

Chiffrement des portables

Mise en œuvre et utilisation

	Prénom Nom	Service
Propriétaire	François Morris	CNRS/DSI/RSSI
Rédigé par	François Morris	CNRS/DSI/RSSI
Validé par		

Historique des mises à jour			
Version	Date	Modifié par	Description du changement
1.0	21/03/2011	François Morris	Version initiale
1.0.1	14/03/2011	François Morris	Corrections de typos

Classification	Diffusion CNRS
Référence	manuel.docx
Version	1.0.1
Date	14/04/2011

Table des matières

Introduction.....	6
Séquestre et recouvrement	7
Mise en garde.....	7
Définitions	7
Séquestre d'un mot de passe d'un disque chiffrant	7
Séquestre du de passe d'un volume système TrueCrypt sous Windows.....	7
Séquestre du mot de passe d'un conteneur TrueCrypt.....	7
Séquestre du mot de passe FileVault sous Mac OS X	7
Séquestre du mot de passe dm-crypt sous Linux.....	7
Séquestre du code PIN d'une clé Corsair Padlock 2	8
Utilisation des outils de chiffrement.....	9
Utilisation d'un disque chiffrant sous Windows	10
Premier démarrage du PC chiffré.....	10
Démarrage du PC chiffré	11
Oubli du mot de passe.....	14
Démarrage de Windows avec un disque système chiffré avec TrueCrypt.....	15
Utilisation de FileVault sous MacOS X.....	16
Création d'un conteneur TrueCrypt sous Mac OS X.....	17
Création d'un conteneur (volume) chiffré	17
Séquestre.....	23
Utilisation d'un conteneur TrueCrypt Mac OS X.....	24
Montage d'un conteneur (volume) chiffré.....	24
Utilisation d'un disque chiffrant sous Linux	30
Démarrage du PC chiffré	30
Changement de mot de passe.....	30
Oubli du mot de passe.....	30
Démarrage avec dm-crypt sous Linux	31
Clé USB Corsair Padlock 2.....	32
Recommandations.....	32
Initialisation.....	32
Utilisation	32

Table des matières

Changement de code PIN	32
Création et utilisation de conteneurs chiffrés.....	32
Création d'un conteneur TrueCrypt sous Windows	34
Création d'un conteneur (volume) chiffré	34
Séquestre.....	38
Utilisation d'un conteneur TrueCrypt sous Windows	38
Montage d'un conteneur (volume) chiffré.....	38
Création d'un conteneur TrueCrypt sous Linux.....	42
Introduction.....	42
Création d'un conteneur (volume) TrueCrypt.....	42
Séquestre du mot de passe	48
Utilisation d'un conteneur TrueCrypt sous Linux.....	49
Montage d'un conteneur (volume) chiffré TrueCrypt.....	49
Démontage d'un conteneur (volume) chiffré TrueCrypt	51
Installation et administration des outils de chiffrement.....	54
Initialisation d'un disque chiffrant sous Windows	55
Introduction.....	55
Informations de recouvrement	55
Installation.....	55
Création d'un utilisateur.....	62
Installation de TrueCrypt sous Windows	66
Récupération du logiciel.....	66
Installation de TrueCrypt.....	66
Installer le français	69
Chiffrement d'un disque système sous Windows à l'aide de TrueCrypt	70
Recommandations.....	70
Chiffrement du disque système	70
Séquestre.....	84
Utilisation	84
Activation du chiffrement sous MacOS X.....	86
Mise en garde	89
Activation de FileVault	89
Séquestre.....	95
Installation de TrueCrypt sous Max OS X	96

Table des matières

Récupération du logiciel.....	96
Installation de TrueCrypt.....	96
Disque chiffrant sous Linux	100
Généralités	100
Installation d'une machine en dual boot Windows / Linux.....	100
Installation d'une machine sous Linux seul.....	101
Chiffrement du système avec dm-crypt sous Linux	102
Installation de Linux sur une partition chiffrée	102
Sauvegarde de l'en-tête	103
Installation de TrueCrypt sous Linux	104
Installation de TrueCrypt.....	104
Modification du fichier /etc/sudoers	104
FAQ.....	106
Que faire si le disque tombe en panne ?.....	106
Quid des clés USB avec empreinte digitale ?	107
Pourquoi la mise en veille est-elle désactivée ?.....	107
Quelle est la différence entre la protection offerte par un disque chiffrant et un disque verrouillé par un mot de passe au BIOS ?.....	107
Qu'apportent les nouvelles instructions AES ?	107
Comment savoir si la machine possède un disque chiffrant ?	108
Que faire si le mot de passe a été compromis ?	108

Introduction

La [note](#) du 16 janvier 2011 définit la politique de chiffrement à mettre en œuvre pour assurer la protection des ordinateurs portables.

Elle traduit la volonté de garantir au mieux la sécurité des données dans un souci de facilité de déploiement et surtout d'utilisation, gage d'appropriation pérenne par les utilisateurs.

Cette documentation décrit le déploiement du chiffrement. Il ne faut pas s'affoler devant la taille de cette-ci, elle est due à la nécessaire prise en compte de la multiplicité des matériels, des systèmes d'exploitation. De plus une très grande partie ne concerne que les administrateurs qui installent initialement les machines. Pratiquement pour l'usage quotidien, les utilisateurs n'ont besoin que d'un nombre très limité d'informations.

La documentation est organisée selon la séquence suivante :

1. Considération générales sur le chiffrement
2. Utilisation des outils chiffrement
3. Création et utilisation de conteneurs chiffrés
4. Installation et administration des outils de chiffrement
5. FAQ (questions fréquemment posées)

L'ensemble de la documentation est disponible sous la forme d'un manuel [PDF](#) ou de [pages web](#).

Il existe une liste chiffrement@services.cnrs.fr pour faciliter les échanges entre les personnes qui ont à mettre en œuvre ces différents outils. Pour s'abonner à cette liste se connecter à <https://listes.services.cnrs.fr/www/subscribe/chiffrement>

Séquestre et recouvrement

Mise en garde

Attention la mise en place d'une procédure de recouvrement comme le séquestre du mot de passe ne dispense absolument pas de la sauvegarde régulière des données.

Définitions

Le recouvrement est la procédure qui permet d'accéder à une information qui a été chiffrée en cas d'oubli du mot de passe ou de l'indisponibilité de son détenteur.

La méthode la plus simple consiste tout simplement à noter le mot de passe sur une feuille de papier que l'on met dans une enveloppe cachetée et rangée en lieu sûr. On parle alors de séquestre.

Il est aussi possible de permettre à une autre personne d'accéder, avec son propre mot de passe, à l'information. Cette personne est appelée agent de recouvrement. A moins d'avoir plusieurs agents de recouvrement, il faudra procéder au séquestre du mot de passe de l'agent de recouvrement.

Séquestre d'un mot de passe d'un disque chiffrant

Le mot de passe à conserver est celui de l'administrateur qui a été choisi lors de l'initialisation du disque. Il permet de débloquent un utilisateur qui aurait perdu son mot de passe. Il n'est donc pas utile de séquestrer le mot de passe de l'utilisateur. Le mieux est de conserver la feuille qui a été imprimée ou une copie du fichier généré sur une clé USB lors de l'initialisation du disque.

Séquestre du mot de passe d'un volume système TrueCrypt sous Windows

Pour un chiffrement du système avec TrueCrypt, il faut conserver à la fois le mot de passe et le CD de récupération. Le plus simple est de mettre le CD dans la même enveloppe que le mot de passe.

Séquestre du mot de passe d'un conteneur TrueCrypt

Il faut bien évidemment à chaque changement de mot de passe procéder à nouveau à l'opération de séquestre. Cependant cette opération n'est pas conseillée par les auteurs de TrueCrypt. En effet le changement de mot de passe ne modifie pas la clé maîtresse qui sert au chiffrement symétrique du disque et si on suspecte que le mot de passe a été compromis, on doit aussi présumer que la clé maîtresse l'a été aussi. La bonne démarche est alors de créer un nouveau conteneur chiffré, avec un nouveau mot de passe et d'y transférer le contenu de l'ancien conteneur.

Il n'est pas vraiment utile de procéder à une sauvegarde de l'en-tête du conteneur car il existe une sauvegarde de l'en-tête ailleurs dans le conteneur.

Séquestre du mot de passe FileVault sous Mac OS X

Le mot de passe à conserver est le mot de passe maître qui a été choisi lors de l'initialisation du chiffrement du répertoire personnel de l'utilisateur. Il permet de débloquent un utilisateur qui aurait perdu son mot de passe. Il n'est donc pas utile de séquestrer le mot de passe de l'utilisateur.

Séquestre du mot de passe dm-crypt sous Linux

A la différence d'autres outils de chiffrement dm-crypt/LUKS ne maintient pas en interne de copie de l'en-tête. Cela signifie que si pour une raison ou une autre, il est corrompu ou illisible, il ne sera pas possible de récupérer les informations. Il est donc conseillé de conserver outre le mot de passe une sauvegarde de l'en-tête.

Séquestre du code PIN d'une clé Corsair Padlock 2

Il est théoriquement possible d'établir un code maître pour permettre le recouvrement en cas d'oubli par l'utilisateur de son mot de passe. L'opération s'avère délicate et la notice à ce sujet est peu claire sinon erronée. Comme une clé USB n'est destinée qu'à transférer de l'information d'une machine à une autre et que l'on attendra d'être sûr que les données ont été copiées sur la machine de destination avant de les effacer de la machine source, le séquestre n'est pas d'une absolue nécessité.

Utilisation des outils de chiffrement

La documentation est organisée par système d'exploitation

1. Windows
2. Mac OS X
3. Linux
4. Clé USB chiffrée (indépendant des systèmes d'exploitation)

Utilisation d'un disque chiffrant sous Windows

Utilisation d'un disque chiffrant sous Windows

Premier démarrage du PC chiffré

Le disque chiffrant doit avoir préalablement [initialisé](#) par un administrateur.

Au démarrage, l'écran suivant apparait



Choisir l'utilisateur, le domaine et donner le mot de passe provisoire du disque.

Ouvrir une session Windows en fournissant l'identifiant et le mot de passe Windows. Par la suite l'ouverture de la session Windows sera automatique et il n'y aura plus à fournir que le mot de passe protégeant le disque.

Il est demandé de changer le mot de passe provisoire du disque, donner comme nouveau mot de passe celui de Windows.

Démarrage du PC chiffré

Au démarrage, l'écran suivant apparait

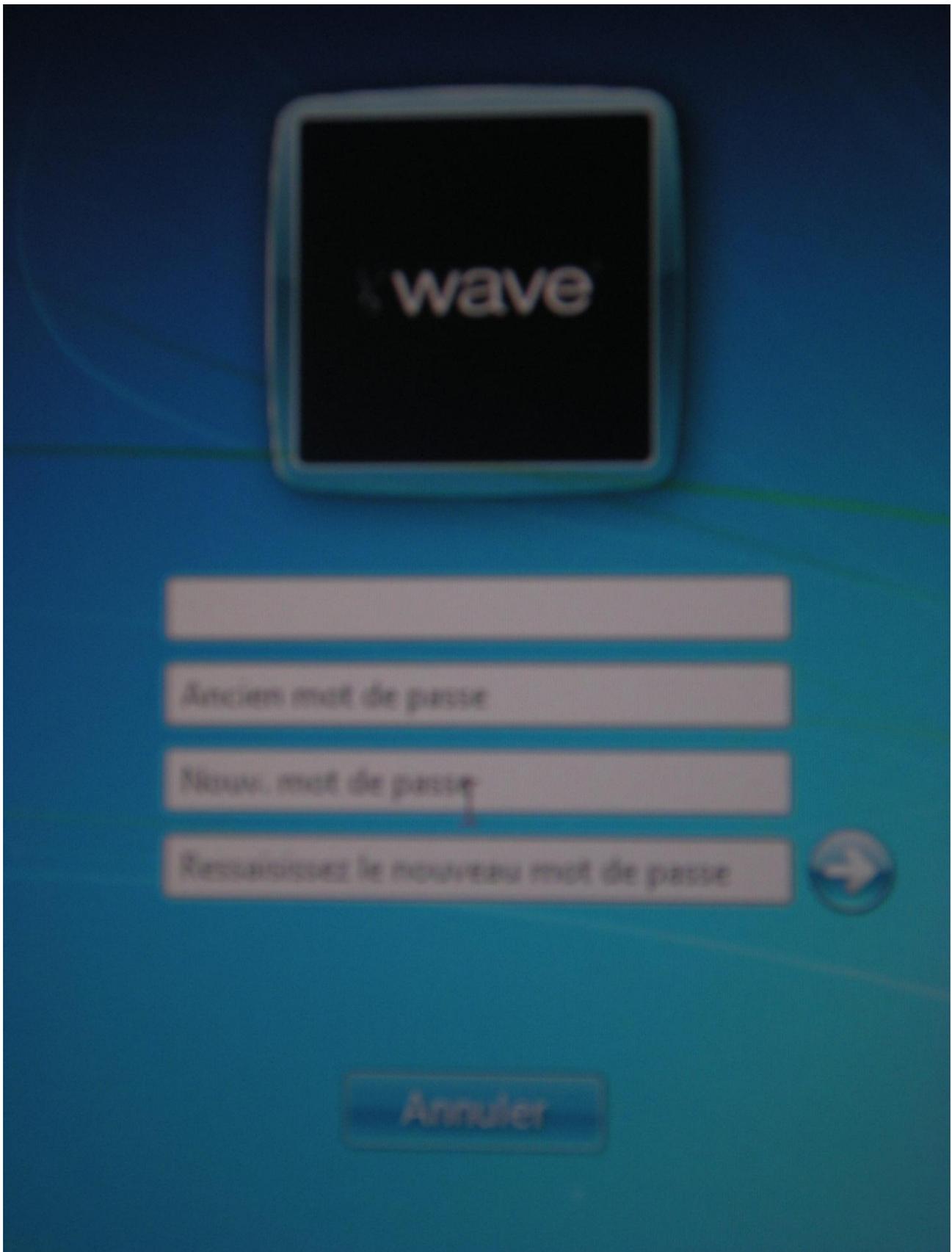


L'utilisateur étant mémorisé d'une session sur l'autre, il suffit d'entrer le mot de passe. Le disque sera alors déverrouillé et automatiquement la session Windows sera ouverte.

Changement de mot de passe

Le changement de mot de passe Windows s'effectue de la façon habituelle.

Ctrl+Alt+Suppr puis « Modifier un mot de passe... »



Le changement de mot de passe Windows sera automatiquement répercuté sur celui protégeant le disque.

Utilisation d'un disque chiffrant sous Windows

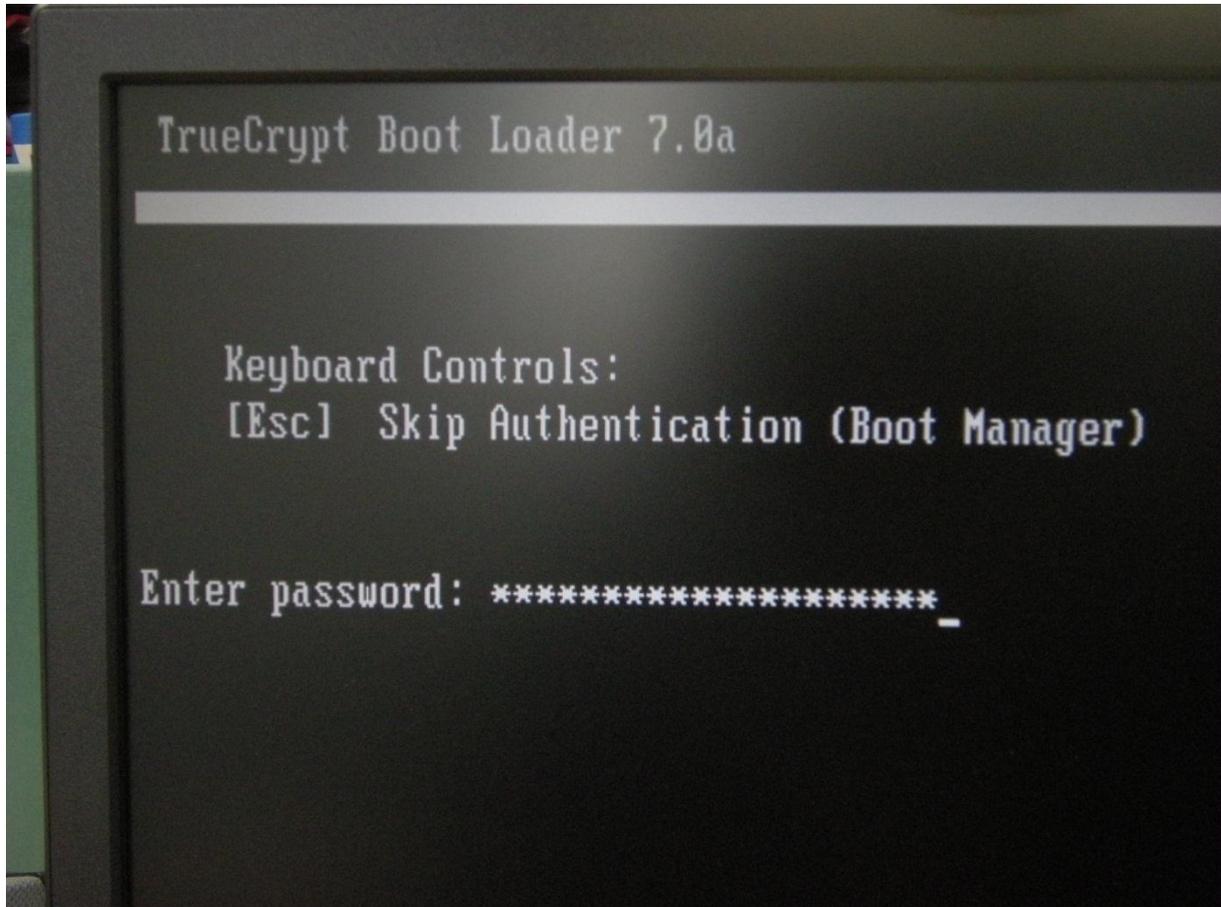
Oubli du mot de passe

En cas d'oubli de son mot de passe il faut s'adresser à son administrateur qui procédera au recouvrement.

Démarrage de Windows avec un disque système chiffré avec TrueCrypt

Démarrage de Windows avec un disque système chiffré avec TrueCrypt

Avant le démarrage de Windows il faut fournir le mot de passe TrueCrypt.



Ensuite le démarrage de Windows s'effectue normalement.

Utilisation de FileVault sous MacOS X

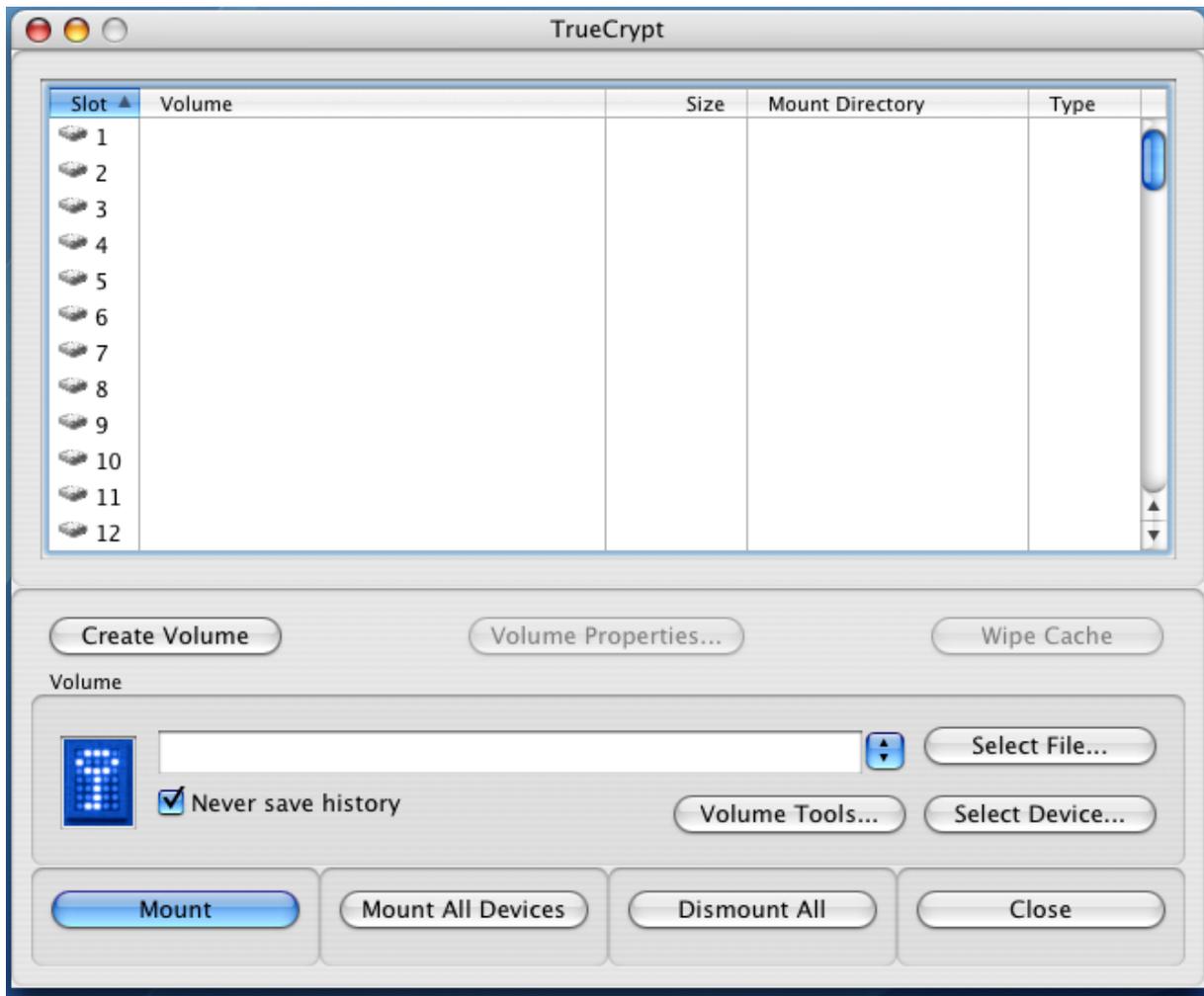
L'utilisation d'un répertoire chiffré avec FileVault est totalement transparente à l'utilisateur. Le fait de fournir son mot de passe pour ouvrir une session déverrouille l'accès et permet le déchiffrement du répertoire.

Création d'un conteneur TrueCrypt sous Mac OS X

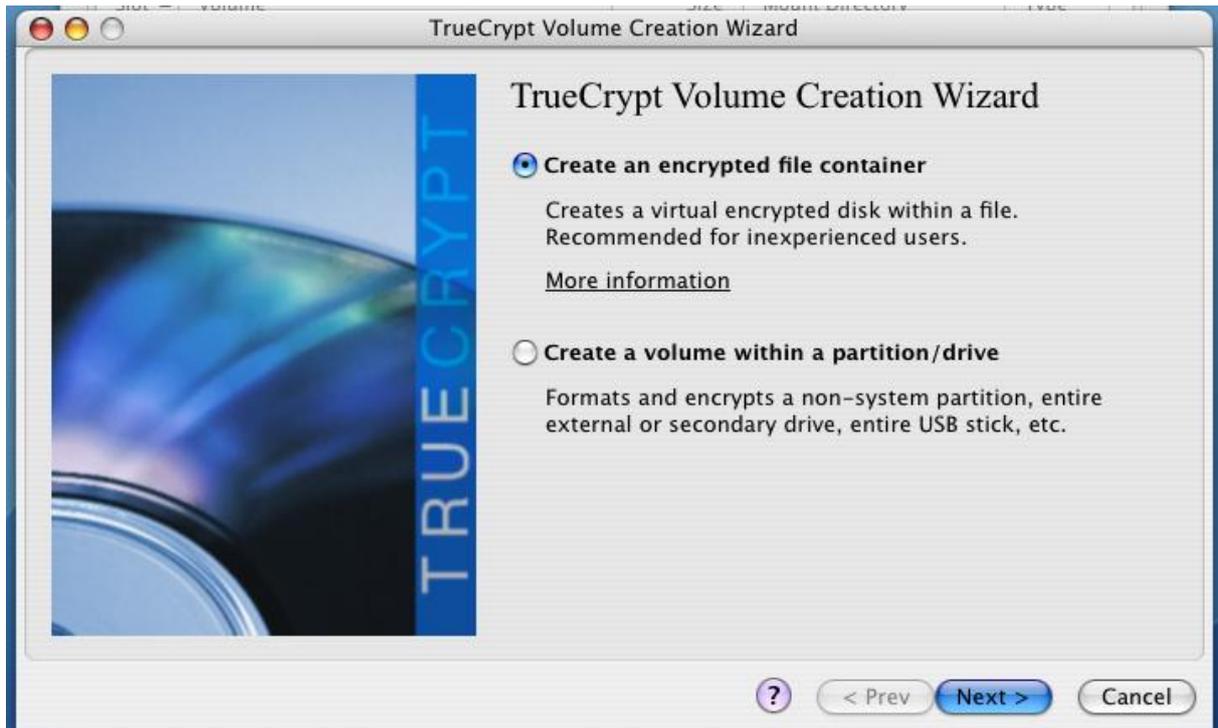
Création d'un conteneur (volume) chiffré

Le logiciel TrueCrypt doit avoir préalablement été [installé](#) par une personne possédant les privilèges administrateur.

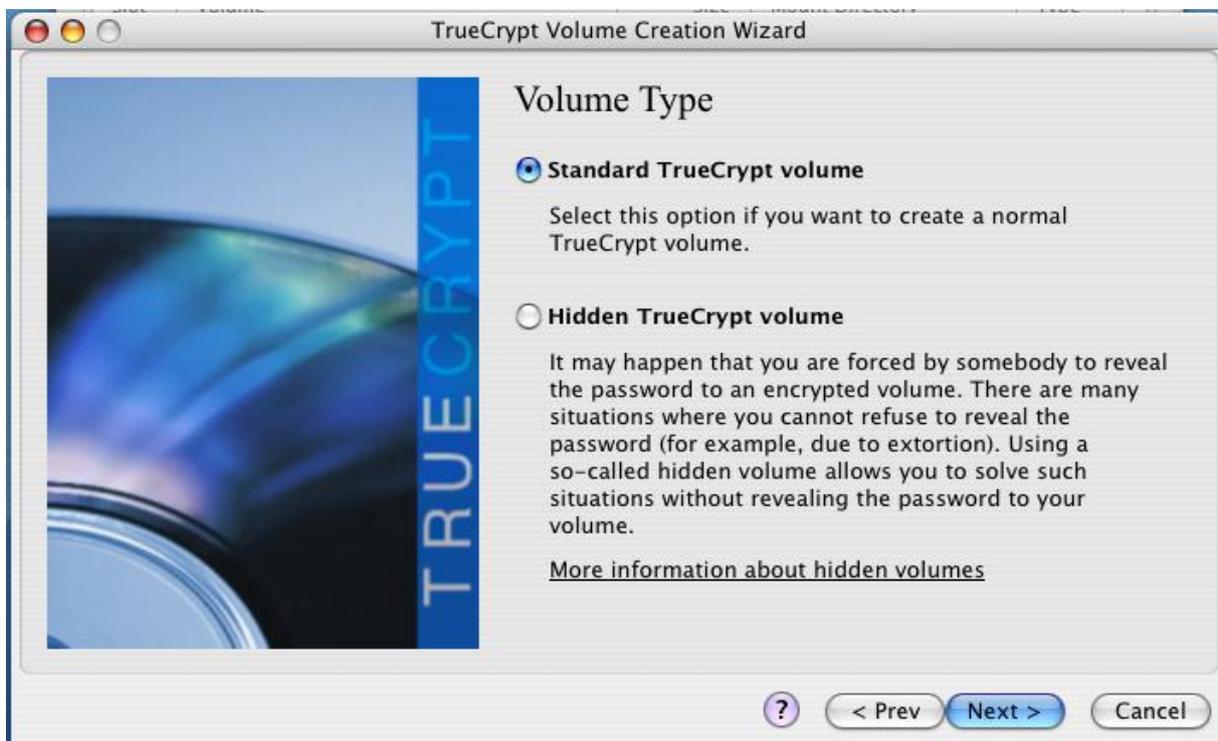
Lancez TrueCrypt



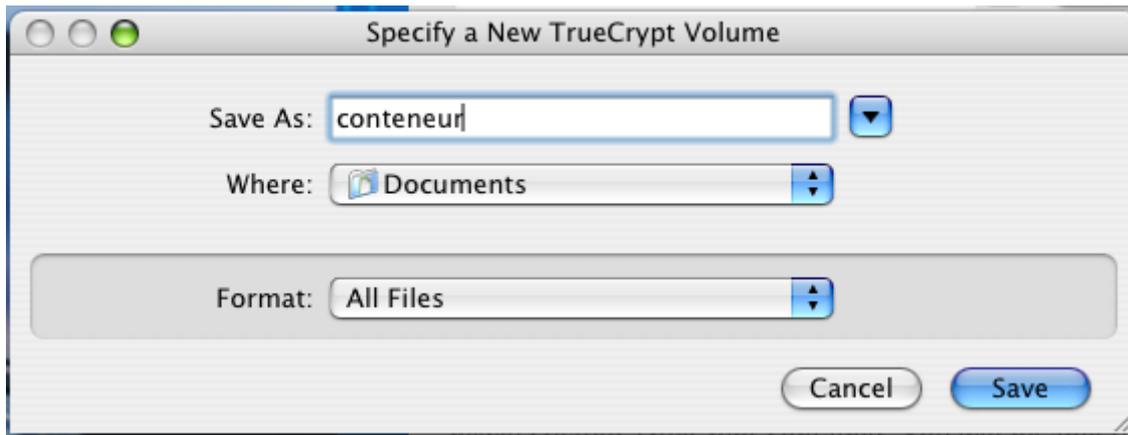
Cliquez sur « **Create Volume** »



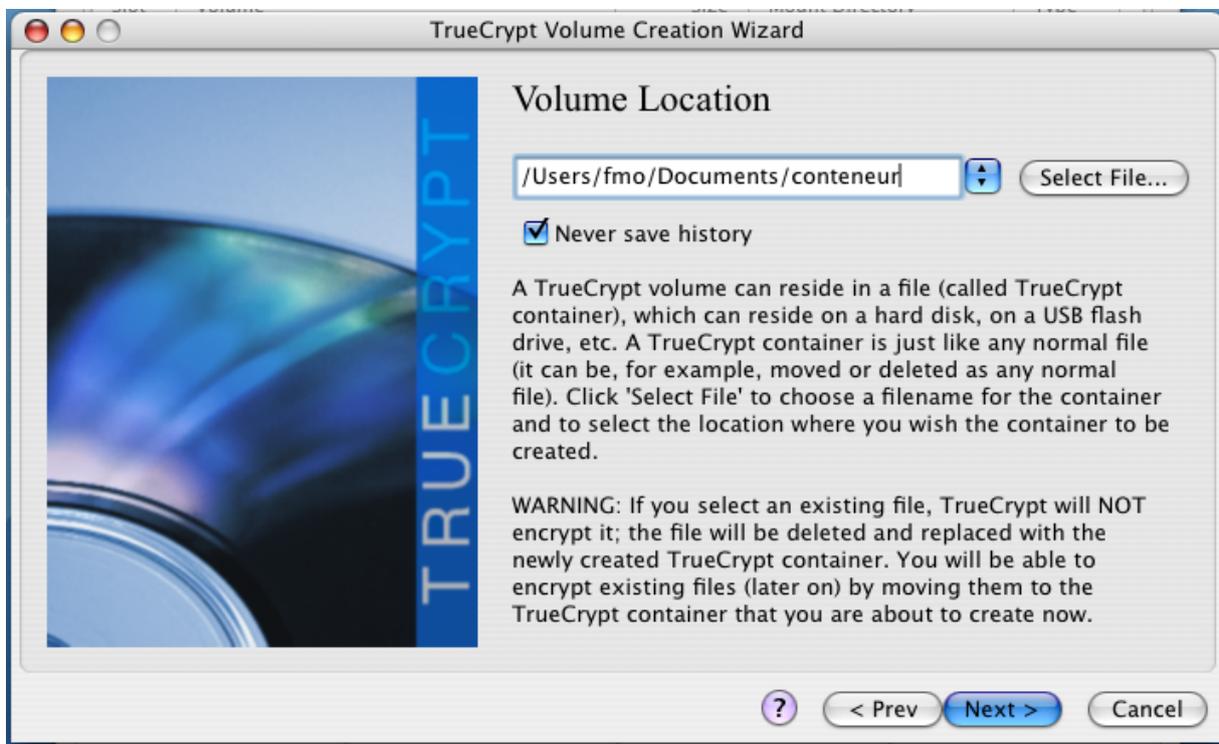
Cocher « **Create an encrypted file container** » et cliquer sur « **Next >** »



Cocher « **Standard TrueCrypt volume** » et cliquer sur « **Next >** »

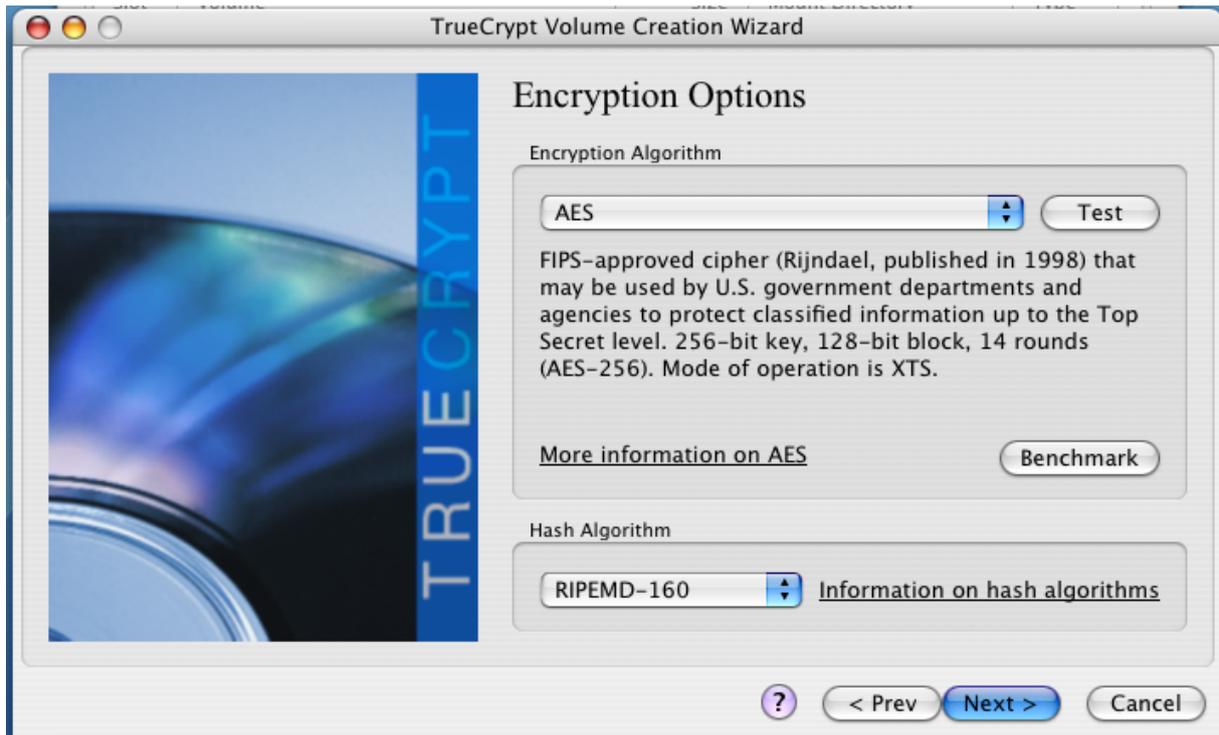


Choisissez un fichier et cliquez sur « **Save** »

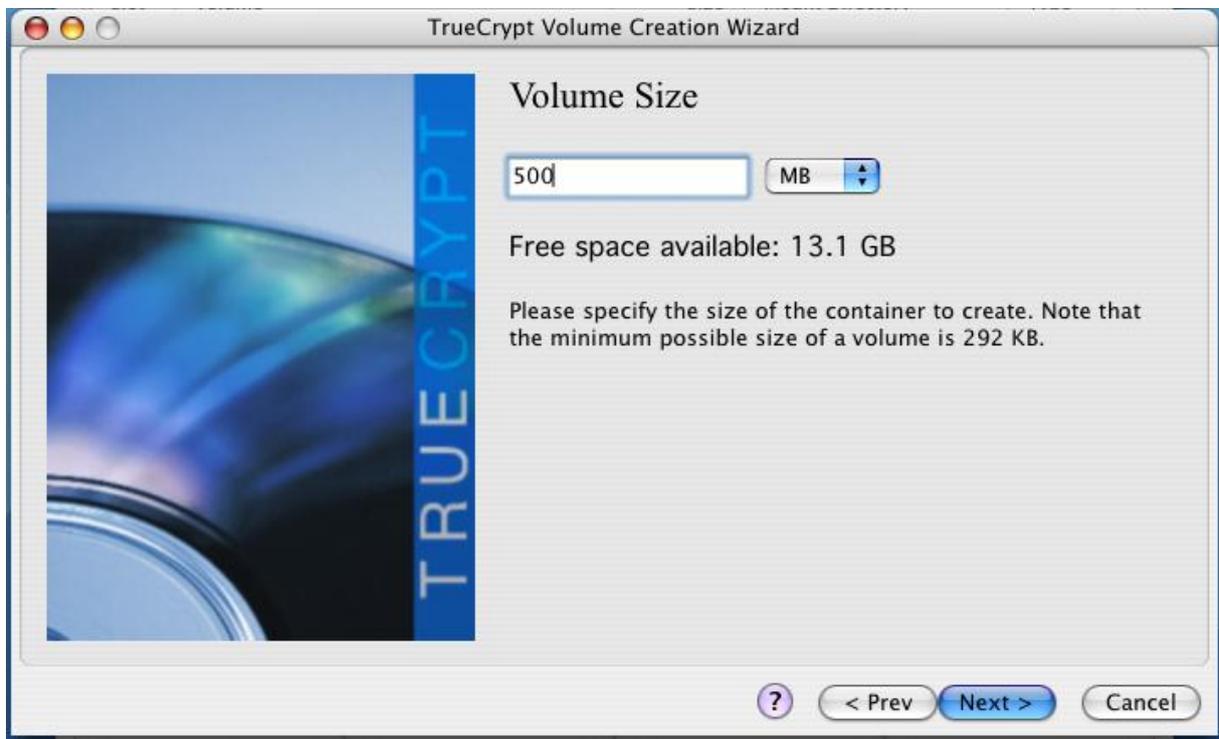


Cochez « **Never save history** » et cliquer sur « **Next >** »

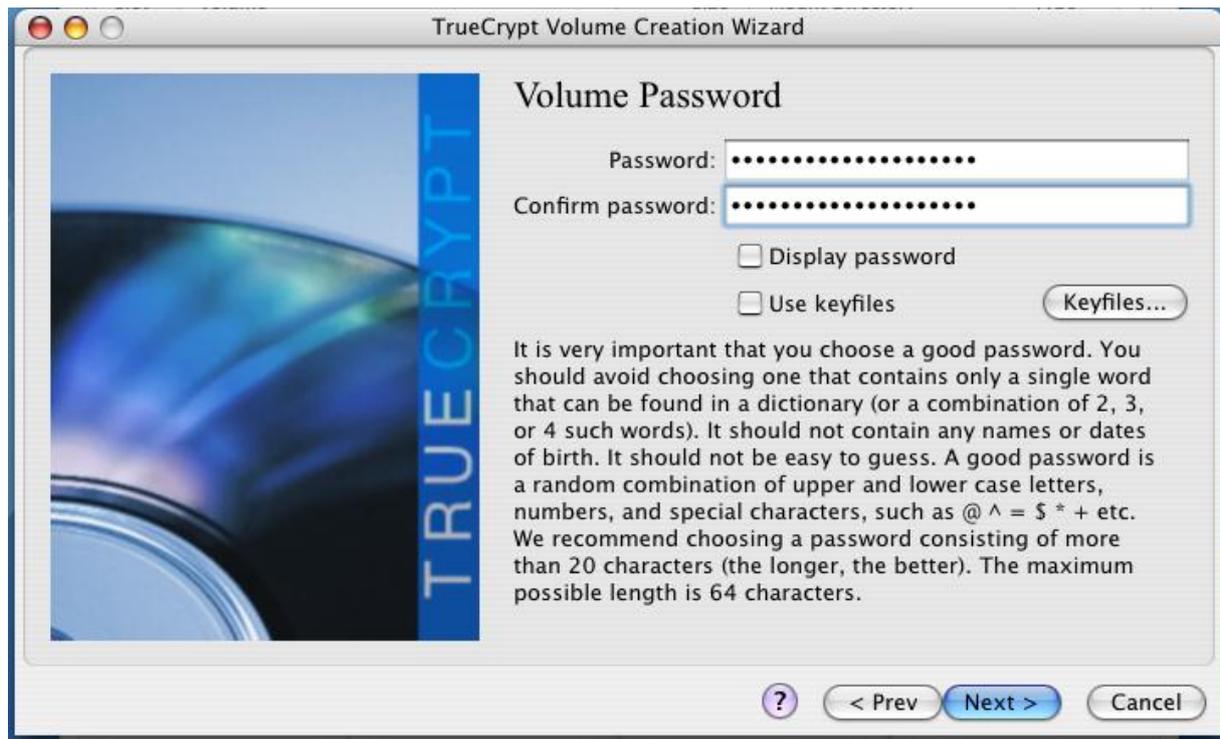
Création d'un conteneur TrueCrypt sous Mac OS X



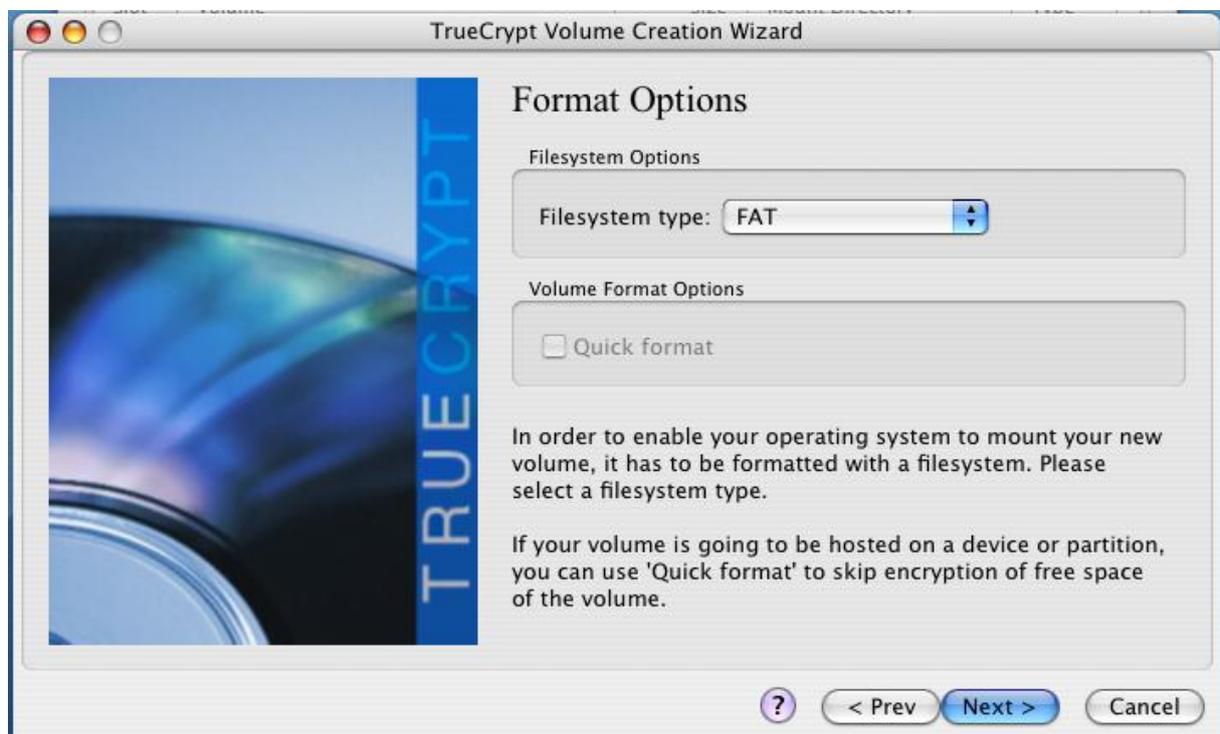
Conservez les valeurs par défaut « **AES** » pour l'algorithme de chiffrement et « **RIPEMD-160** » pour l'algorithme de hachage et cliquez sur « **Next >** »



Choisir une taille de volume et cliquez sur « **Next >** »

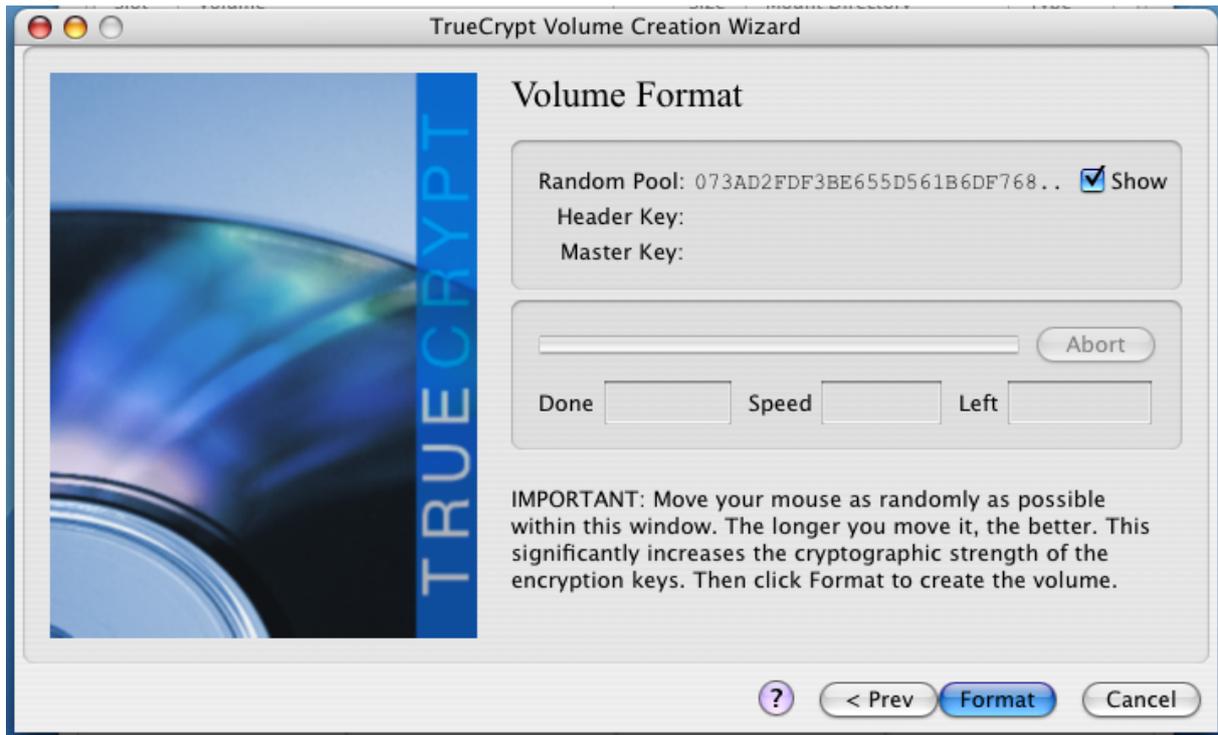


Choisissez un mot de passe robuste. Cliquer sur « **Next >** »



Pour créer un conteneur sur un support amovible (clé USDB, carte SD, etc., il est préférable de choisir lorsque cela est possible un système de fichiers « FAT ». En effet celui-ci est compatible avec les différentes plateformes (Windows, MacOS, Linux). Cliquez sur « **Next >** »

Création d'un conteneur TrueCrypt sous Mac OS X



Déplacer la souris aléatoirement comme demandé et cliquer sur « **Format** »



Cliquer sur «**OK** »



Cliquer sur « **Exit** »

Séquestre

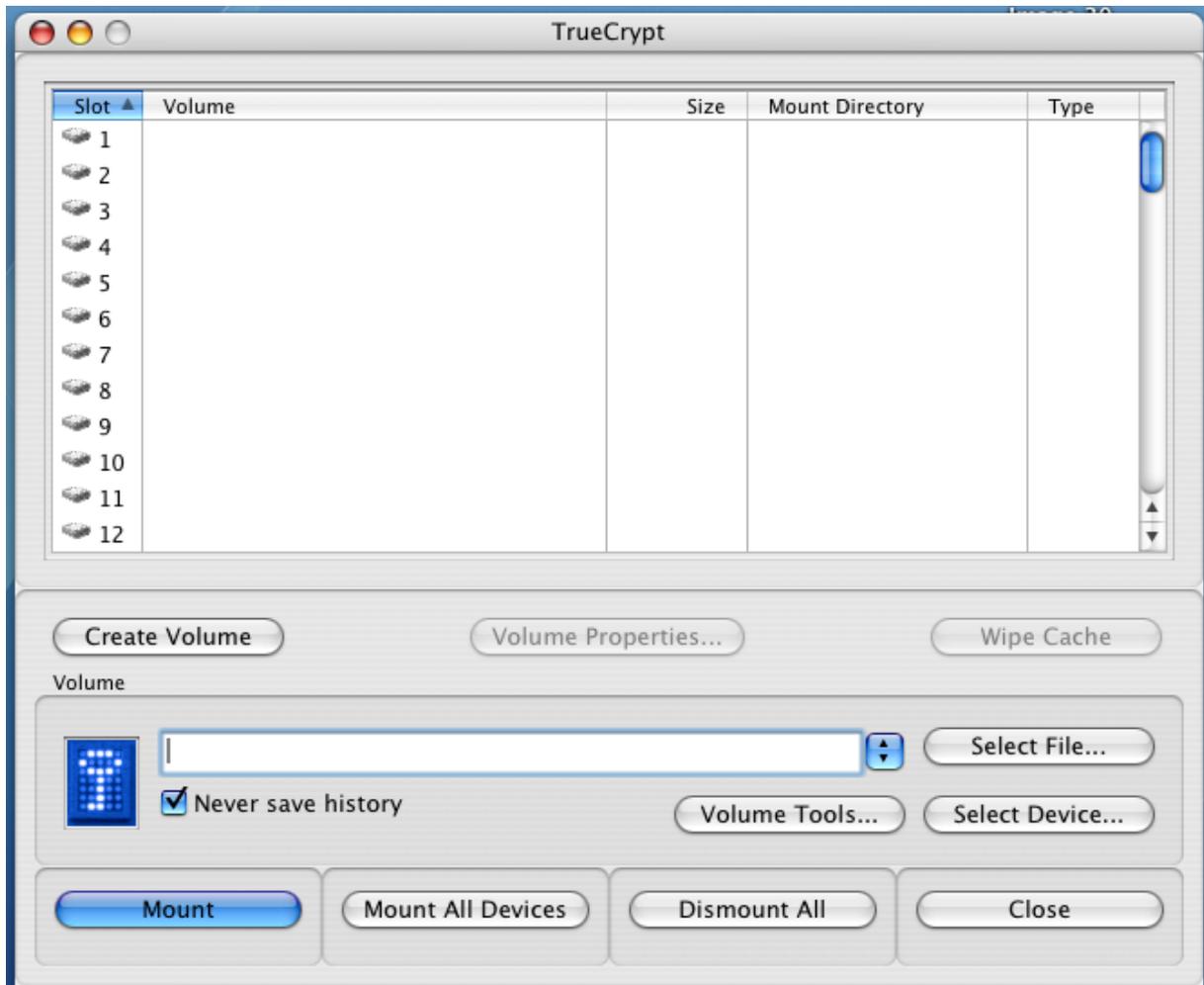
Pour permettre le recouvrement en cas d'oubli du mot de passe ou d'indisponibilité de l'utilisateur, il est impératif de procéder au [séquestre](#) du mot de passe, en le notant et le rangeant en lieu sûr.

Utilisation d'un conteneur TrueCrypt Mac OS X

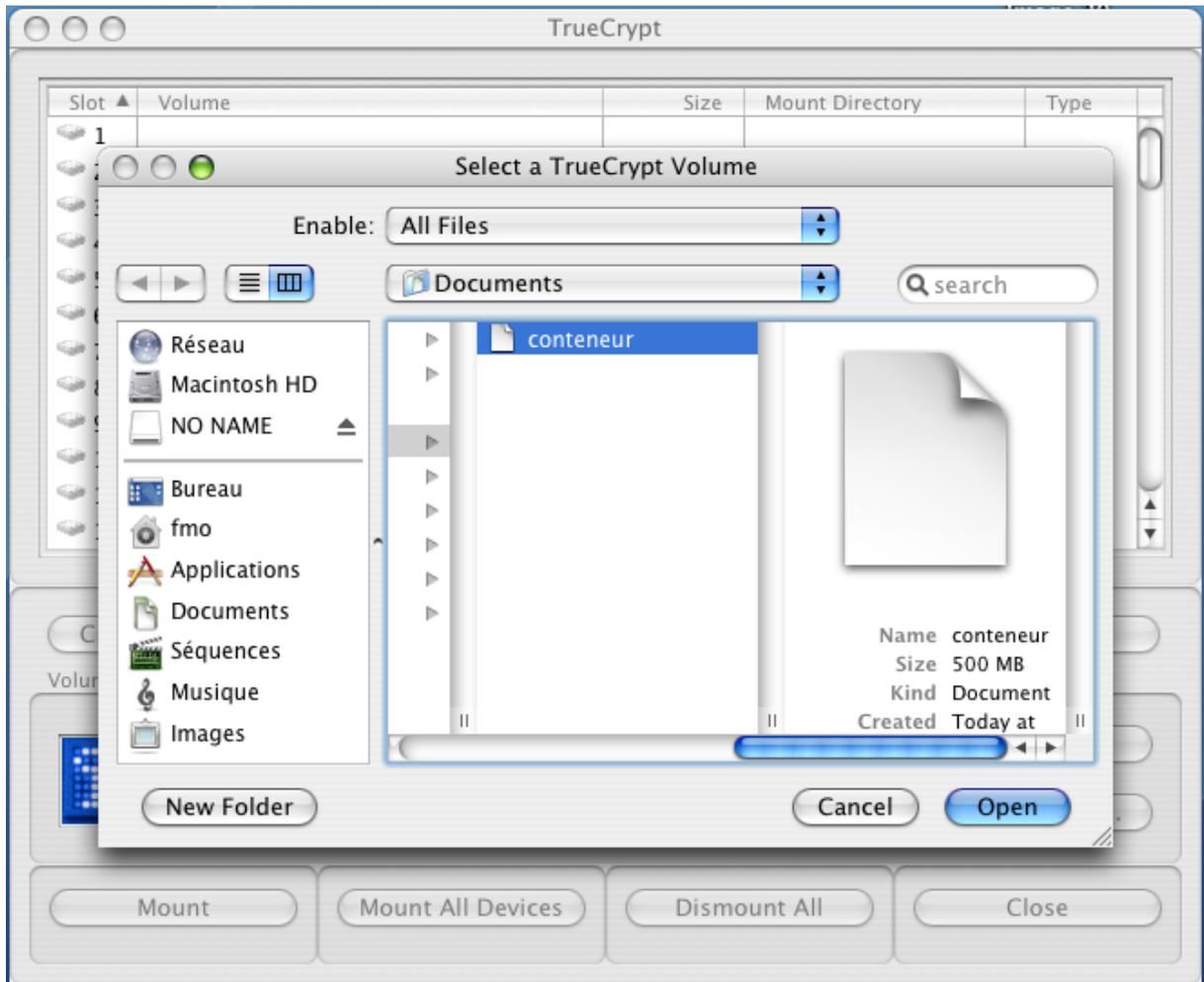
Montage d'un conteneur (volume) chiffré

Il faut au préalable avoir [créé](#) un conteneur (volume) TrueCrypt.

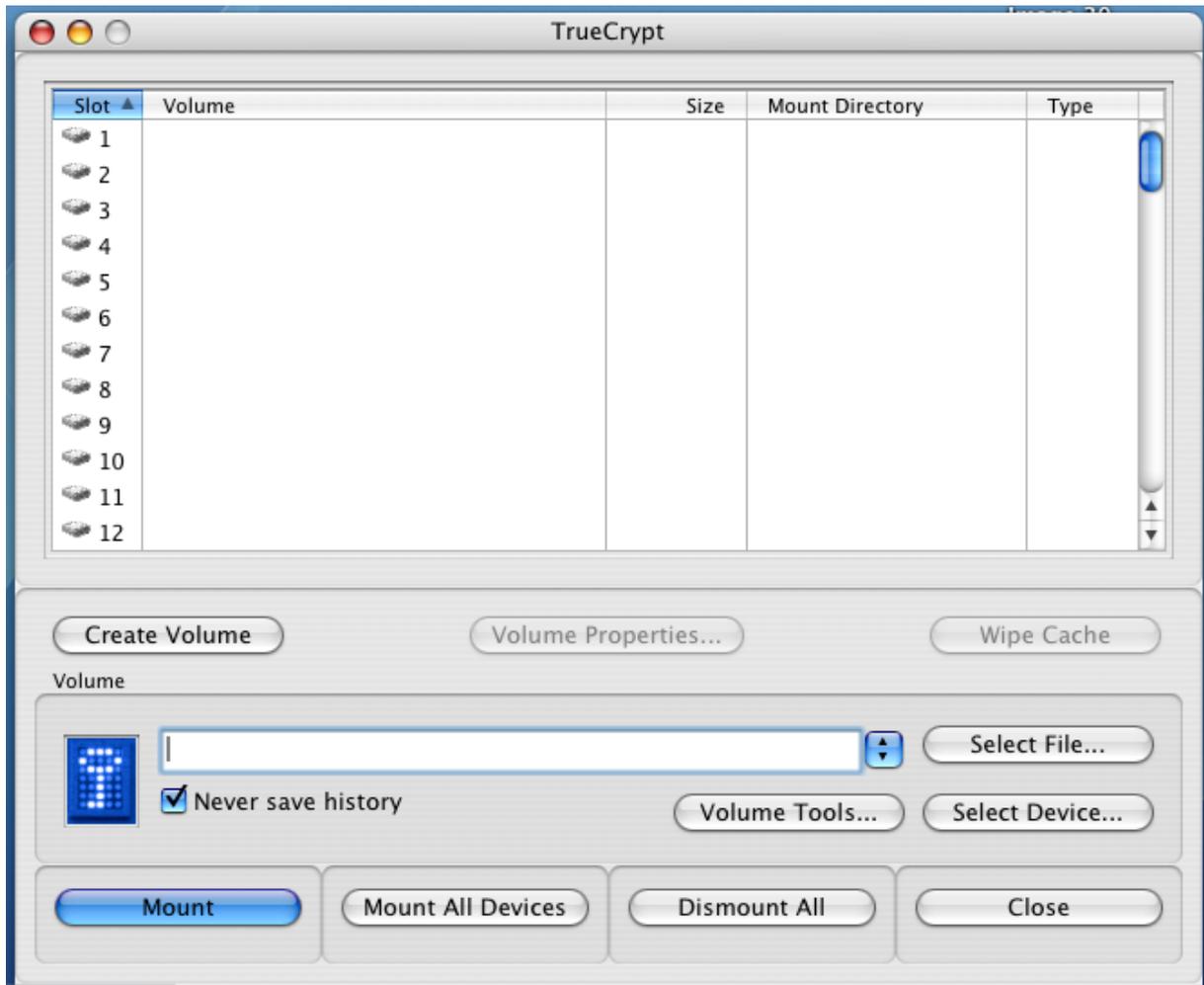
Lancez le logiciel TrueCrypt



Cliquez sur « **Select File...** »



Choisissez le fichier et cliquez sur « **Open** »



Sélectionnez un numéro de slot libre et cliquez sur « **Mount** »



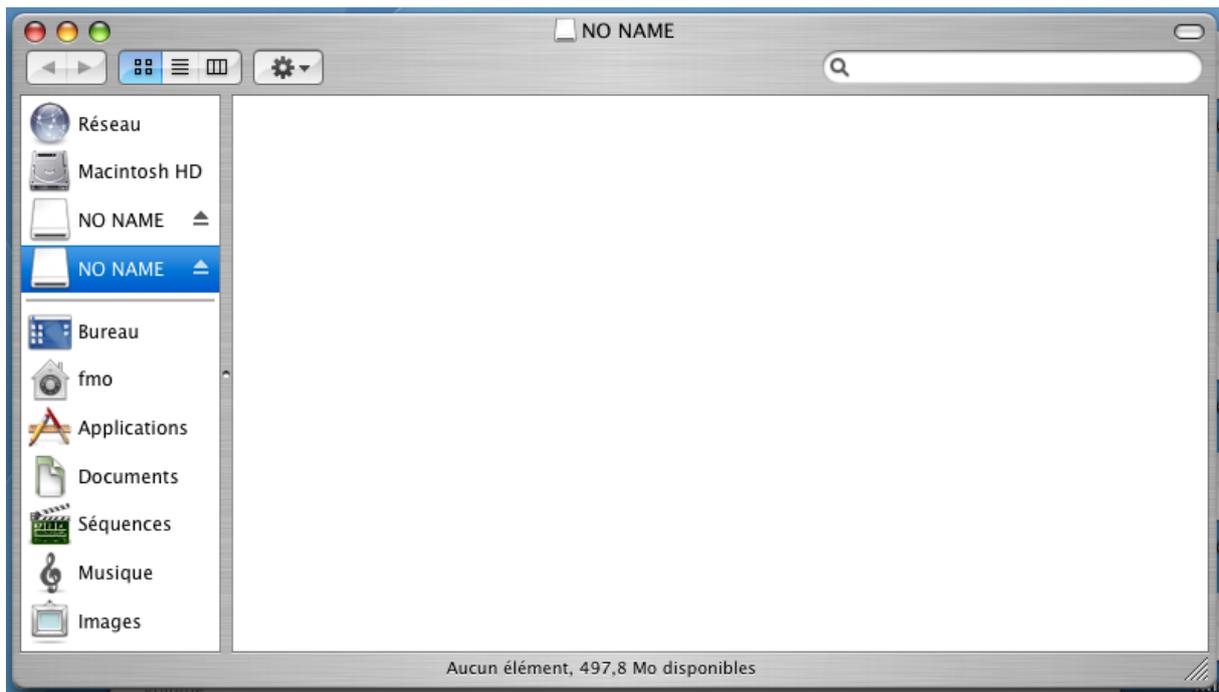
Entrez le mot de passe et cliquez sur « **OK** »

Désormais un nouveau disque (NO NAME) est visible



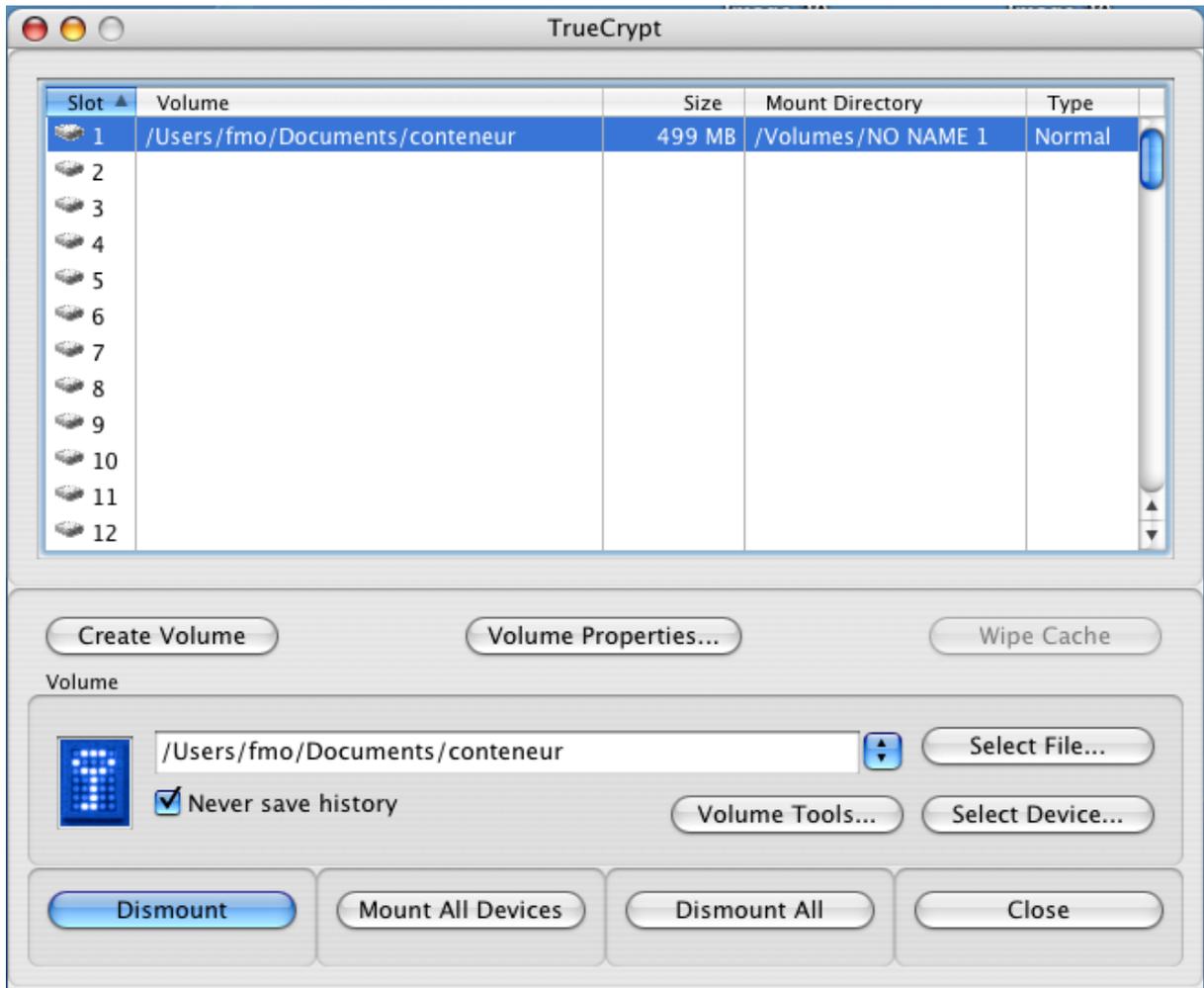
Utilisation d'un conteneur TrueCrypt sous Mac OS X

Il est utilisable comme un disque classique.

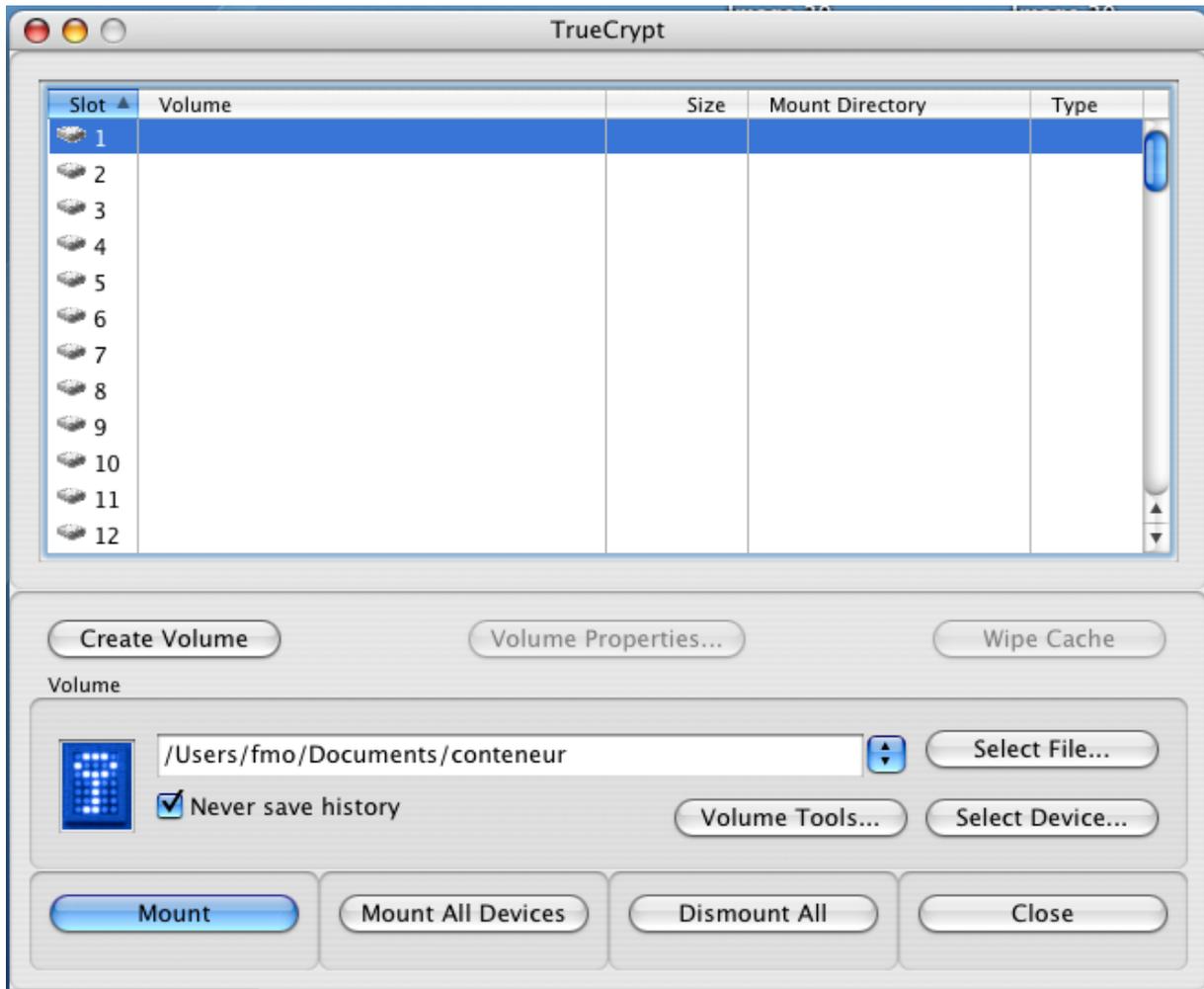


Démontage d'un conteneur (volume) chiffré

Si la fenêtre TrueCrypt n'est pas visible, la faire apparaître en cliquant sur l'icône TrueCrypt



Sélectionner le conteneur (volume) et cliquer sur « **Dismount** »



Cliquer sur « **Close** »

Utilisation d'un disque chiffrant sous Linux

Le disque chiffrant doit avoir préalablement [initialisé](#) sous Windows par un administrateur.

Démarrage du PC chiffré

Au démarrage, l'écran suivant apparaît



L'utilisateur étant mémorisé d'une session sur l'autre, il suffit d'entrer le mot de passe. Le disque sera alors déverrouillé et le système Linux démarrera de la façon habituelle.

Changement de mot de passe

Le changement de mot de passe du disque ne peut s'effectuer que sous Windows.

Oubli du mot de passe

En cas d'oubli de son mot de passe, il faut s'adresser à son administrateur qui procédera au recouvrement.

Démarrage avec dm-crypt sous Linux

Démarrage avec dm-crypt sous Linux

L'utilisation ne pose pas de problème. Au tout début du démarrage du système, il est demandé de fournir le mot de passe qui sert à déchiffrer le disque. Voici un exemple avec une distribution Fedora.

```
Password for filesystem:*****_
```

Ensuite le démarrage se poursuit de la façon habituelle.

Clé USB Corsair Padlock 2

Recommandations

Les clés USB sont destinées à l'échange de données entre machines. Etant donné leur fragilité et la facilité avec laquelle on peut les perdre ou se les faire voler, les clés USB ne doivent pas servir de support primaire pour l'information. Il ne faut pas non plus effacer les données sur la machine source avant d'être certain qu'elles sont bien transférées sur la machine de destination. Une procédure de recouvrement ou un séquestre du mot de passe n'est pas absolument nécessaire puisqu'il est toujours possible de retrouver les informations sur la machine source.

Le chiffrement est matériel, totalement indépendant du système d'exploitation et n'exige aucun logiciel spécifique sur la machine.

La notice est disponible sur le site du fabricant <http://www.corsair.com>

<http://www.corsair.com/media/cms/manual/PadlockUserManual.pdf>

Initialisation

Pour activer le chiffrement et établir le code PIN :

1. Appuyer sur la touche marquée d'un clé pendant 3 secondes, les diodes verte et rouge s'allument.
2. Entrez le code PIN désiré (4 à 10 chiffres) en appuyant sur les touches marquées d'un chiffre, les diodes verte et rouge clignotent une fois et restent allumées.
3. Appuyez sur la touche marquée d'une clé, les diodes verte et rouge clignotent simultanément.
4. Entrez à nouveau le code PIN pour vérification.
5. Appuyez sur la touche marquée d'une clé et la relâchez la, la diode verte s'allume.

Utilisation

Pour déverrouiller la clé :

1. Appuyez sur la touche marquée d'une clé et relâchez la, les diodes verte et rouge clignotent simultanément.
2. Entrez les différents chiffres du code PIN.
3. Pressez sur la touche marquée d'une clé et relâchez la, la diode verte clignote pendant 20 secondes (c'est le délai pendant lequel vous avez à introduire la clé, passé ce délai la clé se verrouille automatiquement) .
4. Introduire la clé dans l'ordinateur, la diode verte reste allumée tant que la clé USB reste connectée à l'ordinateur.

Changement de code PIN

Pour changer le code PIN :

1. Appuyez sur la touche marquée d'une clé et relâchez la, les diodes verte et rouge clignotent simultanément.
2. Entrez le code PIN actuel.
3. Pressez sur la touche marquée d'une clé et relâchez la, la diode verte clignote pendant 20 secondes.

4. Appuyer sur la touche marquée d'un clé pendant 3 secondes, les diodes verte et rouge s'allument.
5. Entrez le code PIN désiré (4 à 10 chiffres) en appuyant sur les touches marquées d'un chiffre, les diodes verte et rouge clignotent une fois et restent allumées.
6. Entrez à nouveau le code PIN pour vérification.
7. Appuyez sur la touche marquée d'une clé et la relâchez-la, la diode verte s'allume.

Création et utilisation de conteneurs chiffrés

Les conteneurs chiffrés constituent un deuxième niveau de protection pour stocker des informations particulièrement sensibles. Leur utilisation n'exclue pas le chiffrement intégral du disque de l'ordinateur portable.

Ils sont aussi utilisés pour protéger les informations transportées sur des clés USB lorsque l'on ne dispose pas de clé USB chiffrée (Corsair Padlock2).

La documentation est organisée par système d'exploitation :

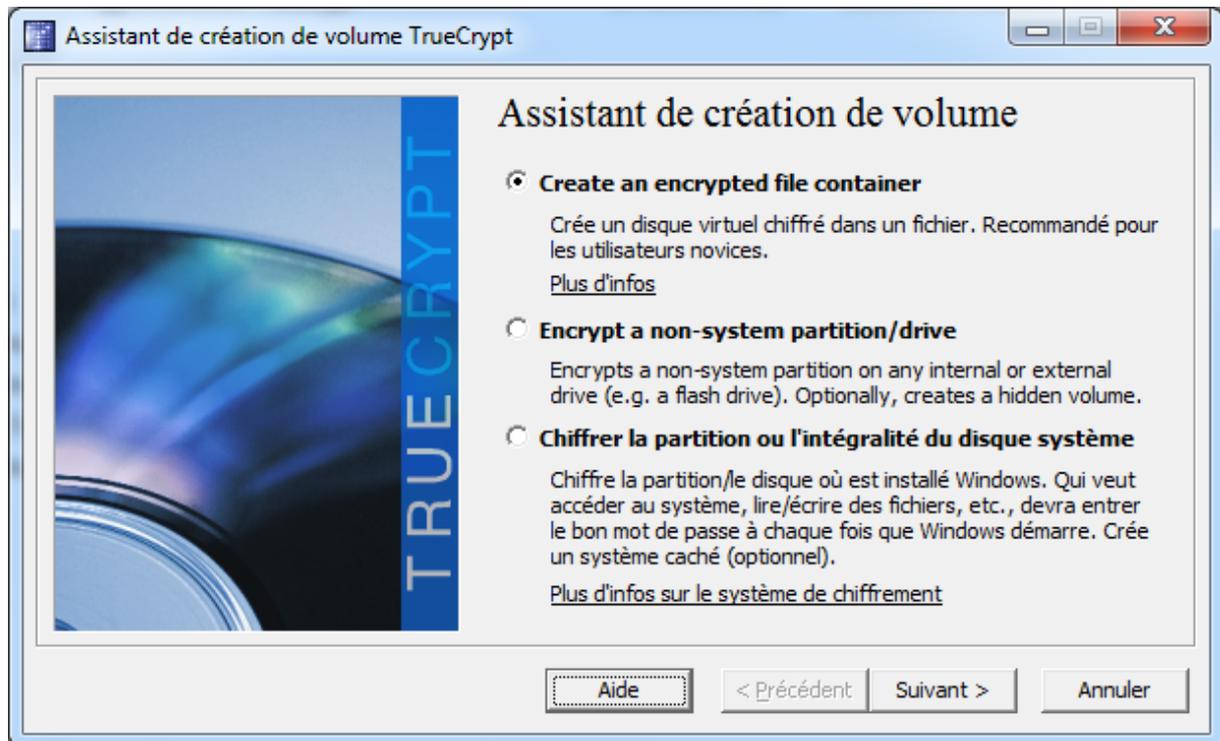
1. Windows
2. Mac OS X
3. Linux

Création d'un conteneur TrueCrypt sous Windows

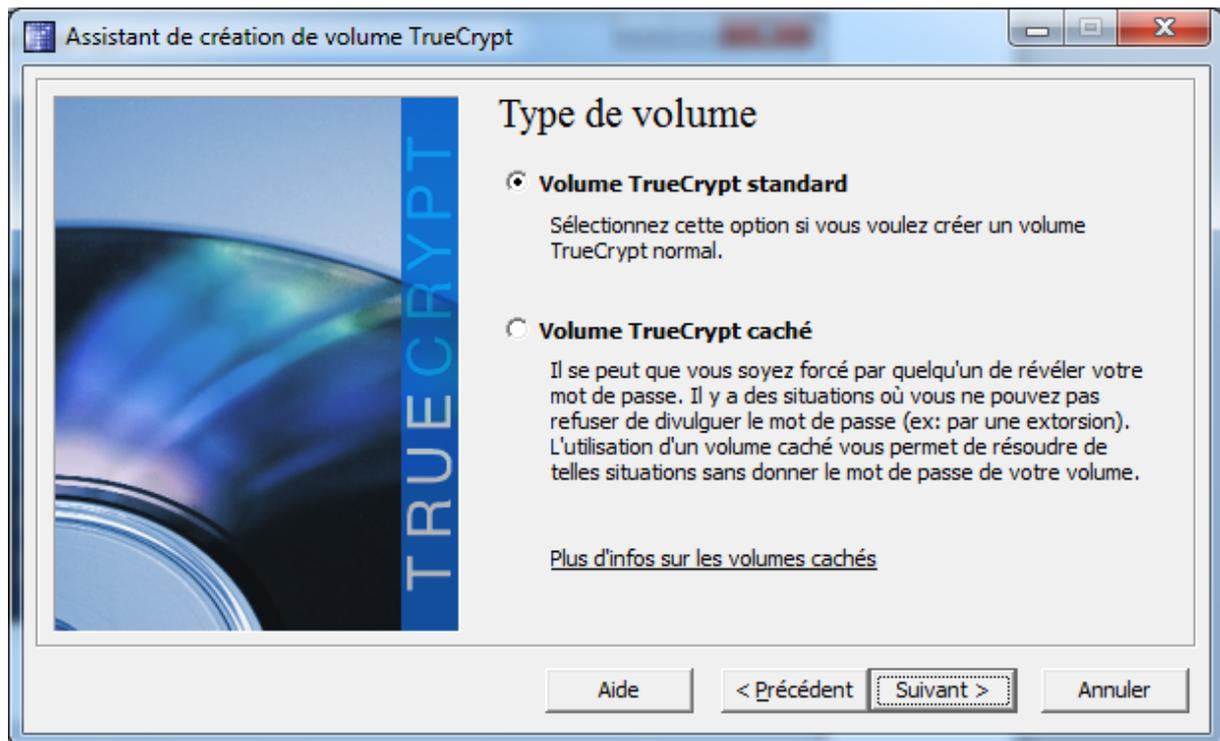
Création d'un conteneur (volume) chiffré

Le logiciel TrueCrypt doit avoir préalablement été [installé](#) par une personne possédant les privilèges administrateur.

Lancer TrueCrypt, aller sur « Outils » → « Assistant de création de volume »



Cocher « **Create an encrypted file container** » et cliquer sur « **Suivant >** »



Cocher « **Volume TrueCrypt standard** » et cliquer sur « **Suivant >** »



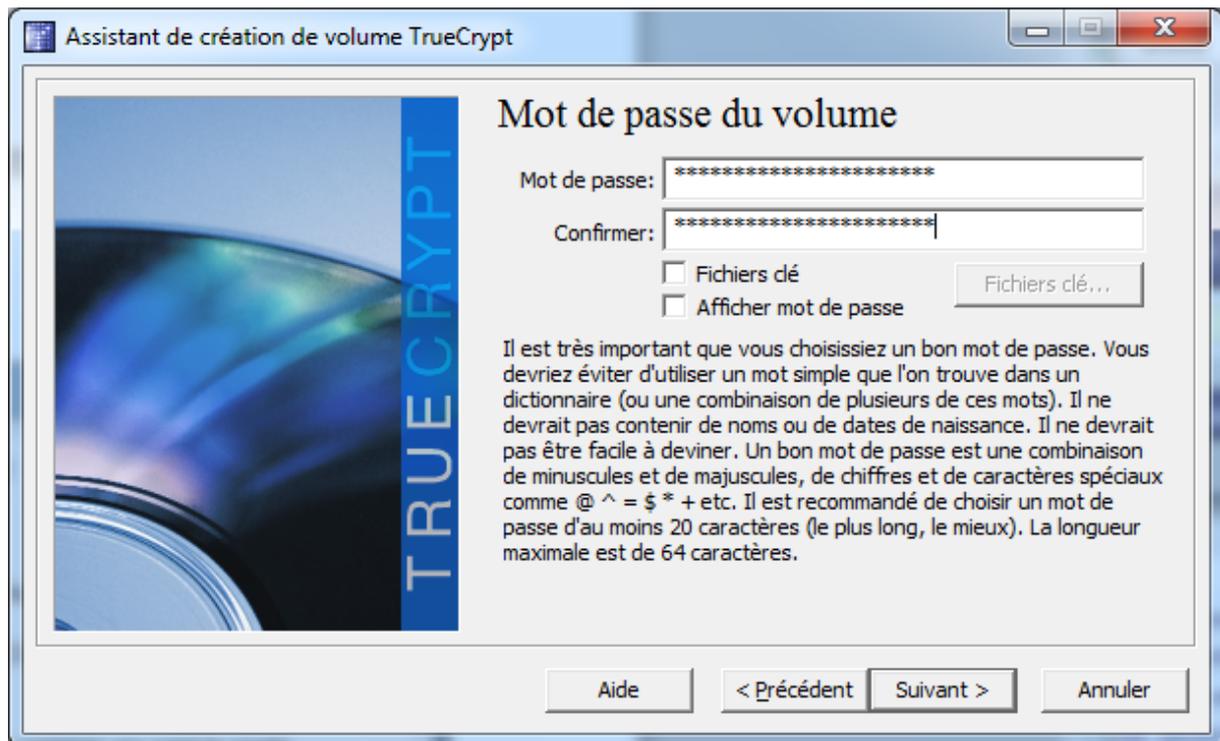
Choisir un fichier pour le conteneur, cocher « **Ne jamais enregistrer l'historique** » et cliquer sur « **Suivant >** »



Conserver les valeurs par défaut « **AES** » pour l'algorithme de chiffrement et « **RIPEMD-160** » pour l'algorithme de hachage et cliquer sur « **Suivant >** »



Choisir une taille de volume et cliquer sur « **Suivant >** »



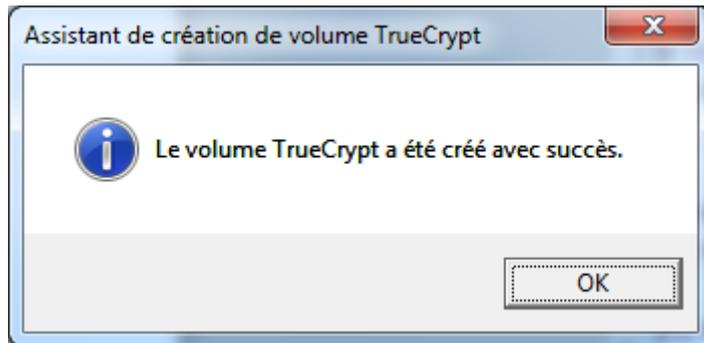
Choisir un mot de passe robuste. Cliquer sur « **Suivant** > »



Pour créer un conteneur sur un support amovible (clé USB, carte SD, etc., il est préférable de choisir lorsque cela est possible un système de fichiers « FAT ». En effet celui-ci est compatible avec les différentes plateformes (Windows, MacOS, Linux).

Déplacer la souris aléatoirement comme demandé et cliquer sur « **Formater** »

Création d'un conteneur TrueCrypt sous Windows



Cliquer sur «OK »



Cliquer sur « **Quitter** »

Séquestre

Pour permettre le recouvrement en cas d'oubli du mot de passe ou d'indisponibilité de l'utilisateur, il est impératif de procéder au [séquestre](#) du mot de passe, en le notant et le rangeant en lieu sûr.

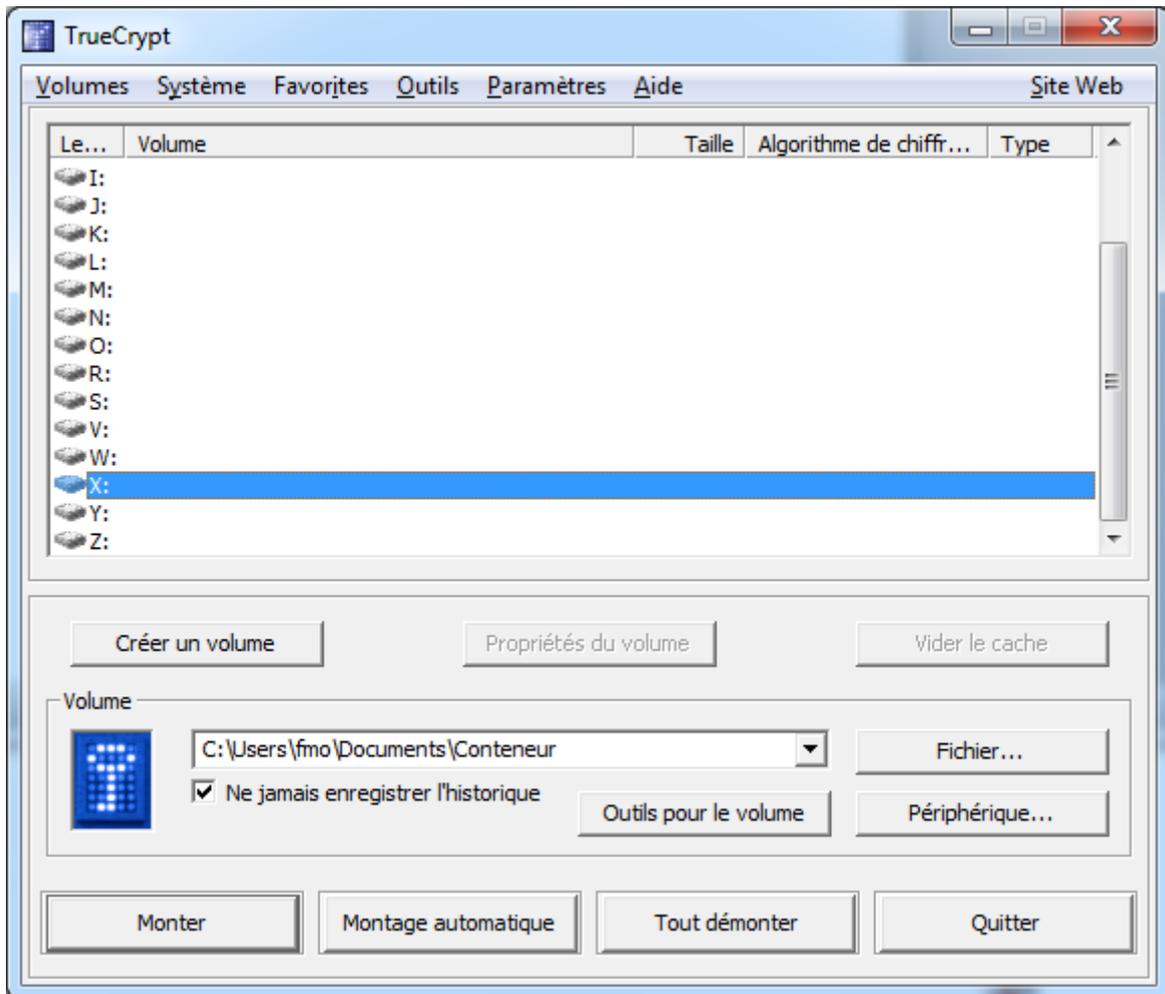
Utilisation d'un conteneur TrueCrypt sous Windows

Montage d'un conteneur (volume) chiffré

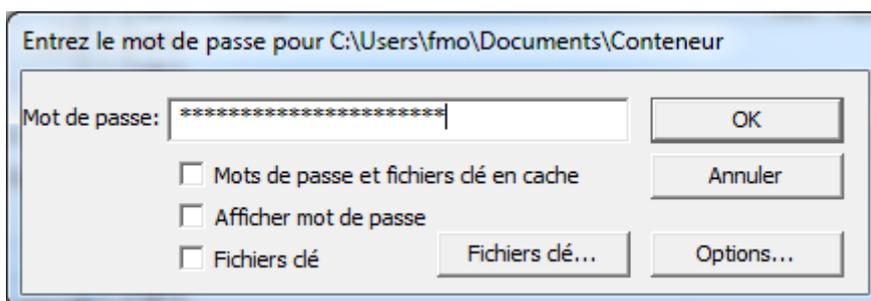
Il faut au préalable avoir [créé](#) un conteneur (volume) TrueCrypt.

Création d'un conteneur TrueCrypt sous Windows

Ouvrir le fichier contenant le conteneur chiffré en double cliquant s'il possède le suffixe « .tc » ou en lançant le logiciel TrueCrypt et en sélectionnant le fichier à partir du bouton « Fichier... »



Cliquer sur « **Monter** »



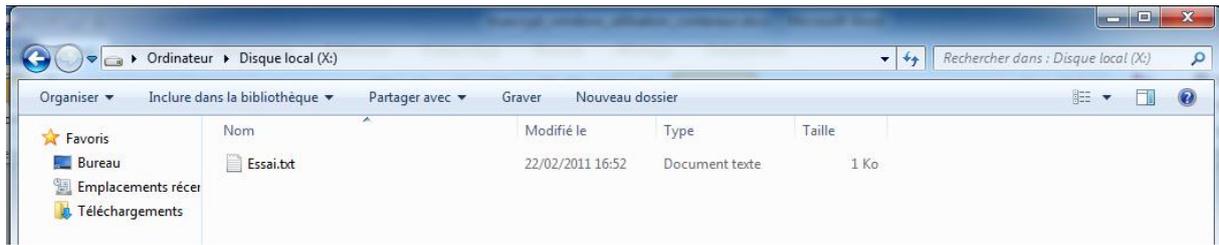
Saisir le mot de passe et cliquer sur « **OK** »

Désormais un nouveau disque (ici X :) est visible



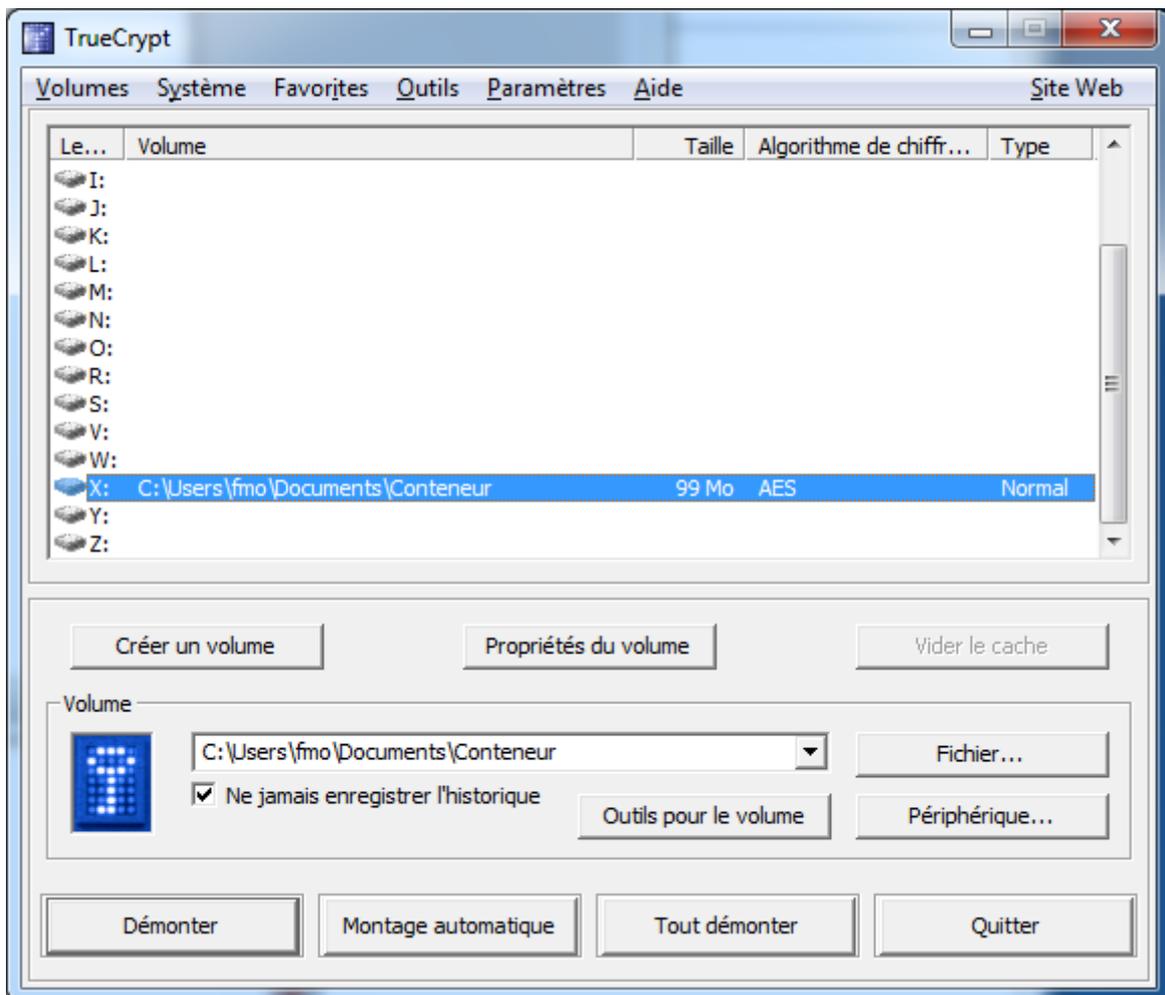
Création d'un conteneur TrueCrypt sous Windows

Il est utilisable comme un disque classique.



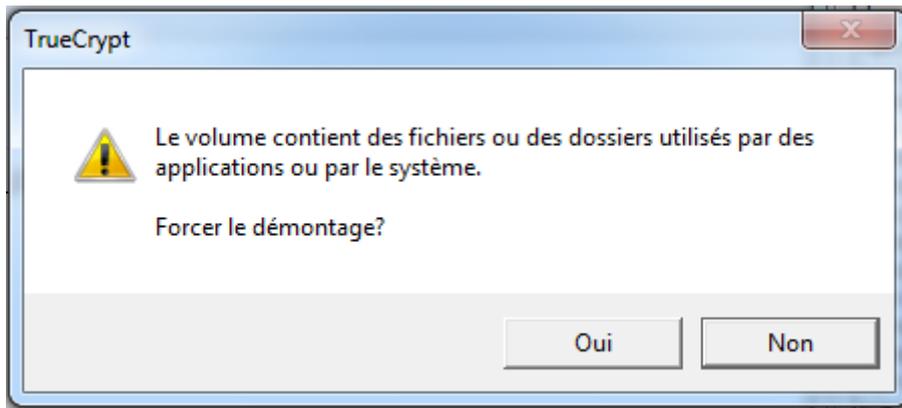
Démontage d'un conteneur (volume) chiffré

Si la fenêtre TrueCrypt n'est pas visible, la faire apparaître en cliquant sur l'icône TrueCrypt dans la barre des tâches.

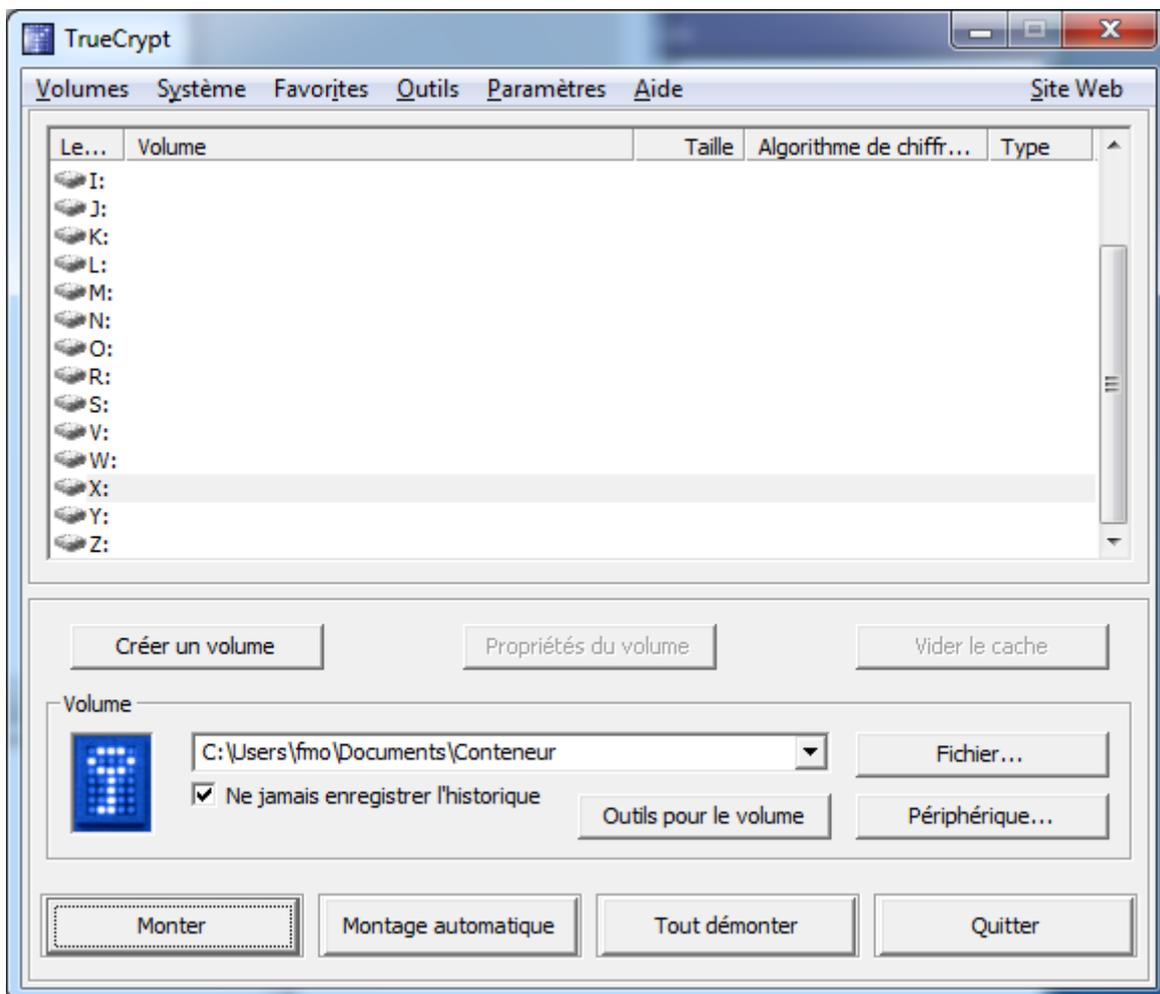


Sélectionner le conteneur (volume) et cliquer sur « **Démonter** »

Création d'un conteneur TrueCrypt sous Windows



Ce message vous signale que des fichiers dans votre conteneur sont actuellement ouverts. Vous devez les fermer avant de démonter le conteneur.



Cliquer sur « **Quitter** »

Création d'un conteneur TrueCrypt sous Linux

Introduction

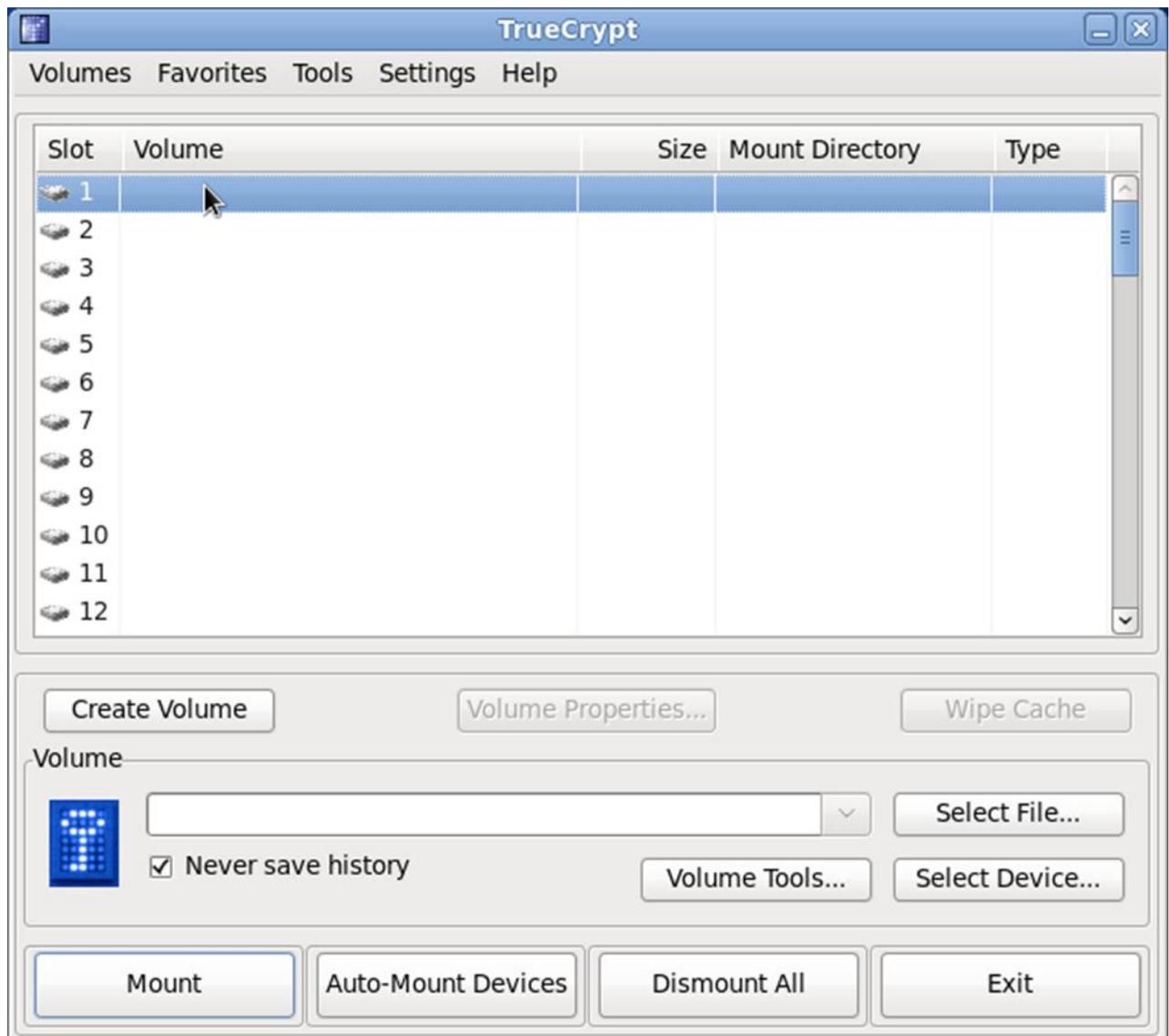
Le logiciel TrueCrypt doit avoir préalablement été [installé](#) par une personne possédant les privilèges administrateur.

Les différentes opérations peuvent aussi s'effectuer à partir de lignes de commandes. Nous ne décrivons ici que l'interface graphique. Les spécialistes Linux trouveront la liste des différents paramètres en exécutant la commande

truecrypt -t -h

Création d'un conteneur (volume) TrueCrypt

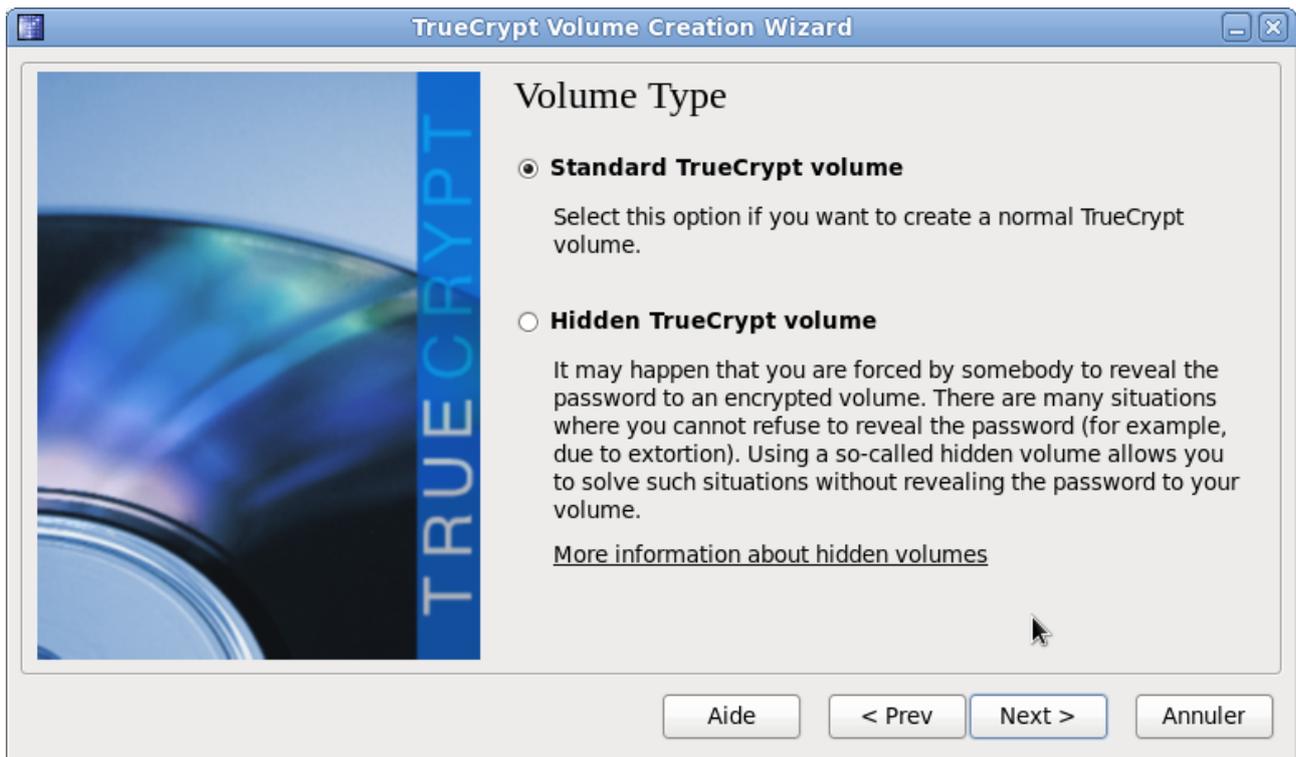
Lancez l'application truecrypt



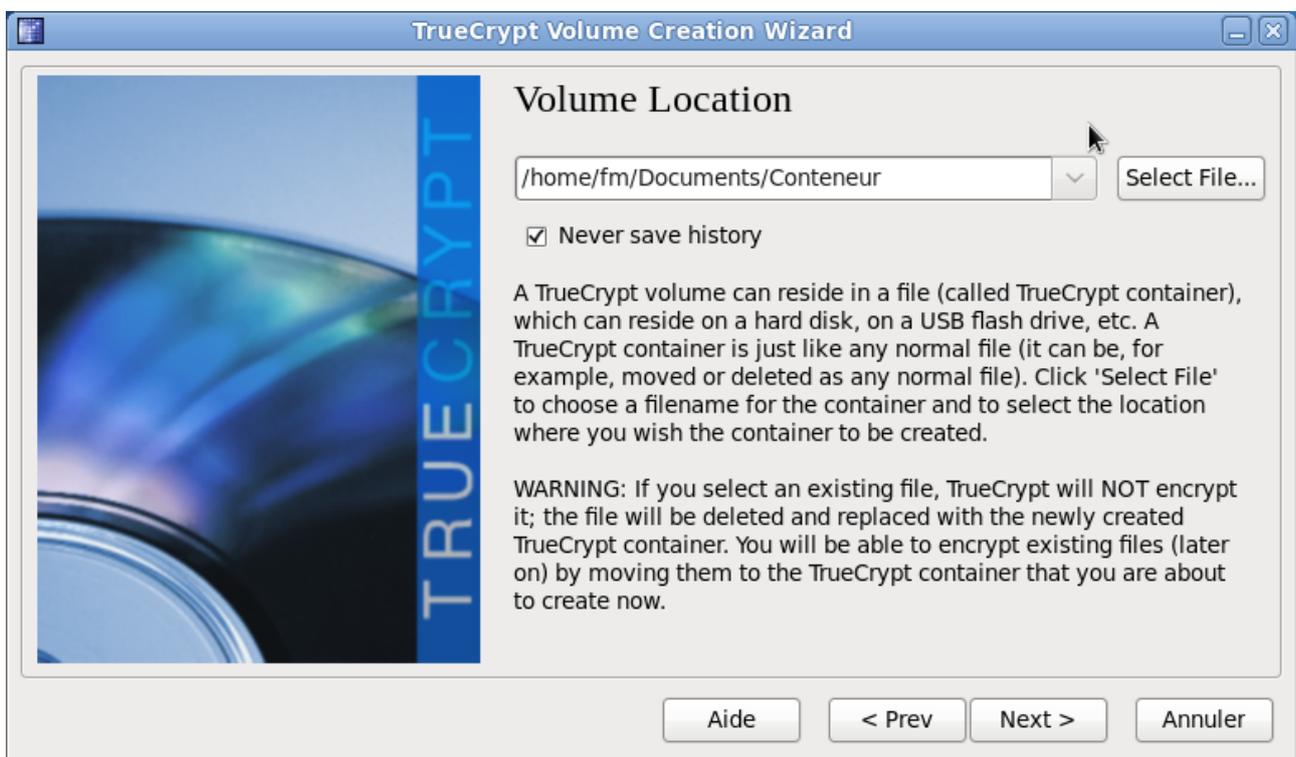
Sélectionnez « **Tools** » → « **Volume Creation Wizard** ».



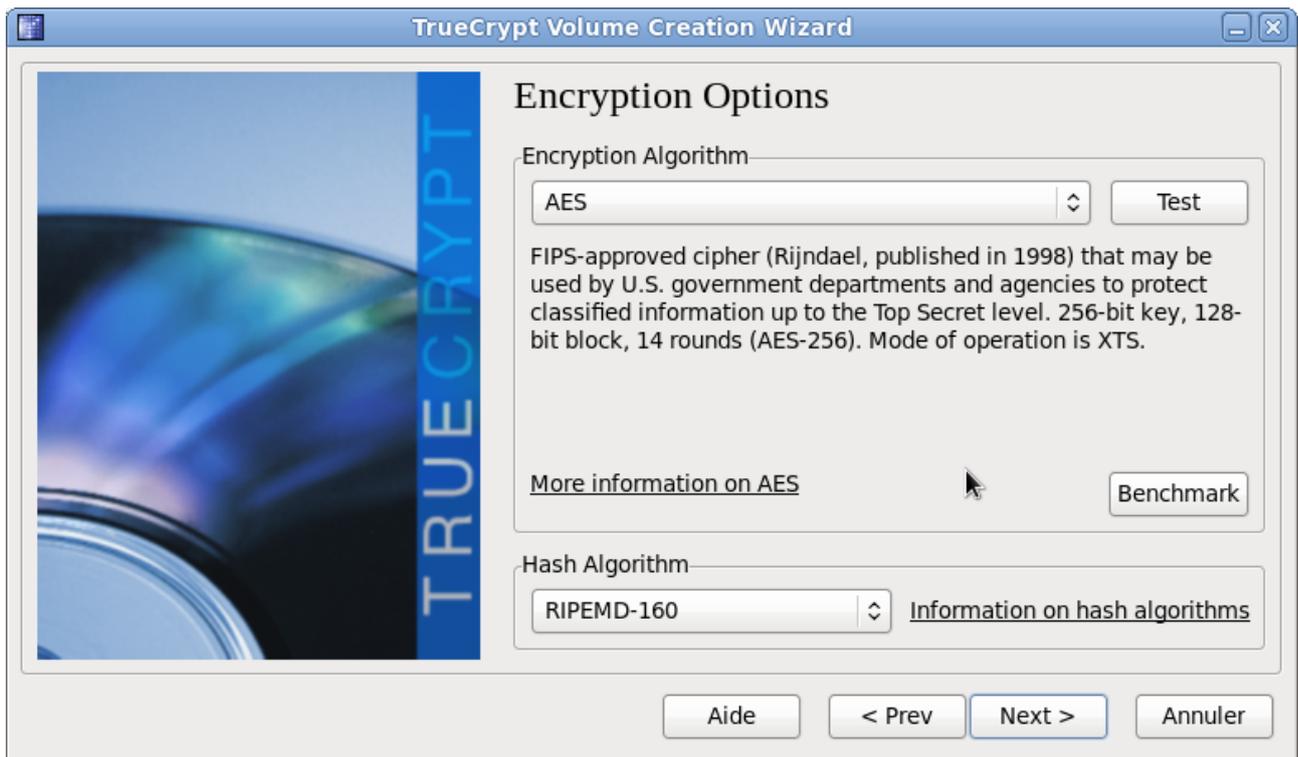
Sélectionnez « **Create an encrypted file container** », puis cliquez sur « **Next >** ».



Sélectionnez « **Standard TrueCrypt volume** », puis cliquez sur « **Next >** ».



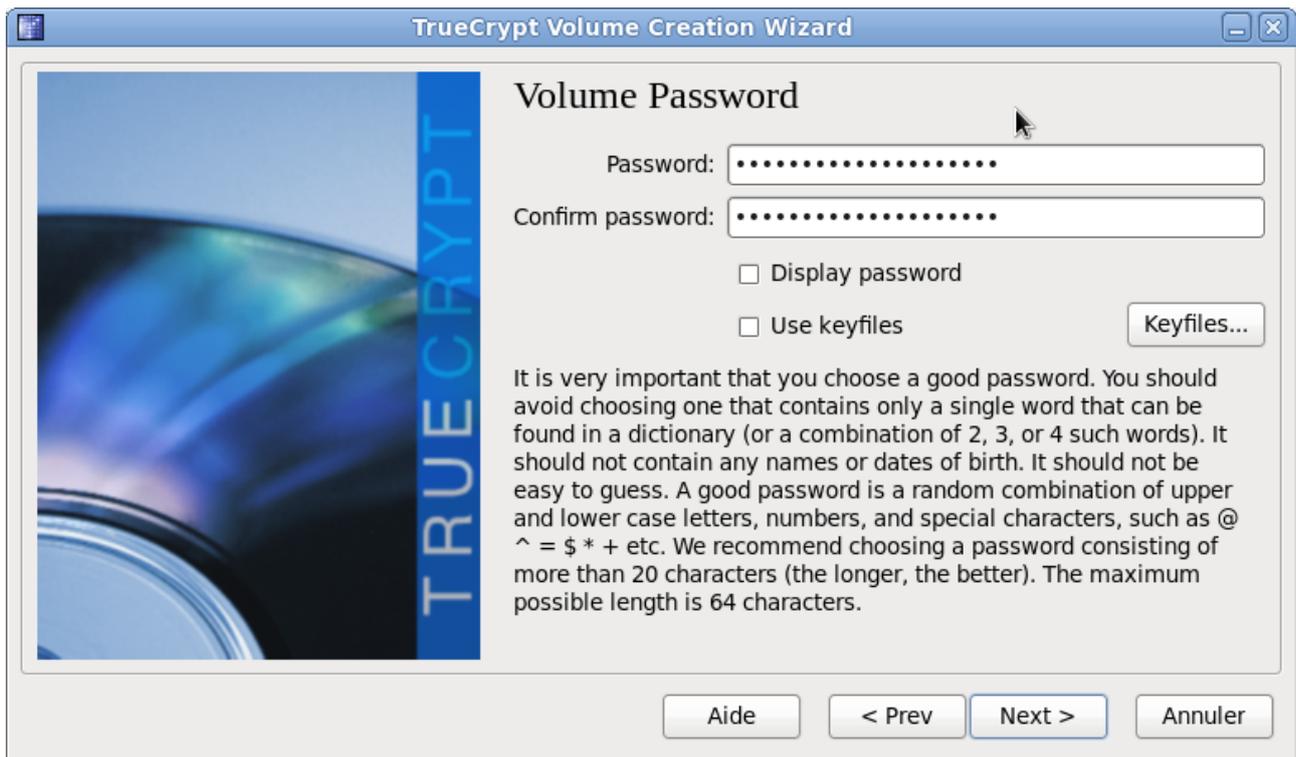
Donnez le nom du fichier puis cliquez sur « **Next >** ».



Conservez les valeurs par défaut et cliquez sur « **Next >** ».



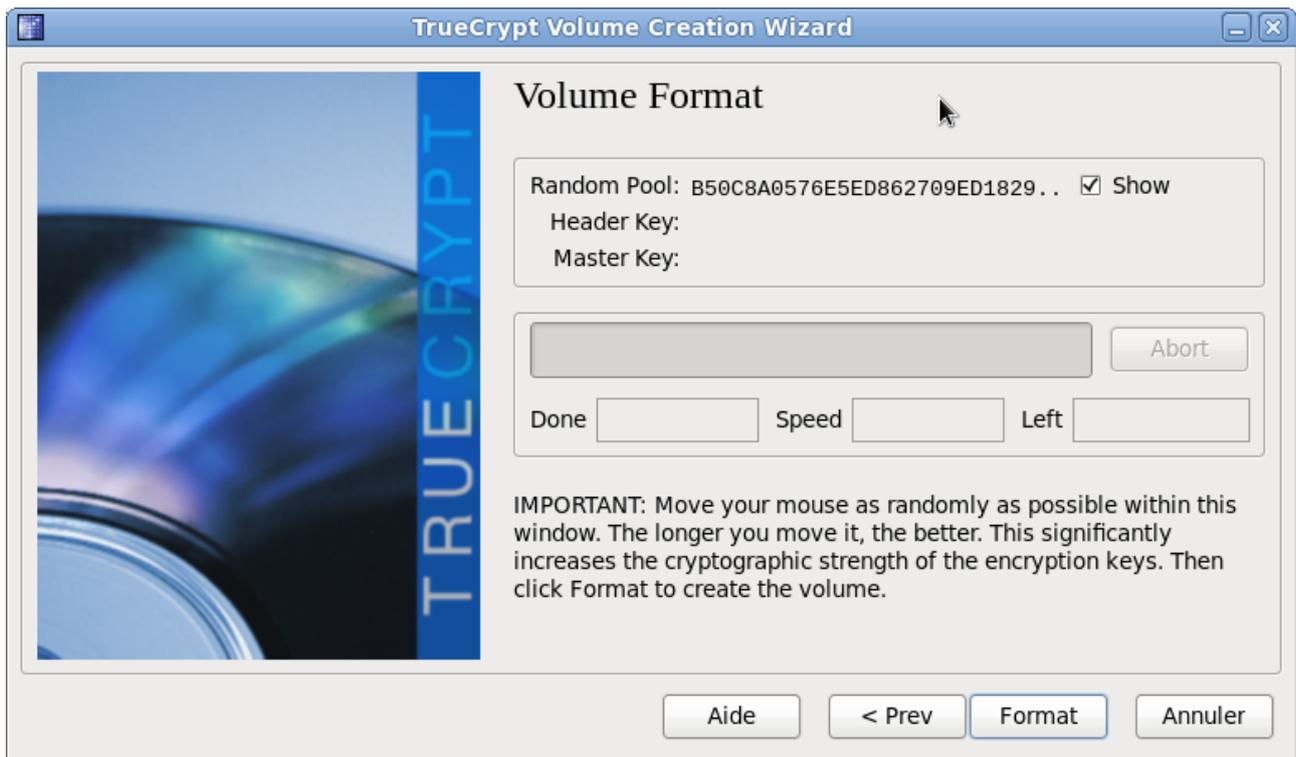
Choisir la taille du conteneur et cliquez sur « **Next >** ».



Choisissez un mot de passe robuste et mémorisez le, puis cliquez sur « **Next >** ».



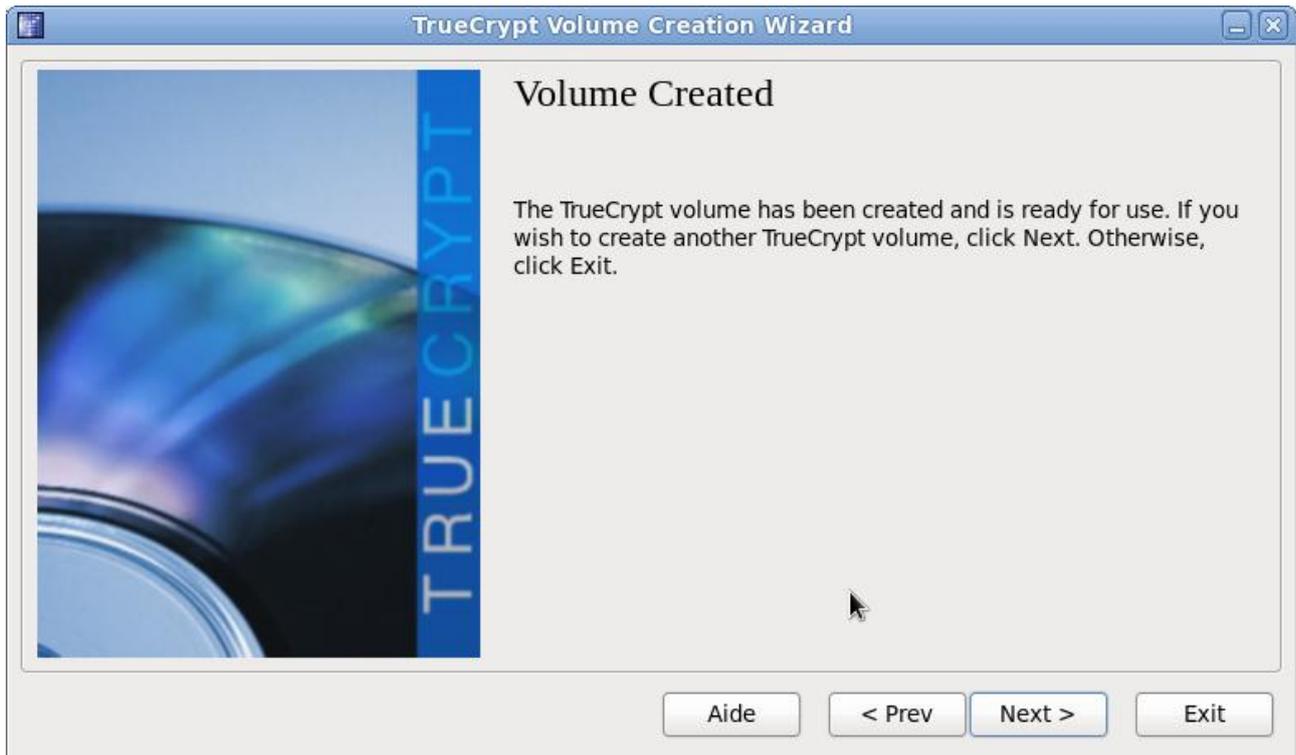
Si le conteneur est destiné à être transporté entre plusieurs systèmes d'exploitation choisissez « FAT » sinon il est possible de choisir un système de fichier Linux comme « ext3 » ou « ext4 ». Cliquez sur « **Next >** ».



Déplacez la souris aléatoirement et suffisamment longtemps dans la fenêtre puis cliquez sur « **Format** ».



Cliquez sur « **Valider** ».



C'est terminé, cliquez sur « **Exit** ».

Séquestre du mot de passe

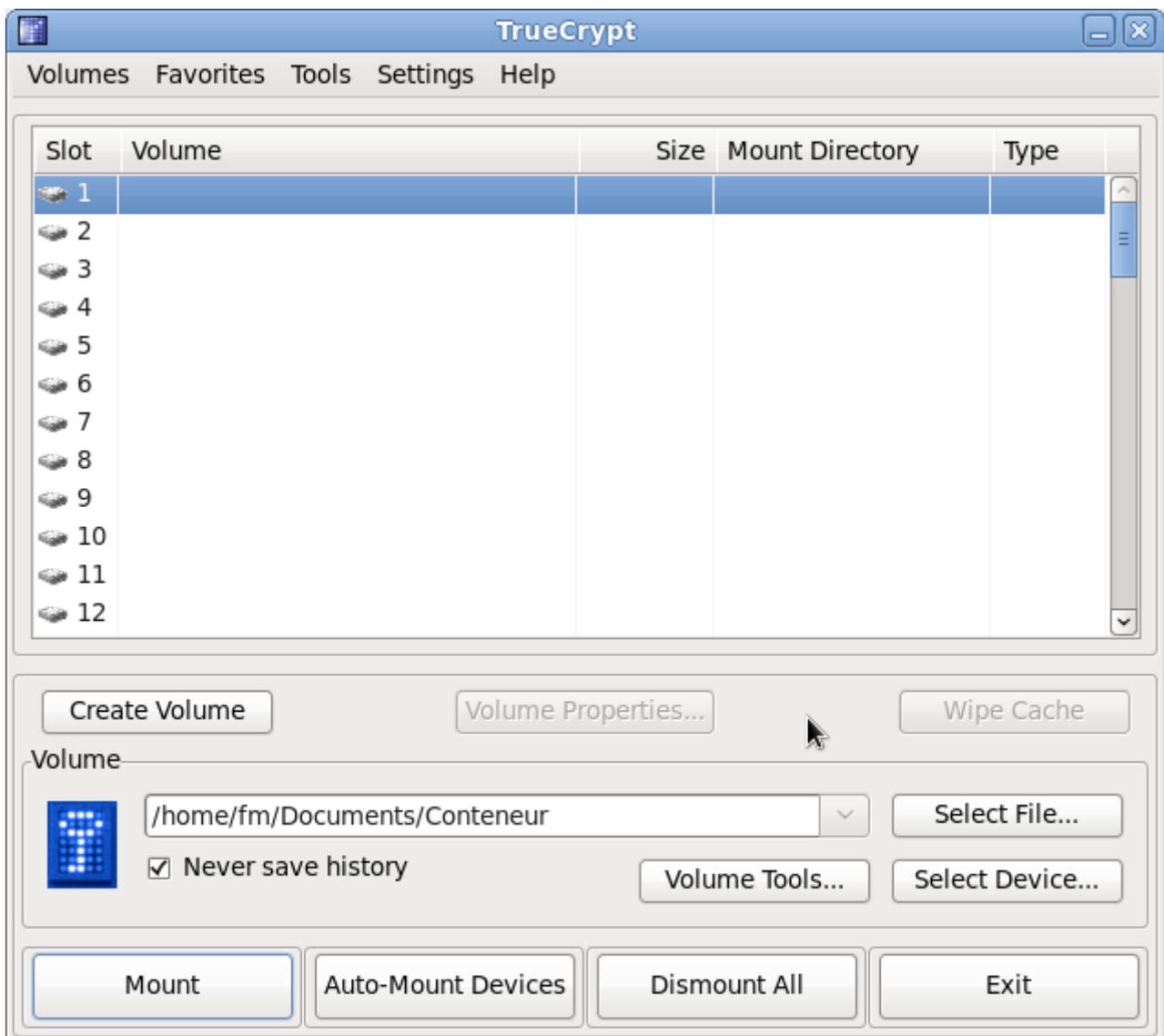
Pour permettre le recouvrement en cas d'oubli du mot de passe ou d'indisponibilité de l'utilisateur, il est impératif de procéder au [séquestre](#) du mot de passe, en le notant et le rangeant en lieu sûr.

Utilisation d'un conteneur TrueCrypt sous Linux

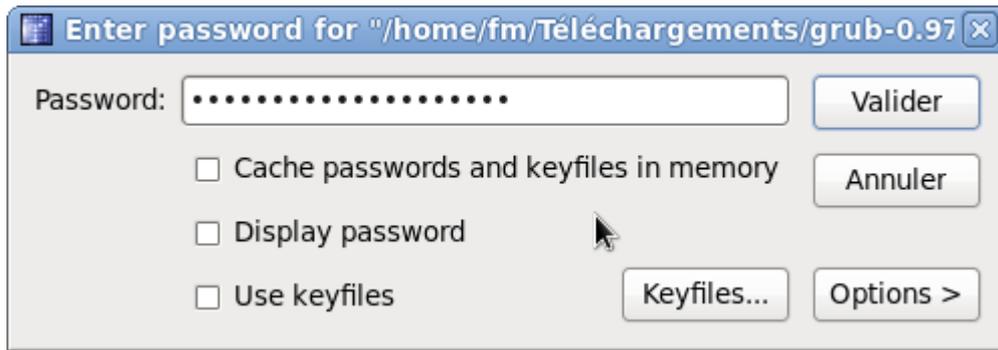
Montage d'un conteneur (volume) chiffré TrueCrypt

Il faut au préalable avoir [créé](#) un conteneur (volume) TrueCrypt.

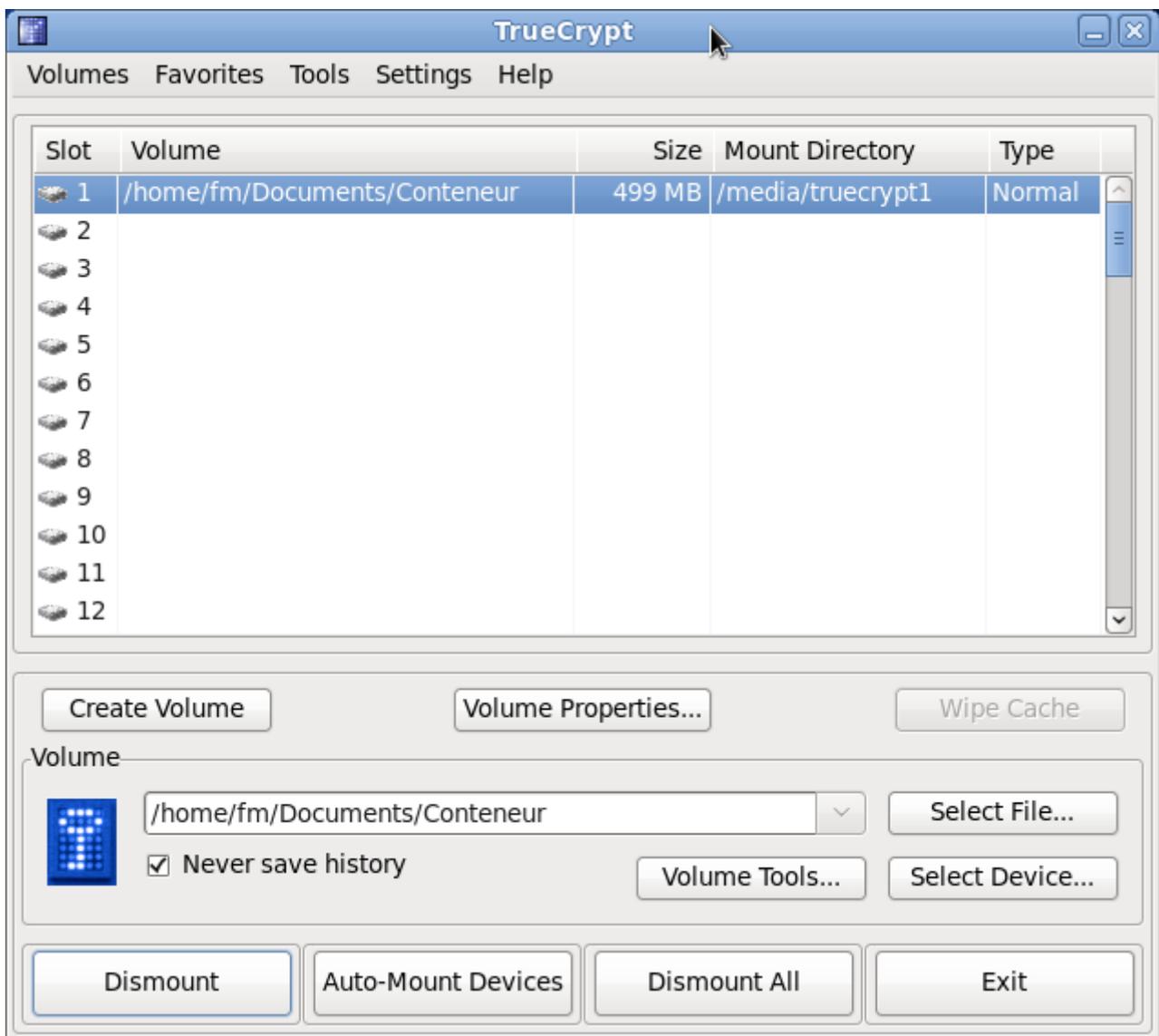
Lancez l'application truecrypt.



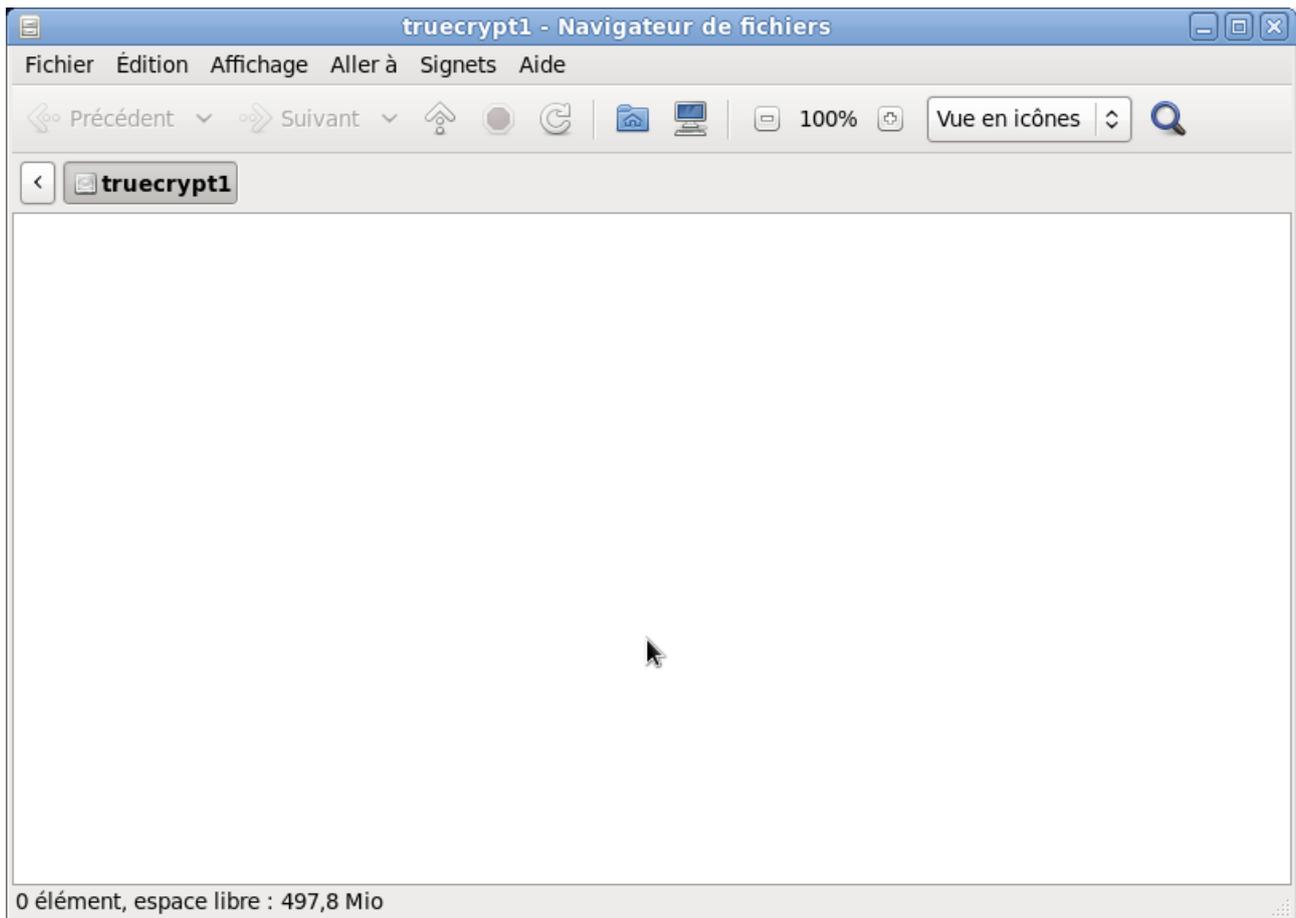
Cliquez sur « **Mount** »



Entrez le mot de passe du conteneur chiffré puis cliquez sur « **Valider** ».

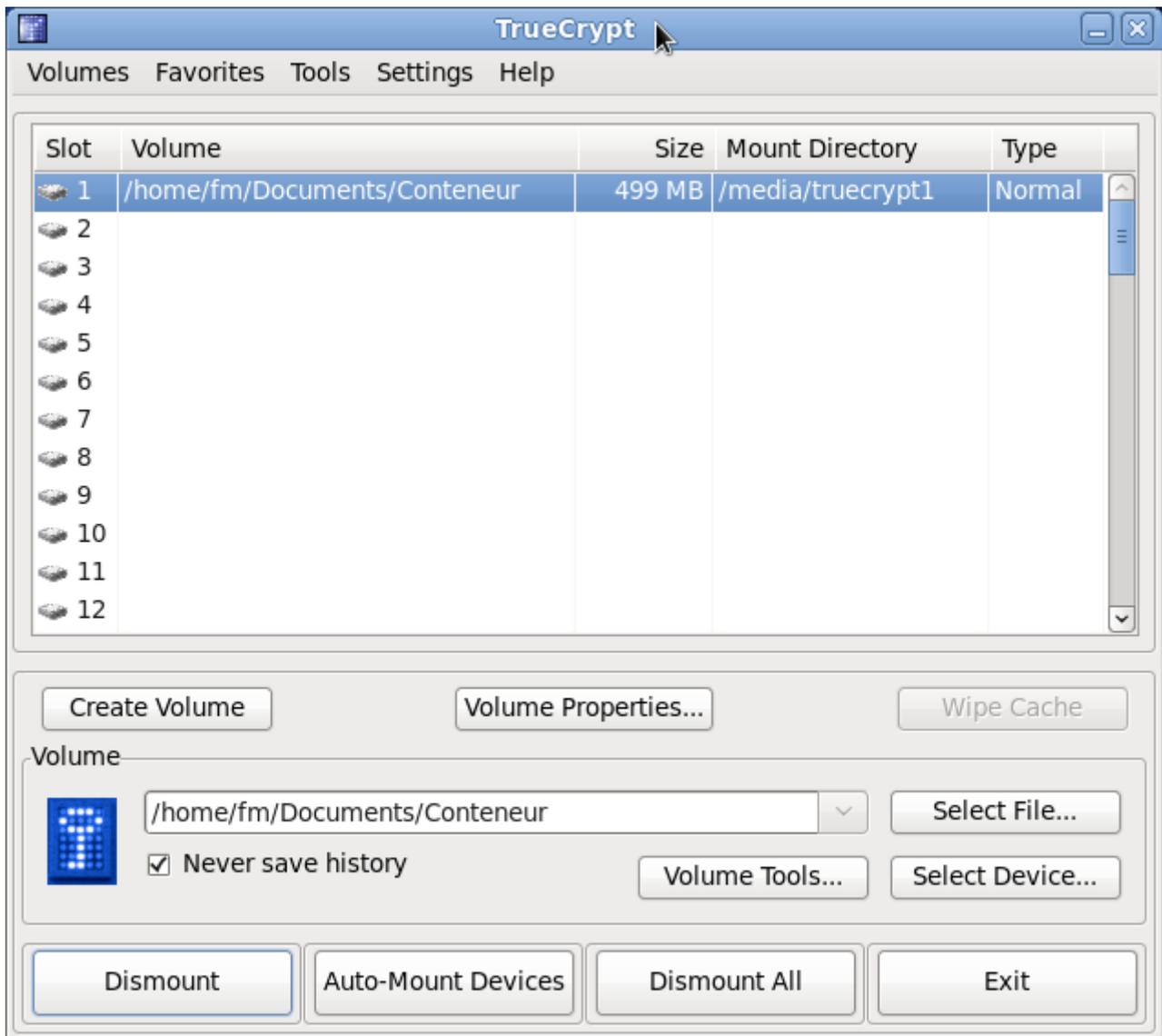


Il apparait alors une icône « **truecrypt1** » sur le bureau, en cliquant dessus on accède au conteneur.

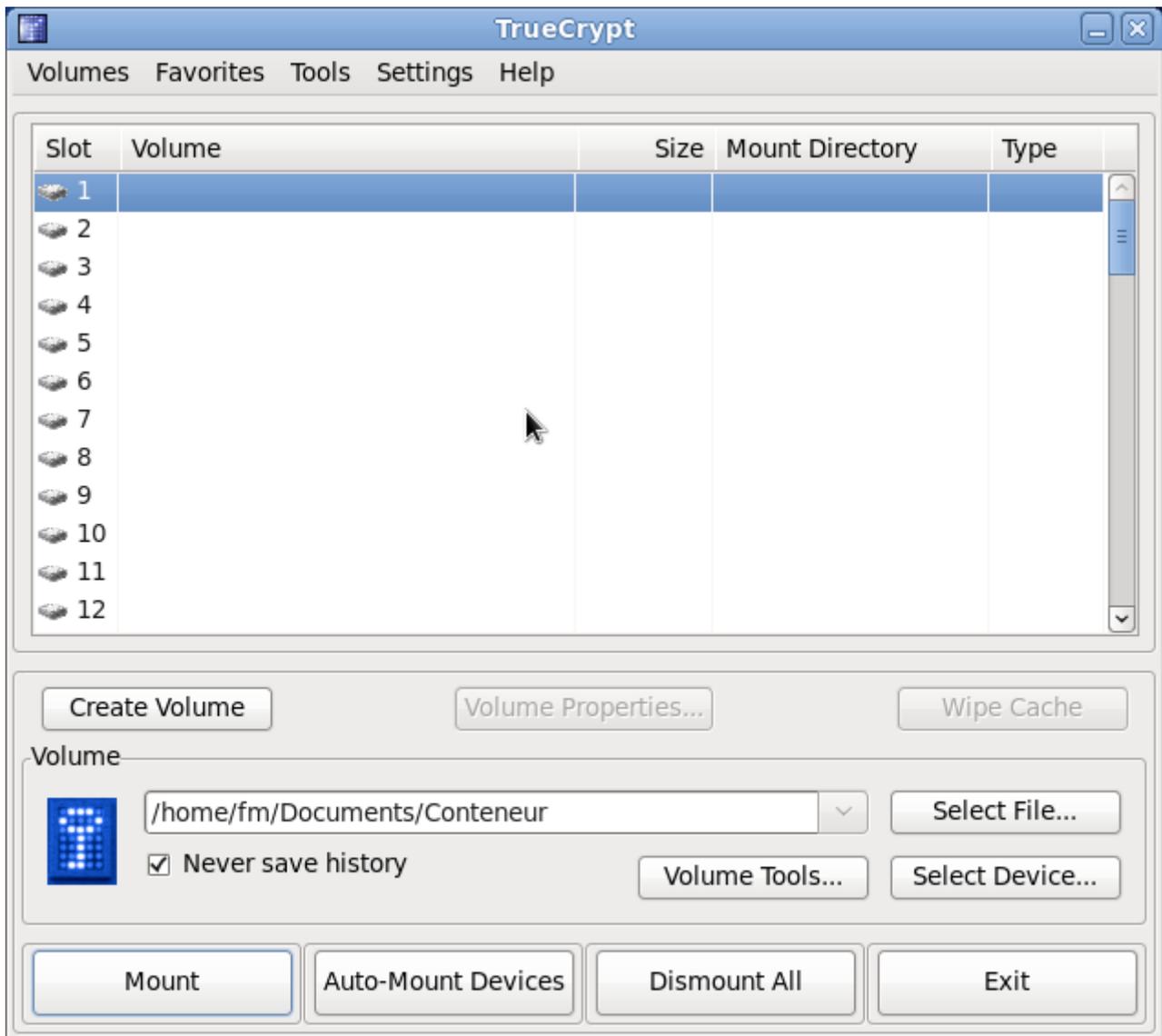


Démontage d'un conteneur (volume) chiffré TrueCrypt

Pour démonter le conteneur (volume) TrueCrypt, il faut d'abord s'assurer que plus aucun fichier n'est ouvert et qu'aucun répertoire courant (current/working directory) ne pointe dessus.



Sélectionnez le volume à démonter et cliquez sur « **Dismount** ».



Vous pouvez quitter TrueCrypt en cliquant sur « **Exit** ».

Installation et administration des outils de chiffrement

La documentation est organisée par système d'exploitation

1. Windows
2. Mac OS X
3. Linux

Initialisation d'un disque chiffrant sous Windows

Introduction

La mise en service du disque de chiffrement DELL est faite avec le logiciel « Embassy Security Center » de la société WAVE.

Cet outil a été intégré dans la suite DELL Access Control Point.

Un manuel d'utilisation du logiciel Wave est disponible sur le site de Wave (attention il ne reflète pas nécessairement la dernière version du logiciel)

http://www.wave.com/support/downloads/TDM_Guide.pdf

Informations de recouvrement

Les informations de recouvrement permettent, en cas de perte du mot de passe de l'utilisateur, à un administrateur de pouvoir accéder à un disque chiffré et de réinitialiser le mot de passe de l'utilisateur.

Ces données sont générées au moment du chiffrement du disque.

Elles peuvent être sous deux formats et il est conseillé d'utiliser les deux :

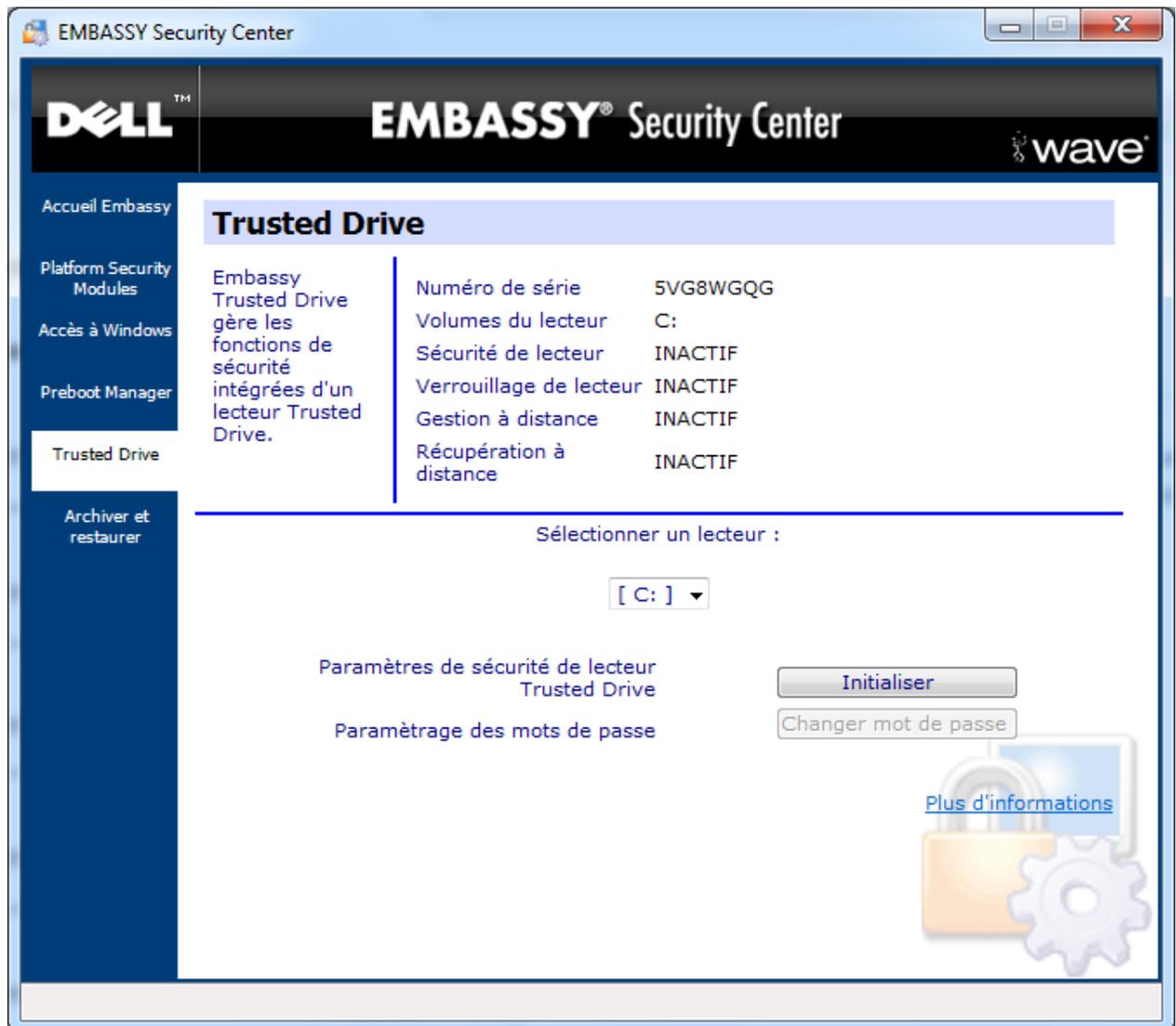
- Numérique : La sauvegarde du fichier doit se trouver sur un espace dont l'accès est contrôlé (droits d'accès restreints ou coffre-fort numérique). Pour des raisons de sécurité il faut en avoir au moins deux exemplaires, éventuellement sur des supports différents et dans des endroits séparés.
- Papier : imprimer les données, mettre la feuille imprimée sous enveloppe et la ranger en lieu sûr (coffre-fort physique, ...)

Installation

L'installation se fera avec un compte administrateur local à la machine.

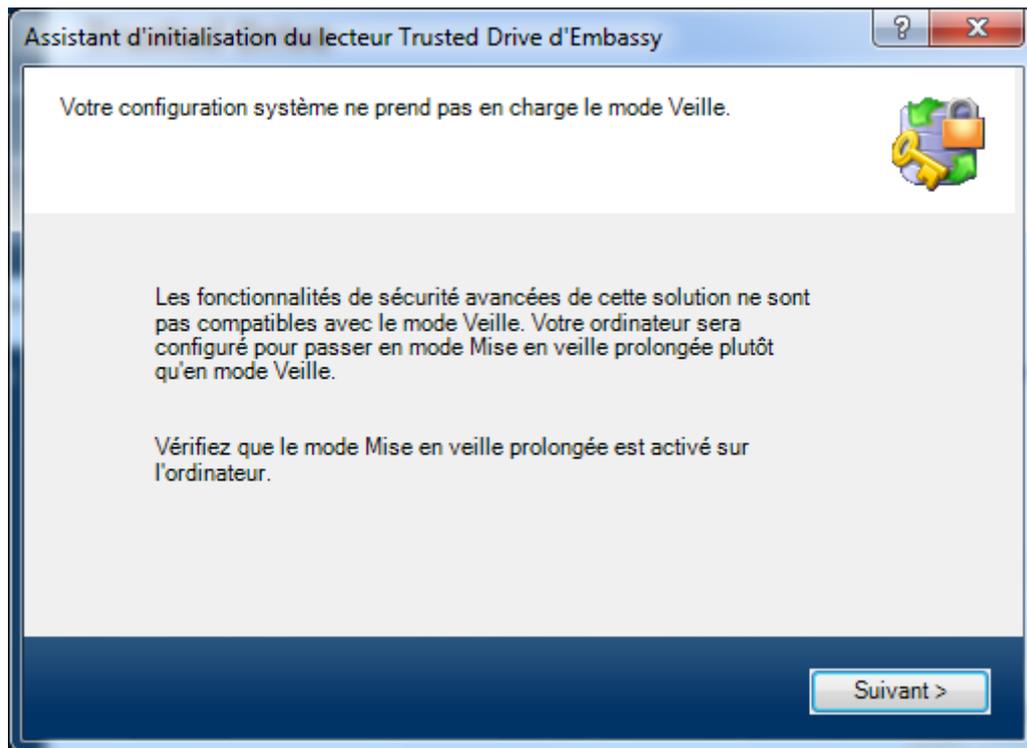
Lancer l'application « EMBASSY Security Center » et cliquer sur « **Trusted Drive** »

La fenêtre suivante apparaît :

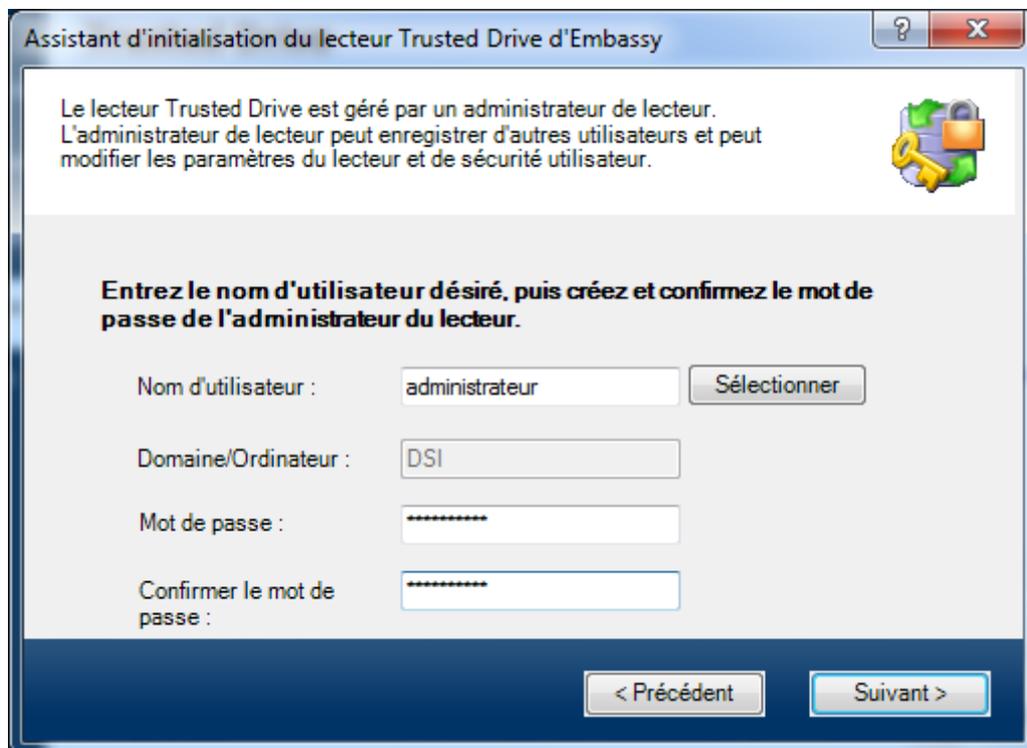


Sélectionner le lecteur à chiffrer et cliquer sur « **Initialiser** ».

Initialisation d'un disque chiffrant sous Windows



Cliquer sur « **Suivant >** »



Choisir un mot de passe suffisamment complexe. Cliquer sur « **Suivant >** »

Assistant d'initialisation du lecteur Trusted Drive d'Embassy

IMPORTANT : Sauf si un utilisateur possède le nom d'utilisateur et le mot de passe adéquat pour déverrouiller le lecteur Trusted Drive, le lecteur restera verrouillé et tous les accès aux données sur le disque seront bloqués.

Afin d'éviter tout risque de blocage, habituez-vous à entrer les données d'identification de l'administrateur Trusted Drive car elles seront nécessaires au prochain démarrage du système.

Nom d'utilisateur : administrateur

Domaine/Ordinateur : DSI

Mot de passe : [masqué]

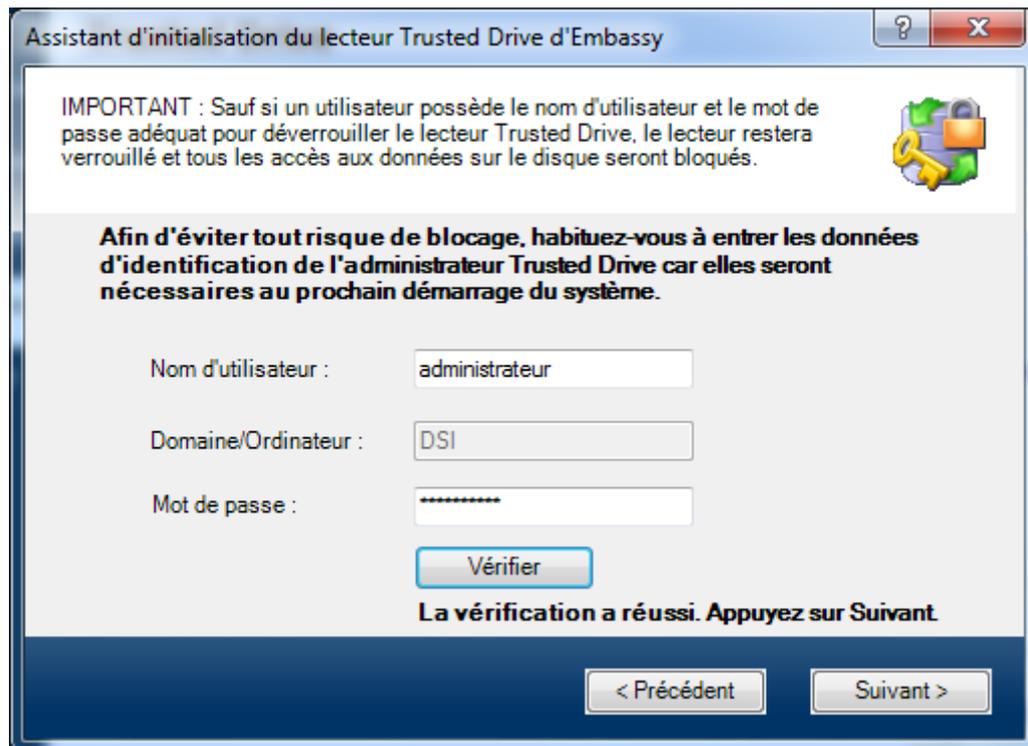
Vérifier

< Précédent Suivant >

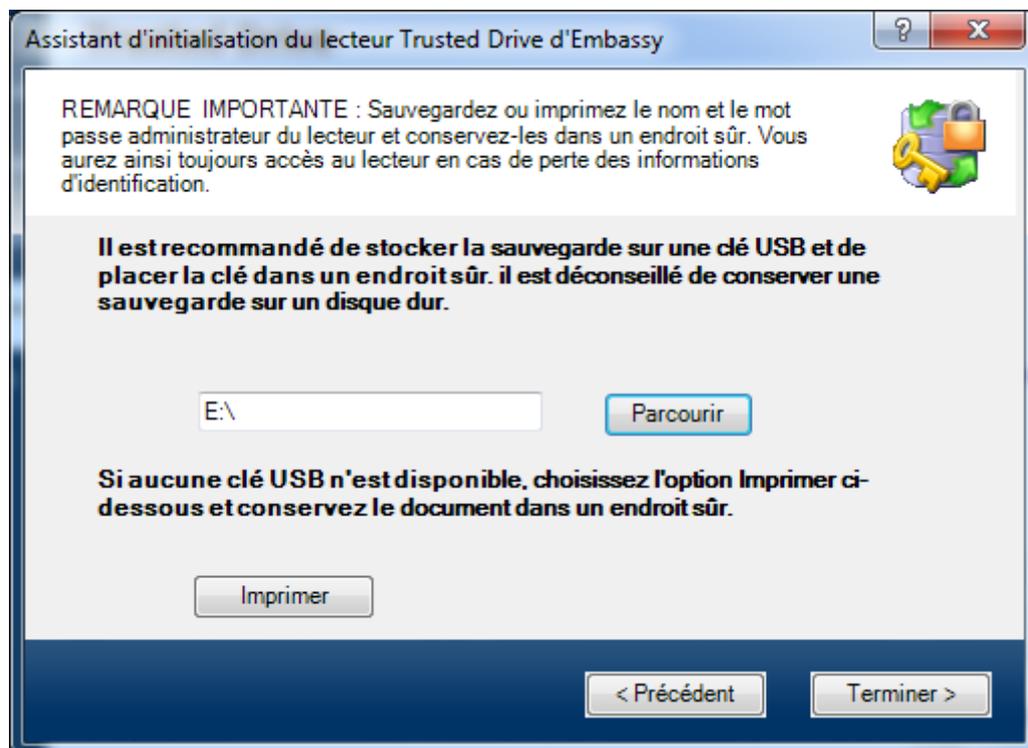
Entrez les identifiants du compte administrateur.

Ce compte ne sera pas donné à l'utilisateur et servira pour le recouvrement en cas de perte du mot de passe de l'utilisateur.

Cliquez sur « Vérifier »



Cliquer sur « **Suivant >** »

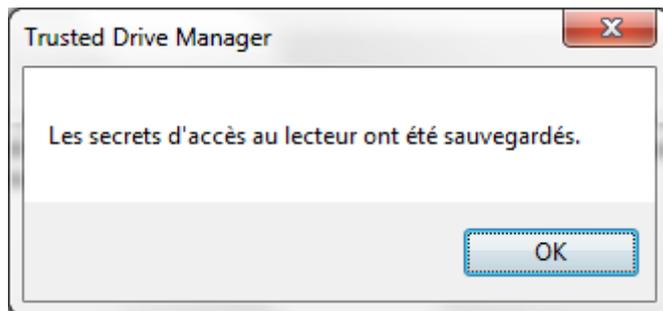


Initialisation d'un disque chiffrant sous Windows

Les informations de recouvrement peuvent soit être stockés de manière numérique sur une clés USB, soit imprimées et rangées en lieu sûr dans un coffre.

Le stockage numérique impose d'avoir à sa disposition un coffre-fort numérique suffisamment sécurisé et redondé.

Si on choisit la sauvegarde sur une clé USB, cliquez sur « Terminé »



Cliquer sur « **OK** »

Il a été créé un fichier portant le nom de **wave_tdm_backup_2011_2_7_15_18_.txt** et dont le contenu est (ici le mot de passe a été remplacé par des *) :

[DriveSerial]

DriveSerial=5VG8WGQG

[DriveAdmin]

SecurityID=S-1-5-21-4142567773-1519229258-3008456440-14623

Name=administrateur

Domain=DSI

Password="*****"

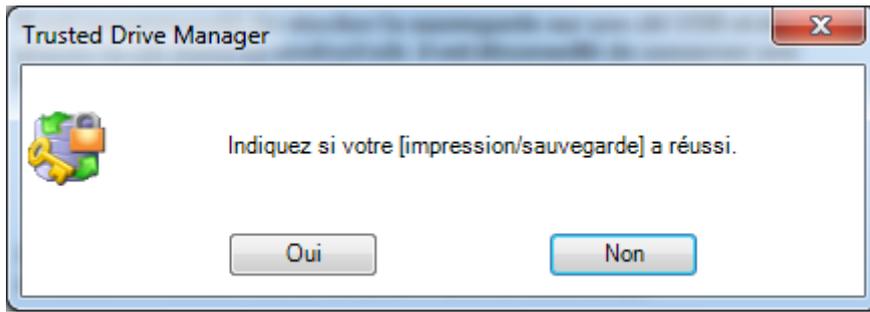
[KeyBoardLayout]

KeyBoardLayout=0000040C

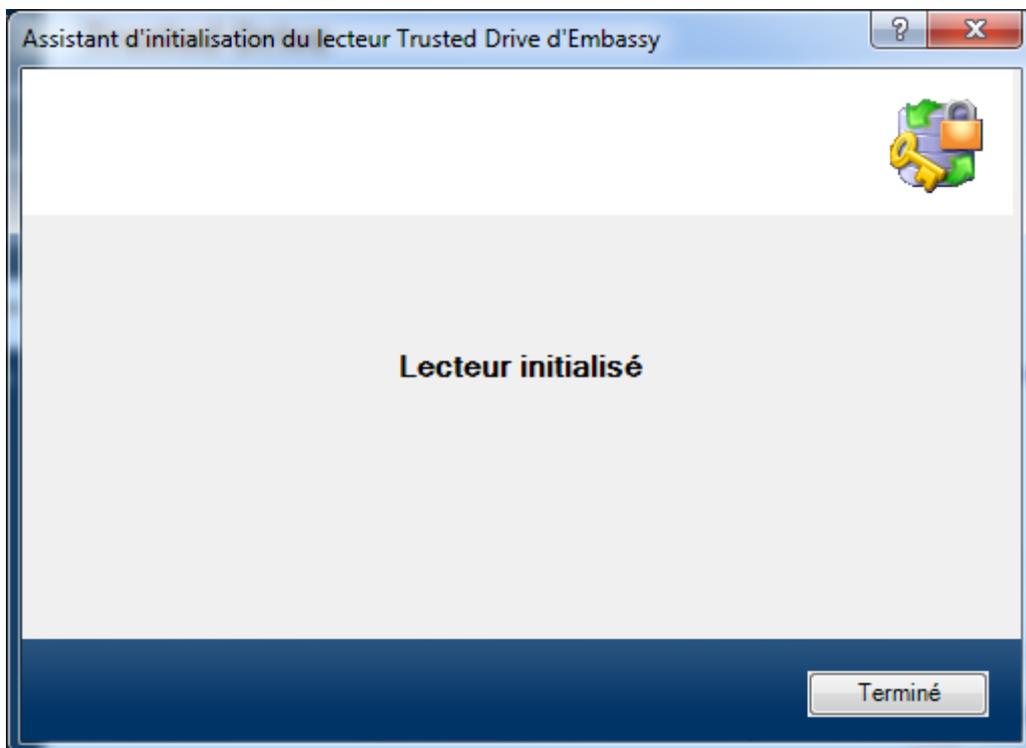
Cliquez sur « **Imprimer** » afin d'avoir aussi une copie papier.

Cliquez sur « **Terminer** »

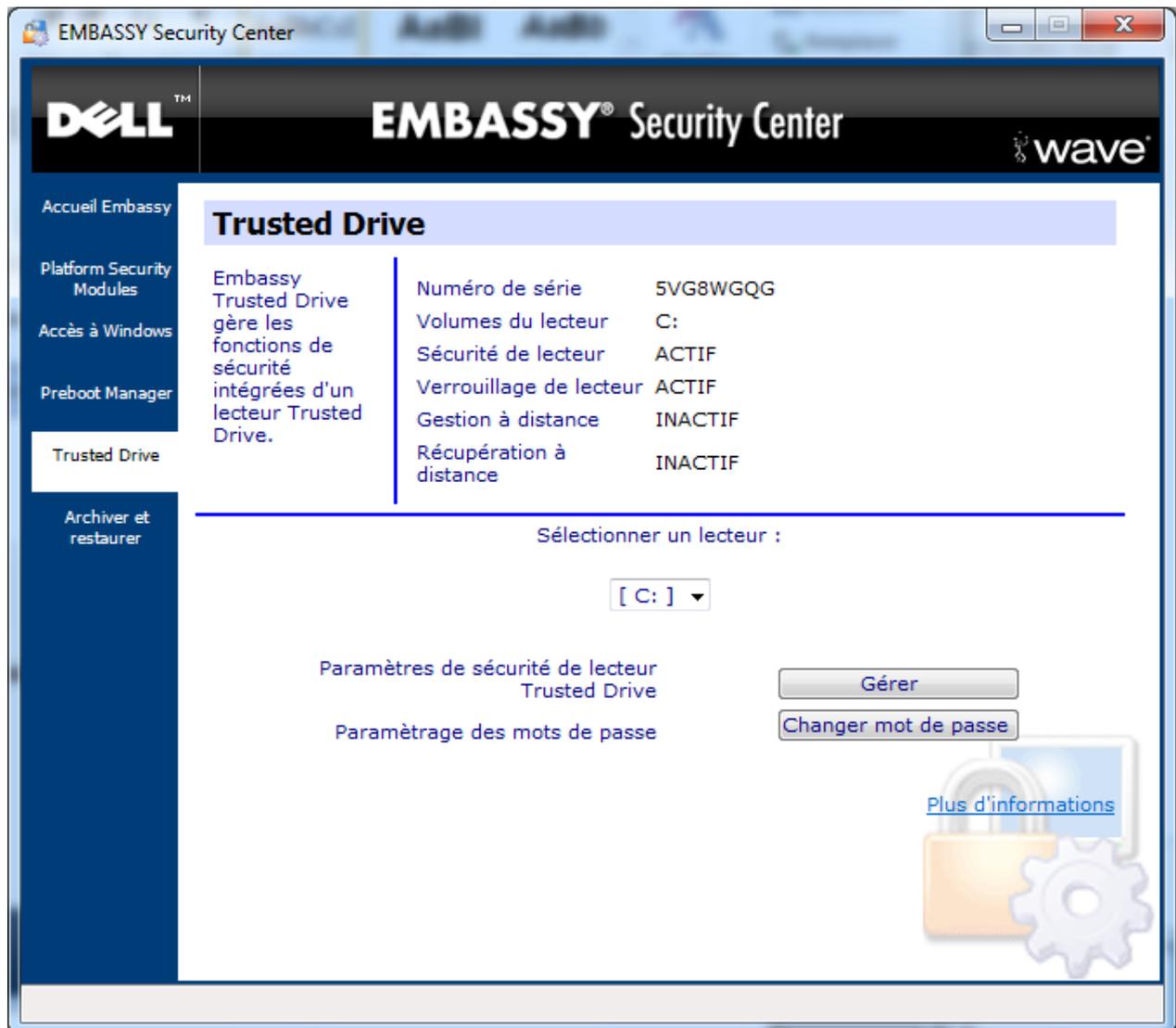
Initialisation d'un disque chiffrant sous Windows



Si la sauvegarde et l'impression se sont correctement déroulé cliquer sur « **Oui** »



Cliquez sur « **Terminé** » et vous revenez à l'écran principale



Notez que « **Sécurité du lecteur** » et **Verrouillage** » de lecteur ont désormais le statut « **ACTIF** ».

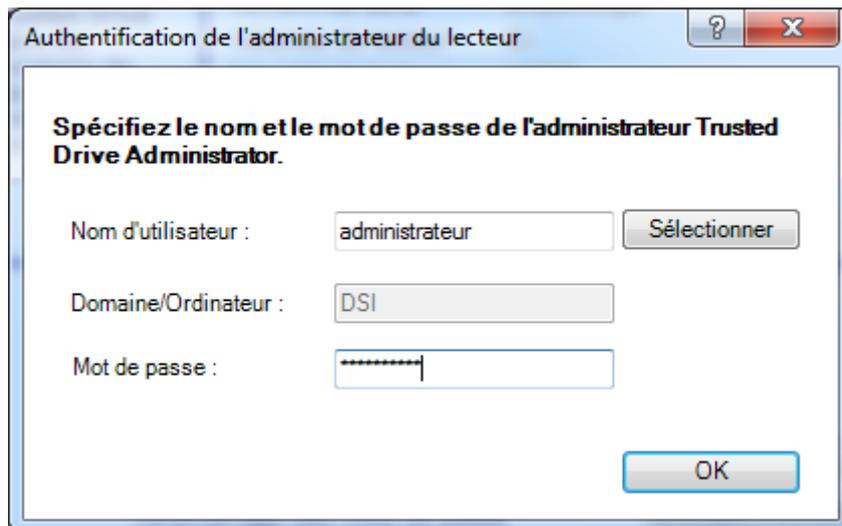
Création d'un utilisateur

Une fois le disque chiffré, seul l'administrateur y a accès.

On doit créer un utilisateur qui correspondra au possesseur du PC. Le cas échéant pour une machine partagée, il est possible de créer plusieurs utilisateurs.

Dans le panneau principale, cliquer sur « Gérer »

Initialisation d'un disque chiffrant sous Windows



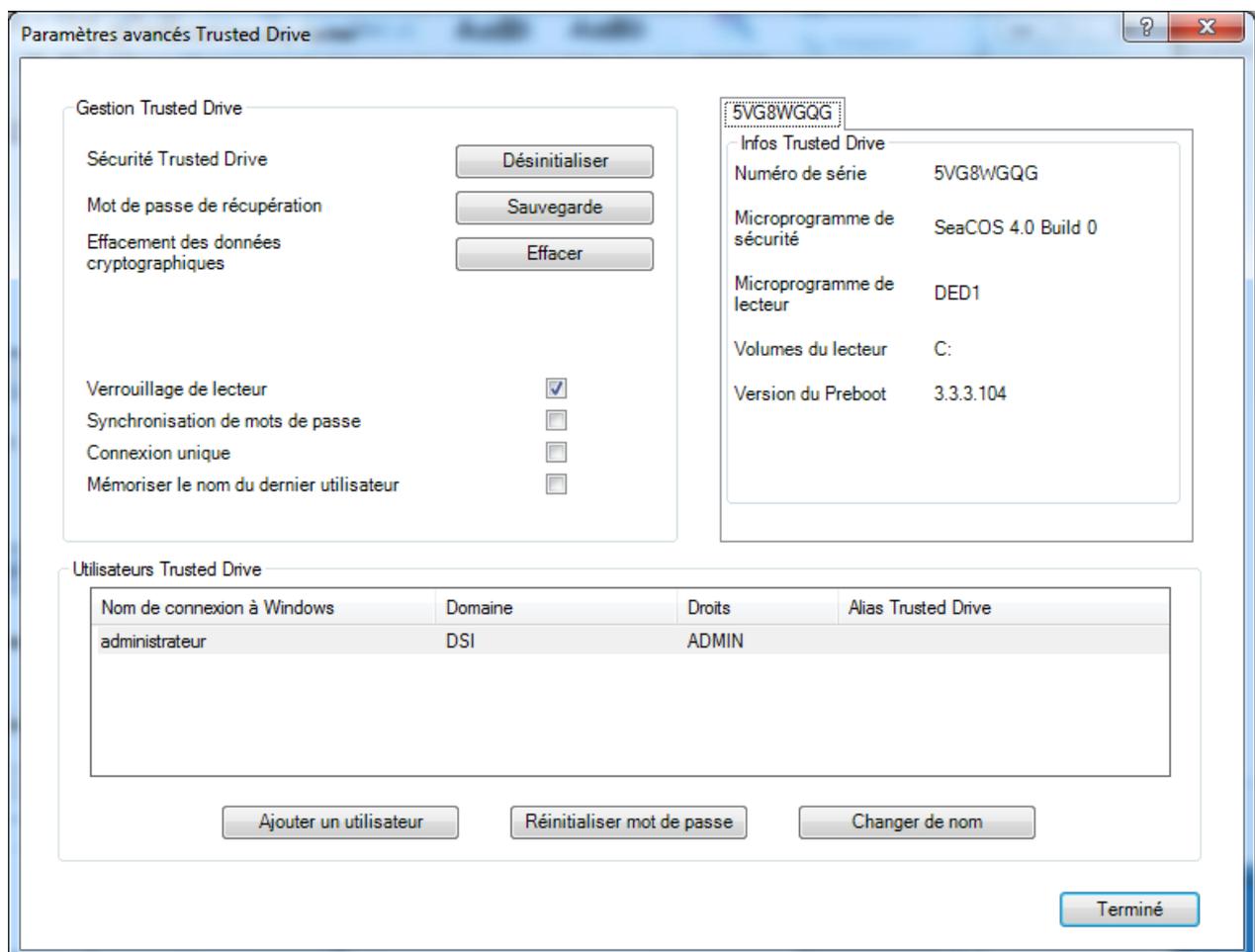
Authentification de l'administrateur du lecteur

Spécifiez le nom et le mot de passe de l'administrateur Trusted Drive Administrator.

Nom d'utilisateur : administrateur

Domaine/Ordinateur : DSI

Mot de passe :



Paramètres avancés Trusted Drive

Gestion Trusted Drive

Sécurité Trusted Drive

Mot de passe de récupération

Effacement des données cryptographiques

Verrouillage de lecteur

Synchronisation de mots de passe

Connexion unique

Mémoriser le nom du dernier utilisateur

Infos Trusted Drive

5VG8WGQG

Numéro de série 5VG8WGQG

Microprogramme de sécurité SeaCOS 4.0 Build 0

Microprogramme de lecteur DED1

Volumes du lecteur C:

Version du Preboot 3.3.3.104

Utilisateurs Trusted Drive

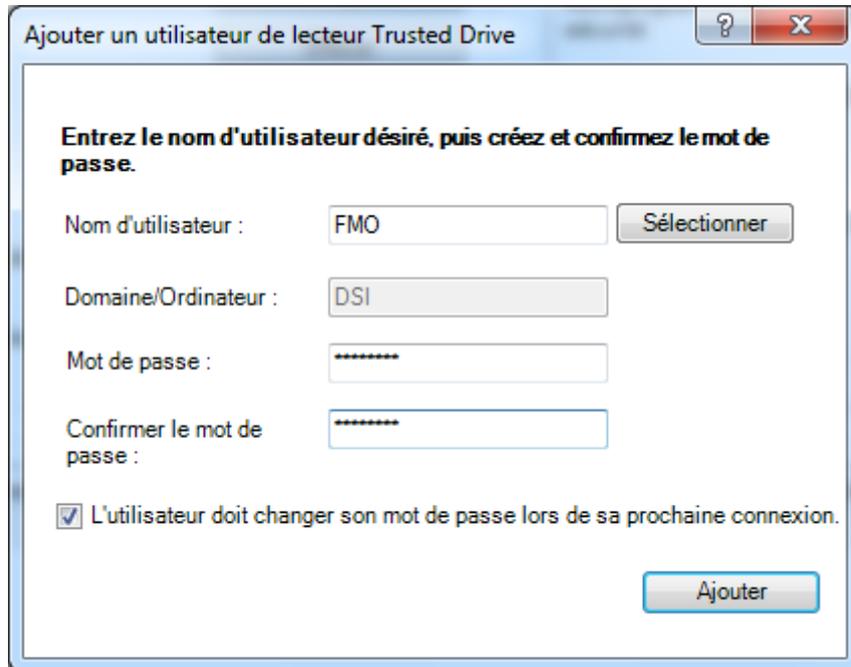
Nom de connexion à Windows	Domaine	Droits	Alias Trusted Drive
administrateur	DSI	ADMIN	

Cliquer sur « **Ajouter un utilisateur** »

Bien que non obligatoire, il est préférable de choisir ici le même nom d'utilisateur que pour l'ouverture de session à Windows.

Initialisation d'un disque chiffrant sous Windows

Donner un mot de passe provisoire et cochez la case pour changer le mot de passe.



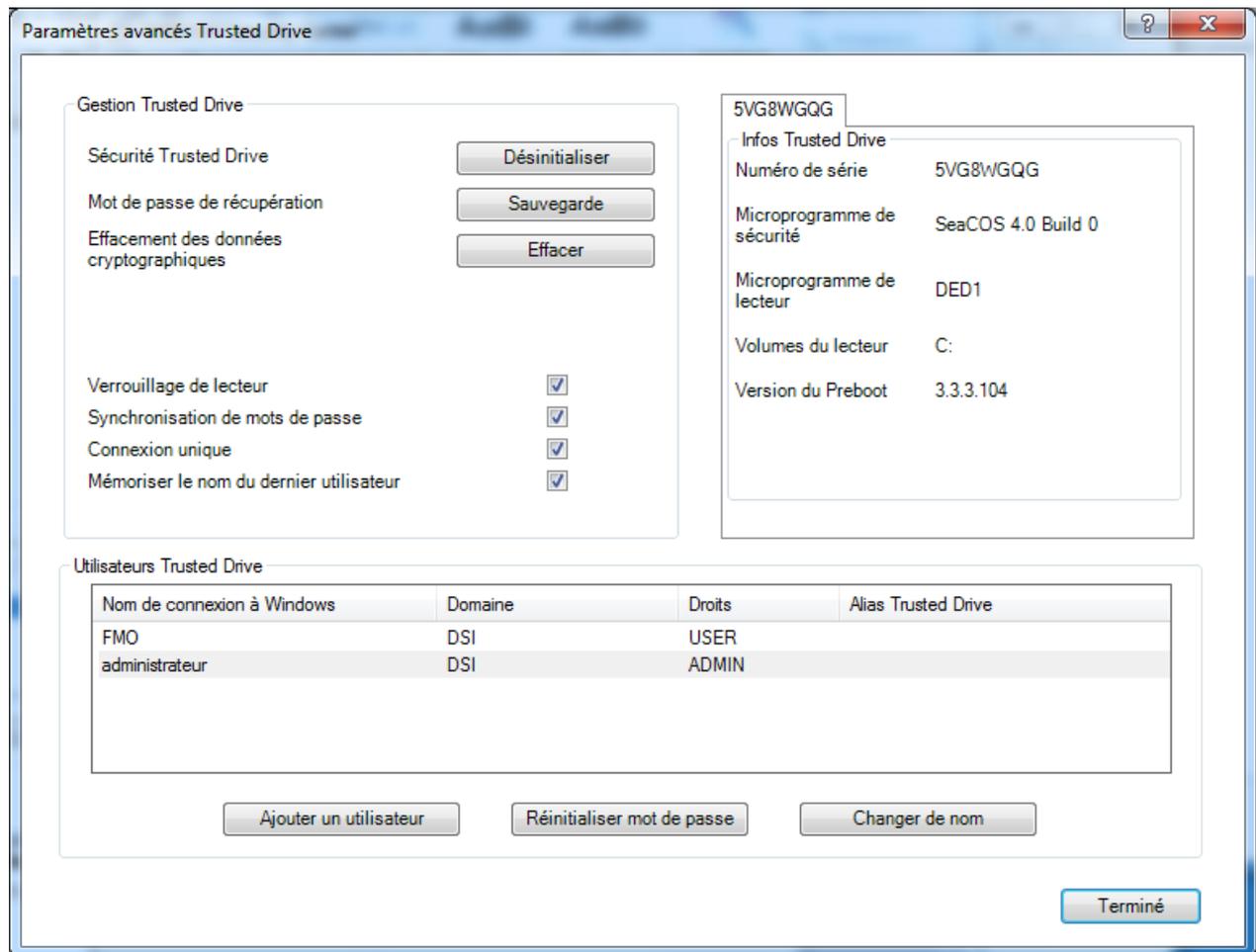
The image shows a Windows dialog box titled "Ajouter un utilisateur de lecteur Trusted Drive". The dialog contains the following fields and controls:

- Entrez le nom d'utilisateur désiré, puis créez et confirmez le mot de passe.**
- Nom d'utilisateur :** A text box containing "FMO" and a "Sélectionner" button.
- Domaine/Ordinateur :** A text box containing "DSI".
- Mot de passe :** A text box with masked characters (dots).
- Confirmer le mot de passe :** A text box with masked characters (dots).
- L'utilisateur doit changer son mot de passe lors de sa prochaine connexion.**
- Ajouter** button.

Cliquer sur « **Ajouter** »

On obtient donc,

Initialisation d'un disque chiffrant sous Windows



Cocher les cases

- « **Synchronisation de mots de passe** »,
- « **Connexion unique** »,
- « **Mémoriser le nom du dernier utilisateur** ».

Ceci n'a rien d'obligatoire mais facilite l'utilisation.

Cliquer sur « **Terminé** »

Fermer l'application « EMBASSY Security Center »

Arrêter la machine.

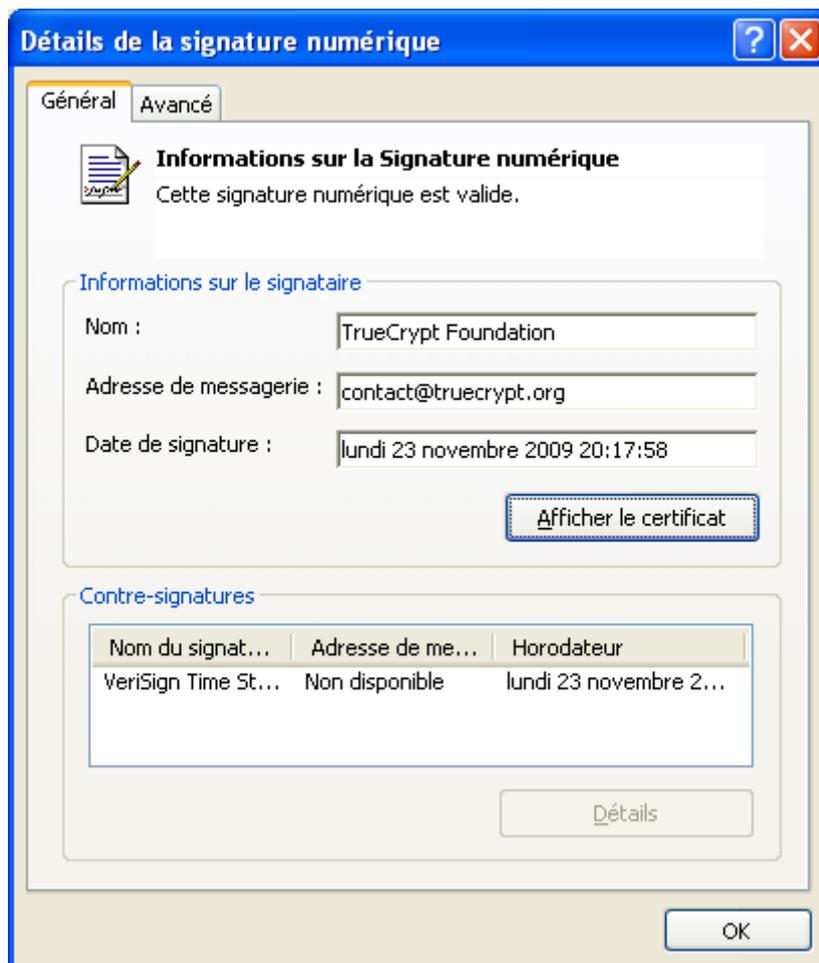
L'étape initialisation du disque chiffrant par l'administrateur est désormais terminée et la machine est prête à être livrée à l'utilisateur. Voir le [guide de l'utilisateur](#).

Installation de TrueCrypt sous Windows

Cette installation demande d'avoir des privilèges administrateur.

Récupération du logiciel

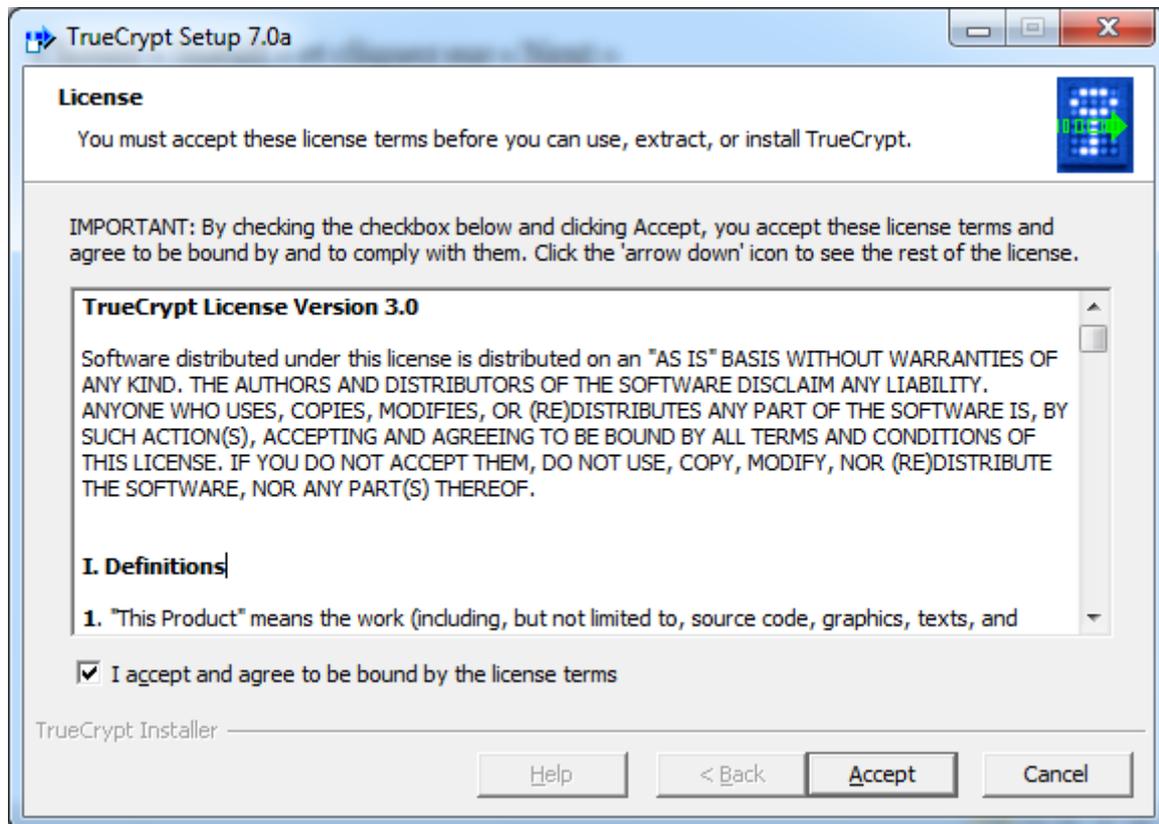
- Télécharger le logiciel TrueCrypt sur <http://www.truecrypt.org/downloads>
- Vérifier la signature de l'exécutable
 - Bouton de droite -> Propriétés -> Onglet « **Signatures numériques** »
 - Sélectionner la signature
 - Cliquer sur le bouton « **Détails** »
 - S'assurer que la signature est bien valide. Dans le cas contraire ne pas poursuivre, le logiciel récupéré est suspect



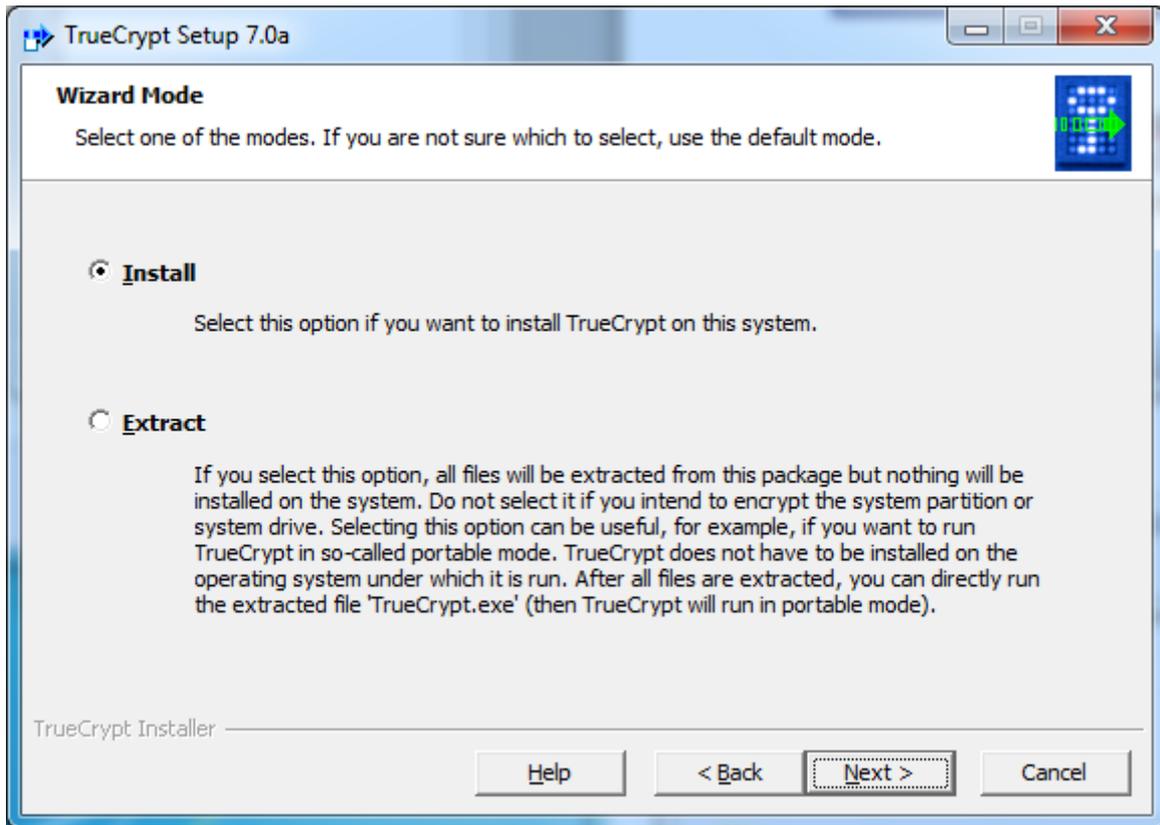
Installation de TrueCrypt

- Lancer l'exécutable

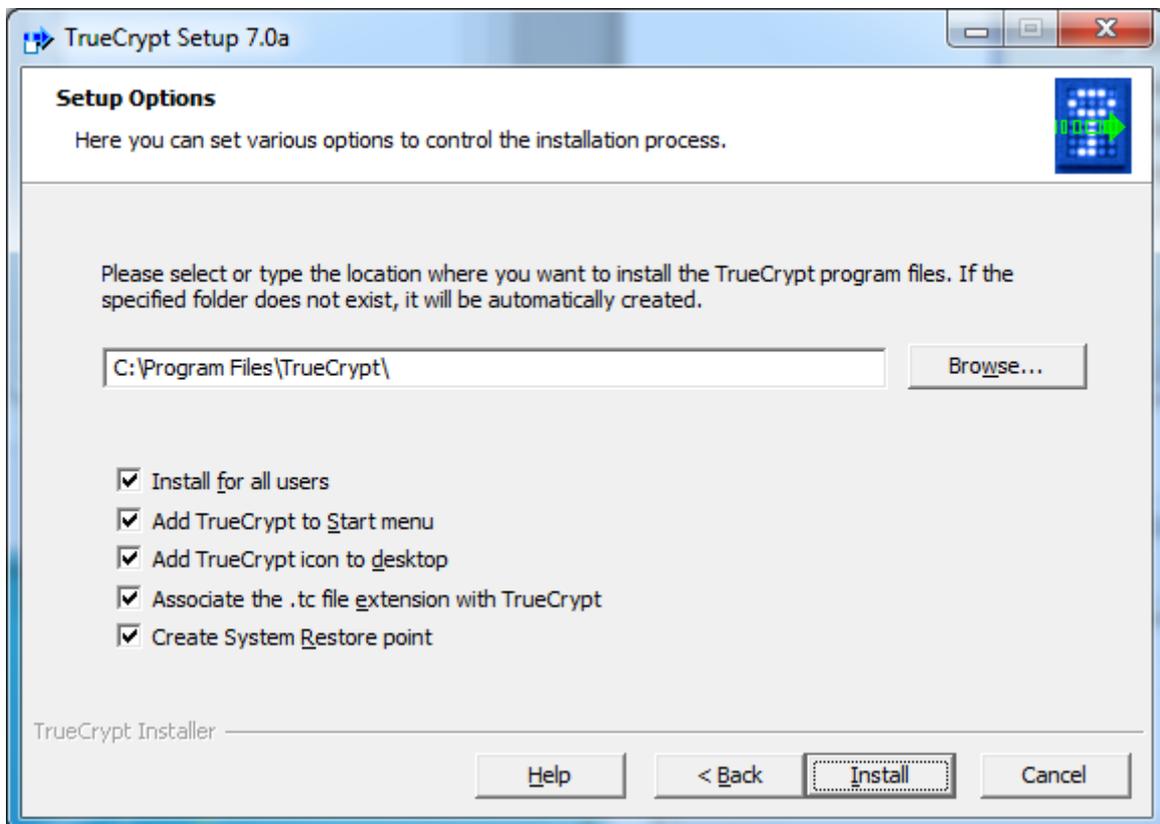
- Accepter la licence en cochant la case « **I accept...** » puis en cliquant sur « **Accept** »



Choisir « Install » et cliquez sur « **Next** »



Conserver les valeurs par défaut et cliquer sur « **Install** »



Installer le français

- Récupérer sur <http://www.truecrypt.org/localizations> le « *language pack* » correspondant au français
- extraire l'archive
- copier le fichier **Language.fr.xml** dans le répertoire où est installé TrueCrypt, généralement **C:\Program Files\TrueCrypt**
- Démarrer TrueCrypt, aller dans « **Settings (Paramètres)** » → « **Language (Langue)** », choisir « **Français** » et valider en cliquant sur « **OK** »

TrueCrypt peut désormais être utilisé pour chiffrer un [disque système](#) ou des [conteneurs](#).

Chiffrement d'un disque système sous Windows à l'aide de TrueCrypt

Recommandations

Cette installation demande d'avoir des privilèges administrateur.

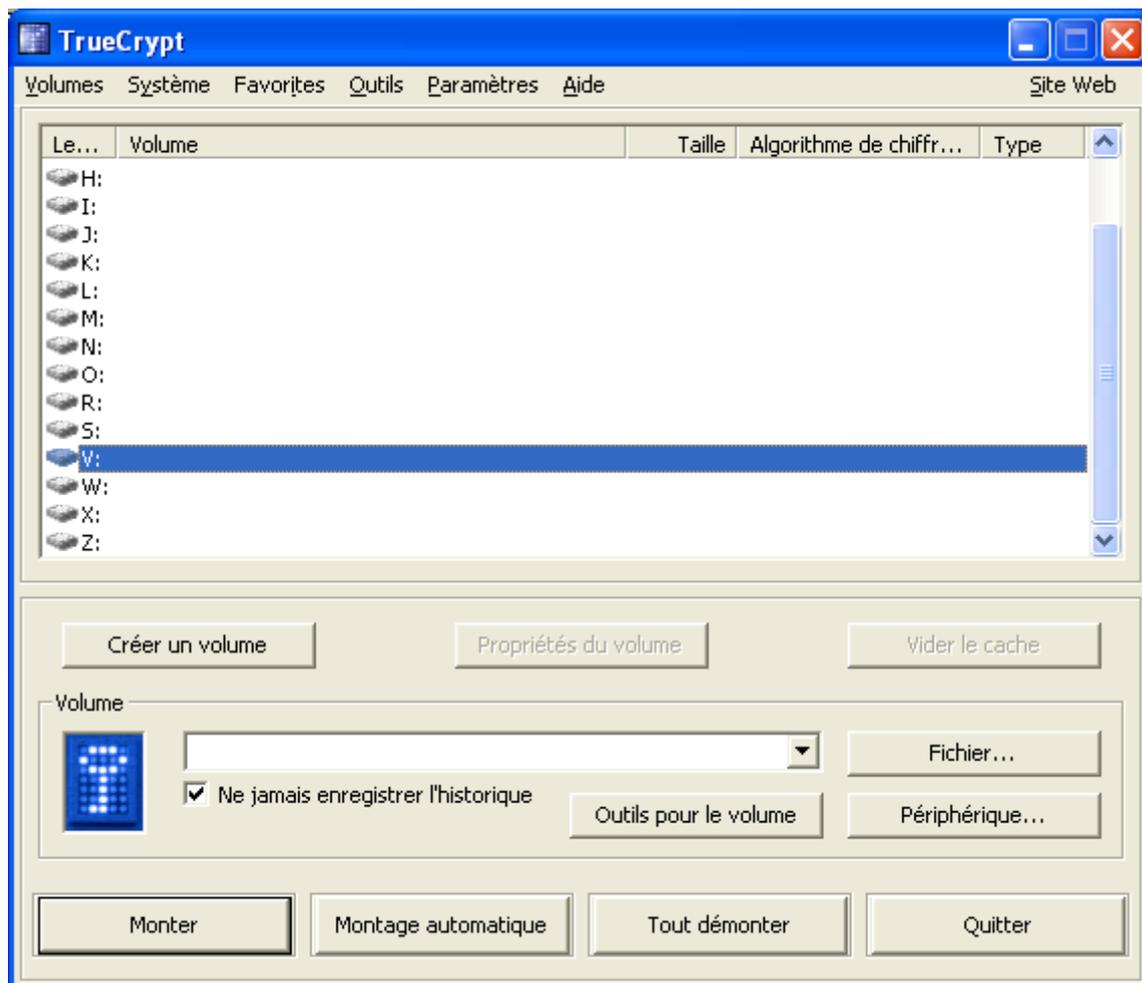
Le logiciel TrueCrypt doit avoir été préalablement [installé](#).

Pour se prémunir des conséquences d'un éventuel problème lors de l'opération et par mesure de précaution, il est impératif d'avoir un sauvegarde des données de l'utilisateur.

Cela étant dit, la procédure est robuste avec de nombreux tests pour s'assurer de la réversibilité des opérations et les risques de pertes d'information devraient donc être très faibles.

Chiffrement du disque système

Démarrez TrueCrypt



Sélectionnez « **Outils** → **Assistant de création de volume** ».



Choisissez « **Normal** » puis cliquez sur « **Suivant >** ».



Choisissez « **Chiffrer l'intégralité du disque** » puis cliquez sur « **Suivant >** ».



Cliquez sur « **Suivant >** ».

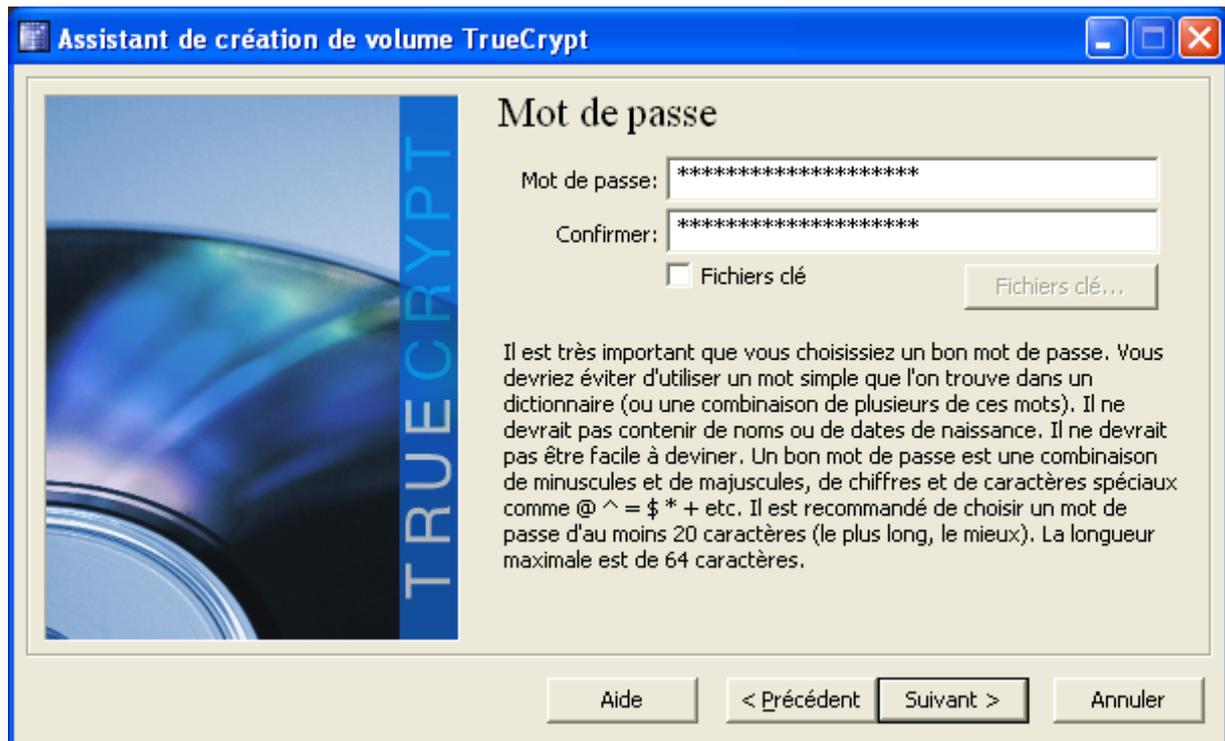


Chiffrement d'un disque système sous Windows à l'aide de TrueCrypt

Dans le cas fréquent où il n'y a qu'un seul système d'exploitation sélectionnez « **Amorçage** » et cliquez sur « **Suivant >** ».



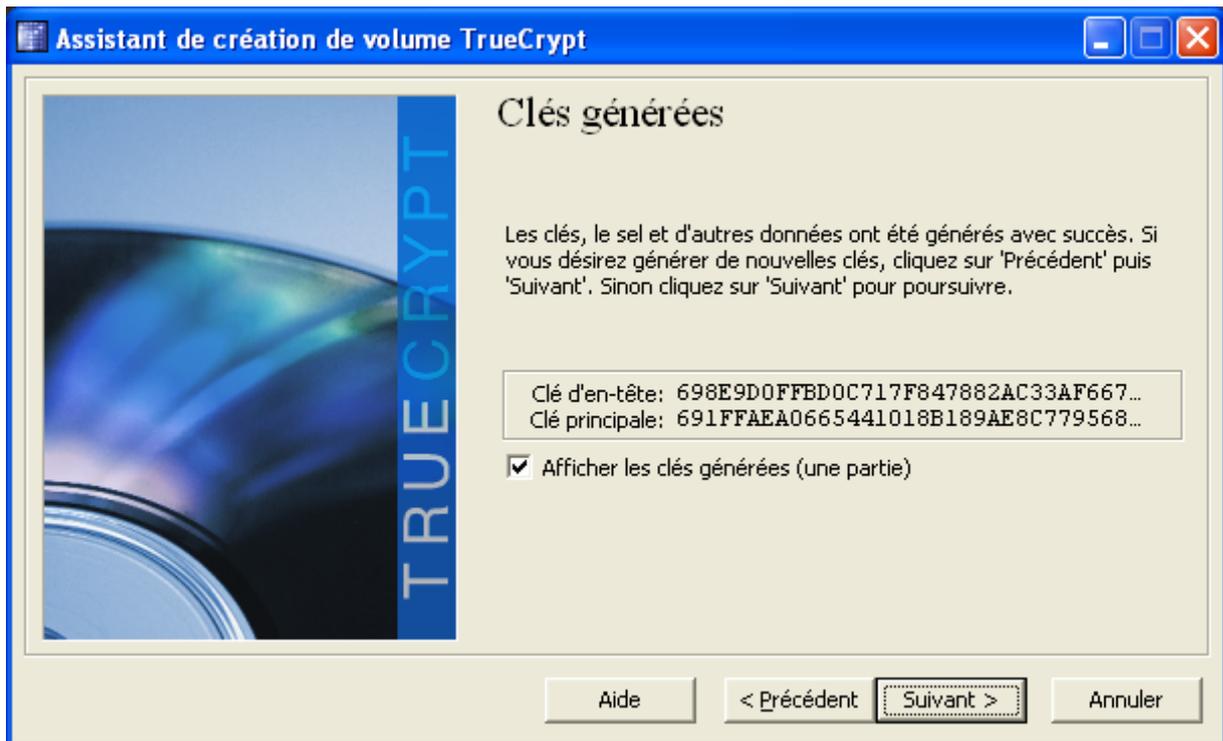
Conservez les valeurs par défaut et cliquez sur « **Suivant >** ».



Choisir un mot de passe robuste et mémorisez le puis cliquez sur « **Suivant >** ».



Déplacez la souris dans le fenêtre puis cliquez sur « **Suivant >** ».



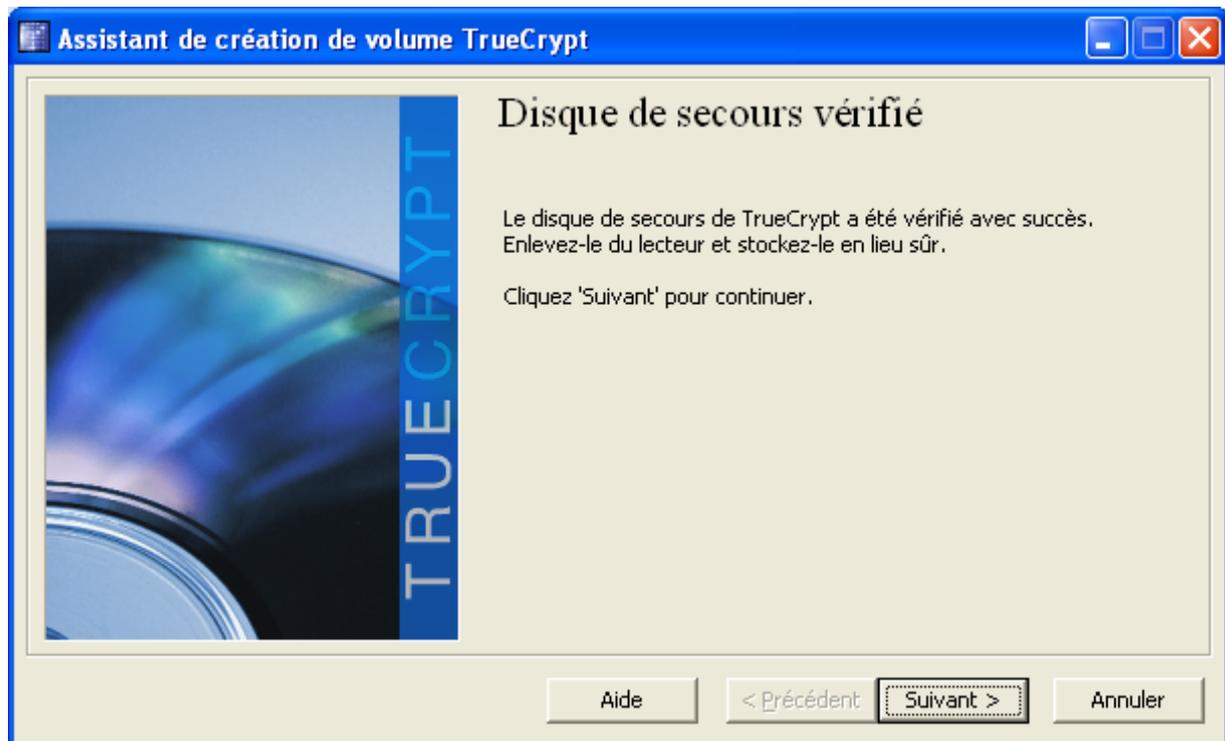
Cliquez sur « **Suivant** > ».



Cliquez sur « **Suivant** > ».



Gravez l'image ISO du CD qui vient d'être générée, insérez le CD gravé puis cliquez sur « **Suivant** > ».



Chiffrement d'un disque système sous Windows à l'aide de TrueCrypt

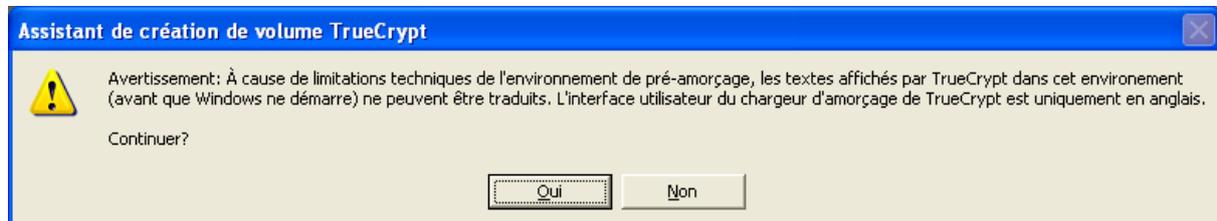
Cliquez sur « **Suivant** > ».



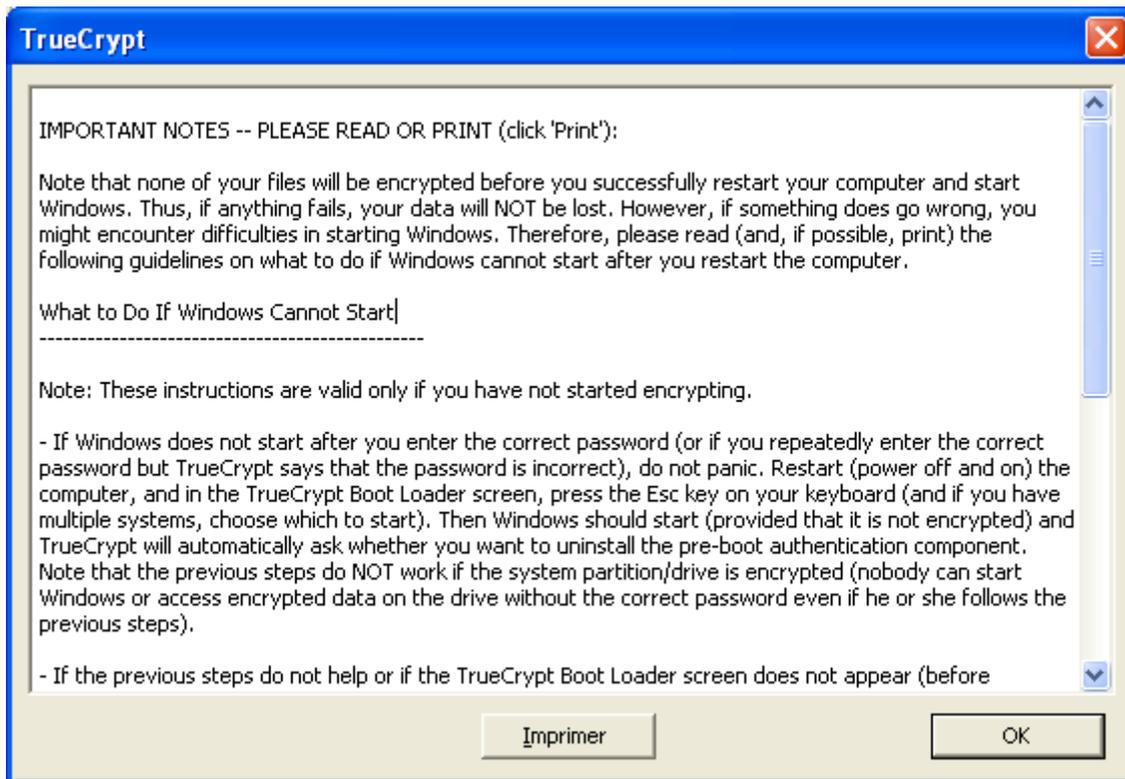
Cliquez sur « **Suivant** > ».



Cliquez sur « **Test** ».



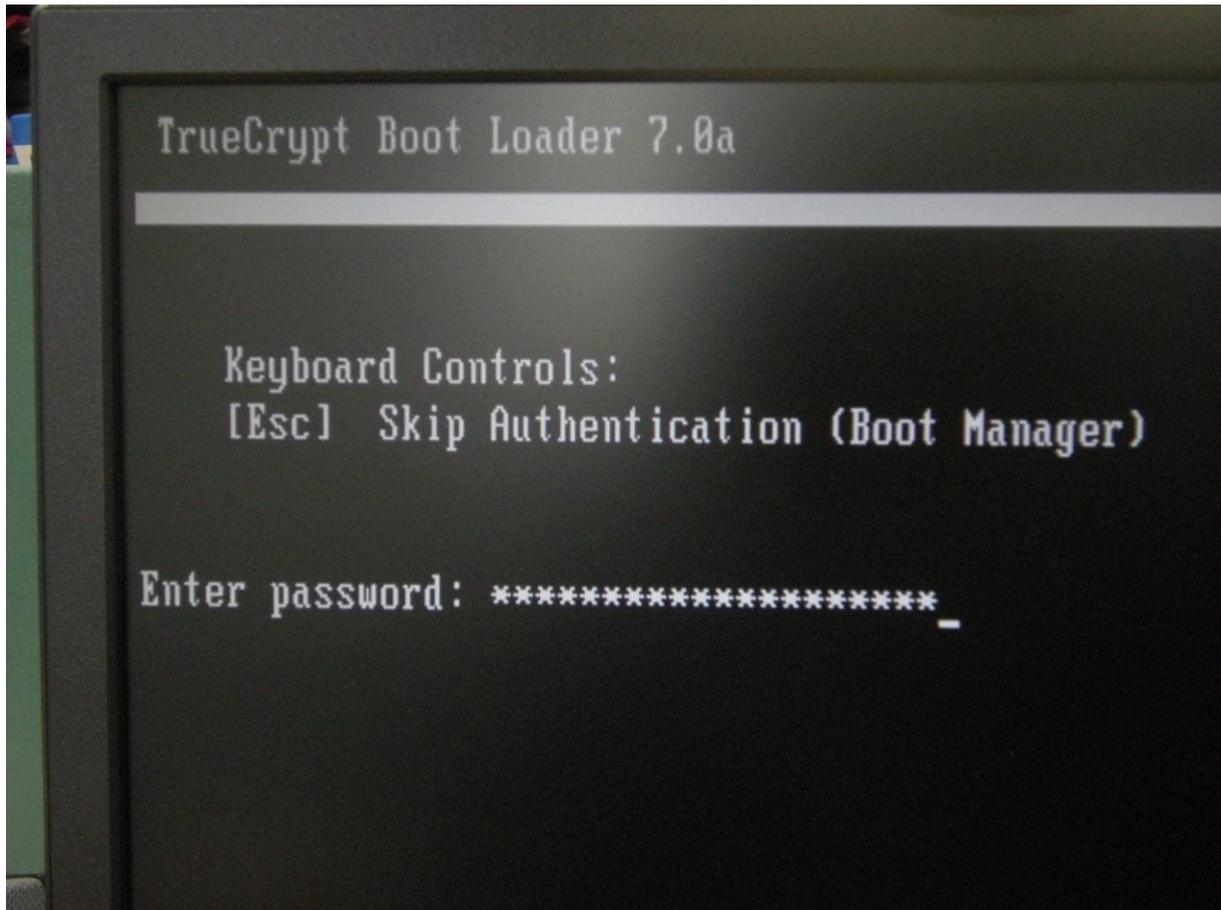
Cliquez sur « **Oui** ».



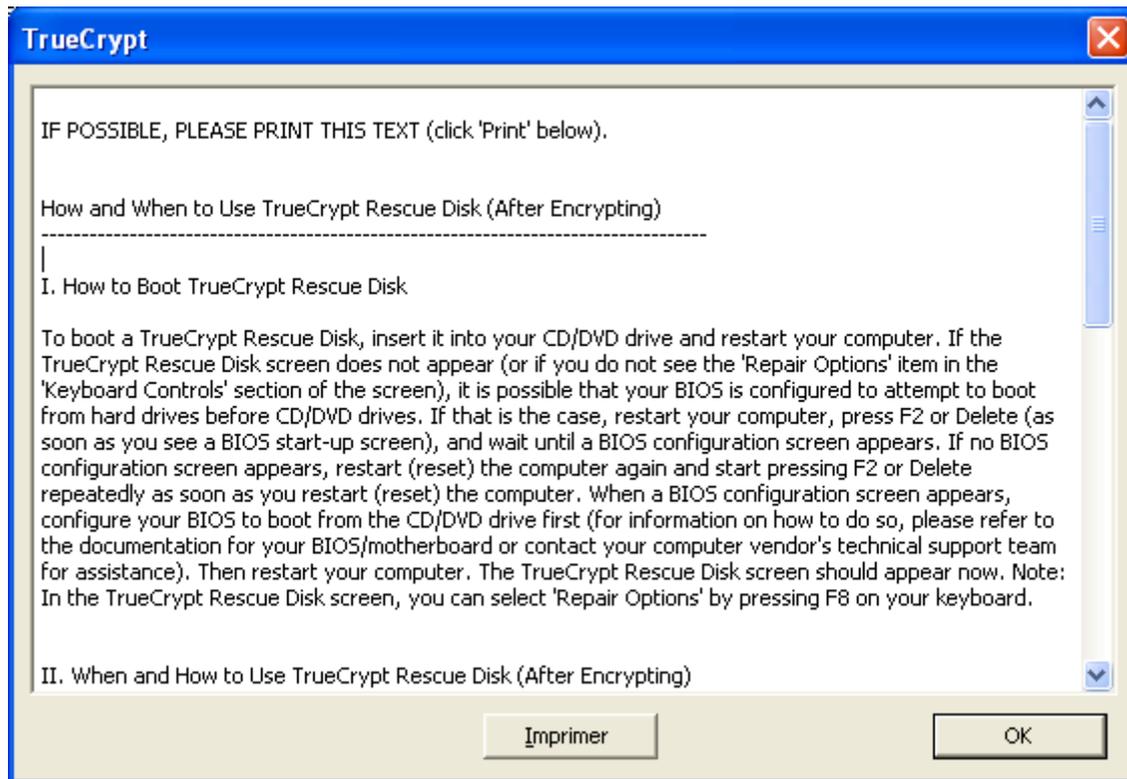
Imprimez le texte en cliquant sur « **Imprimer** » et conservez le puis cliquez sur « **OK** ».



Cliquez sur « **Oui** » pour redémarrer l'ordinateur.



Lors du « preboot » TrueCrypt saisissez votre mot de passe TrueCrypt puis ouvrez une session Windows.



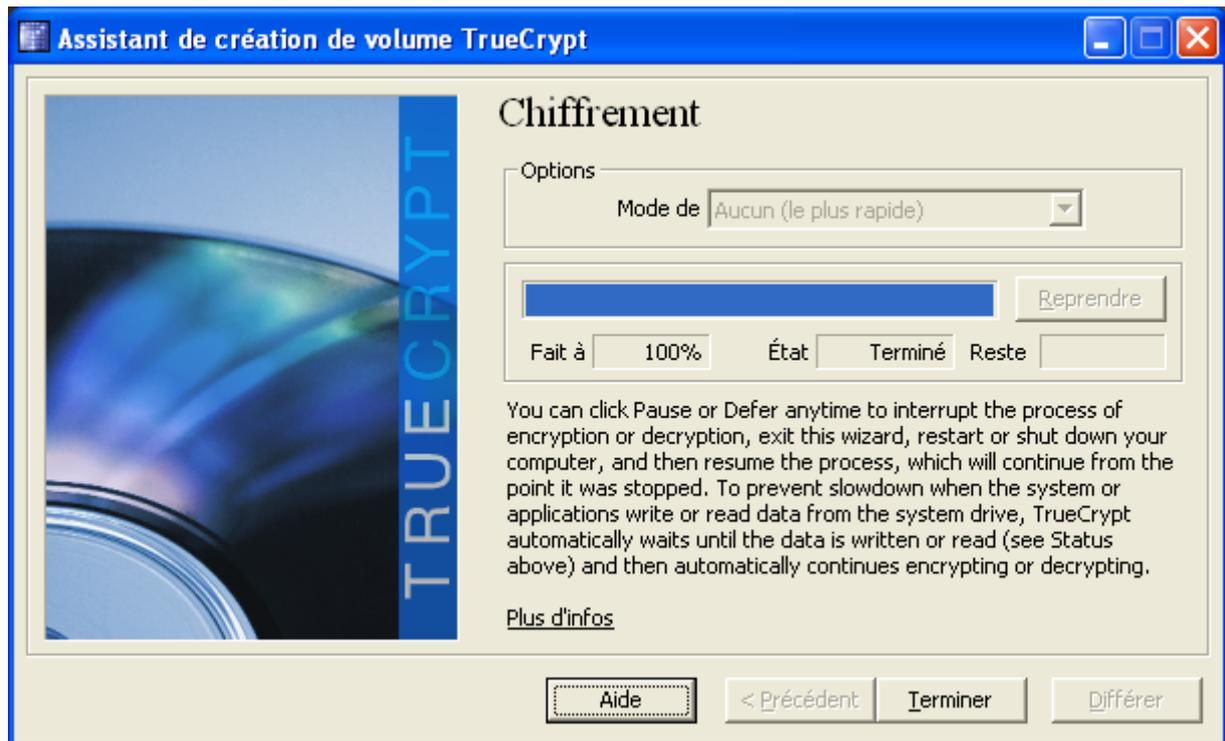
Imprimez le texte en cliquant sur « **Imprimer** » et conservez le puis cliquez sur « **OK** ».



Attendre que le disque soit entièrement chiffré. Il est possible de travailler pendant que le chiffrement s'effectue mais ce n'est pas réellement conseillé car l'opération sollicite énormément les disques.



Cliquez sur « **OK** ».



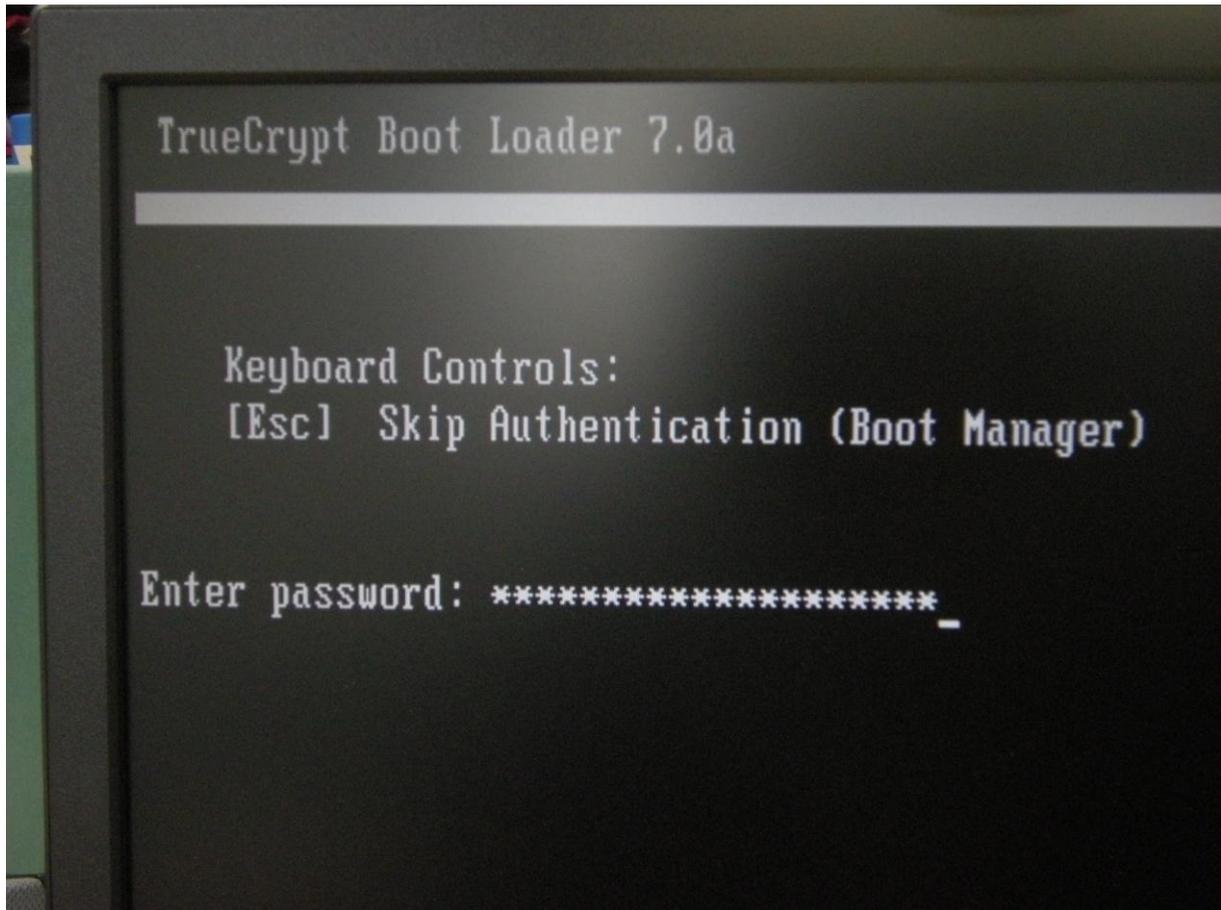
Cliquez sur « **Terminer** ». Le disque est désormais chiffré.

Séquestre

Il faut alors procéder au [séquestre](#) du mot de passe qui a servi au chiffrement ainsi du CD de récupération.

Utilisation

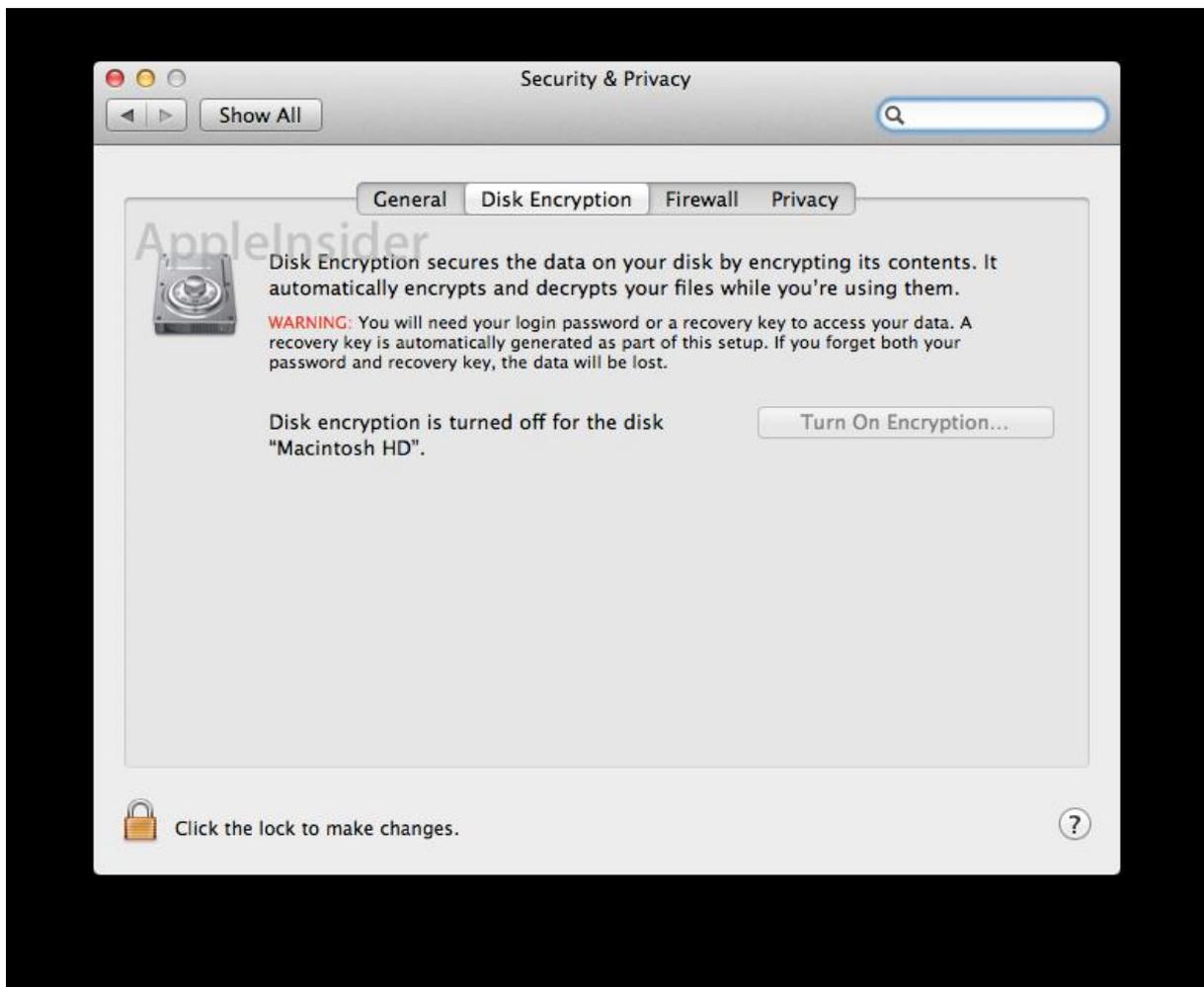
L'utilisation d'un volume système chiffré avec TrueCrypt est très simple. Il suffit de fournir lors du « preboot » le mot de passe TrueCrypt puis d'ouvrir normalement une session Windows.



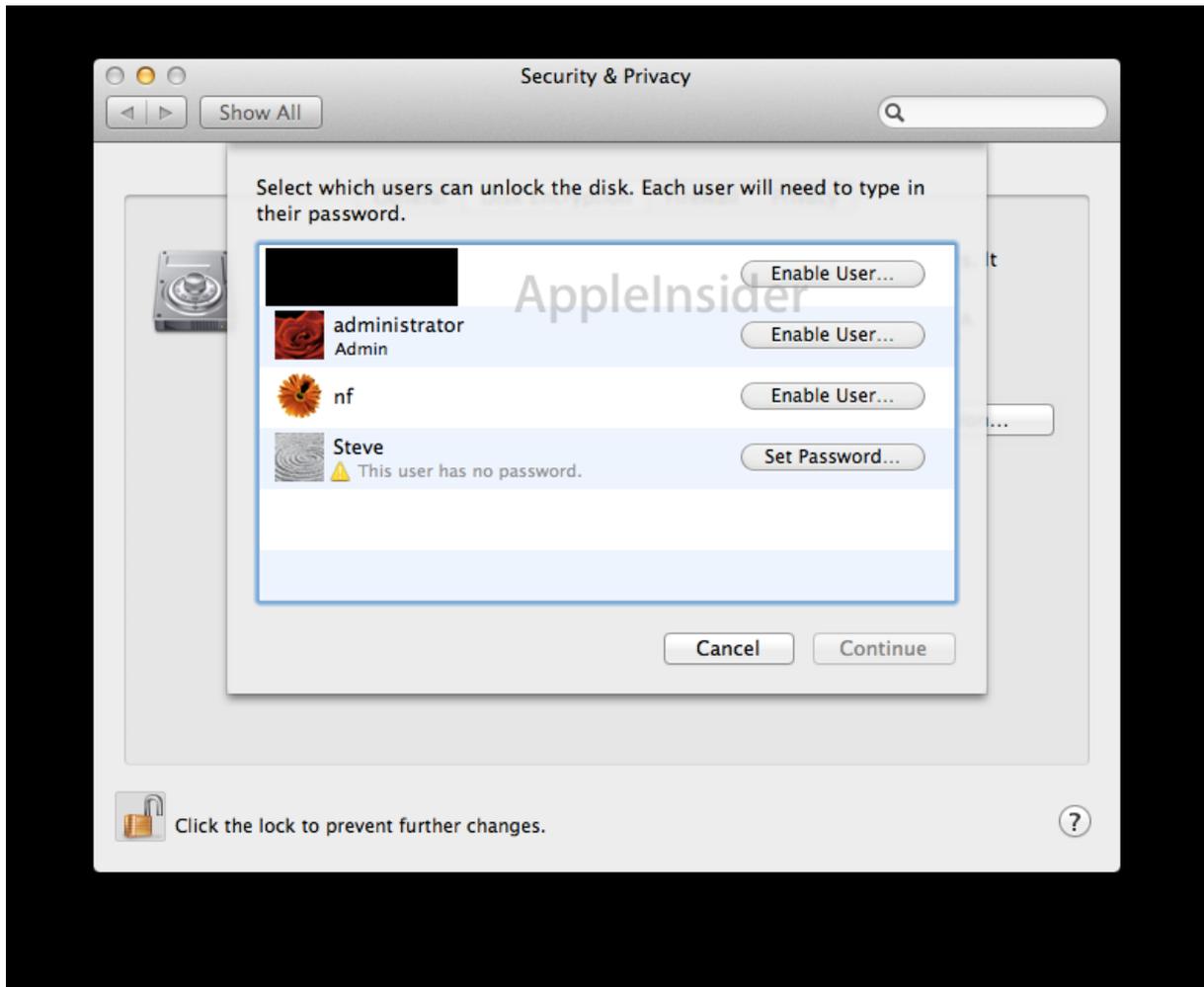
Activation du chiffrement sous MacOS X

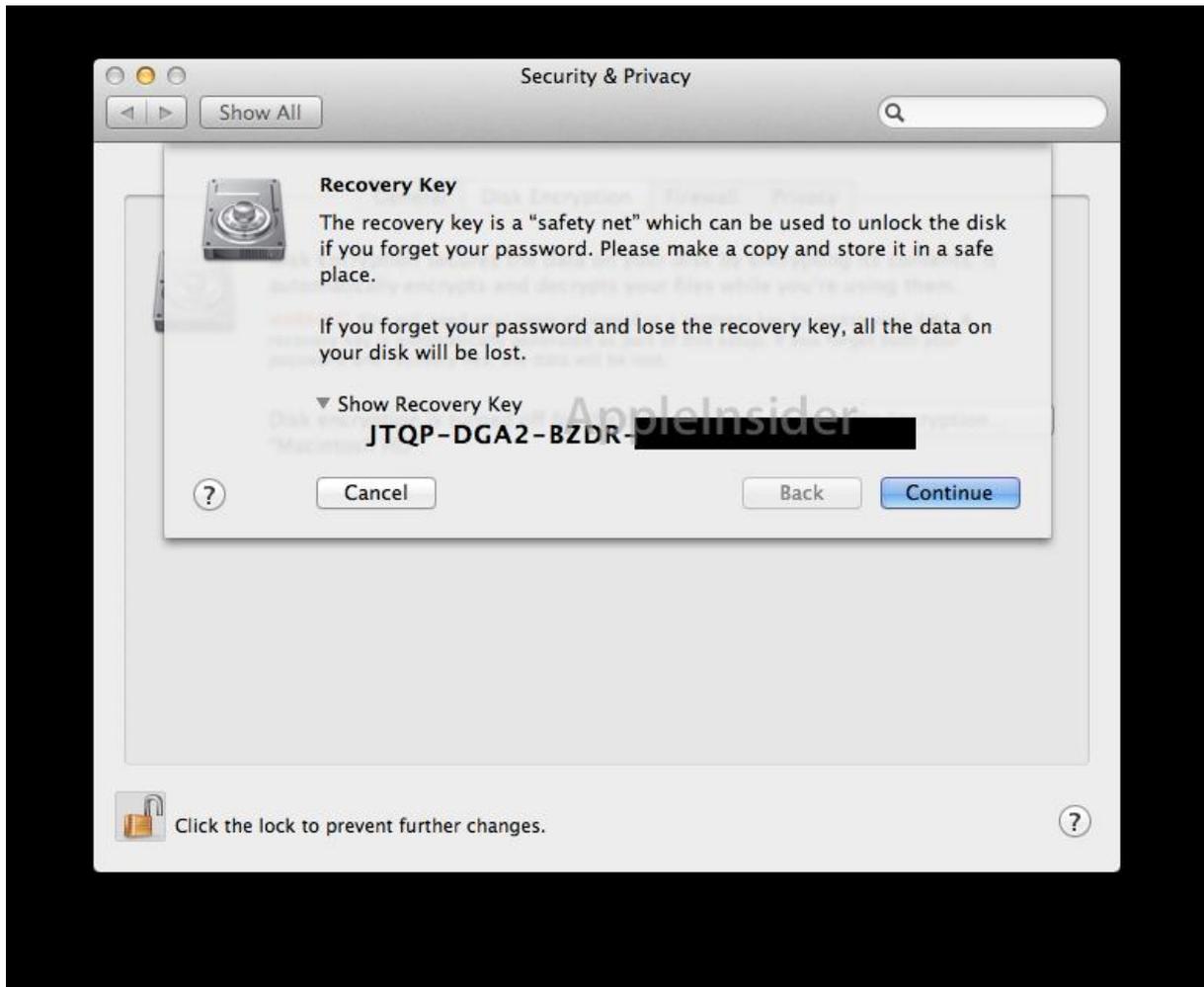
Les dernières versions du système Mac OS X incluent FileVault qui permet de chiffrer le répertoire de l'utilisateur. Pratiquement il s'agit d'un conteneur chiffré qui contient l'ensemble du répertoire de l'utilisateur. Il est protégé par le mot de passe de session de l'utilisateur (la clé symétrique de chiffrement est chiffrée par un dérivé du mot de passe). Il existe aussi un mot de passe principal appelé « filet de sécurité » qui permet le recouvrement (la clé symétrique de chiffrement est aussi chiffrée par un dérivé de ce mot de passe).

La nouvelle version (Lion) de Mac OS X, prévue pour l'été 2011 devrait intégrer un chiffrement intégral du disque, ce qui sera alors la méthode à employer pour protéger les informations. Voici quelques copies d'écrans récupérées sur internet¹.



¹ <http://www.appleinsider.com/>







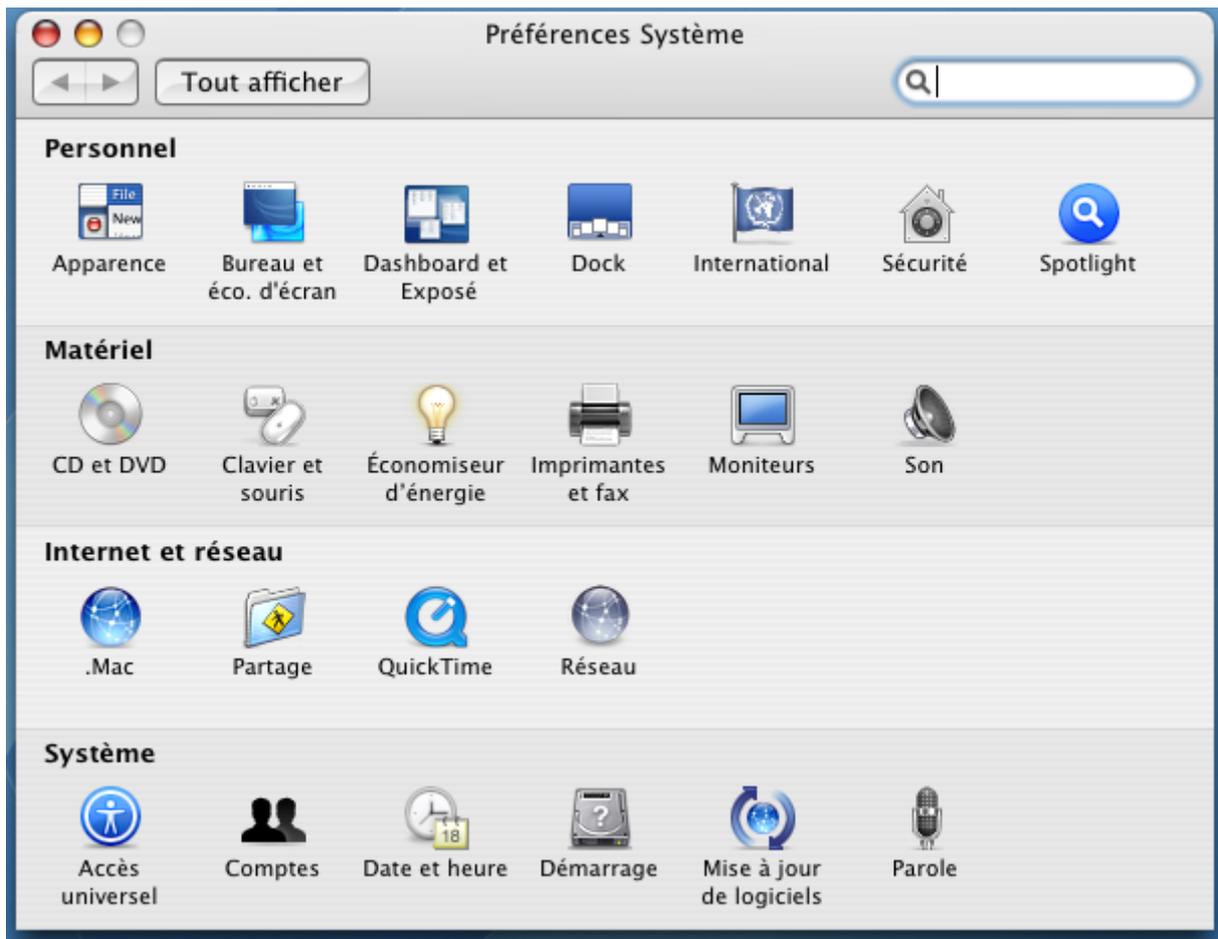
Mais il faudra se méfier des fausses bonnes idées et bien évidemment ne jamais stocker le mot de passe chez Apple.

Mise en garde

Avant de chiffrer un répertoire utilisateur avec FileVault, il faut en effectuer une sauvegarde. C'est une sage précaution au cas où il y aurait un problème lors de l'opération.

Activation de FileVault

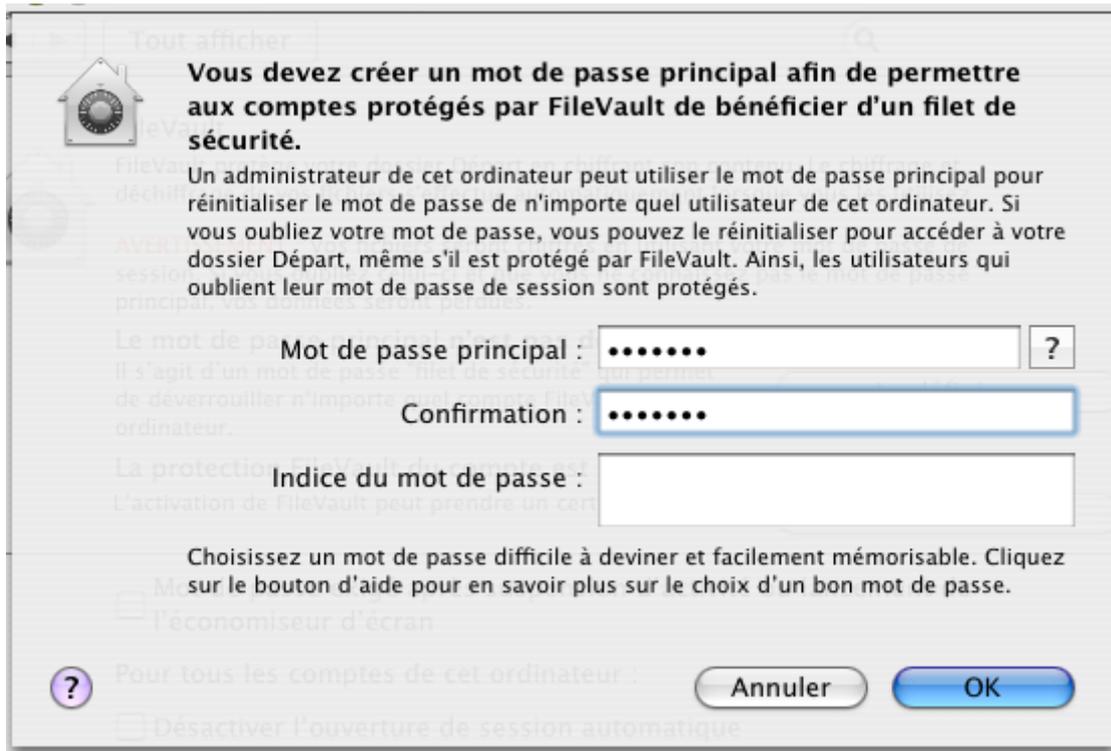
Allez dans le menu pomme et sélectionnez « **Préférences Systèmes** ».



Cliquez sur l'icône « **Sécurité** »



Si le mot de passe principal n'a pas été préalablement défini, cliquez sur « Le définir ».



Saisissez le mot de passe puis cliquez sur « **OK** ».

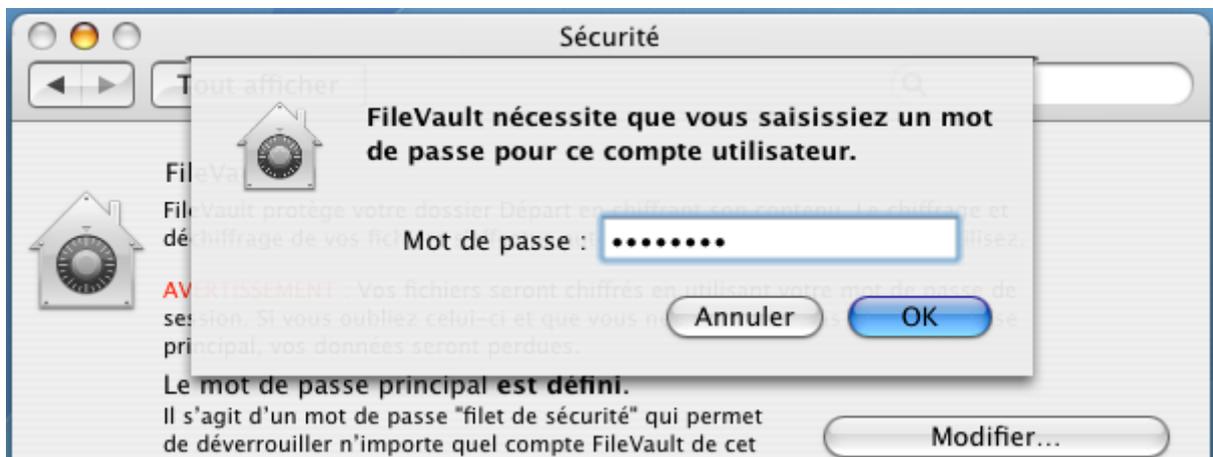


Cochez l'ensemble des cases correspondant à de bonnes pratiques en matière de sécurité. En particulier il est impératif d'activer le chiffrement du *swap* en cochant la case « **Utiliser la mémoire virtuelle sécurisée** ».

Lorsqu'il est demandé fournir le nom et le mot de passe d'un compte administrateur.



Saisissez le nom et le mot de passe d'administrateur, puis cliquez sur « OK ».

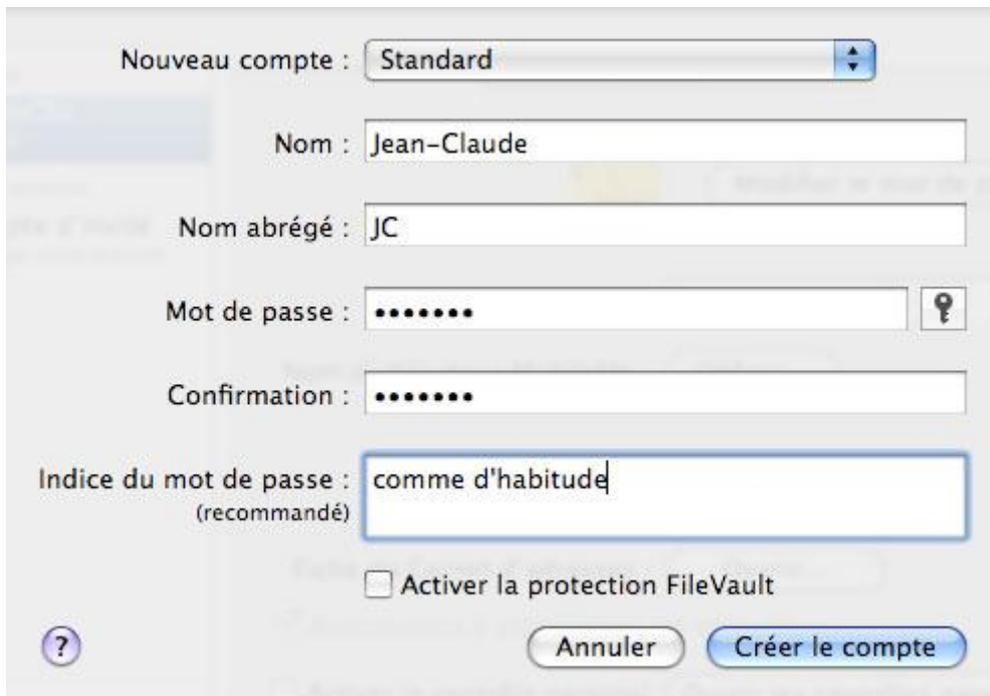


Demandez à l'utilisateur de saisir son mot de passe, puis cliquez sur « OK ».



Cochez la case « **Utiliser l'effacement sécurisé** » ce qui permet de s'assurer que les fichiers supprimés ne seront pas récupérables puis cliquez sur « **Activer FileVault...** ».

L'opération va prendre un certain temps qui sera d'autant plus long que le répertoire de l'utilisateur est volumineux. Il est donc conseillé d'activer FileVault à la création du compte.



Séquestre

Il est impératif de procéder au [séquestre](#) du mot de passe principal (« filet de sécurité »).

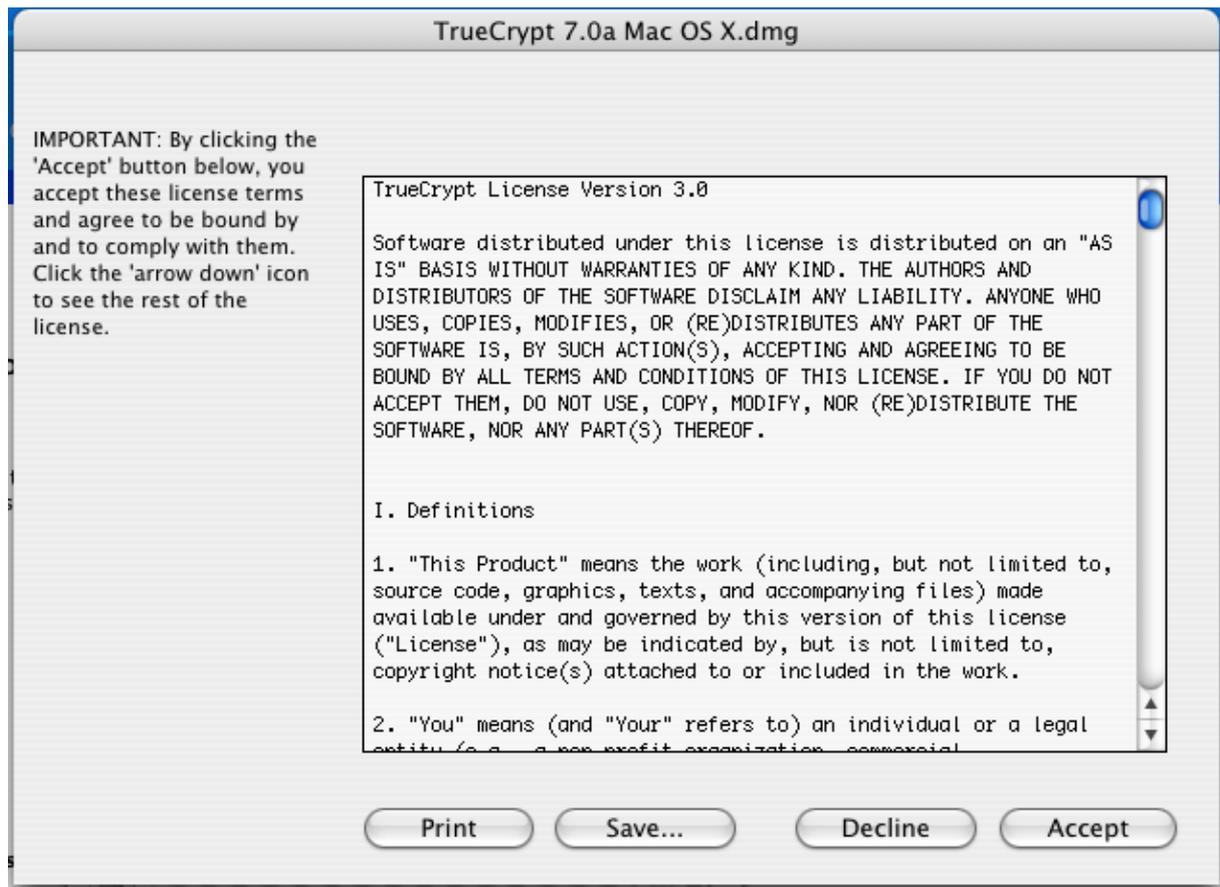
Installation de TrueCrypt sous Max OS X

Cette installation demande d'avoir des privilèges administrateur.

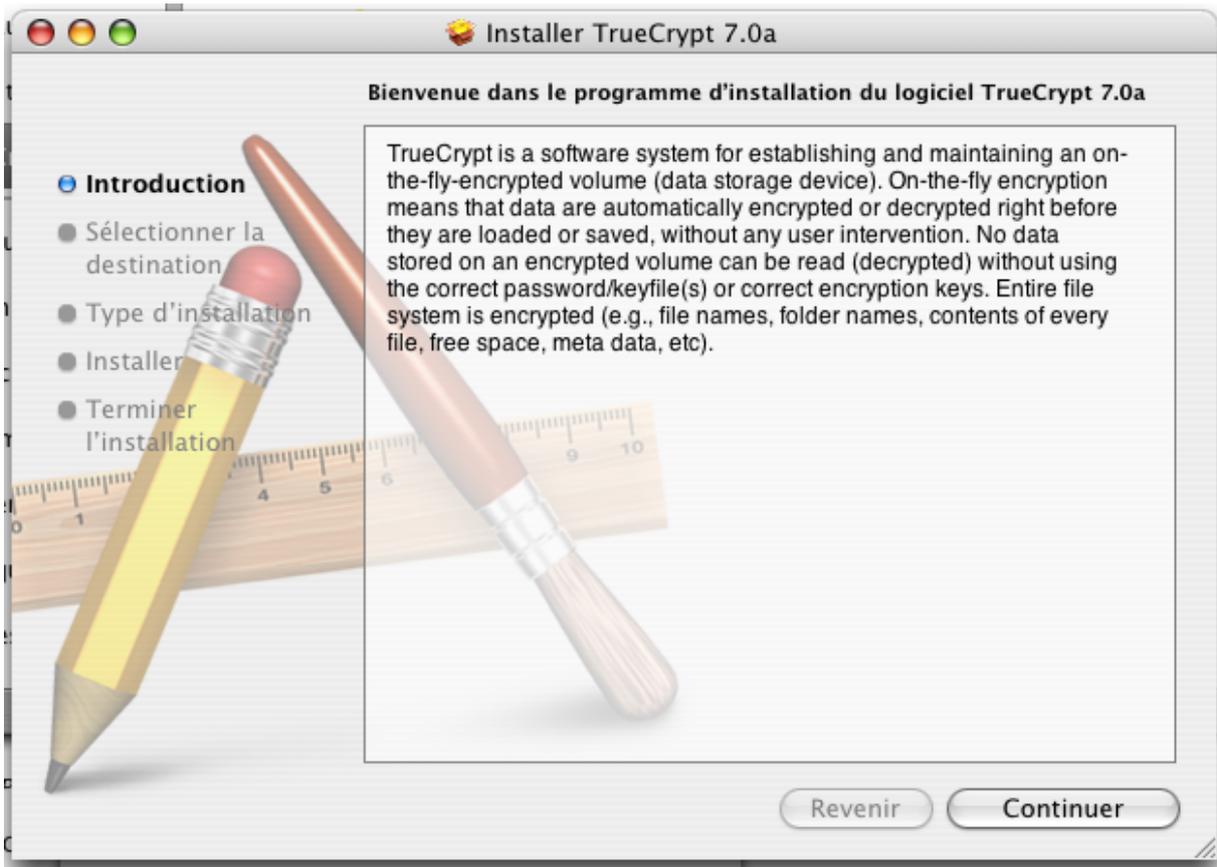
Récupération du logiciel

Téléchargez le logiciel TrueCrypt sur <http://www.truecrypt.org/downloads>

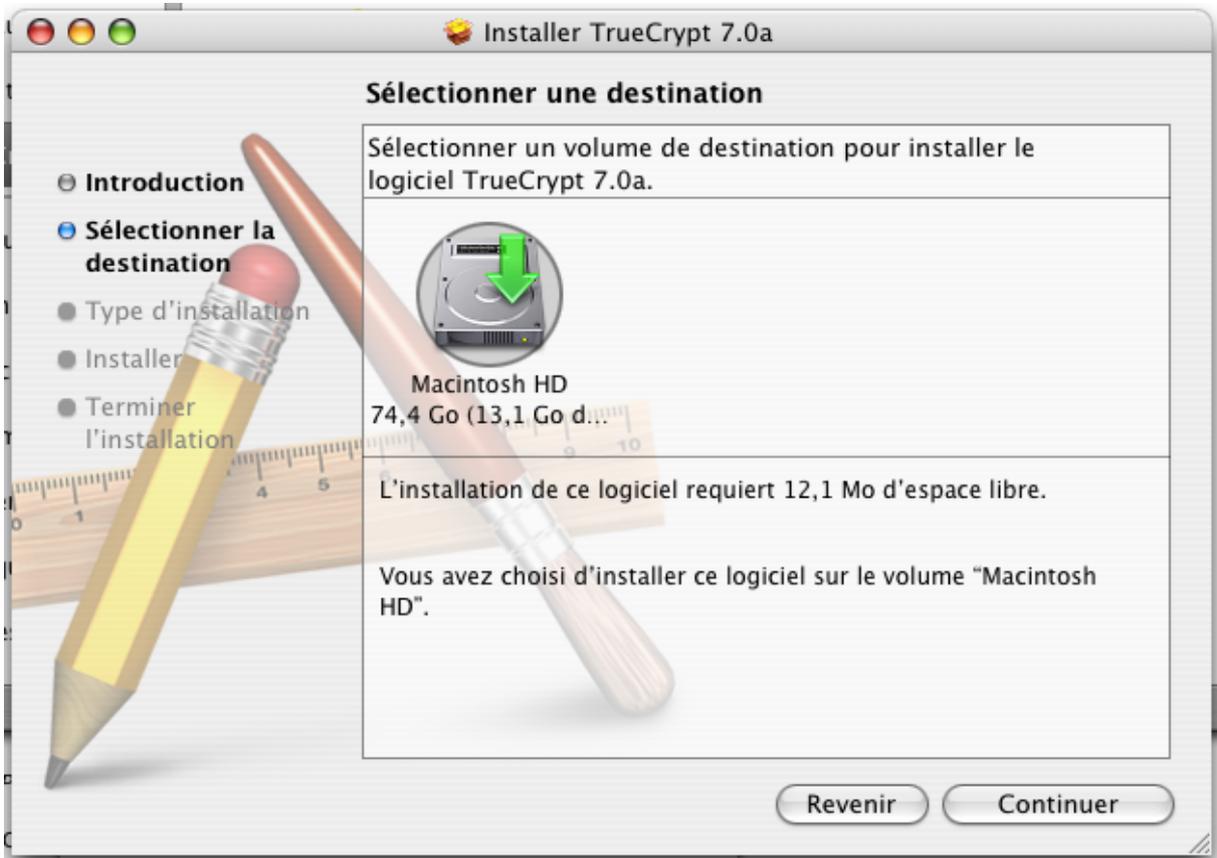
Installation de TrueCrypt



Acceptez la licence en cliquant sur « **Accept** »

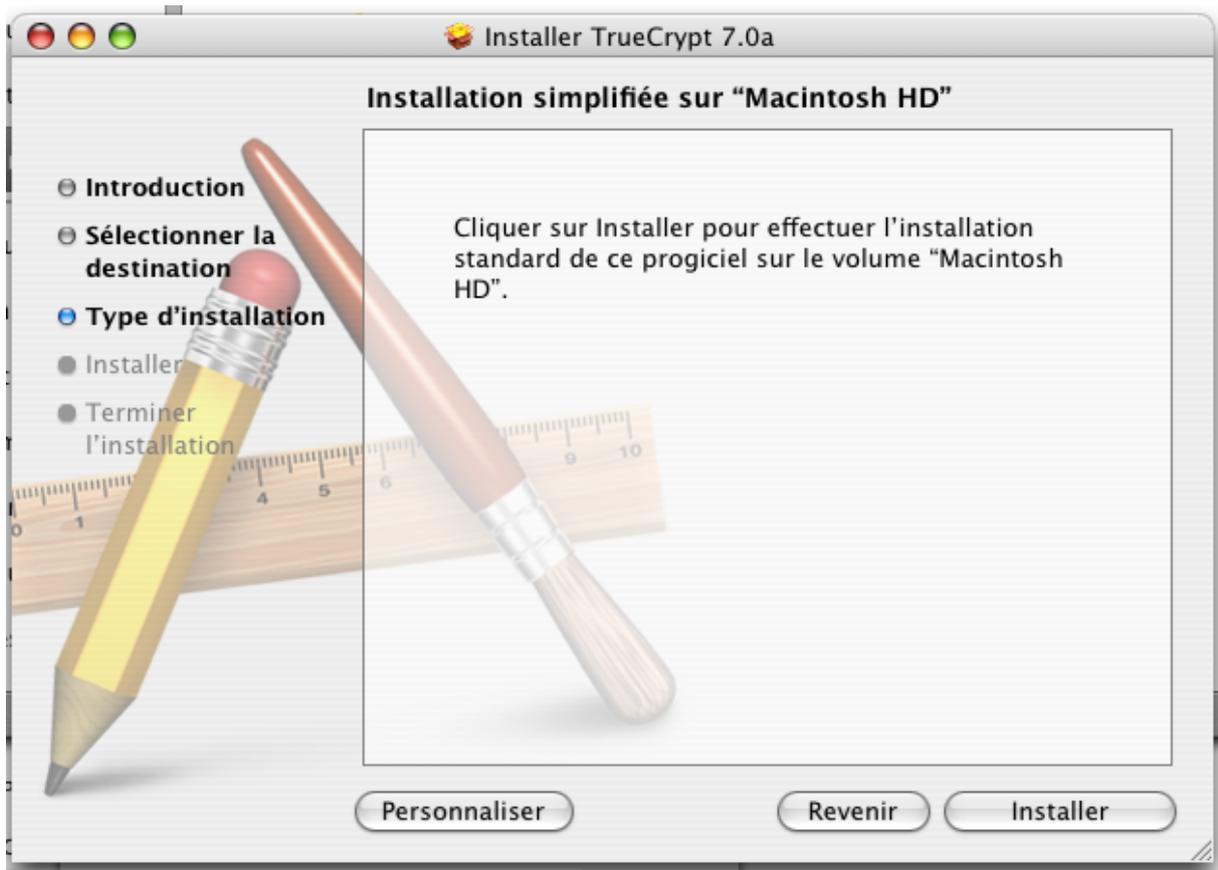


Cliquez sur « Continuer »

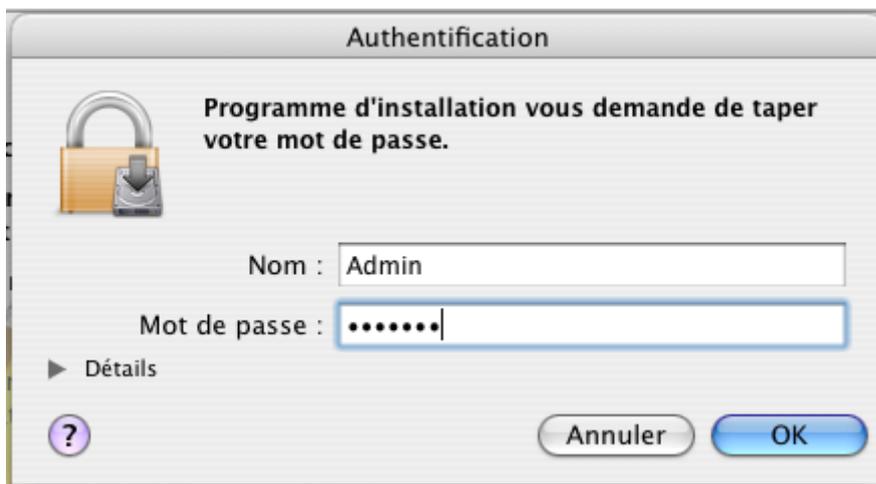


Installation de TrueCrypt sous Mac OS X

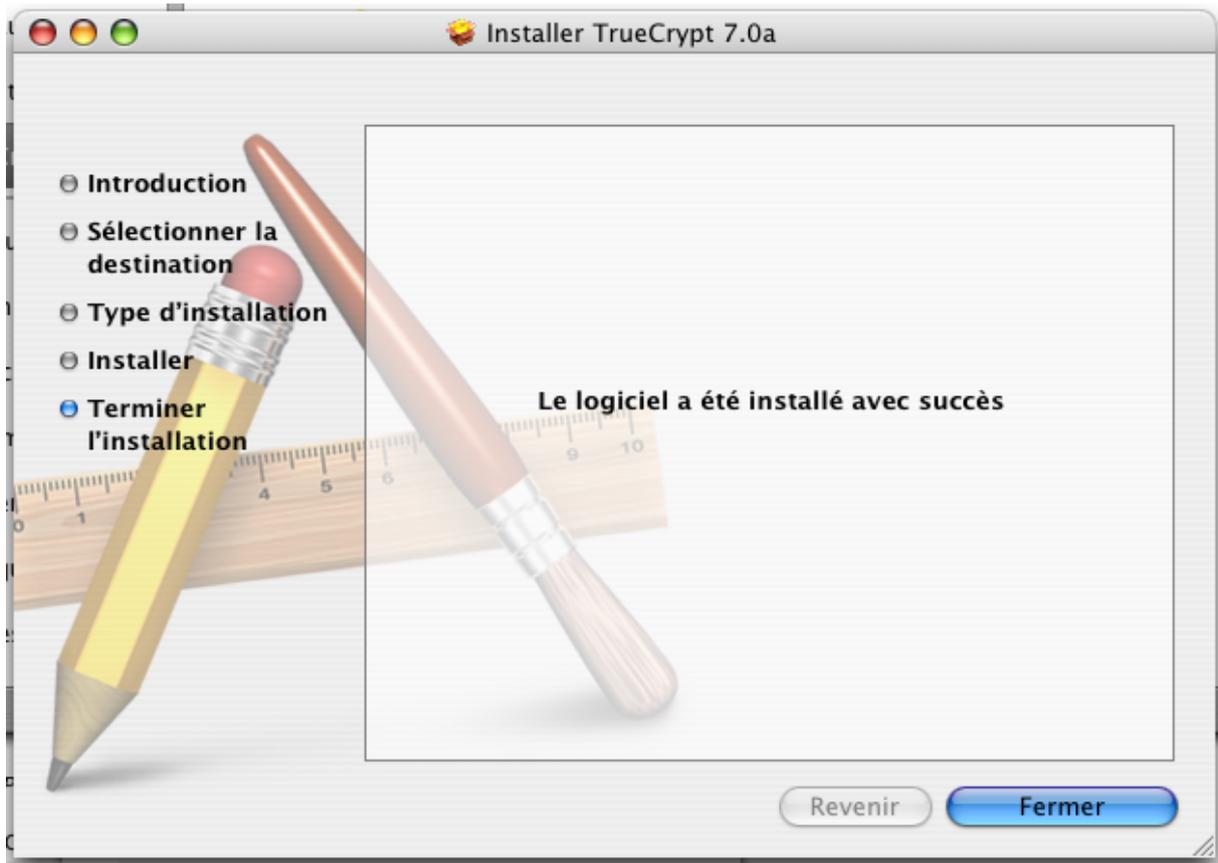
Cliquez sur « **Continuer** »



Cliquez sur « **Installer** »



Entrez le mot de passe du compte administrateur et cliquez sur « **OK** »



TrueCrypt peut désormais être utilisé pour chiffrer des [conteneurs](#).

Disque chiffrant sous Linux

Généralités

Le logiciel Wave Embassy permettant d'initialiser un disque chiffrant n'est disponible que sous Windows. Cependant une fois que le disque a été initialisé, le « pre-boot » installé, ce logiciel n'est plus nécessaire. Il est donc parfaitement possible d'utiliser un disque chiffrant avec une machine en « dual boot » Windows/Linux voire uniquement Linux seul.

Il a été constaté dans certains contextes une incompatibilité entre le « pre-boot » du logiciel Wave Embassy et le chargeur Grub de Linux. Une solution a été trouvée². L'origine du problème n'est pas bien déterminée, elle serait probablement liée au fait que Grub legacy ne s'exécute pas en mode réel.

Installation d'une machine en dual boot Windows / Linux

On part d'une machine où Windows est installé et donc le disque n'est pas chiffré (initialisé dans la terminologie Wave).

Après repartitionnement on installe Linux selon la méthode habituelle et les goûts de l'utilisateur. Si le portable a été livré avec Windows 7 préinstallé, on suppose que le partitionnement initial comporte trois partitions : « sda1 » (diagnostics), « sda2 » (boot Windows) et « sda3 » (Windows 7). Linux sera donc très vraisemblablement installé sur plusieurs partitions toutes regroupées en une étendue sda4. On suppose ici que la partition Linux « /boot » est « sda5 » (transposer au besoin).

Très important : la partition Linux « /boot » doit être formatée en ext2 ou ext3, surtout pas ext4 (qui serait incompatible avec la suite).

Installer Grub (legacy) sur le MBR, et configurer « grub.conf » (qui doit avoir un lien symbolique « menu.lst ») pour booter Windows 7.

Booter le Linux devenu opérationnel, récupérer Grub4DOS (version la plus récente stable à ce jour = 0.4.4 sur <http://gna.org/projects/grub4dos/>).

Copier le fichier « grldr » de la distribution Grub4DOS dans le répertoire « /boot », obligatoirement à la racine (« grldr » n'est pas compatible avec ext4, c'est la raison qui impose ext2 ou ext3 pour /boot, mais peu importe, cette partition ne sert qu'à booter).

Utiliser l'exécutable « bootlace.com » pour installer le preboot de Grub4DOS sur le MBR : commande « **bootlace.com /dev/sda** ».

Rebooter, cela doit fonctionner, on a le même menu que avec Grub legacy, ("grldr" scanne toute les partitions à la recherche du menu « menu.lst », il n'y a pas à lui indiquer où il est).

Revenir à Windows, « [initialiser](#) » le disque chiffrant avec Wave Embassy, et c'est terminé.

Cette méthode est compatible avec les mises à jour de Linux, il suffit de ne pas écraser le MBR. S'il venait à l'être quand même par erreur, il suffirait d'un Grub4DOS sur une clé USB ou un CD bootable pour rétablir la situation.

² Merci à Bernard Perrot qui est à l'origine de ce document

Disque chiffrant sous Linux

Il y a peut-être/sans doute d'autres moyens (je n'avais pas le matériel suffisant pour tester d'autres cas de figure), mais cette méthode fonctionne (actuellement) très bien, et ne présente aucune contrainte puisque le fonctionnement est exactement le même que si on utilisait Grub legacy comme il est habituel sous Linux.

Installation d'une machine sous Linux seul

La méthode décrite ici doit être applicable à un Linux seul (et non pas un double boot) du moment qu'on utilise un Windows 7 sur un support bootable externe pour initialiser le chiffrement du disque après installation (les numéros de partitions indiquées ici ne sont plus les mêmes, transposer).

Chiffrement du système avec dm-crypt sous Linux

Les distributions Linux récentes incluent le produit de chiffrement dm-crypt qui est intégré au noyau. Il permet de chiffrer l'ensemble du disque à l'exception de la partition « /boot » utilisée au démarrage. C'est la solution à utiliser pour protéger les machines n'ayant pas de disque chiffrant.

Installation de Linux sur une partition chiffrée

Il suffit lors de la procédure d'installation du système de spécifier que l'on veut activer le chiffrement et de fournir le mot de passe qui servira pour le chiffrement.

Voici un exemple lors d'une installation standard d'une distribution Fedora.

fedora™

Quelle type d'installation souhaitez-vous effectuer ?

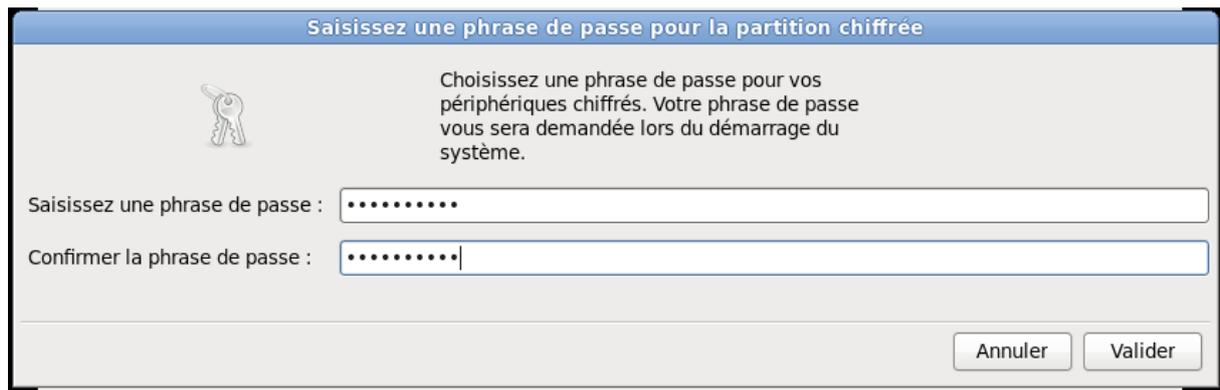
- Utiliser tout l'espace**
Supprimer toutes les partitions sur les périphériques sélectionnés y compris les partitions créées par d'autres systèmes d'exploitation.
Attention : Cette option supprimera les données des périphériques sélectionnés. Assurez-vous de disposer de sauvegardes.
- Remplacer les systèmes Linux existant**
Supprimer toutes les partitions Linux sur les périphériques sélectionnés. Cette option n'affecte pas les autres partitions présentes sur vos périphériques de stockage (comme les partitions VFAT ou FAT32).
Attention : Cette option supprimera les données des périphériques sélectionnés. Assurez-vous de disposer de sauvegardes.
- Réduire la taille du système actuel**
Redimensionner les partitions existantes et libérer de l'espace pour le partitionnement par défaut.
- Utiliser l'espace libre**
Utilise l'espace non partitionné sur les périphériques sélectionnés sans modifier vos données et partitions. Vous devez disposer de suffisamment d'espace disque.
- Créer un partitionnement personnalisé**
Créer à l'aide de l'outil de partitionnement votre schéma de partitions personnalisé sur les périphériques sélectionnés.

Chiffrer le système

Examiner et modifier la structure de partitionnement

Précédent Suivant

Il suffit alors de cocher la case « **Chiffrer le système** ». Il sera alors demandé de saisir la phrase de passe protégeant le disque chiffré.



The screenshot shows a window titled "Saisissez une phrase de passe pour la partition chiffrée". It contains a key icon and the text: "Choisissez une phrase de passe pour vos périphériques chiffrés. Votre phrase de passe vous sera demandée lors du démarrage du système." Below this are two input fields: "Saisissez une phrase de passe :" and "Confirmer la phrase de passe :", both containing masked characters. At the bottom right are "Annuler" and "Valider" buttons.

Il est impératif de procéder au [séquestre](#) du mot de passe.

L'utilisation ne pose pas de problème. Au tout début du démarrage du système, il est demandé de fournir le mot de passe qui sert à déchiffrer le disque.

```
Password for filesystem:*****_
```

Il est difficile de faire plus simple, il n'y a donc aucune raison lorsque l'on ne possède pas de disque chiffrant de se passer de la sécurité offerte par le chiffrement logiciel.

Sauvegarde de l'en-tête

A la différence d'autres outils de chiffrement LUKS ne maintient pas en interne de copie de l'en-tête. Cela signifie que si pour une raison ou une autre, il est corrompu ou illisible (secteur défectueux par exemple), il ne sera pas possible de récupérer les informations. Il est donc vivement conseillé de conserver outre le mot de passe, une sauvegarde de l'en-tête. Cela se fait à l'aide de la commande suivante :

```
Cryptsetup luksHeaderBackup --verbose --header-backup <backup> <device>
```

Où <backup> est le nom du fichier qui contiendra la sauvegarde.

Où <device> est le nom du *device* qui contient la partition chiffrée, par exemple « /dev/sda2 ».

Installation de TrueCrypt sous Linux

Installation de TrueCrypt

La licence de TrueCrypt ne remplissant pas tous les critères de la définition de l'*open source*, ce logiciel n'est pas inclus dans plusieurs grandes distributions Linux comme Debian, Ubuntu, Fedora, OpenSUSE, Gentoo. Il convient donc de l'installer.

Récupérez le paquetage qui correspond à votre architecture (32 ou 64 bits) à partir de <http://www.truecrypt.org/downloads>

Extrayez le fichier contenu dans l'archive (le nom du fichier est à adapter en fonction de la version)

```
tar xvzf truecrypt-7.0a-linux-x64.tar.gz
```

Lancez l'exécution du fichier qui vient d'être extrait :

```
./truecrypt-7.0a-setup-x64
```

TrueCrypt 7.0a Setup

Installation options:

1) Install truecrypt_7.0a_amd64.tar.gz

2) Extract package file truecrypt_7.0a_amd64.tar.gz and place it to /tmp

To select, enter 1 or 2:

Choisissez l'option **1** et acceptez la licence.

La commande effectue un « sudo » pour installer le logiciel avec les droits « root », fournissez votre mot de passe.

Modification du fichier `/etc/sudoers`

TrueCrypt effectue des montages de volumes. Cette opération exige les privilèges de « root ». Pour permettre à un utilisateur de monter un volume TrueCrypt, il faut ajouter au fichier `/etc/sudoers` les lignes suivantes :

```
USER_ALIAS TRUECRYPT = FM  
DEFAULTS:TRUECRYPT !REQUIRETTY  
TRUECRYPT localhost=NOPASSWD: /usr/bin/truecrypt --core-service
```

La première ligne doit être adaptée avec la liste de tous les utilisateurs autorisés à utiliser TrueCrypt. En fonction des distributions et des versions de sudo, la deuxième ligne n'est pas forcément nécessaire. La troisième ligne évite à l'utilisateur d'avoir à fournir son mot de passe mais l'ouverture a été limitée au maximum (uniquement pour certains utilisateurs, uniquement à partir de la machine locale, uniquement pour la commande TrueCrypt demandant le montage).

Installation de TrueCrypt sous Linux

TrueCrypt peut désormais être utilisé pour chiffrer des [conteneurs](#).

FAQ

Que faire si le disque tombe en panne ?

Tout d'abord on ne répètera jamais assez que pour prévenir les conséquences d'une panne du disque, **il est impératif d'effectuer des sauvegardes régulières que le disque soit chiffré ou non.**

Le chiffrement n'empêche pas d'utiliser les méthodes classiques employées pour tenter de récupérer des informations sur un disque en panne ou ayant un système de fichiers corrompu.

En présence d'un disque présentant des signes de détériorations (secteurs illisibles), il est important de tenter de récupérer le maximum d'informations tant que cela est possible. Un outil comme `ddrescue`³ permet d'effectuer une image du disque en mettant en œuvre différentes méthodes pour récupérer, malgré les erreurs de lecture, le maximum de secteurs. Cette utilitaire `ddrescue` est disponible sur différents CD ou clé USB « bootable » comme `SystemRescueCd`⁴.

Une fois déverrouillé un disque chiffrant est accessible exactement comme un disque ordinaire. Pour déverrouiller un disque chiffrant plusieurs stratégies sont possibles :

- Démarrer (boot) sur le disque chiffrant, fournir le mot de passe pour déverrouiller le disque. Redémarrer (reboot) la machine et choisir un périphérique de boot contenant le système (Windows ou Linux) qui accédera normalement aux partitions (elles sont déchiffrées) du disque chiffré. En effet lorsqu'un disque chiffrant a été déverrouillé (en fournissant le mot de passe), un redémarrage (reboot) sans arrêt du disque le laisse en l'état.
- Connecter le disque sur une machine Windows ayant le logiciel Wave ou démarrer à partir d'un disque externe avec un système Windows possédant le logiciel Wave. Ce logiciel permet de déverrouiller le disque ou de supprimer provisoirement la protection par mot de passe.

Un disque système Windows chiffré avec TrueCrypt ou une image obtenue avec `ddrescue` par exemple peut être traité à partir d'un autre système. La commande permettant de monter une telle opération est :

```
truecrypt -mount-options=system <disque> <point de montage>
```

Une difficulté est liée au fait que le mot de passe doit être saisi avec un clavier US, en effet au moment du preboot la configuration FR n'a pas encore été activée. Les commandes `loadkeys` pour un environnement texte et `setxkbmap` pour un environnement graphique, permettent le basculement du clavier entre les deux langues. Avant de lancer `truecrypt`, il est possible d'exécuter `loadkeys us` ou `setxkbmap us` pour faciliter la saisie du mot de passe. `loadkeys fr` ou `setxkbmap fr` permettront de rétablir le clavier après la commande `truecrypt`.

Il est aussi possible d'utiliser le CD créé lors du chiffrement initial du disque système pour déchiffrer le disque.

³ http://www.gnu.org/software/ddrescue/ddrescue_fr.html

⁴ http://www.sysresccd.org/Page_Principale

Quid des clés USB avec empreinte digitale ?

Il existe des clés USB chiffrées dont le déverrouillage se fait non par la saisie d'un code PIN mais en passant son doigt sur un lecteur d'empreinte. Indépendamment de toutes questions d'ergonomie et de sécurité, il faut bien voir que la biométrie est un sujet extrêmement sensible. La CNIL est très pointilleuse et l'utilisation de la biométrie exige une autorisation préalable. On pourrait considérer que les risques pour la vie privée avec une empreinte uniquement stockée sur la clé sont minimes et qu'une autorisation pourrait être assez facilement obtenue. Mais aucune démarche en ce sens n'a été effectuée et de telles clés n'ont pas été évaluées.

Pourquoi la mise en veille est-elle désactivée ?

Il existe deux modes de mise en veille, la mise en veille simple et la mise en veille prolongée (hibernation). Le premier maintient l'alimentation de la mémoire pour faciliter un redémarrage rapide. Le second recopie le contenu de la mémoire sur disque avant d'arrêter complètement la machine. Ce dernier s'il a l'avantage de ne rien consommer a l'inconvénient d'être plus long à redémarrer.

Pour des raisons techniques, il y peut y avoir incompatibilité entre le chiffrement et la mise en veille simple. En outre des considérations de sécurité conduisent à interdire cette mise en veille simple. Le chiffrement du disque offre une protection uniquement lorsque la machine est éteinte. La mémoire vive pouvant contenir des données extrêmement sensibles y compris des clés de chiffrement, il est important lorsque l'on cesse de travailler sur une machine de vider sa mémoire en l'éteignant⁵. Afin d'éviter ce risque les produits de chiffrement du disque volontairement désactivent la veille simple pour ne permettre que la veille prolongée.

Quelle est la différence entre la protection offerte par un disque chiffrant et un disque verrouillé par un mot de passe au BIOS ?

Les spécifications du protocole ATA prévoient la possibilité de verrouiller le disque. Le déverrouillage se fait en saisissant un mot de passe au démarrage de la machine (BIOS). Ce n'est qu'un verrouillage logique au niveau du contrôleur du disque, les données restent en clair sur les plateaux. La sécurité offerte est toute relative puisqu'il existe des techniques permettant de passer outre cette protection en employant des moyens qui ne sont pas démesurés. Certaines sociétés offrent ce service. Par contre avec un disque chiffrant, les données sur les plateaux sont chiffrées et il est impossible de les récupérer sans connaissance du mot de passe (sauf peut-être pour certaines agences gouvernementales).

Qu'apportent les nouvelles instructions AES ?

Ces instructions (http://en.wikipedia.org/wiki/AES_instruction_set) disponibles sur les nouveaux processeurs accélèrent grandement l'exécution de l'algorithme de chiffrement AES. Quelques mesures effectuées avec TrueCrypt 7.0a sur un Dell Latitude 4310 donnent un débit de chiffrement d'environ 800 Moctets/s. Comparé au débit des disques, le chiffrement ne peut plus être considéré comme dégradant significativement les performances. Cependant les nouvelles machines devant être commandées avec un disque chiffrant, le chiffrement logiciel du disque n'est plus nécessaire.

⁵ Il faut attendre plusieurs secondes avant que cela ne soit effectif, cf. « cold boot attack ».

Comment savoir si la machine possède un disque chiffrant ?

Pour une machine Dell allez sur le site Dell et choisissez « Support », entrez le numéro de série puis sélectionner l'onglet « Configuration système ». Si le disque est chiffré c'est indiqué dans la configuration. (« DISQUES DURS : DISQUE DUR CHIFFRE 250GO »).

Que faire si le mot de passe a été compromis ?

Pour les solutions logicielles de chiffrement, en cas de compromission avérée ou simplement suspectée du mot de passe, il faut considérer que la clé symétrique qui sert au chiffrement du disque n'est plus secrète. Le mot de passe ne sert qu'à protéger cette clé symétrique. Celui qui a eu connaissance à un moment donnée du mot de passe a pu récupérer la clé symétrique de chiffrement et sera en mesure de déchiffrer les informations même si le mot de passe a été changé entre temps. En effet un changement de mot de passe ne modifie pas la clé symétrique de chiffrement du disque.

Il est donc impératif de procéder à un déchiffrement complet du disque suivi d'un nouveau chiffrement qui va utiliser une nouvelle clé symétrique, ce qui en fonction de la capacité du disque peut être une opération particulièrement longue.

Pour les disques chiffrants, la clé ne peut sortir du disque et il un changement de mot de passe suffit. C'est l'un des atouts des solutions matérielles de chiffrement.