Encryption for the masses E4M

Olivier Hoarau (olivier.hoarau@fnac.net)

V1.0 du 20.8.00

1 Préambule

Ce document présente E4M (Encryption for the masses) qui permet de crypter des répertoire, des partitions, des lecteurs logiques sous Windows 9X.
La dernière version de ce document est téléchargeable à l'URL http://funix.free.fr. Ce document peut être reproduit et distribué librement dès lors qu'il n'est pas modifié et qu'il soit toujours fait mention de son origine et de son auteur, si vous avez l'intention de le modifier ou d'y apporter des rajouts, contactez l'auteur pour en faire profiter tout le monde.
Ce document ne peut pas être utilisé dans un but commercial sans le consentement de son auteur. Ce document vous est fourni "dans l'état" sans aucune garantie de toute sorte, l'auteur ne saurait être tenu responsable des quelconques misères qui pourraient vous arriver lors des manipulations décrites dans ce document.

2 Présentation

Le problème avec windows 9X est qu'il n'est pas possible de protéger des documents voire des répertoires, si le poste est multi-utilisateurs rien n'empêche un utilisateur d'aller voir les fichiers d'un autre. De même vous ne pouvez faire confiance à la protection par mot de passe d'outils comme Office, ces protections sont facilement "cassables" ou peuvent être contournées. **E4M** est un outil qui permet de crypter des répertoires complets en utilisant des algorithmes de cryptage performant, en plus il est conforme à la loi française sur la cryptologie à savoir qu'il utilise une clé de cryptage de 128bits.

En cryptant un répertoire **E4M** va créer un fichier appelé volume, les volumes apparaissent comme de simples fichiers mais en fait ce sont des systèmes de fichiers complets, dans la terminologie **E4M** on appelle ça un "file hosted volume". Vous pouvez aussi crypter des partitions entières qu'on appellera des "raw partition volumes".

Pour le récupérer, il suffit de se connecter sur le site de **E4M** www.e4m.net, vous y trouverez la version 2.0.1 de **E4M**.

3 Installation

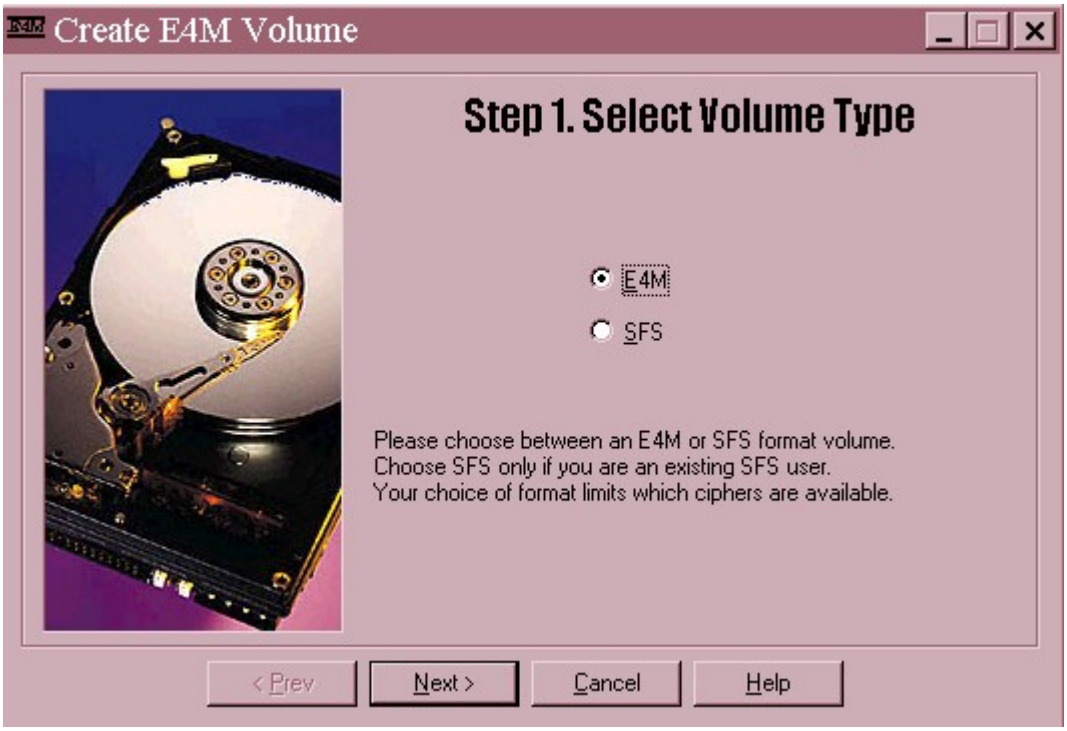
L'archive est un exécutable qu'il faut exécuter. La première fenêtre vous demande si vous voulez installer E4M ou non. La deuxième fenêtre propose un chemin par défaut pour l'installation, par défaut **c:\program files\E4M**. Vous pouvez aussi associé les fichiers volumes **.vol** à **E4M** (par défaut), rajouter **E4M** dans le menu **Démarrer** (par défaut) et prévoir le support de désinstallation (par défaut). En cliquant sur **Install** on accepte la licence. A la fin de l'installation n'oubliez pas de rebooter le PC même si ce n'est pas indiqué.

4 Création d'un volume

Pour créer un volume, dans le menu **Démarrer**

Programmes->E4M->Create Volume

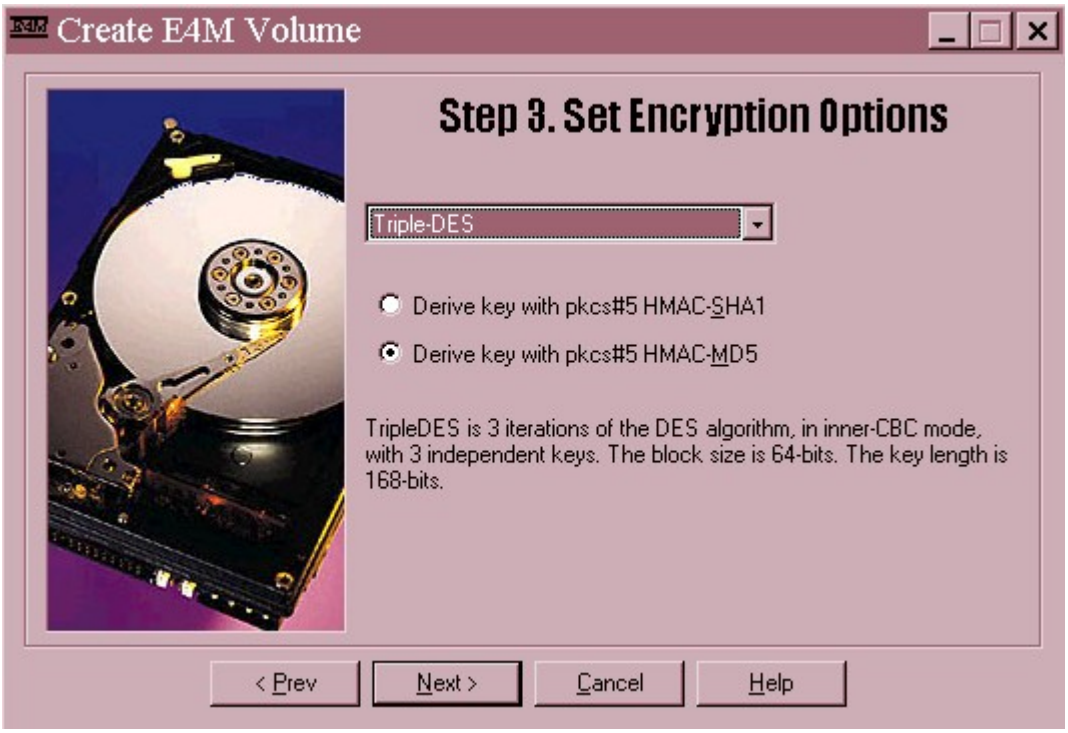
La fenêtre suivante apparaît:



Vous avez deux types de format disponible. Le format SFS est à utiliser pour des volumes sous DOS ou windows 3.1, il nécessite un driver particulier pour Windows 9.X. Choisissez plutôt E4M.

Vous devez ensuite choisir l'endroit où va se trouver votre fichier volume, donner lui également un nom.

Dans cette même fenêtre vous pouvez choisir une partition complète à crypter avec **Raw Devices**.

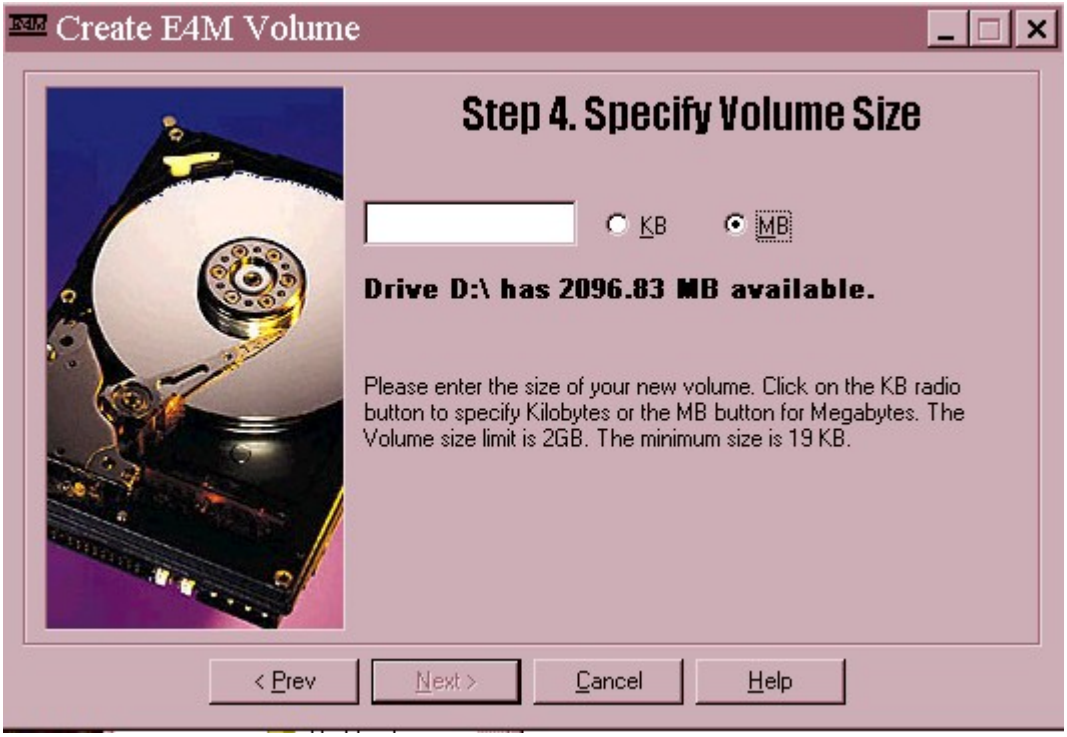


Vous pouvez choisir dans les algorithmes de cryptage suivant:

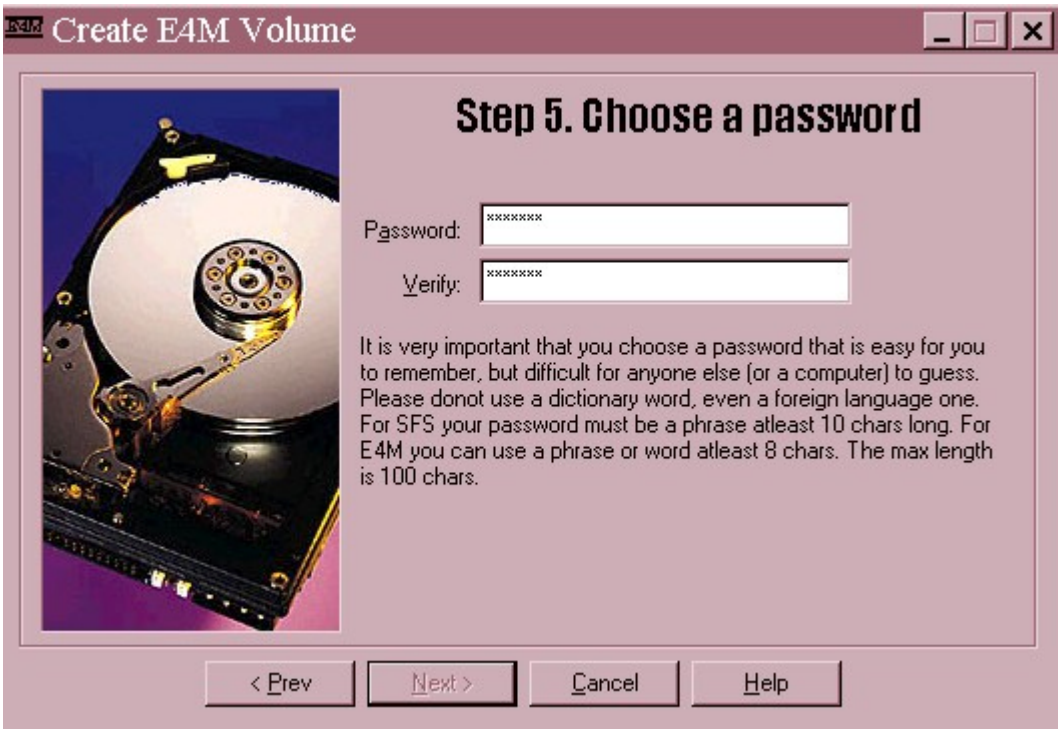
- Triple DES avec une clé de 168bits (supérieure au 128bits réglementaire en France)
- IDEA avec une clé de 128bits
- DES avec une clé de 56 bits
- blowfish avec une clé de 256 bits
- CAST avec une clé de 128 bits

Personnellement j'ai choisi IDEA car c'est un algorithme rapide et avec une longueur de clé qui va bien. Appuyez alors sur **Next**.

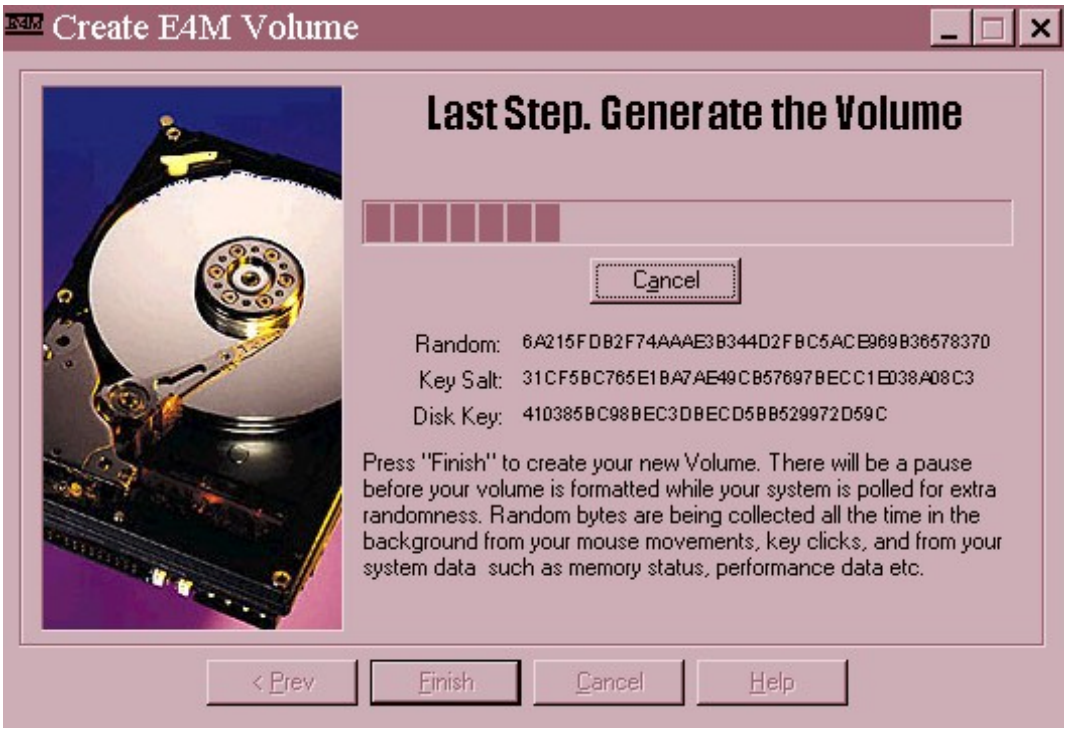
La troisième étape est la fixation de la taille du volume crypté.



Vous pouvez fixer une taille de volume entre 19ko et 2Go, à vous de fixer la taille suivant vos besoins. A présent il faut fixer le mot de passe pour accéder au volume.



Notez bien que ce password doit avoir une longueur minimum de 8 caractères pour les volumes E4M et de 10 pour les volumes SFS (100 caractères maximum). Il génère ensuite le volume.



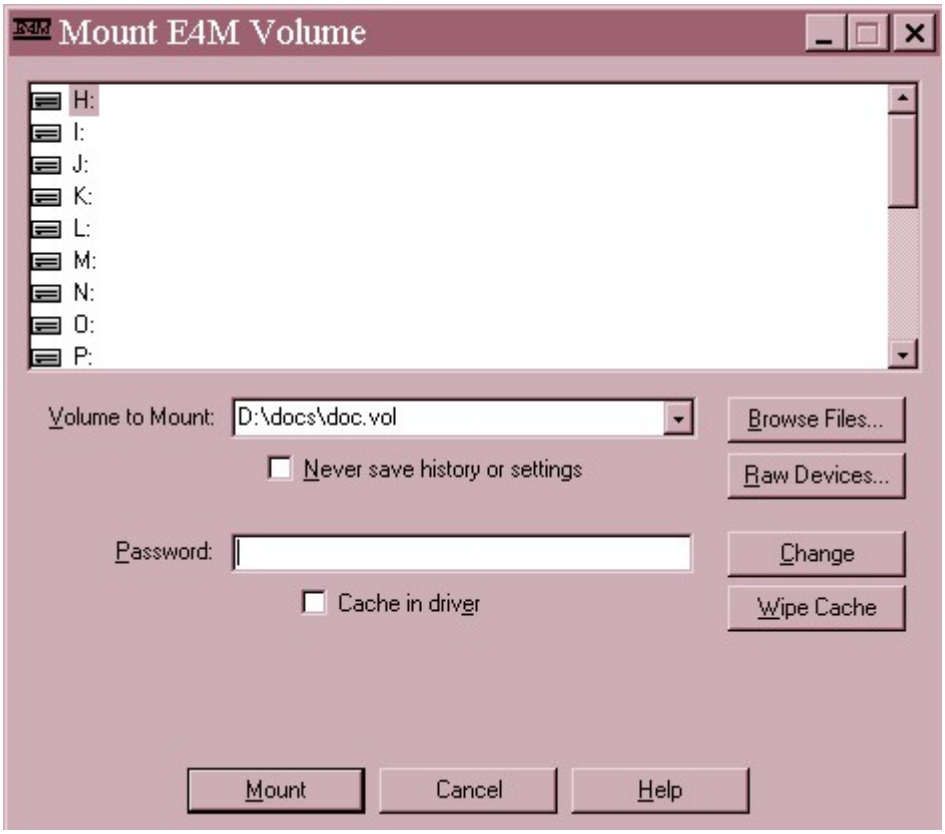
Appuyer sur **Finish**, ça peut prendre un certain temps suivant la puissance du PC. Pendant la génération vous devez faire un certain nombre d'actions (clique de souris, clavier, ouverture de fenêtre, ...), il sera d'autant plus difficile de casser votre code que vous aurez fait ces actions en grand nombre. A la fin de la génération une fenêtre apparaît donnant des statistiques sur le volume nouvellement créé.

5 Monter un volume

Pour pouvoir accéder à un volume crypté il faut pouvoir le monter pour qu'il apparaissent comme un lecteur logique (comme c:). Pour cela dans le menu **Démarrer**:

Programmes->E4M->Mount Volume

La fenêtre suivante apparaît:



Dans la partie du haut vous devez sélectionner le nom du lecteur logique qui sera utilisé pour monter votre volume (ici H:), dans **Volume to mount** vous devez saisir le volume à monter, dans **Password** le mot de passe associé. Appuyez ensuite sur **Mount**.
A ce moment là votre volume est vu dans le gestionnaire de fichier comme un lecteur logique classique, vous pouvez y mettre les fichiers que vous voulez dans la limite de la taille du volume.

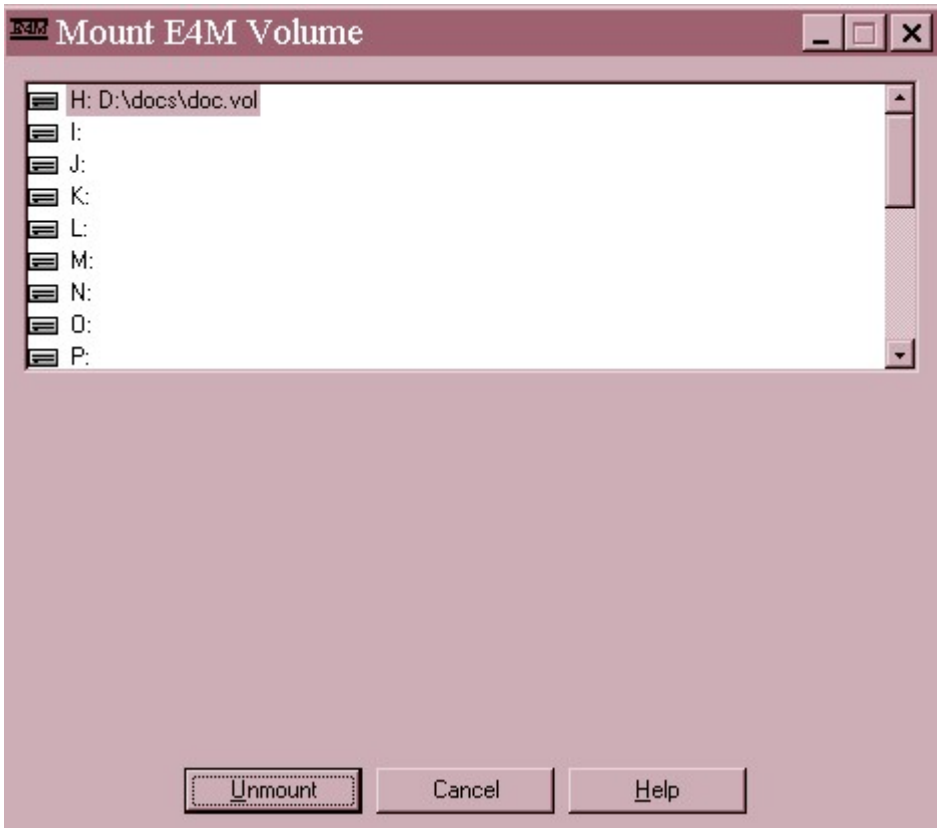
Noter que dans cette fenêtre vous avez la possibilité de changer le mot de passe du volume en cliquant sur **Change**.

6 Démonter un volume

Quand vous avez fini de transférer vos fichiers dans le volume crypté, vous pouvez le démonter et donc le crypter, pour cela dans le menu **Démarrer**:

Programmes->E4M->Unmount Volume

La fenêtre suivante apparaît.



Sélectionner le volume, puis appuyez sur **Unmount**.