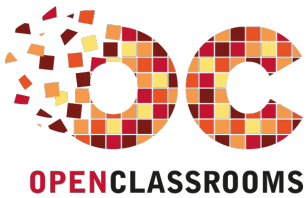
Chiffrer des données avec TrueCrypt

Par Mut



www.openclassrooms.com

Dernière mise à jour le 10/12/2009

Sommaire

Chiffrer des données avec TrueCrypt

Par  Mut

Mise à jour : 10/12/2009
Difficulté : Facile

Imaginons : vous avez sur votre disque dur un journal intime, des photos de vacances ou les plans de la porte des étoiles, et vous seriez extrêmement embêté si quelqu'un de malintentionné s'en emparait (par exemple en cas de vol d'ordinateur portable ou d'interrogatoire des services secrets). Il faut donc cacher ces fichiers. Oui, mais comment ? Changer l'extension d'un fichier ou le cacher au fin fond d'un dossier du système peut marcher pour se protéger de quelqu'un sans connaissances en informatique, mais quelqu'un qui s'y connaît aura peu de mal à les retrouver.

Ce serait bien de trouver un moyen de rendre invisibles les fichiers que l'on souhaite cacher, ou de les protéger par un mot de passe. Ça tombe bien, il existe des logiciels permettant de faire ça. Je vous propose d'utiliser **TrueCrypt**, un logiciel libre de chiffrement très puissant.

Ce logiciel est multiplateforme : je fais les manipulations sous Linux, mais TrueCrypt s'utilise quasiment de la même manière sous Windows et Mac OS X.

Sommaire du tutoriel :

Installer TrueCrypt

Pour utiliser TrueCrypt, il faut bien entendu commencer par le télécharger. Il suffit simplement d'aller dans la section de téléchargement du site officiel, et de télécharger le fichier correspondant à votre système d'exploitation (paquet DEB ou RPM sous Linux, selon votre distribution). Si vous ne savez pas s'il faut choisir la version x86 ou 64 bits, alors il est très probable que c'est la version x86 qui vous convienne.

TrueCrypt est un logiciel en anglais : il existe des traductions, mais malheureusement, elles sont incomplètes et ne marchent pour l'instant que sous Windows.

Une fois installé, pour lancer TrueCrypt, il suffit de taper la commande truecrypt ou d'utiliser le raccourci qui a été créé dans *Applications* > *Accessoires* > *TrueCrypt* (en tout cas pour les utilisateurs de GNOME sous Ubuntu).

Créer un volume chiffré

Principe des disques virtuels chiffrés

TrueCrypt ne permet pas de crypter des fichiers individuellement. Au lieu de ça, il crée un grand fichier qui contient les données à protéger. C'est ce qu'on appelle un disque virtuel chiffré : pour l'utiliser, il faut le monter, c'est-à-dire qu'il apparaîtra comme un disque dur ou une clé USB. Une fois démonté, le fichier chiffré ne sert à rien si on ne connaît pas le mot de passe.

L'avantage, c'est que l'on peut déplacer ce fichier et même le transporter sur un support externe, et l'ouvrir sur n'importe quel

ordinateur où TrueCrypt est installé.

L'inconvénient, c'est que n'importe qui ayant accès à ce fichier peut le supprimer, à défaut de pouvoir l'ouvrir.

Création du volume

La fenêtre principale de TrueCrypt ressemble à ceci.

On va donc cliquer sur le bouton *Create volume* (créer un volume). Vous avez ensuite le choix entre deux options : choisissez *Create an encrypted file container* (créer un fichier conteneur chiffré).

Vous avez le choix entre *Standard TrueCrypt volume* (volume TrueCrypt standard) et *Hidden TrueCrypt volume* (volume TrueCrypt caché). Pour le moment, c'est le volume standard qui nous intéresse.

Le logiciel vous demande alors un fichier : mettez-le où vous voulez, et appelez-le comme vous voulez.

Vous pouvez donner à votre fichier une extension comme .zip pour que ce fichier n'ait pas l'air d'un fichier crypté (même si quelqu'un qui fouille le disque dur s'en doutera en s'apercevant qu'aucune application ne sait l'ouvrir).

Ne choisissez pas le nom d'un fichier qui existe déjà : il sera effacé et remplacé par le volume TrueCrypt.

Vous devez maintenant choisir l'algorithme de chiffrement : c'est celui qui sera utilisé pour chiffrer les données contenues dans le volume. Vous avez le choix entre AES, Serpent et Twofish. Comme vous n'avez sans doute aucune idée de la différence entre ces algorithmes (et, à vrai dire, moi non plus), choisissez celui que vous voulez. Ils sont tous très efficaces. Vous pouvez même choisir une combinaison de ces algorithmes, mais *a priori* un seul d'entre eux sera largement suffisant.

L'algorithme de hashage servira à protéger le mot de passe du fichier. Vous avez le choix entre RIPEMD-160, SHA-512 et Whirlpool. Encore une fois, prenez celui que vous voulez.

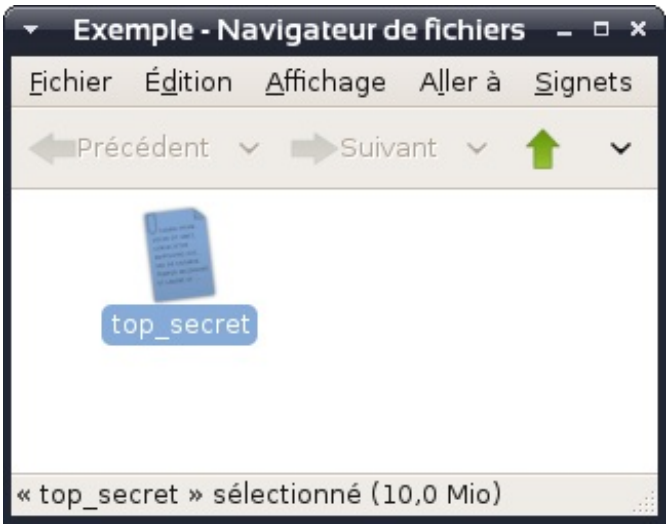
Il faut maintenant choisir la taille du disque virtuel. Attention : si vous choisissez 100 Mio, le fichier chiffré occupera 100 Mio sur votre disque dur, même si vous n'avez encore rien mis dedans.

L'étape suivante est le choix du mot de passe. Suivez de préférence les recommandations habituelles : mélange de minuscules, majuscules, chiffres et symboles ; il doit être difficile à deviner (donc ne mettez pas votre prénom) et assez long. (Pour plus d'informations, je vous conseille d'aller lire le tutoriel sur le choix d'un mot de passe.) TrueCrypt, qui ne plaisante pas avec la sécurité, conseille même de choisir un mot de passe d'au moins vingt caractères.

Vous devez alors choisir le système de fichiers : FAT, ext2 ou ext3. (Sous Windows, on vous propose FAT ou NTFS ; sous Mac OS X, FAT ou Mac OS Extended) Si vous savez ce que vous faites, vous pouvez choisir ; sinon FAT suffira. C'est même préférable si vous avez l'intention d'accéder à votre volume sous plusieurs systèmes d'exploitation.

Et, enfin, la dernière étape : la clé de chiffrement. Le logiciel vous demande d'agiter votre souris au hasard pour la générer. Faites-le, puis cliquez sur *Format* pour formater le disque virtuel.

Cliquez sur *Exit*, et voilà. Vous avez un beau disque virtuel chiffré.



Remarquez que le fichier obtenu pèse 10 Mio (la taille que j'ai choisie pour le disque virtuel) même si je n'ai encore rien mis dedans.

Accéder aux données chiffrées

Maintenant qu'on a créé un volume chiffré, on aimerait bien voir ce qu'il y a dedans et pouvoir y mettre des documents. Rassurez-vous : le plus dur est fait.

Dans la fenêtre principale de TrueCrypt, cliquez sur *Select file…*, choisissez le fichier et cliquez sur *Mount*. Le logiciel vous demandera alors le mot de passe du fichier, ainsi qu'un mot de passe d'administrateur de Linux pour avoir le droit de monter le volume.

Et hop, le disque virtuel est monté comme n'importe quel disque, et vous n'avez plus qu'à l'utiliser comme vous le feriez avec une clé USB. Son point de montage est, par défaut, /media/truecrypt1 (ou un autre chiffre que 1, selon le nombre de disques montés).

Quand vous avez fini, pour le démonter, choisissez-le dans la liste des volumes montés dans TrueCrypt et cliquez sur *Dismount*.

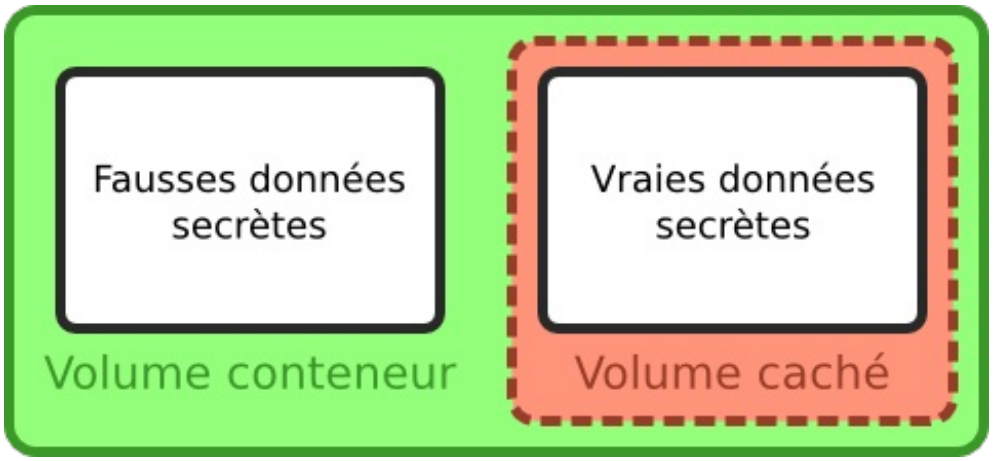
Créer un volume chiffré invisible

Principe

Vous l'aurez peut-être constaté en voyant les différentes options de TrueCrypt : ce logiciel a été conçu pour satisfaire les utilisateurs les plus paranos. C'est à ça que servent les volumes chiffrés invisibles.

L'inconvénient des volumes chiffrés, c'est que si quelqu'un tombe dessus, il saura qu'il y a *quelque chose* de caché, même s'il ne sait pas ce que c'est. Le mieux, pour éviter que des données chiffrées soient décryptées, c'est que personne ne se doute qu'il y ait quelque chose à décrypter.

TrueCrypt permet justement de créer des volumes invisibles à l'intérieur d'un volume conteneur, selon le principe suivant.



Supposons que quelqu'un vous soutire le mot de passe du volume conteneur sous la torture. Il verra seulement les fichiers que vous y avez mis, et n'aura aucun moyen de savoir qu'il y a un autre volume chiffré caché dedans. L'espace libre des volumes de TrueCrypt est rempli avec des données aléatoires, et il est impossible de distinguer le volume caché (tant qu'il est démonté) de données aléatoires : il apparaîtra comme de l'espace libre. Vous pourrez donc affirmer de façon tout à fait crédible qu'il n'y a rien de caché dans le volume conteneur. (C'est ce qu'on appelle le déni plausible.)

Création d'un volume chiffré invisible

Créez un nouveau volume, comme précédemment. Choisissez à nouveau *Create an encrypted file container*, mais à l'étape suivante, vous sélectionnerez cette fois *Hidden TrueCrypt volume* (volume TrueCrypt caché). Comme avant, choisissez un fichier, les algorithmes, la taille du disque conteneur et son mot de passe.

C'est à partir de là que les choses sont différentes : TrueCrypt monte le volume conteneur et vous demande d'y mettre des données (de préférence des données qui semblent secrètes mais qui ne le sont pas). Il ne vous laissera pas passer à l'étape suivante tant que le volume sera vide.

Vous pouvez maintenant créer le volume caché proprement dit. TrueCrypt vous demande encore de choisir les algorithmes (vous n'êtes pas obligé d'utiliser les mêmes que pour le volume conteneur), puis la taille du volume. Remarquez que la taille maximale possible correspond à la taille du volume conteneur moins la taille des données que vous y avez mises. Enfin, choisissez un mot de passe.

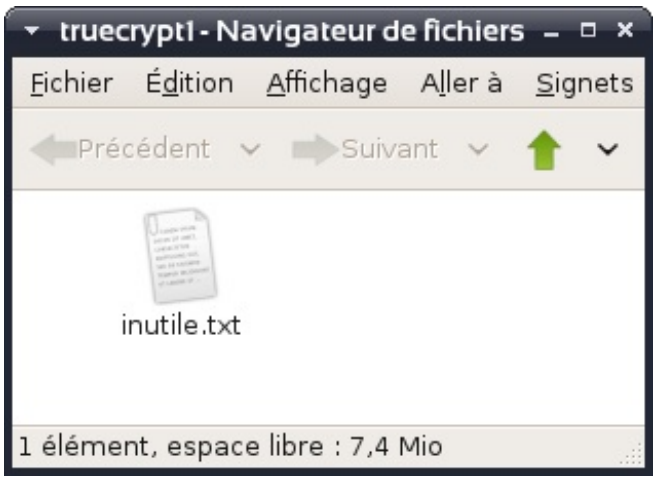
Le mot de passe du volume caché doit être différent de celui du volume conteneur.

Il ne reste qu'à choisir le système de fichiers, à générer une clé de chiffrement, et c'est terminé.

Accéder aux données

Comme pour un volume chiffré classique, sélectionnez votre fichier avec TrueCrypt et cliquez sur *Mount*. Vous devez alors taper un mot de passe. C'est ici que se situe l'astuce :

- si vous entrez le mot de passe du volume conteneur, c'est le volume conteneur qui sera monté ;
- si vous entrez le mot de passe du volume caché, c'est le volume caché qui sera monté.

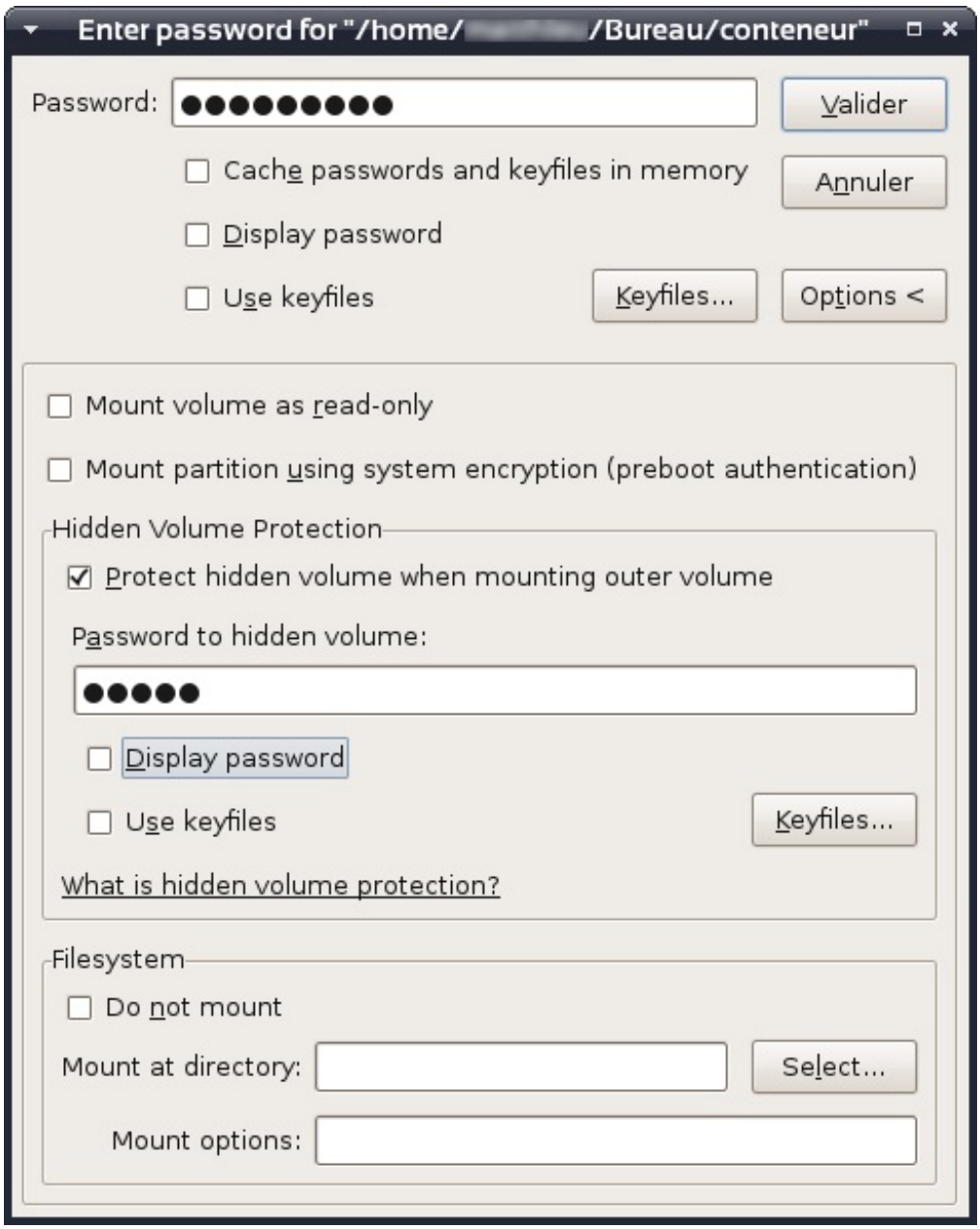


Exemple : j'ai créé un volume conteneur de 10 Mio, que j'ai rempli avec un fichier d'un peu plus de 2 Mio. J'ai créé un volume caché de 7 Mio, que j'ai rempli avec 5 Mio de données. On voit bien que, si on monte le volume conteneur, le volume caché est considéré comme de l'espace libre.

Comme le volume invisible est considéré comme de l'espace libre, vous risquez d'écrire par dessus si vous utilisez le volume conteneur, ce qui le rendra certainement inutilisable.

Il y a deux moyens d'éviter cela. Au moment où vous devez taper votre mot de passe, cliquez sur *Options*.

- Première possibilité : cochez la case *Mount volume as read-only* (monter le volume en lecture seule). Vous ne pourrez alors rien écrire dedans, mais vous serez sûr que le volume caché ne sera pas endommagé.
- Deuxième possibilité : cochez la case *Protect hidden volume when mounting outer volume* (protéger le volume caché en montant le volume externe), puis entrez le mot de passe du volume caché. Si vous essayez de mettre dans le volume externe des données qui empièteraient sur le volume caché, vous aurez un message d'erreur (si TrueCrypt est toujours lancé). Attention toutefois à ne pas en abuser, cela peut créer des problèmes. (Par exemple, dans mon cas, il arrive que l'espace libre affiché dans le volume externe diminue alors qu'il ne devrait pas. Mais cela doit dépendre du système de fichiers utilisé.)



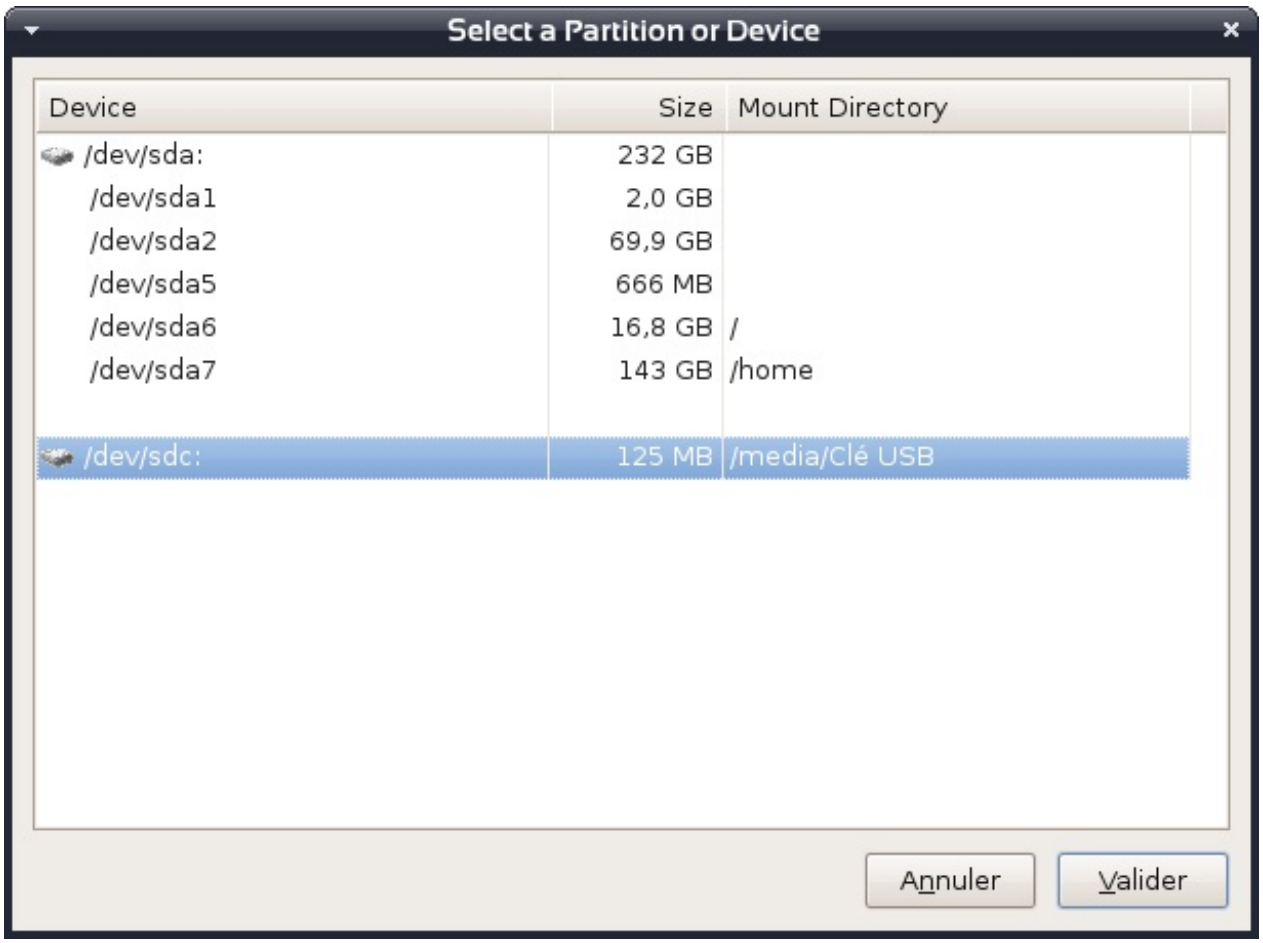
Chiffrer une partition

Peut-être que vous trouvez que devoir créer un disque virtuel qui occupe beaucoup de place, c'est trop contraignant. Heureusement, vous pouvez chiffrer une partition entière, qu'elle soit sur le disque dur de votre ordinateur ou un périphérique externe (comme une clé USB).

Créez un volume TrueCrypt de la même façon qu'avant. Mais cette fois, sélectionnez *Create a volume within a partition/drive* (créer un volume à l'intérieur d'une partition ou d'un lecteur). Vous avez, là aussi, le choix entre un volume standard ou caché.

À l'étape suivante, au lieu de choisir un fichier, vous devez choisir la partition qui sera chiffrée. Cliquez donc sur *Select device...* (choisir un périphérique).

Si vous chiffrez une partition, toutes les données qui sont déjà dessus seront détruites. Faites donc bien attention à ne pas vous tromper.



Dans mon cas, je choisis une clé USB.

Vous devez ensuite choisir le mot de passe, les algorithmes, etc., mais vous connaissez déjà, je vous fais confiance.

Pour pouvoir utiliser votre partition chiffrée, vous devez simplement cliquez sur le bouton *Select device…* dans la fenêtre principale de TrueCrypt, choisir la partition, puis taper votre mot de passe, comme d'habitude.

Utiliser un fichier comme mot de passe

Vous trouvez qu'un seul mot de passe, c'est un peu léger ? TrueCrypt vous permet d'utiliser un fichier (ou plusieurs) pour déchiffrer vos volumes. Le principe : pour monter votre volume chiffré, en plus de taper un mot de passe (ou à la place), vous devrez indiquer à TrueCrypt le chemin d'un fichier qui sera utilisé pour le déchiffrer.

Pour cela, quand vous créez un volume chiffré, à l'étape de choix du mot de passe, cochez l'option *Use keyfiles* (utiliser des fichiers-clés), puis cliquez sur *Keyfiles…*. Cliquez ensuite sur *Add files…* pour ajouter un fichier (ou même plusieurs). L'ordre des fichiers n'a pas d'importance. TrueCrypt peut aussi générer des fichiers-clés de 64 octets si vous cliquez sur *Generate random keyfile…* (générer un fichier-clé aléatoire).

Vous pouvez choisir n'importe quel fichier. Vous n'êtes pas obligé de mettre un mot de passe si vous utilisez des fichiers-clés, mais vous pouvez tout à fait combiner les deux.

C'est un exemple, choisissez un nom plus discret que Fichier-clé. 

L'avantage de cette méthode, c'est qu'elle rend les attaques par force brute impossibles. Vous pouvez aussi choisir un fichier sur un support externe, ce qui empêchera de déchiffrer vos données sans le support en question. Et le chemin d'un fichier peut être

plus facile à retenir qu'un long mot de passe.

L'inconvénient majeur est bien entendu que si vous perdez un des fichiers-clés, vous ne pourrez plus accéder au volume chiffré.

Qui plus est, si un seul bit des 1024 premiers Kio d'un fichier-clé est modifié, vous êtes fichu. Ce serait comme si vous tapiez un mot de passe en changeant un caractère. Choisissez donc des fichiers que vous êtes sûr de ne jamais modifier.

Pour monter un volume chiffré avec cet méthode, au moment où on vous demande son mot de passe, cochez l'option *Use keyfiles* et choisissez les fichiers de la même manière que précédemment.
Vous êtes maintenant capable de protéger vos fichiers de manière plus qu'efficace. Si vous respectez bien les recommandations de sécurité (notamment en ce qui concerne le choix des mots de passe), vos données seront en pratique inviolables.

Sachez que TrueCrypt a des fonctions encore plus poussées (on peut par exemple chiffrer un système d'exploitation), mais ce que je vous ai présenté devrait être largement suffisant dans la plupart des cas.