrète). Ensuite, tout se fait directement avec l'utilitaire fourni sur la première partition de la clé USB, en versions Mac et Windows. Une seconde partition sert d'espace de stockage.

Il faut commencer par cliquer sur le logiciel qui demande d'entrer le mot de passe. Il est inutile d'installer l'utilitaire sur le Mac, ça fonctionne depuis la clé (alors que sur PC, il faut l'installer).

UNE CLÉ TRÈS « PERSONNELLE »

On ne peut lire que les fichiers chiffrés à l'aide de sa propre clé, et on ne peut utiliser qu'une seule clé par ordinateur. En revanche, KryptKey peut être utilisée sur plusieurs machines (votre Mac à la maison, votre MacBook, un PC en entreprise).

J'ai pu ainsi passer des fichiers d'un Mac à un PC et vice versa, sans soucis.

Le chiffrement rend les fichiers illisibles,



avec une icône générique et sans possibilité de les prévisualiser avec la fonction Quicklook.

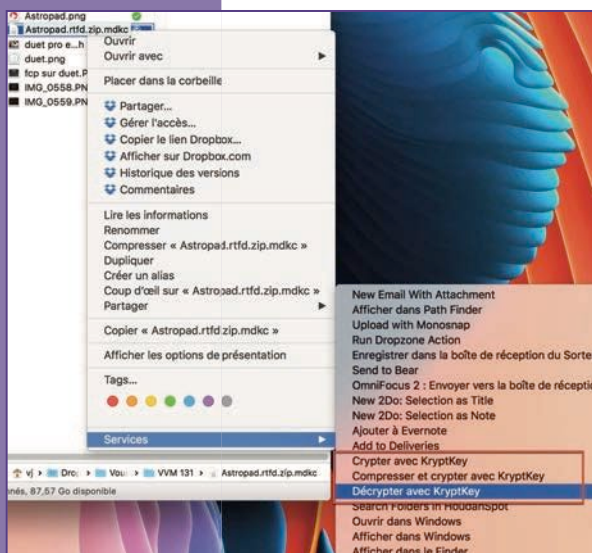
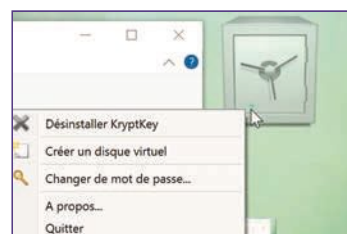
En présence de la clé (et après avoir entré le mot de passe), on peut les utiliser le plus normalement du monde. Les fichiers sont automatiquement de nouveau chiffrés dès qu'on les sauvegarde et qu'on les referme. L'espace de stockage de la clé monte sur le Bureau : tout ce que l'on dépose dessus est instantanément chiffré. Les fichiers peuvent être bien entendu utilisés, modifiés et copiés, mais ils resteront protégés.

UN UTILITAIRE POLYVALENT

On peut aussi utiliser la clé pour simplement chiffrer/déchiffrer sans y stocker quoi que ce soit. Il suffit de glisser un fichier sur l'icône du coffre-fort montée sur le bureau. Ça marche que l'élément soit rangés sur le disque interne, un disque externe ou même un cloud.

On retrouve les mêmes options dans le menu contextuel. Enfin, on peut créer un coffre-fort virtuel, sur l'ordinateur cette fois. C'est, par défaut, une image disque de 150 Mo que l'on peut agrandir ou supprimer. Cet espace peut recevoir des documents de la même façon que la clé physique, mais il restera caché tant que la clé n'est pas branchée au Mac.

Les images, les documents RTF ou Office sont supportés. Attention par contre si, comme moi, vous utilisez toujours le format RTFD; ces fichiers ne peuvent être utilisés tels quels. Il faut les archiver (zip)



avant de les chiffrer. Sinon, ils sont décomposés en dossier plus images, protégés un par un (il est alors impossible de lancer un RTFD par double-clic, sans l'avoir déchiffré au préalable – ce qui n'a pas semblé poser de soucis particuliers). Changer de phrase secrète est facile. Je regrette toutefois, du moins sur le Mac, de ne pas disposer d'une option pour déchiffrer tous les fichiers d'un coup, ni de pouvoir utiliser le logiciel via son icône dans le Dock. Et puis, pour démonter le KryptKey, il faut d'abord quitter le logiciel puis éjecter, j'aurais aimé que ce soit automatique.

JENNY LEMESSAGER