Table des matières

Public : tout public.

Chiffrer des données avec Cryptomator

Cryptomator est un logiciel libre permettant de chiffrer des données. Il est disponible pour Linux, macOS et Windows mais aussi pour Android et iOS.

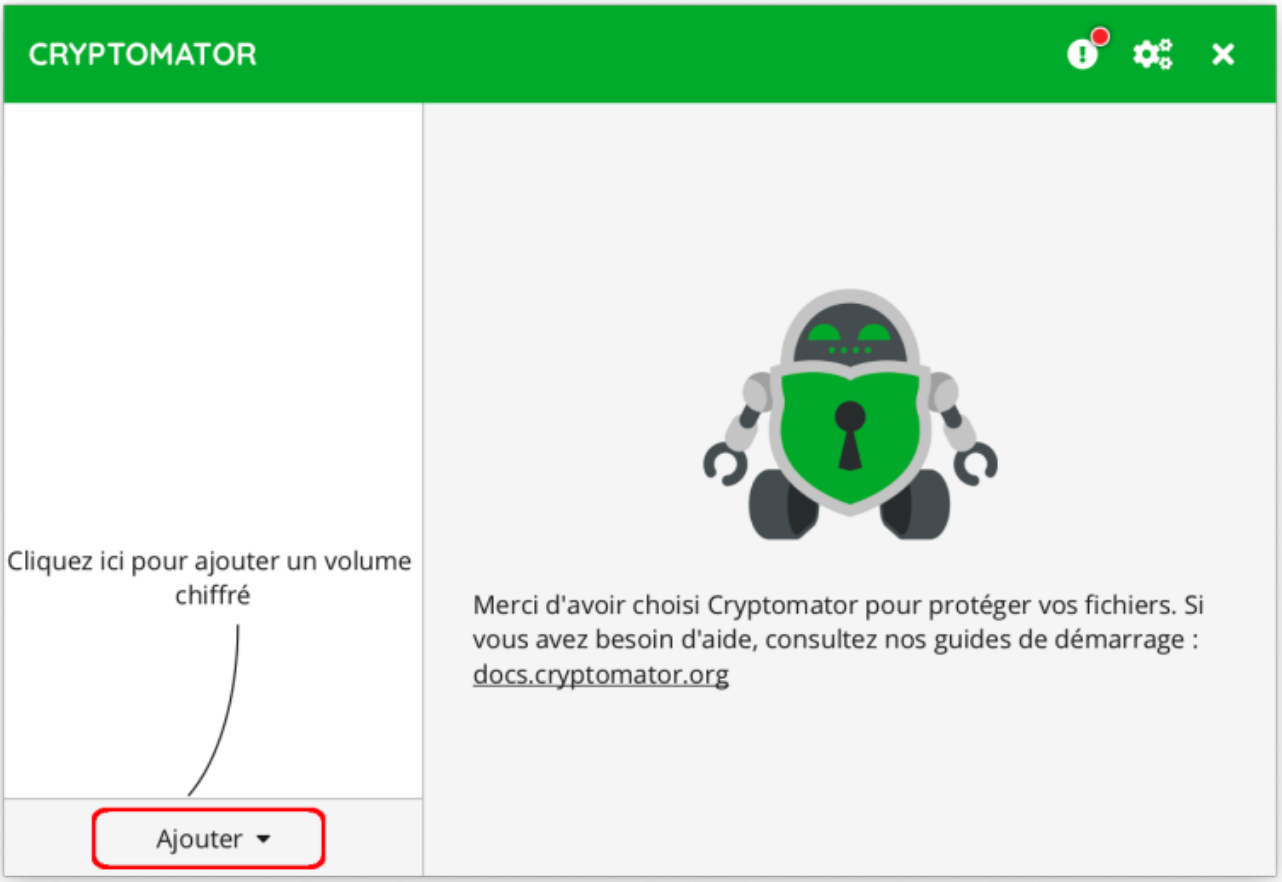
Il **chiffre des données** dans une arborescence de fichiers et de répertoires. Il faut le voir comme un conteneur sécurisé. Ce conteneur est protégé par un mot de passe à consigner soigneusement, par exemple dans KeePassXC. De même ce conteneur doit être sauvegardé.

Nota Bene : Cryptomator est complémentaire de la solution de chiffrement des disques (Chiffrement_de_disque), il ne protège pas des mêmes risques. Le chiffrement du disque (BitLocker avec Windows, FileVault avec macOS ou LUKS avec Linux) protège en cas de vol du matériel éteint : dès que le système est lancé et qu'une session est ouverte, les fichiers sont accessibles et en clair. Avec Cryptomator, les fichiers ne sont en clair que lorsque le volume est déverrouillé. De plus, on peut copier les fichiers chiffrés sans crainte, y compris sur un stockage de type cloud comme OneDrive.

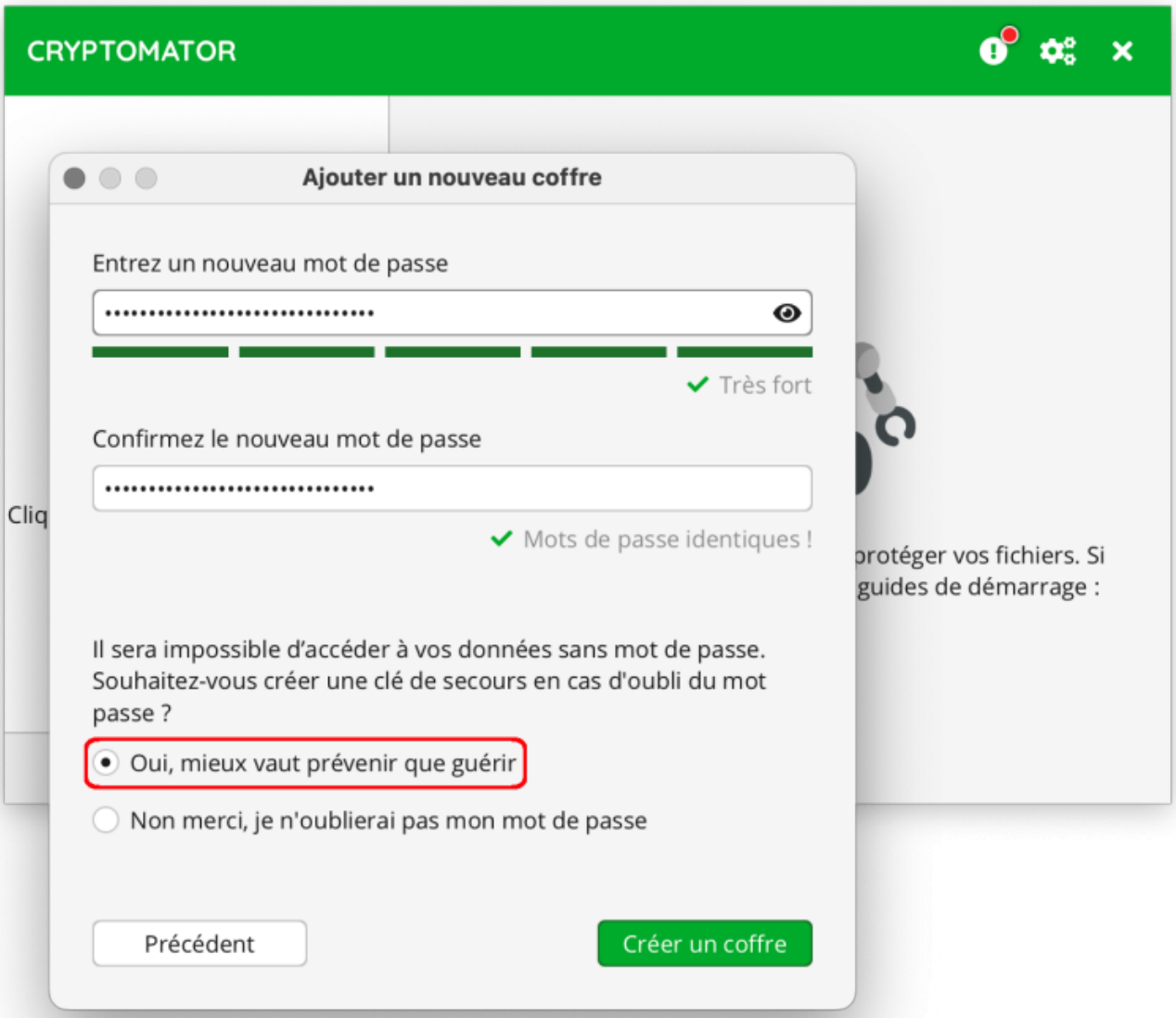
La suite constitue une prise en mains succincte. Se référer à la documentation officielle pour aller plus loin.

Utilisation basique

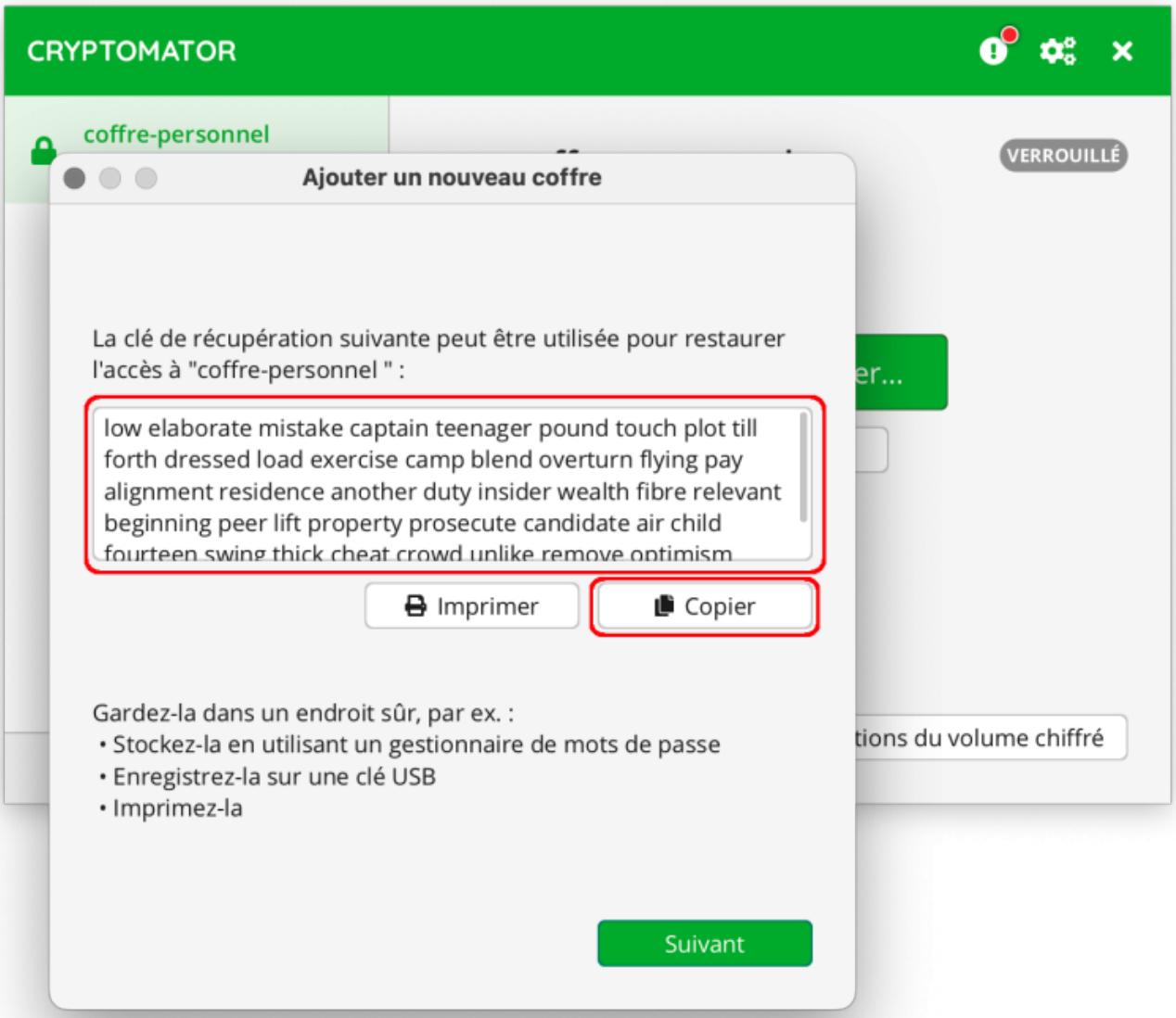
Une fois installé, lancer l'application. Créer un nouveau volume chiffré :



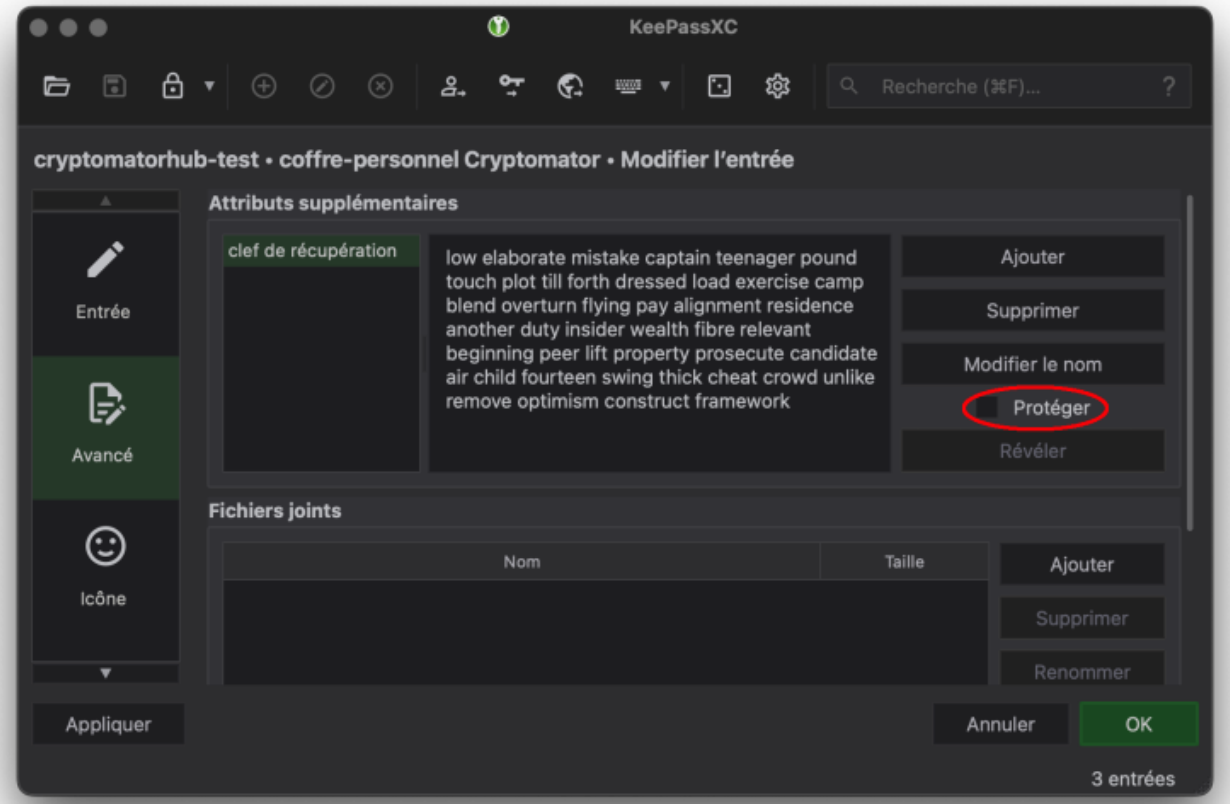
Se laisser guider et choisir un « mot de passe fort » ; ne pas manquer de créer une clef de récupération :



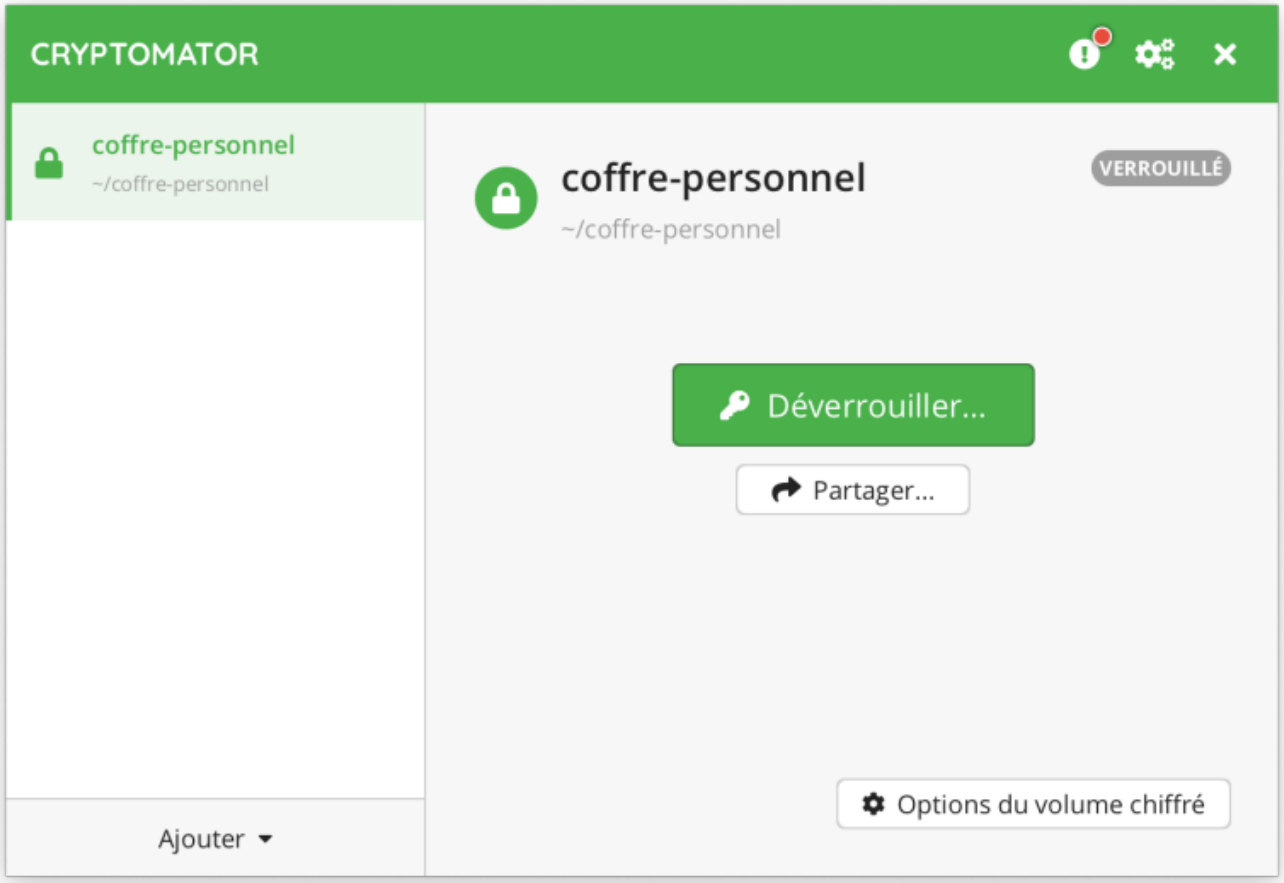
Copier la clef de récupération :



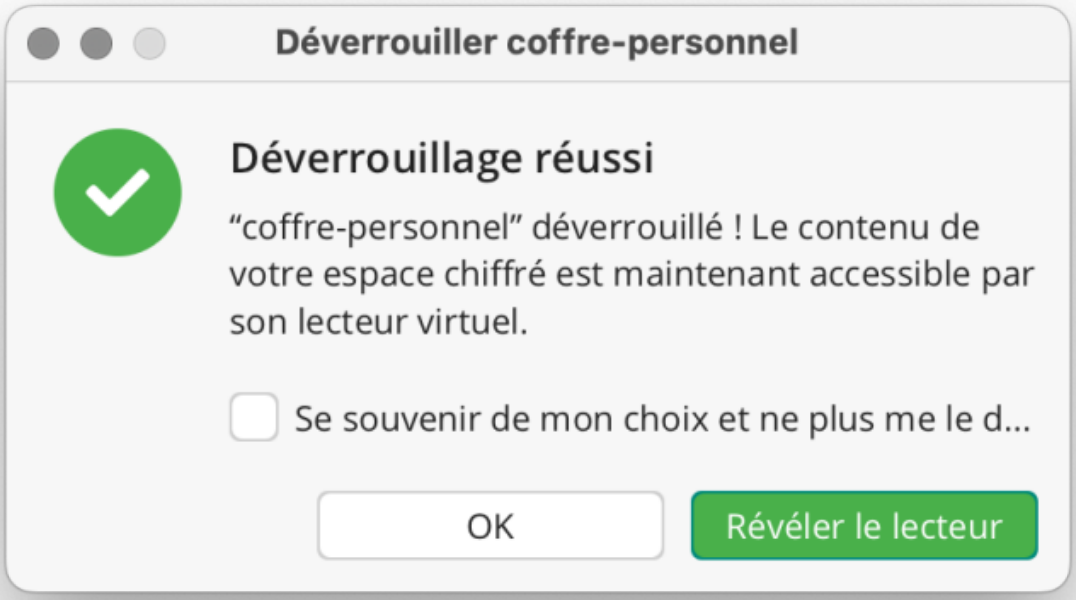
Enregistrer le mot de passe dans KeePassXC ; dans « Avancé », ajouter un champ personnalisé pour la clef de récupération copiée précédemment. Ne pas oublier de cliquer sur « Protéger » à droite pour masquer cette clef.



Avant de pouvoir lire ou écrire, il faut déverrouiller le volume :



Le mot de passe permet de le déverrouiller.

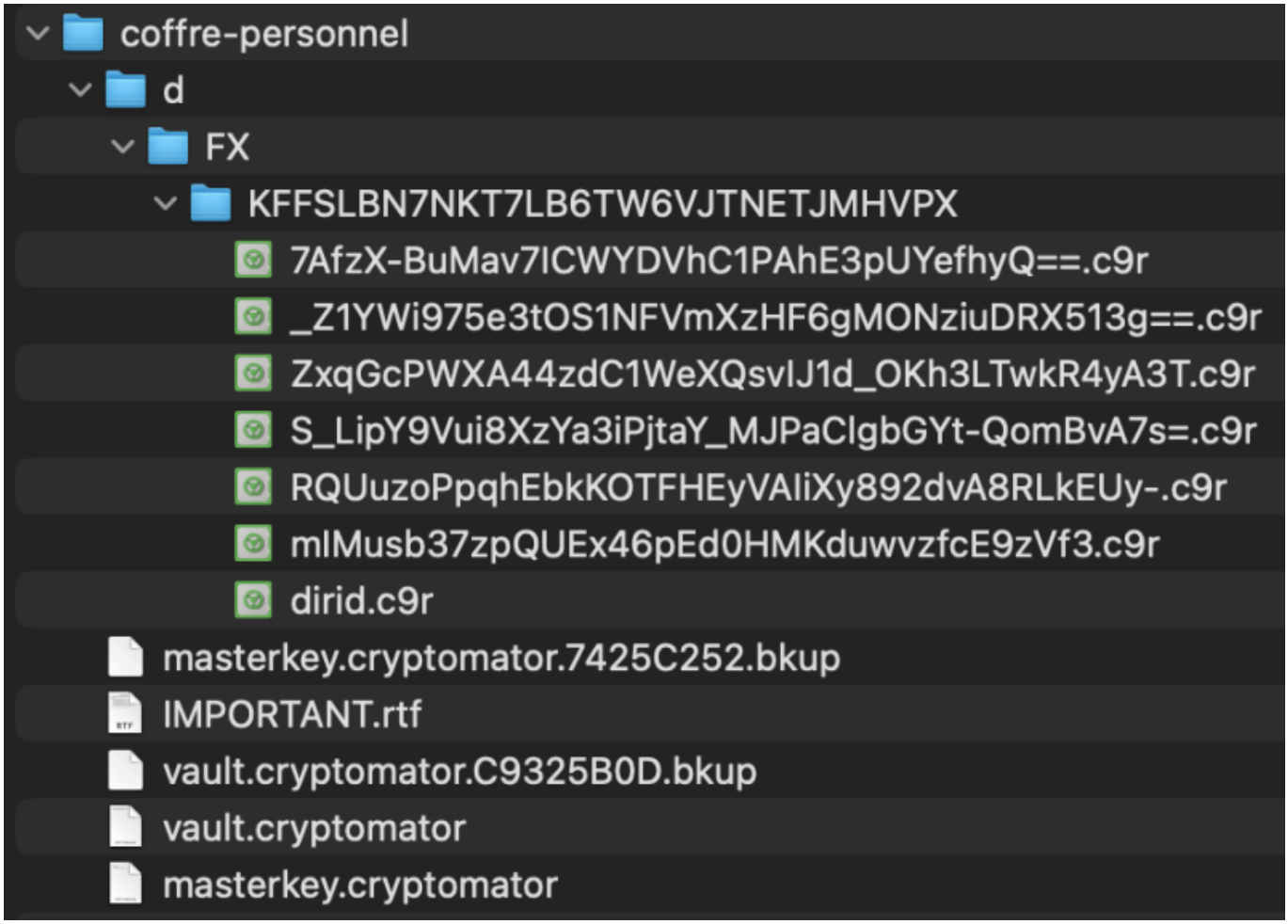


Le volume se présente comme un disque à part. Par défaut, il contient `BIENVENUE.rtf`. Les fichiers à protéger doivent être enregistrés dans ce volume pour être chiffrés.

Synchronisation

Attention : il s'agit de copier non pas le contenu du volume déverrouillé mais bien le conteneur chiffré !

Dans l'exemple ci-dessus, le conteneur est situé dans `~/coffre-personnel`, il s'agit d'un répertoire qui se présente sous la forme suivante :



Après une modification (ajout, suppression, édition de fichiers...), ce répertoire peut être compressé dans une archive ZIP ou copié tel quel ailleurs, par exemple avec Rclone.

Partage

Cryptomator utilise un mot de passe pour protéger les conteneurs. Pour partager un conteneur sans partager le mot de passe, contacter assistance@cnam.fr.