Sur votre PC ou sur votre smartphone, sur votre clé USB ou dans vos nuages, Chiffrez vos données pour qui vous voulez !

Nos données

Connectés à Internet ou non, presque tous les outils informatiques que nous utilisons aujourd'hui exposent nos données.
C'est la « mondialisation de nos données »
Dans certains cas, cela a l'avantage de nous permettre de retrouver nos informations personnelles dans les multiples endroits que nous fréquentons.
A l'incrédulité de nombre d'entre nous, nos données personnelles intéressent aussi beaucoup d'indélicats; comme les entreprises qui les classent et les vendent aux plus offrants (Google, Amazon, Facebook, Apple, Microsoft) ou comme les officines des États qui ont la fâcheuse envie de contrôler tous vos faits et gestes, vos goûts et vos envies, vos déplacements et vos amis, vous coups de téléphones et vos photos … leur curiosité n'a pas de limite.

Non seulement cela ne les regarde pas mais en plus ils stockent vos données à votre insu dans des endroits vulnérables … il ne passe pas une journée sans qu'un pirate ne s'y introduise.

Alors, que faire ?

- Abandonner tous ces appareils intrus et revivre comme nos grands-parents (« Écouter, voir et se taire » était la devise de ma grand-mère!) ?
  → Nous y perdrions aussi les quelques avantages que ces appareils nous procurent !
- mettre toutes nos données sensibles (emails, fichiers, échanges) sous clef comme nous le

faisons pour toutes nos données non informatiques ?

Mettre sous clef, pourquoi pas … mais comment ?

Selon Wikipedia, «Le chiffrement ou cryptage est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement».
L'informatique nous proposent des outils qui permettent de chiffrer nos données. Une fois de plus, nous prendrons le soin d'utiliser des outils et services libres, seuls outils auxquels nous pouvons faire confiance.
Nous veillerons aussi à utiliser des outils qui permettent de migrer facilement nos données d'un système d'exploitation à un autre.
Nous nous pencherons enfin sur les pratiques d'échanges de données dans les nuages (cloud computing).

Nos données sur notre ordinateur

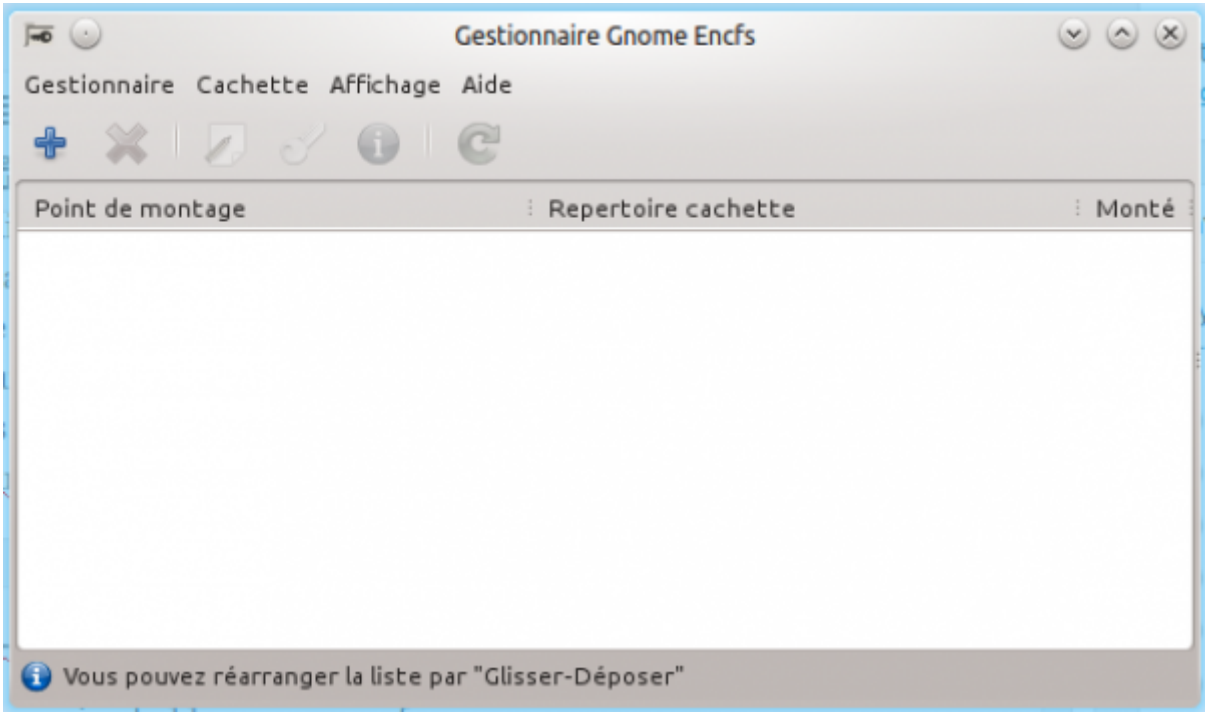
Quels outils ?
Selon les outils, la puissance du chiffrement peut varier. Notre objectif immédiat n'est pas tant de trouver le meilleur outil mais de s'habituer à prendre soin de la confidentialité de nos données et adopter les bons réflexes. Les outils varient au fil du temps et un comportement opportun s'adaptera facilement à tout outil, il permettra même de maîtriser l'outil qui convient le mieux aux règles que chacun souhaite adopter.

un outil libre et gratuit pour vos ordinateurs Linux

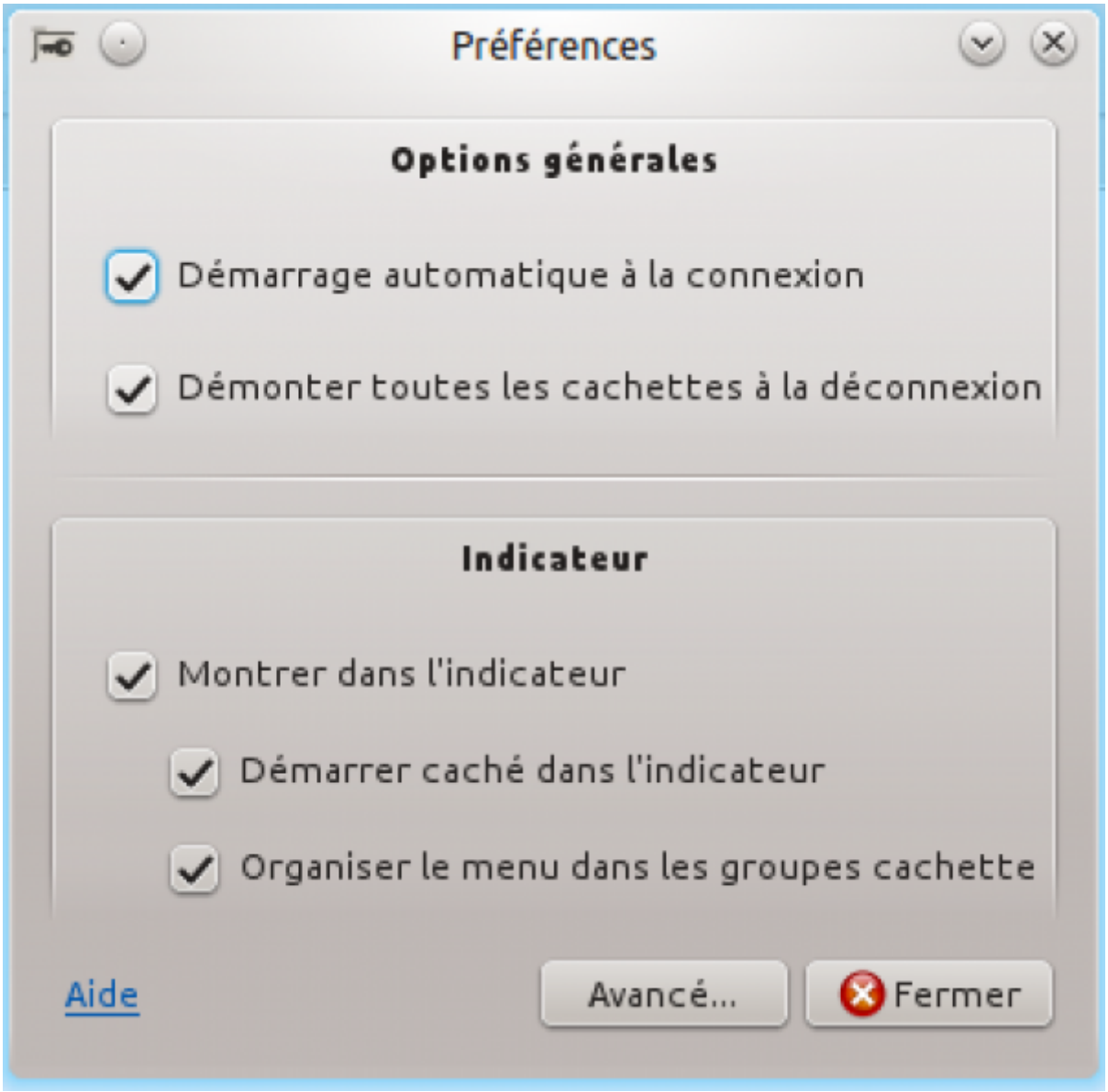
L'outil que nous vous suggérons est **Gnome Encfs Manager**.
Pour l'installer sous Ubuntu (il faut disposer des droits d'administrateur pour l'installation):

```
sudo add-apt-repository ppa:gencfsm
sudo apt-get update
sudo apt-get -y install gnome-encfs-manager
```

Voilà, l'outil est installé, il faut maintenant le paramétrer pour son premier usage.
Pour cela, il suffit de la démarrer, par le menu système ou par une fenêtre terminal.



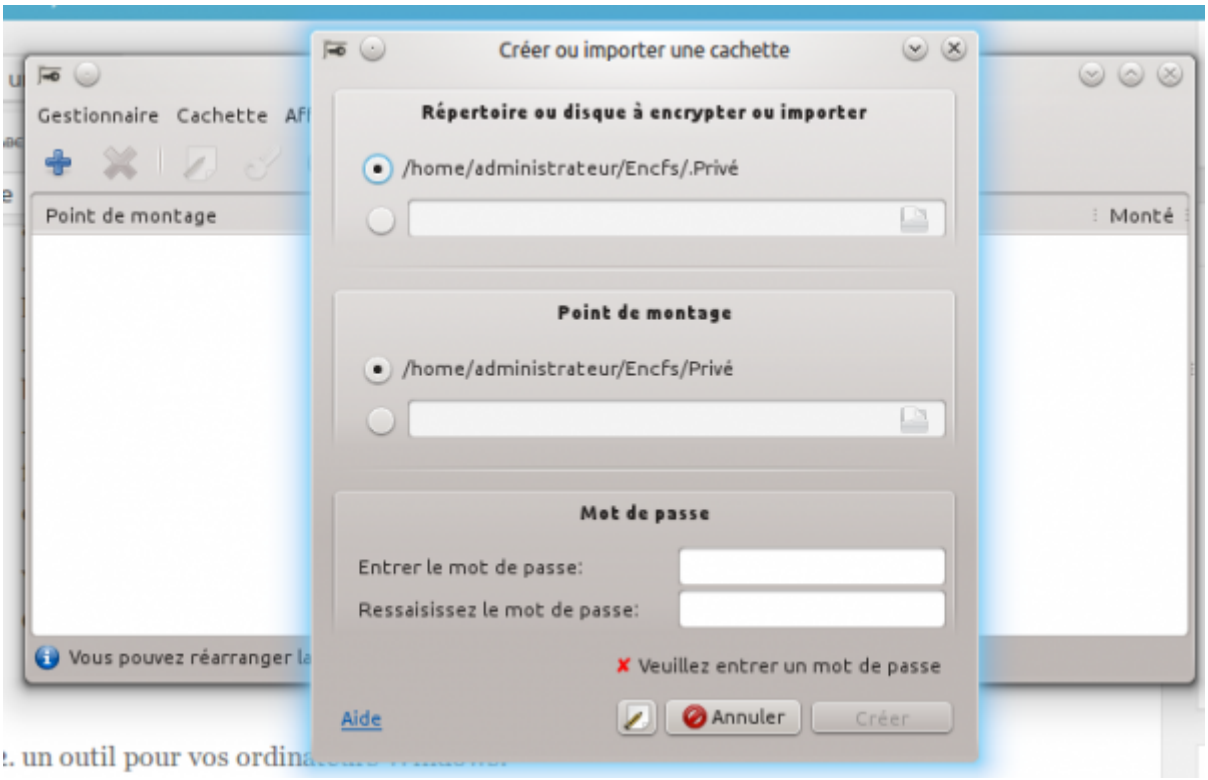
\\Allons vérifier les préférences du logiciel (en cliquant successivement sur Gestionnaire puis sur Préférences)



- la case à cocher « Démarrage automatique à la connexion » permettra le lancement automatique de Gencfs au démarrage de chaque session utilisateur (quand vous allumer l'ordinateur).
- la case à cocher « Démonter toutes les cachettes à la déconnexion » permettra de fermer l'accès aux dossiers cachés à la fermeture de chaque session utilisateur.
- la case à cocher « Montrer dans l'indicateur » permettra d'ajouter un indicateur dans votre barre d'icônes système.
- la case à cocher « Organiser le menu dans les groupes cachette » permettra d'accéder plus facilement à ses dossiers cachés s'ils ceux-ci sont très nombreux (plus de 3 ou 4 par exemple).

Voilà, le logiciel Gencfs est installé et configuré ... il ne reste plus qu'à s'en servir !

Création du premier dossier chiffré : un dossier chiffré sur mon ordinateur !



Après avoir cliquer sur le bouton

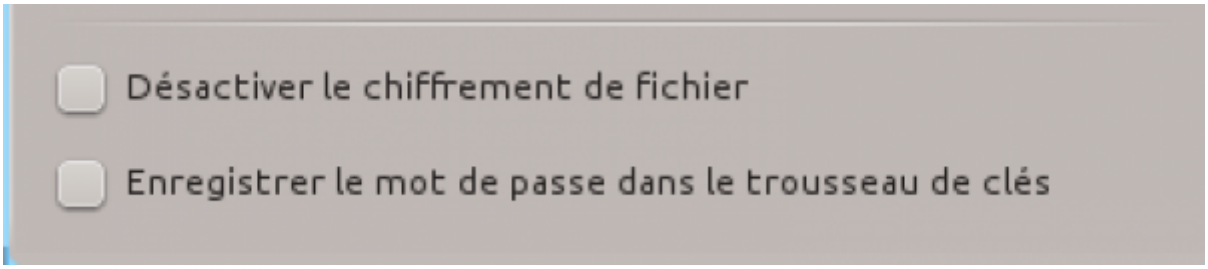
dans la barre d'icône du logiciel, le logiciel propose de créer ou d'importer un dossier sur votre ordinateur.
A cet instant, nous allons créer un nouveau dossier (/répertoire) dans le disque de notre ordinateur.
En réalité, Gencfs créera une paire de dossier:

- un premier dossier, nommé ***« cachette »***, contiendra une version chiffrée des fichiers que vous souhaitez protéger; le point devant le nom de dossier indique au système d'exploitation que le dossier chiffré ne devra pas être affiché dans les listes.
- un dossier ***« Point de montage »*** qui contiendra une version non chiffrée des fichiers que vous voulez protéger. Ce dossier n'existe que le temps pendant lequel le dossier chiffré (la cachette) sera monté/ouvert, montage qui ne se fera qu'après avoir saisi le mot de passe de la cachette.
- le mot de passe, pour être efficace, devra répondre aux critères habituels des mots de passe

(composés de caractères numériques ou alphanumériques et aussi des caractères spéciaux) ou des phrases de passe du type : **=1*Sesame*,*ouvre*-*toi=1**

- options supplémentaires:

En cliquant sur le bouton qui se trouve devant le bouton Annuler (gencfs 6), vous pourrez accéder à deux options supplémentaires importantes:



– désactiver le chiffrement de fichier est une option mal nommée; il s'agit en réalité de choisir si le nom de fichier sera, lui aussi chiffré et donc non lisible. – enregistrer le mot de passe dans le trousseau de clés permettra de stocker le mot de passe du dossier chiffré dans le trousseau de clés de votre distribution Linux et simplifier la gestion de dossiers chiffrés multiples.

L'utilisateur sauvegardera, copiera, déplacera les fichiers qu'il souhaite crypter dans le dossier 'point de montage' et Gencfs en créera immédiatement et automatiquement une copie dans le dossier cachette. Au moment du démontage du dossier, le dossier 'point de montage' n'existera plus dans le dossier personnel de l'utilisateur et seuls les fichiers cryptés de la cachette resteront. Après déconnexion et reconnexion ou après re montage du dossier, le dossier point de montage sera a nouveau présent et contiendra une version non chiffrée des fichiers qui étaient resté dans la cachette. Il faudra donner le mot de passe / phrase de passe pour que le montage puisse se faire.

Création d'un dossier crypté sur une clé USB !

Il s'agira dans ce cas de créer un dossier caché sur le périphérique USB (sans omettre le point devant le nom du fichier). Le point de montage sera placé sur l'ordinateur de l'utilisateur. Point de montage.

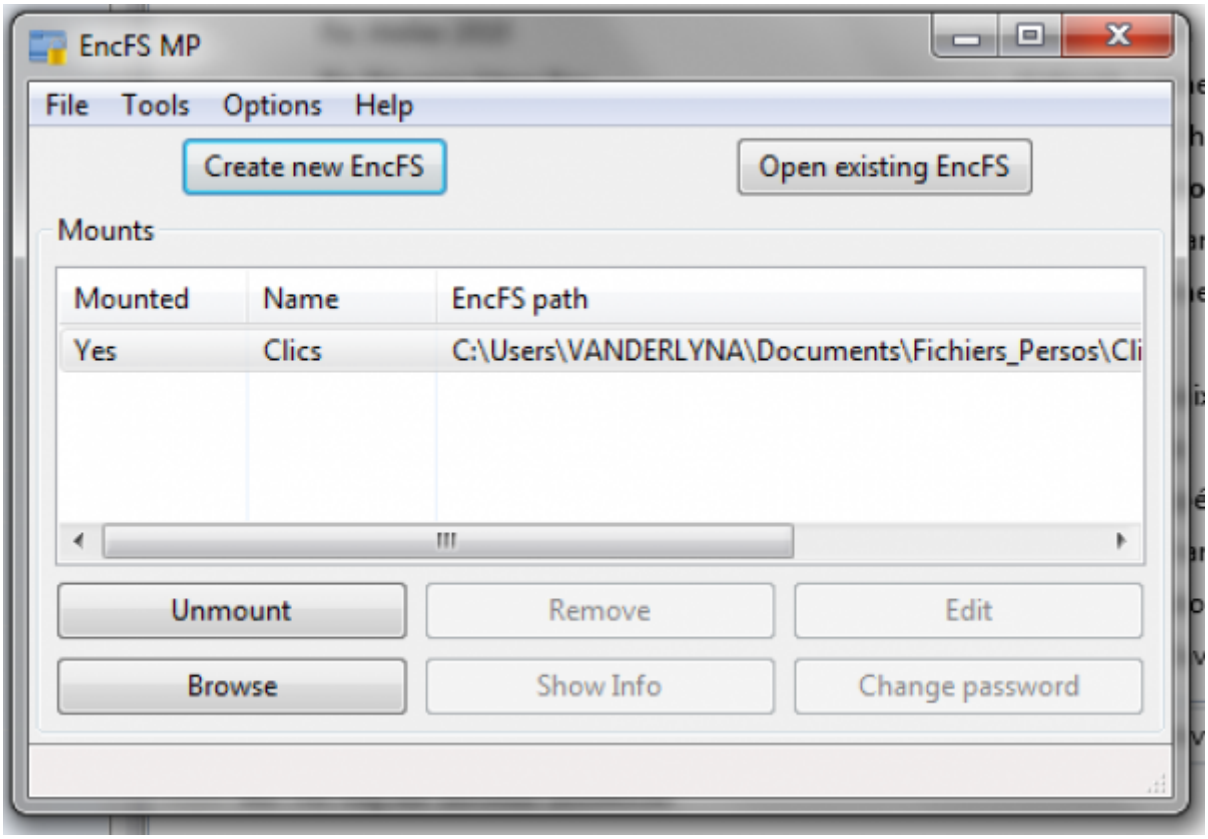
Comme les fichiers chiffrés seront automatiquement copiés sur la clé USB par le logiciel de chiffrement Gencfs, l'utilisateur devra enregistrer, copier, déplacer son fichier dans le dossier de point de montage. Attention: pour être exploitable, le fichier chiffré sur la clé devra être déchiffré par Gencfs ou tout autre logiciel compatible.

des outils pour vos ordinateurs sous Windows et Mac

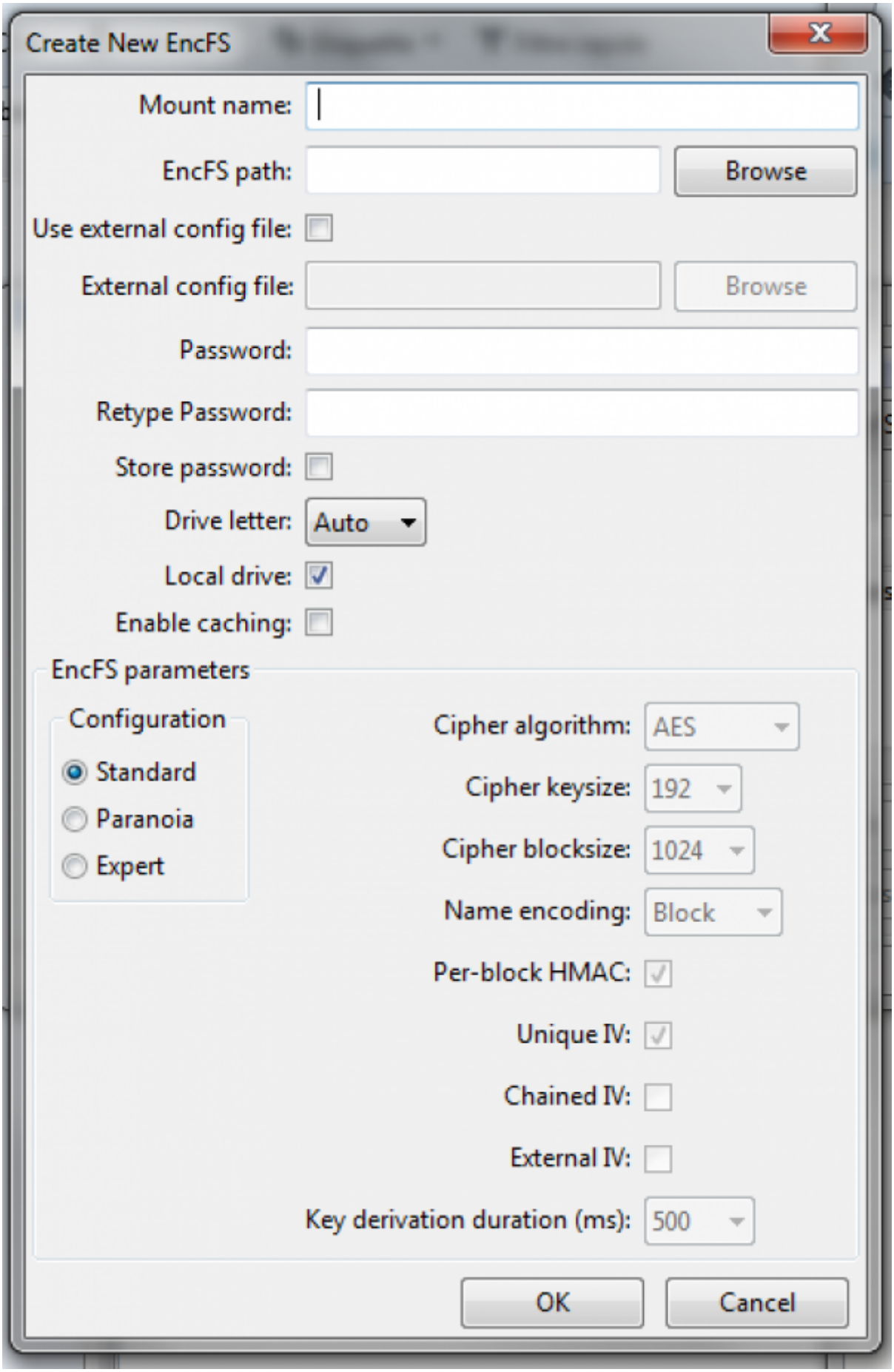
Sous Windows, le logiciel EncFSMP remplira des fonctions identiques à **Gnome Encfs Manager**. Son installation est simple : Téléchargez le fichier d'installation, double-cliquez dessus et suivez les instructions.
(si vous souhaitez désinstaller EncFSMP, sélectionnez "Désinstaller" dans le dossier EncFSMP du menu Démarrer ou allez dans les Panneaux de configuration, ouvrez le panneau "Programmes et fonctionnalités" et double-cliquez sur EncFSMP.)
Si vous voulez mettre à jour une installation existante, exécutez simplement le programme d'installation de la nouvelle version. Il n'est pas nécessaire de désinstaller la version précédente.

Pour créer un nouveau dossier EncFS sous Windows, cliquez sur le bouton "Créer un nouveau dossier

EncFS". Une nouvelle fenêtre de dialogue apparaît. Entrez les informations suivantes :



Un formulaire vous permet alors de donner des précisions sur le dossier que vous allez créer:



Nom du montage : Le nom du volume est bre, il doit cepaendant être unique sur l'ordinateur.
Chemin EncFS : Entrez le chemin d'accès à un répertoire vide, où les fichiers chiffrés seront stockés.

Il peut s'agir d'un sous-dossier dans votre dossier personnel ou d'un sous-dossier dans vos dossiers Dropbox/Google Drive, etc
Utiliser un fichier de configuration externe : si vous cochez cette case, le chemin d'accès au fichier de configuration d'encfs peut être défini dans un dossier différent de celui du dossier de données encfs. Cela peut améliorer la sécurité, mais ne devrait être utilisé que par les utilisateurs avancés. Attention: si le fichier de configuration est perdu, les données ne peuvent pas être récupérées !
Fichier de configuration externe : Le chemin d'accès au fichier de configuration externe.
Mot de passe : Entrez un mot de passe pour le volume, puis tapez-le à nouveau. **Plus c'est complexe, mieux c'est**. Mais s'il vous plaît, gardez à l'esprit : Si le mot de passe est perdu, les données ne peuvent pas être récupérées !
Enregistrer mot de passe : Si vous cochez la case “Enregistrer mot de passe”, le mot de passe sera enregistré sur cet ordinateur. Toute personne ayant un accès physique à cet ordinateur pourra le lire. C'est pourquoi je suggère de ne pas le stocker, mais de l'entrer chaque fois que le dossier est monté. Si vous êtes comme moi et que vous ne vous souvenez pas de mots de passe forts, utiliser la méthode algorithmique proposée ici Choisir des mots de passe sécurisés et s'en souvenir !
Lettre de lecteur : Sélectionnez une lettre de lecteur qui sera assignée au répertoire EncFS monté. Si vous sélectionnez “Auto”, un lecteur aléatoire sera désigné par le système d'exploitation au moment du montage. Si vous choisissez un lecteur désigné pour une lettre, votre dossier sera accessible à cette adresse. Cela pourra vous simplifier la vie si vous utilisez les données stockées dans ce volume avec un logiciel (de bureautique par exemple. Si vous sélectionnez “Aucun”, le dossier EncFS ne sera pas monté comme un lecteur, mais apparaîtra uniquement sous “C:\Volumes\” (comme sous Linux).
Lecteur local : Si vous cochez cette case, le lecteur monté sera affiché en tant que lecteur local dans l'explorateur Windows. Si la case n'est pas cochée, le lecteur monté apparaîtra comme un lecteur réseau.
Activer la mise en cache : Ceci permet d'activer une certaine mise en cache sur le dossier, ce qui peut aider à améliorer les performances sur les dossiers montés en réseau.
La mise en cache est actuellement marquée “experimental”, veuillez vous assurer que vous ne l'activez que lorsque vous travaillez sur des données sans importance. Cela peut être très utile, en particulier pour les dossiers montés en réseau. La vitesse sur les dossiers locaux n'est pas beaucoup améliorée, si ce n'est pas du tout.
Très important : n'activez la mise en cache sur un dossier partagé que si vous êtes certain que personne d'autre ne modifie le répertoire en même temps. Sinon, vous risquez de perdre des données !
Paramètres EncFS : Choisissez les préréglages Standard ou Paranoïa, ou choisissez le mode Expert où tous les réglages peuvent être ajustés à votre convenance.
Attention: vous vous voulez assurer la compatibilité du volume avec d'autres systèmes d'exploitation, préférez la confrontation standard.

un outil pour vos smartphones / tablettes Androïd:

Il faut installer l’application Cryptonite qui permettra de déchiffrer tout fichier chiffré avec l’un des deux outils ci-dessus.. Échanger des données d’un ordinateur à l’autre, d’une système d’exploitation à l’autre ? Les fichiers chiffrés dans un dossier sur un ordinateur pourront être déchiffrés dans un autre dossier sur un autre ordinateur à une seule condition: les deux dossiers devront être chiffrés avec la même clé de chiffrement cad le même mot de passe. Cela peut aussi se faire facilement avec une clé USB: je crée un dossier chiffré sur une clé USB à partir d’un ordinateur A. Quand je connecte la clé sur un ordinateur B, j’importe le dossier chiffré avec mon logiciel chiffrement (Gencfs sur Linux, Encfs4win sur Windows) … . Quand j’accède au dossier, le logiciel me demande la clé de chiffrement

et, après avoir donné cette clé, un dossier est créé avec les données déchiffrées …. jusqu'à ce que je déconnecte mon périphérique USB..

Échanger des données par les nuages ?

Les points abordés précédemment (chiffrement d'un ou plusieurs dossiers sous Linux, chiffrement d'un ou plusieurs dossiers sous Windows) nous rendent capables de chiffrer des données de manière totalement autonome sur nos postes.
Le cryptage est fait sur le ou les postes de l'utilisateur, la clé de cryptage n'ai pas stockée et devra être saisie à chaque ouverture du dit dossier; elle n'est publiée nulle part.
Pour les nuages, au lieu de synchroniser des fichiers en clair, exploitables par votre hébergeur dans les nuages ou par simple piratage de vos données hébergées, il faut et il suffit de synchroniser les fichiers cryptés.
Nous n'allons pas rentrer dans une longue explication sur les avantages et inconvénients de différentes offres d'hébergement dans les nuages. Pour un usage personnel, regardons y toutefois d'un peu plus près:

- les données seront de préférences hébergées en France, à tout le moins en Europe: exit les Google Drive, Sky machin, DropBox etc
- il faut choisir un prestataire de confiance, donc lister vos critères de confiance et lire les conditions d'utilisation pour vérifier la concordance entre vos critères et ces conditions. Attention, les conditions écrites dans les grands groupes nécessitent le plus souvent une lecture approfondie; les cabinets d'avocats et communicants qui les ont écrites feignent servir les intérêts des utilisateurs pour servir leurs propres intérêts.
- les données pourront être accessibles par simple navigateur Web: il faut pouvoir déplacer les données de son disque / périphérique vers les nuages et des nuages vers son disque / périphérique sans obligatoirement mettre en œuvre un logiciel spécialisé (ce que vous ne pourrez pas forcément faire sur tous les ordinateurs que vous utilisez !).
- le chiffrement des données devra pouvoir être fait avec une maîtrise totale et exclusive des clés de chiffrement, sans qu'elles soient stockées avec les données sur un serveur dans les nuages, ce qui équivaudrait à une absence de chiffrement !
  La solution idéale est de chiffrer ses données sur son ordinateur / smartphone avec les logiciels préconisés et de copier / synchroniser seulement ces données chiffrées sur son espace dans les nuages.
  Avec une contrainte toutefois: il faut pouvoir décrypter sur l'ordinateur qui va accéder aux données !.

Voici quelques tutoriels qui vous aideront à comprendre et utiliser le chiffrement en parallèle sur vos postes et dans les nuages:

- How to Encrypt Cloud Storage on Linux and Windows with EncFS
- How to use encfs in Android?
- Encrypting Online Storage with EncFS

Conclusions

Vos données vous appartiennent, vos relations avec vos amis ne concernent que vous mêmes et vos

amis: ne vous mettez pas en danger et ne les mettez pas danger, aujourd'hui ou demain.
Le chiffrement est une bonne façon de se protéger: apprenez à vous en servir dès que vous vous servez d'outils informatiques cad dès aujourd'hui, avant d'en avoir réellement besoin.

Faites de même et faites nous part de vos expériences en retour !

— *André Vanderlynden* *2019/05/05 22:37*