



TrueCrypt – système chiffré

Pour plus de sécurité, adoptez les réflexes CASES !

Table des matières

1. Installation
2. Chiffrement de la partition système
3. Utilisation du contenant crypté

Avec la prolifération des ordinateurs portables, on peut se demander quel est le niveau de sécurité des données qui y sont stockées. En effet, les risques de perte ou de vol de ces laptops sont élevés, surtout pour certains publics cibles. La confidentialité des données stockées est très souvent compromise.

Ce dossier va vous montrer comment sécuriser votre ordinateur portable et surtout les données qu'il contient grâce à un outil libre, gratuit et simple d'utilisation : TrueCrypt. Beaucoup d'organisations étatiques lui font confiance et l'utilisent couramment.

Dans ce dossier nous allons vous montrer comment chiffrer votre partition système pour qu'une personne malintentionnée ne puisse pas récupérer des données d'un ordinateur volé.



Installation

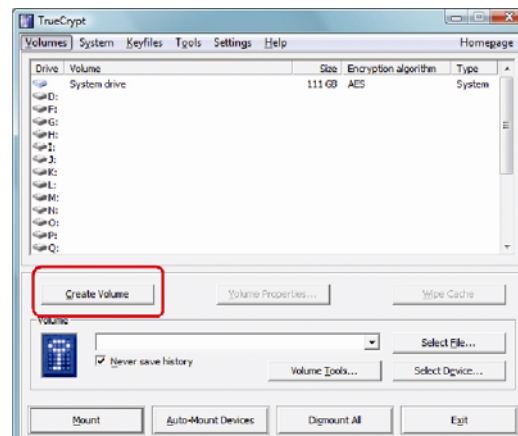
Veillez télécharger l'application TrueCrypt depuis le site officiel : <http://www.truecrypt.org/> et l'installer sur votre ordinateur.

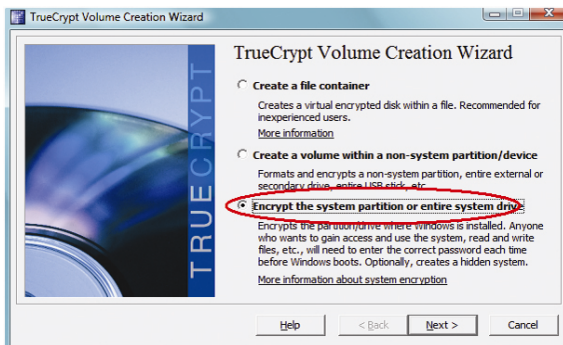


Chiffrement de la partition système

À part la possibilité de chiffrer la partition système, TrueCrypt offre aussi la possibilité de créer des contenants cryptés que vous pourrez utiliser comme tout dossier de votre ordinateur. Tout ce que vous mettrez dans ce dossier sera automatiquement crypté sans aucune autre action de votre part qu'un simple « copier-coller » .

Dans ce dossier nous allons chiffrer la partition système de votre ordinateur portable.

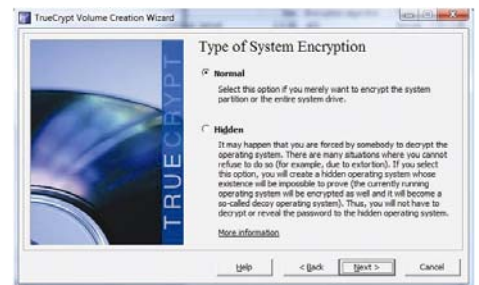




Choisissez ensuite l'option « Encrypt the system partition or entire system drive ».

Avec cette option, TrueCrypt vous donne la possibilité d'encrypter un disque entier. Nous allons utiliser cette option pour chiffrer notre partition système (C'est généralement le disque C :)

TrueCrypt offre deux types de cryptage. Le mode « normal » qui crypte seulement la partition et le mode « hidden » qui crypte la partition, mais la rend aussi invisible. D'après les concepteurs de Truecrypt il serait très difficile de prouver l'existence d'une telle partition. Veuillez choisir l'option "normal".

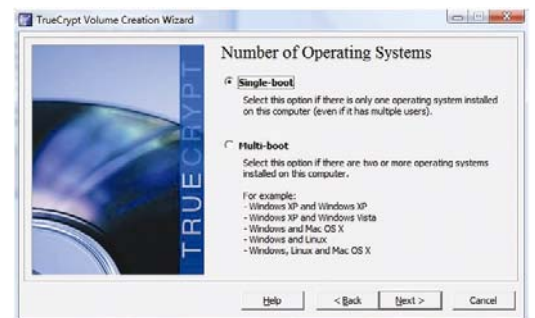


TrueCrypt offre la possibilité de d'encrypter soit tout le contenu du disque dur ou seulement la partition système. Si vous n'avez pas partitionné votre disque, il vous sera conseillé d'encrypter tout le disque, slack space inclus.

Dans notre exemple, nous cochons l'option « Encrypt the windows system partition ».



Une fois l'étape du choix de cryptage passé, veuillez choisir le type de boot (démarrage) du système. Si à part de Windows, aucun autre système d'exploitation n'est installé, vous devriez cocher la première option « Single-Boot », sinon « Multi-Boot ».



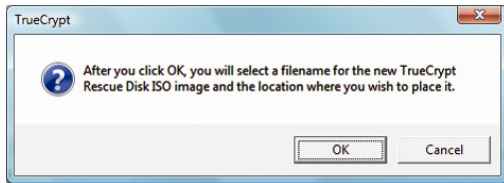
Lors de cette étape, il est demandé de choisir l'algorithme de cryptage et celui de hachage (Par défaut AES et RI-PEMD-160 : ces deux paramètres conviennent parfaitement).



Saisissez et confirmez le mot de passe. Choisissez un bon mot de passe, car ce sera sur la robustesse de ce mot de passe que reposera la sécurité du dossier crypté. Il est donc important que le niveau de robustesse soit élevé (au moins 8 caractères, avec caractères spéciaux, chiffres, lettres, minuscules et majuscules. Veuillez éviter les noms communs, les noms propres ou les noms d'animaux domestiques).



Ensuite, TrueCrypt génère une paire de clés de cryptage. Celle-ci va permettre à Truecrypt de crypter et décrypter le système tout en étant transparent aux yeux de l'utilisateur.



Il faut que vous graviez ce fichier sur un CD. Ainsi, vous aurez un CD de sauvetage pour le cas où vous ne pourriez plus accéder à la partition chiffrée. Veillez à ne pas graver le fichier en tant que tel, mais créez un CD sur base du fichier ISO que vous venez de sauvegarder (graver une image). Une fois le CD gravé, il est nécessaire de le réinjecter dans le lecteur pour que Truecrypt effectue ses opérations de vérifications sur la validité du CD.

Une fois ces vérifications terminées, votre ordinateur va redémarrer avec une interface basique ou le mot de passe créé précédemment est demandé. Ce redémarrage va permettre à Truecrypt d'effectuer des vérifications finales sur le système pour s'assurer que l'encryption est bien possible.

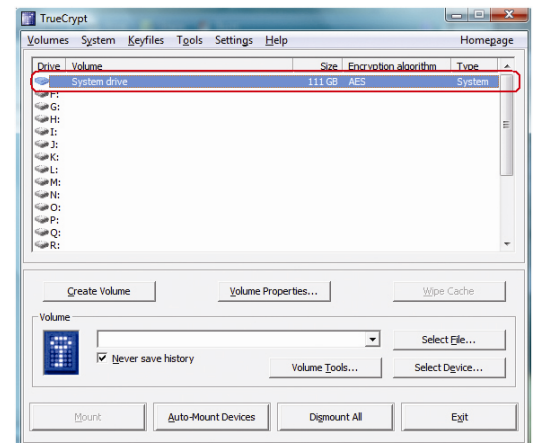
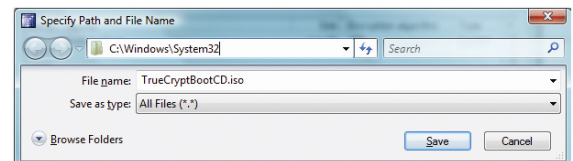
Une fois ces vérifications effectuées, Windows démarre normalement. Lorsque vous entrez dans la session utilisateur, un message Truecrypt apparaît, demandant la confirmation de l'encryption.

Après cette dernière validation, l'encryption de la partition commence. Notez que pour un disque de 100Go il faut environ 1 heure 30 minutes pour que l'opération se termine. Soyez donc patient et attendez la fin des opérations.

Après chiffrement réussi de toute la partition, Truecrypt affiche la partition système comme étant encryptée.

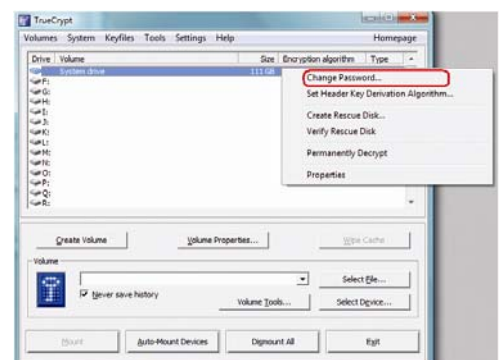


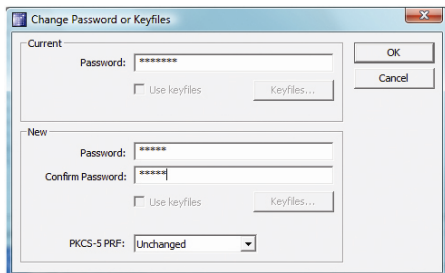
Une fois toutes ces étapes effectuées, l'image d'un disque de secours est générée automatiquement. Vous avez la possibilité de choisir son emplacement de sauvegarde. Le format est en ISO, il contient les outils nécessaires de récupération de Truecrypt dans le cas où le système de montage de la partition système serait défilant au démarrage.



Changement du mot de passe

Dans certains cas, par mesure de précaution, il est conseillé de modifier le mot de passe donnant accès à la partition encryptée. Pour cela, rien de plus simple, veuillez lancer l'outil truecrypt, puis faites un clic droit (bouton droit de la souris) sur la partition « System drive » et sélectionnez « change password ».





Une nouvelle fenêtre s'ouvre, demandant le mot de passe actuel, puis de saisir un nouveau mot de passe et le confirmer en le saisissant à nouveau.

Le message de confirmation annonce que l'opération a réussi.

Après avoir changé le mot de passe, il est conseillé de recréer un nouveau disque de sauvetage. En effet il est toujours possible, même après changement de mot de passe, de booter la partition système cryptée à partir de l'ancien disque de sauvetage en utilisant l'ancien mot de passe. Par mesure de sécurité il est donc indispensable de détruire l'ancien disque de sauvetage, après avoir créé un nouveau.

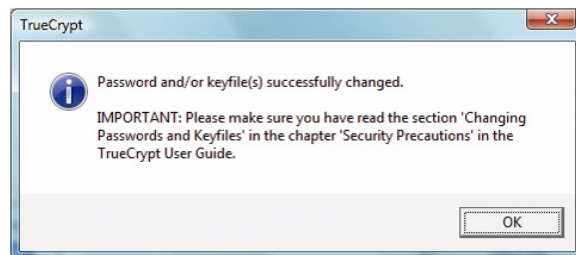
Comme décrit dans le chapitre précédent, l'image d'un disque de secours est générée automatiquement. Vous avez la possibilité de choisir son emplacement de sauvegarde. Le format est en ISO, il contient les outils nécessaires de récupération de Truecrypt dans le cas où le système de montage de la partition système serait défail-
lant au démarrage.

Après avoir créé le disque de sauvetage, vous devriez le contrôler. Ceci est fait en retournant sur l'outil Truecrypt, puis en faisant à nouveau un clic droit sur le « System Drive » et choisir « Verify Rescue Disk ».

Une fois ces étapes passées, le nouveau disque est opérationnel et il ne sera plus possible d'utiliser l'ancien avec l'ancien mot de passe pour booter la partition système encryptée.

Le CD de secours de TrueCrypt que l'on génère possède quelques options intéressantes pour le démarrage, avant d'entrer le mot de passe:

- L'une permet de décider de décrypter la partition de façon permanente
- L'autre permet de restaurer le loader system original sans encryptage. Dans ce cas, il faut avoir préalablement décrypté la partition de façon permanente. Au prochain démarrage, le système ne demandera plus de mot de passe dans l'interface du disque de récupération (fond noir) mais basculera directement sur le boot Windows.



Il est donc impératif de conserver rigoureusement et à l'abri des regards le CD de secours avec le mot de passe associé dans une enveloppe scellée par exemple.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu

©CASES
Édition 2008/10