Chiffrement des portables

Journée Mathrice à Rennes

2 octobre 2013

Mohammed Khabzaoui

CNRS UMR8524

Université Lille1

Plan

- *Chiffrement des portables*
- *Outil de chiffrement matériel*
    - *Disque auto-chiffrant*
- *Outils de chiffrement logiciel*
    - *FileVault pour MAC*
    - *dm-crypt pour linux*
    - *BitLocker et Truecrypt pour windows*
- *Conclusion*

Chiffrement des portables

- **Motivations**
  - Nombreux vols de portables
  - Données à forte valeur économique (dépôt d'un brevet)
- **Dispositif**
  - Disque chiffrant sur portable du marché mathinfo
  - Chiffrement logiciel (BitLocker / TrueCrypt / dm-crypt / FileVault)
- **Chiffrement des disques obligatoire dans unités CNRS** : Directives et Recommandations : https://aresu.dsi.cnrs.fr/?rubrique99
- **Chiffrement des portables :** Mise en œuvre et utilisation https://aresu.dsi.cnrs.fr/IMG/pdf/manuel.pdf

Techniques

	Matériel	Win7	Win8	Linux	Mac OS
Portable DELL Portable HP	Oui Oui *	TrueCrypt	BitLocker (> windows7Pro)	dm-crypt	
PC fixe	NON			dm-crypt	
MAC	NON				FileVault

Support amovible : auto-chiffrant & TrueCrypt (compatible avec tous les OS)

Outil de chiffrement matériel

Un disque dur chiffrant (Self-Encrypting Drive) est une solution matérielle de chiffrement intégral du disque.

L'authentification est nécessaire au démarrage pour déverrouiller l'accès au disque, qui est inutilisable autrement. Pour l'activer il faut utiliser un software windows "Dell Data Protection Access" incompatible avec Windows 8 et Linux

Pour les postes Linux, il faut un windows 7 installé sur une disque USB avec un port eSATA.

Portable DELL : suivre la documentation disponible sur le site de l'Aresu, à l'adresse :

https://aresu.dsi.cnrs.fr/IMG/pdf/procedure-disque-chiffrant-win7-v1.pdf

Sur le site DELL :

http://dell.wave.com/dell-complete-hardware-self-encrypting-drivesed-solution

Portable HP : ?

Outil de chiffrement matériel

Remarque :

Le verrouillage du disque n'est effectif que pour un cycle d'extinction complet, un simple reboot n'est pas suffisant.

Recouvrement

Déclarer un compte utilisateur ADMIN, ce dernier peut donc y être consacré. Le déverrouillage du disque passe par une étape d'authentification au démarrage.

Mac OS
FileVault 2

- Pré-requis : Mac OS X 10.7 (Lion) ou 10.8 (Mountain Lion)
- Transparent à l'utilisateur : l'ouverture d'une session déverrouille l'accès et permet le déchiffrement du disque.

- Références :

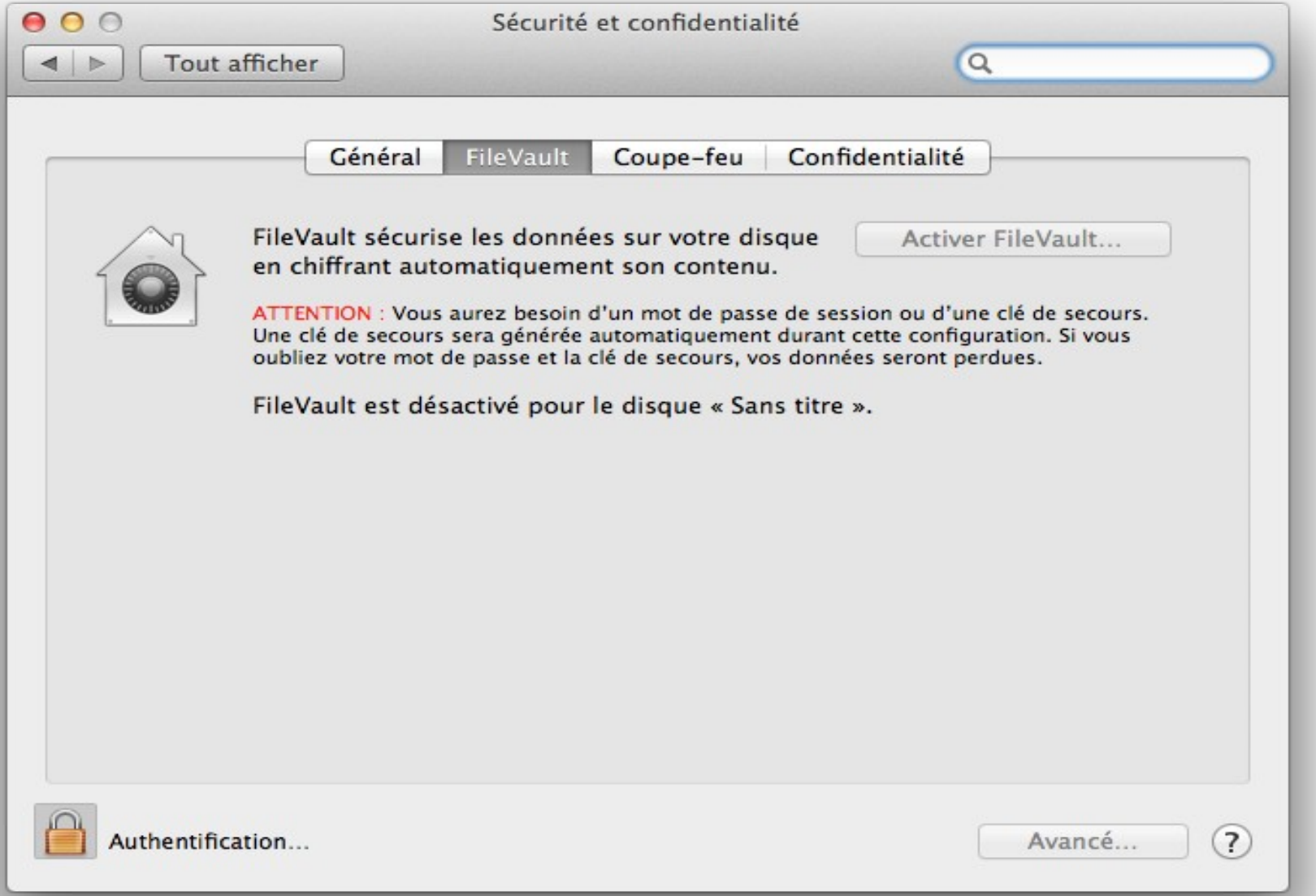
https://aresu.dsi.cnrs.fr/IMG/pdf/CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1-0.pdf

http://support.apple.com/kb/HT4790?viewlocale=fr_FR

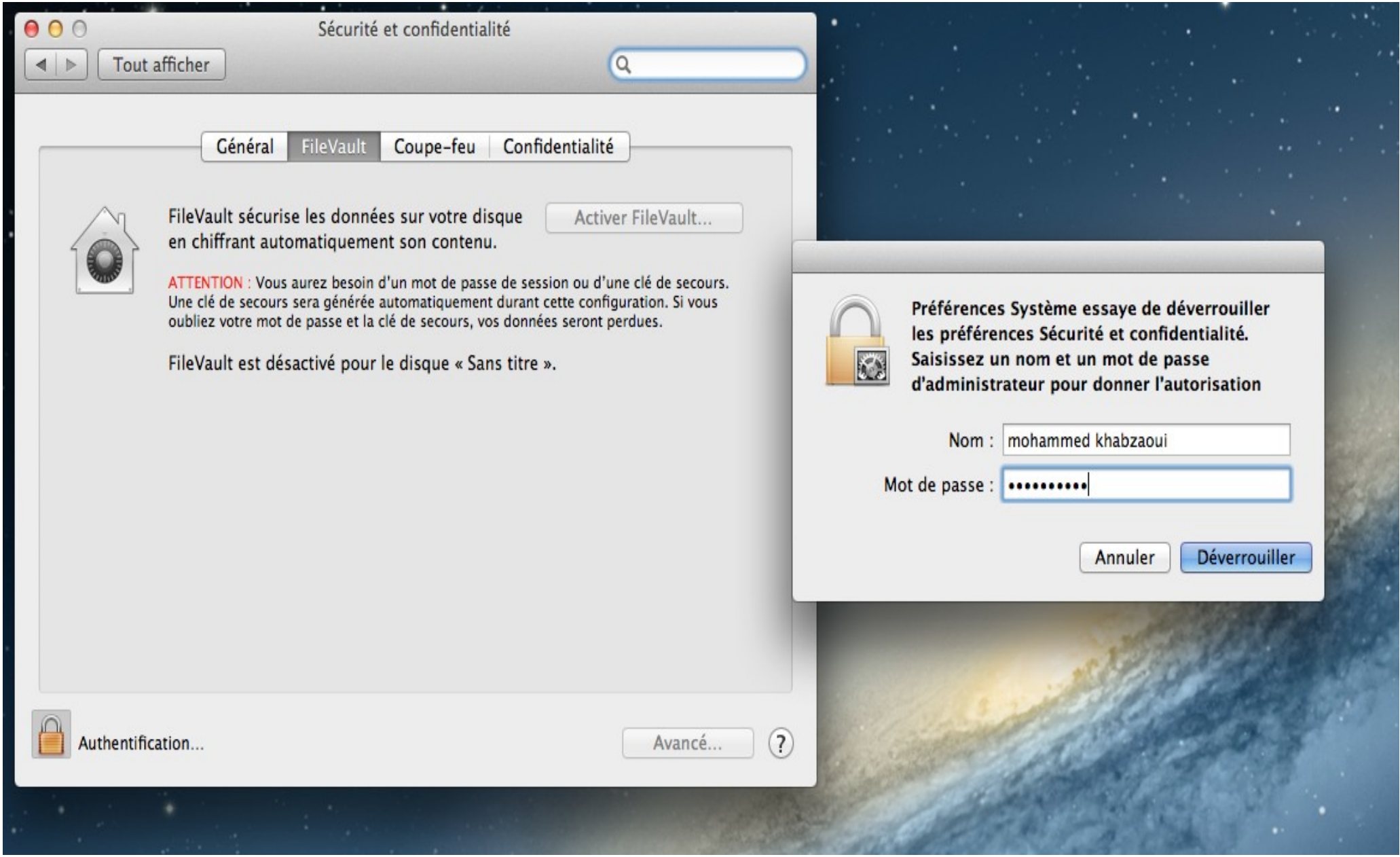
https://aresu.dsi.cnrs.fr/IMG/pdf/manuel.pdf

Ouvrir les préférences système
et cliquer dans « Sécurité et confidentialité »

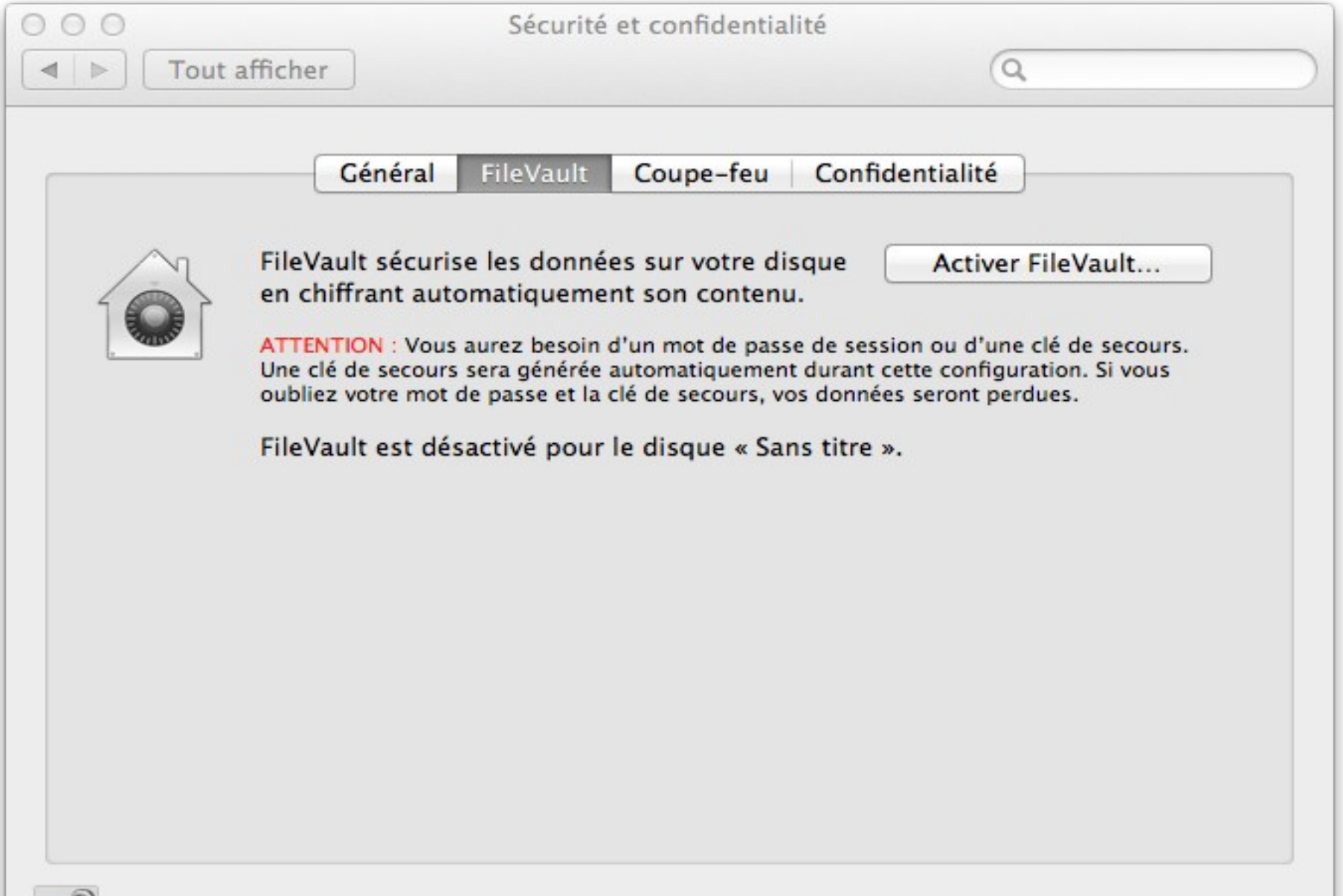
Cliquer dans « FileVault » :



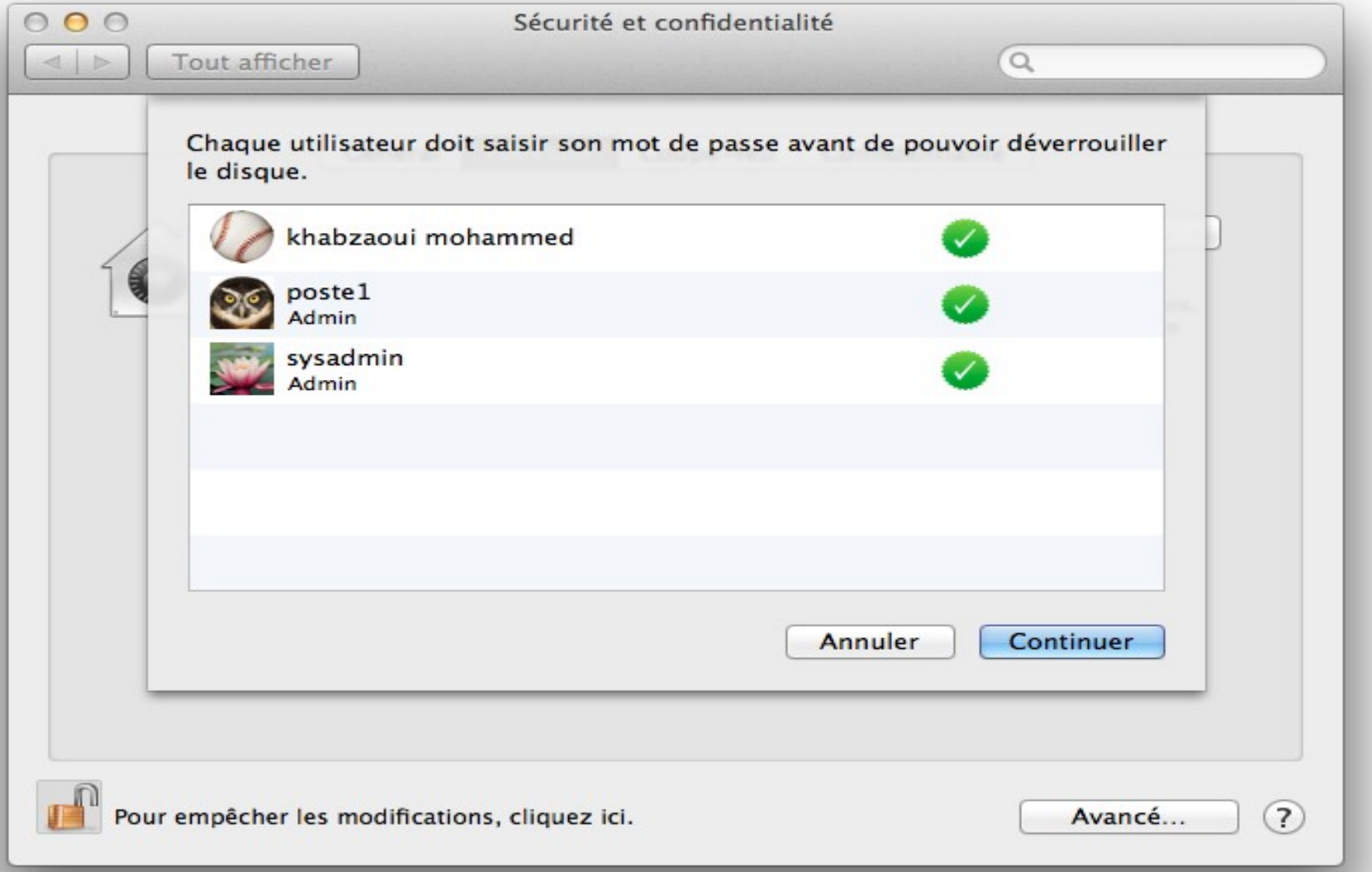
Cliquez dans le cadenas pour pouvoir activer FileVault :



Cliquez dans « Activer FileVault »



Autoriser les utilisateurs



Saisir le mot de passe de chaque utilisateur autorisé

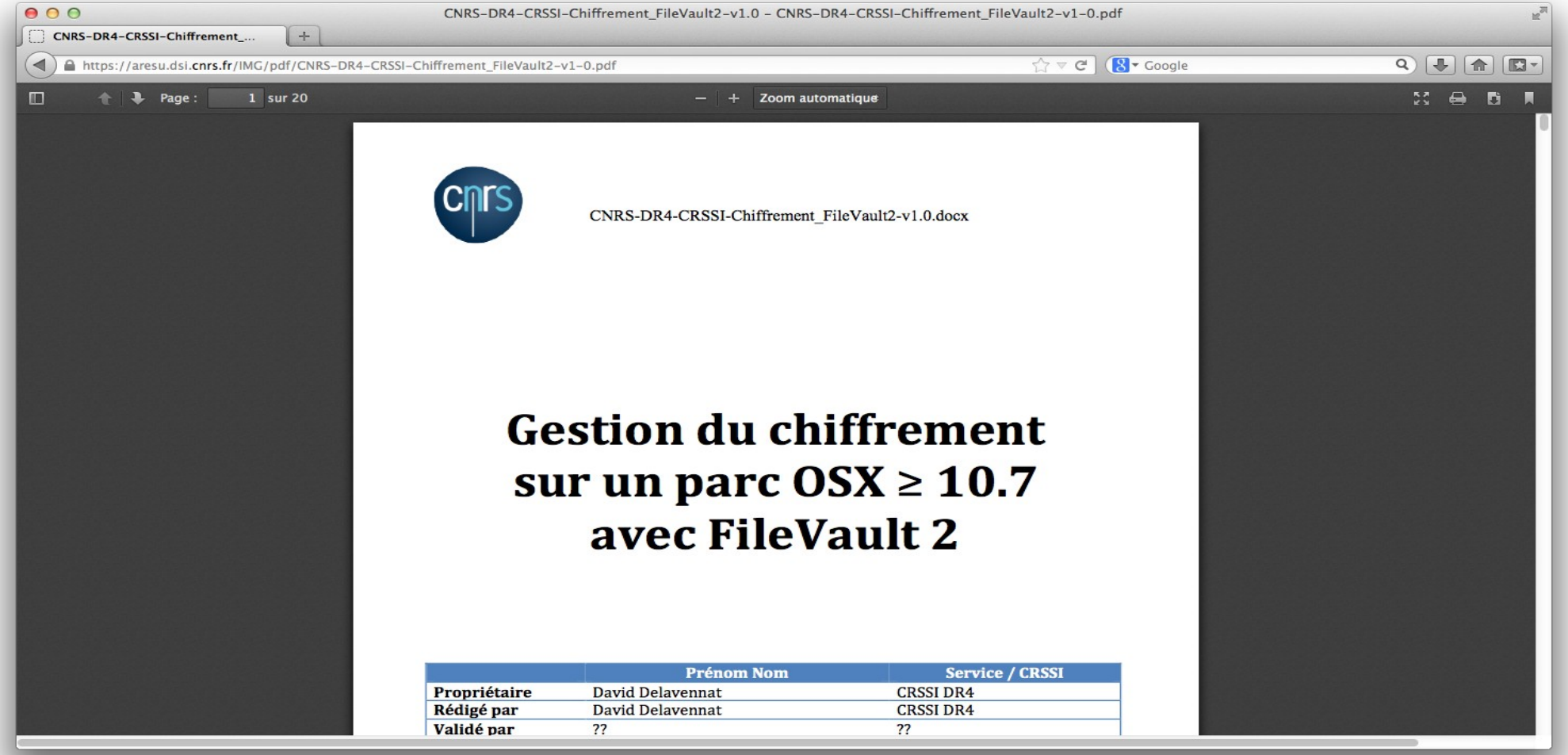

Sécurité et confidentialité
Tout afficher
La clé de secours est un « filet de sécurité » qui peut servir à déverrouiller le disque si vous avez oublié votre mot de passe.
Effectuez une copie et stockez-la en lieu sûr. Si vous oubliez votre mot de passe et perdez la clé de secours, toutes les données de votre disque seront perdues.
O5H5-C27L-KVKP-PYKY-LZWM-JTAV
Annuler
Retour
Continuer
Pour empêcher les modifications, cliquez ici.
Avancé...

Ne jamais stocker la clé de secours dans un tiers


Sécurité et confidentialité
Tout afficher
Cliquez sur le bouton Redémarrer pour redémarrer votre Mac et lancer le processus de chiffrement.
Après avoir redémarré, vous pourrez vous servir de votre Mac pendant le processus de chiffrement. Vous pourrez en vérifier la progression dans les préférences Sécurité et confidentialité.
Annuler
Redémarrer
FileVault est désactivé pour le disque « Sans titre ».
Pour empêcher les modifications, cliquez ici.
Avancé...
?

Gestion du chiffrement sur un parc de MAC

https://aresu.dsi.cnrs.fr/IMG/pdf/CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1-0.pdf



Recouvrement

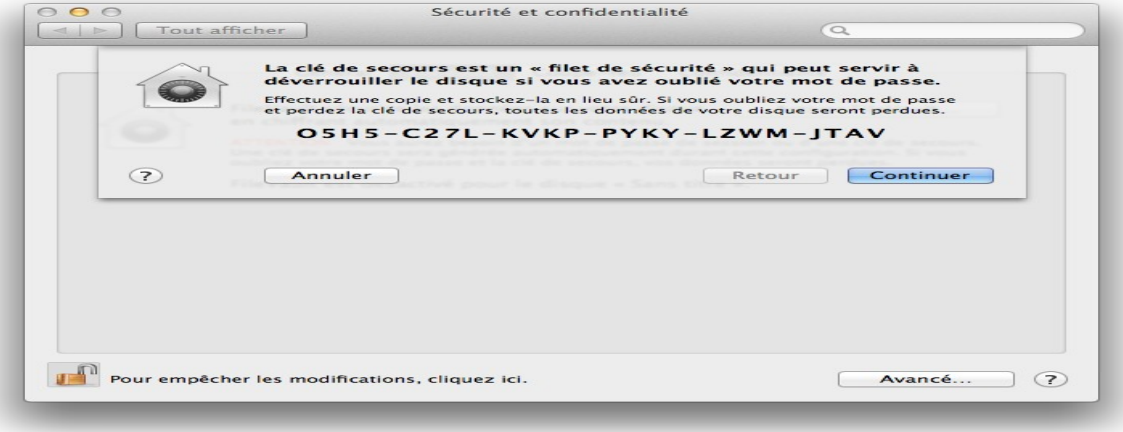
1. Avec un compte admin

   Démarrer la machine avec le compte d'admin

   Changer le mot de passe de l'utilisateur

2. Avec la clé de recouvrement de la machine générée lors de l'activation de FileVault

   au boot, après 3 tentatives de mot de passe infructueuse, cliquer sur le triangle jaune, le prompt de la clé apparaît .



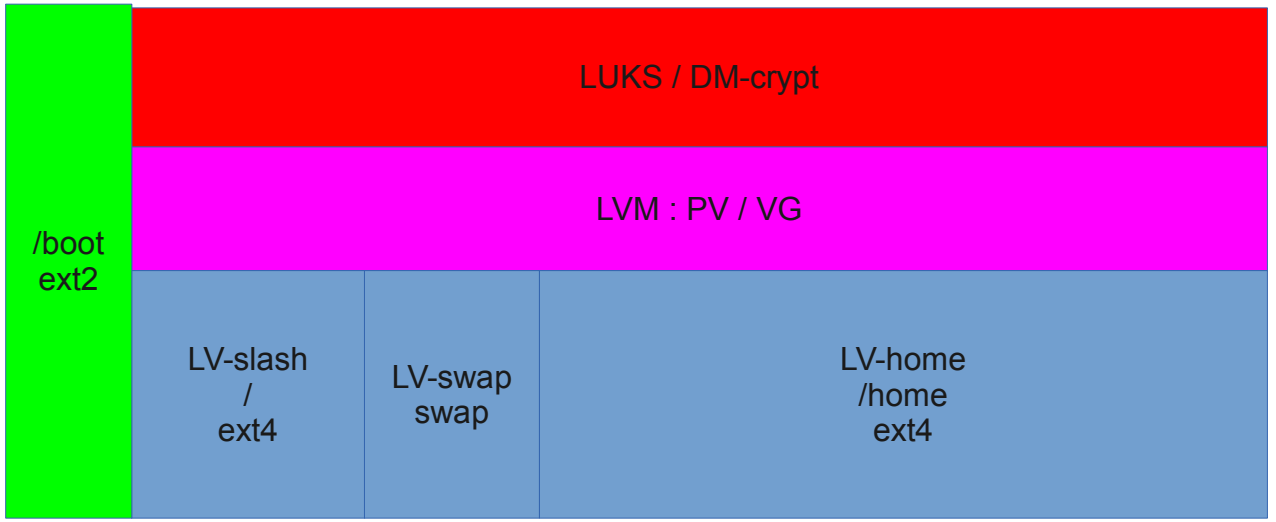
3. Avec un certificat de recouvrement d'établissement commun à tous les disques chiffrés.

Voir la références https://aresu.dsi.cnrs.fr/IMG/pdf/CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1-0.pdf

Dm-Crypt / LUKS

Dm-crypt : C'est le chiffrement de devices virtuels en mode bloc

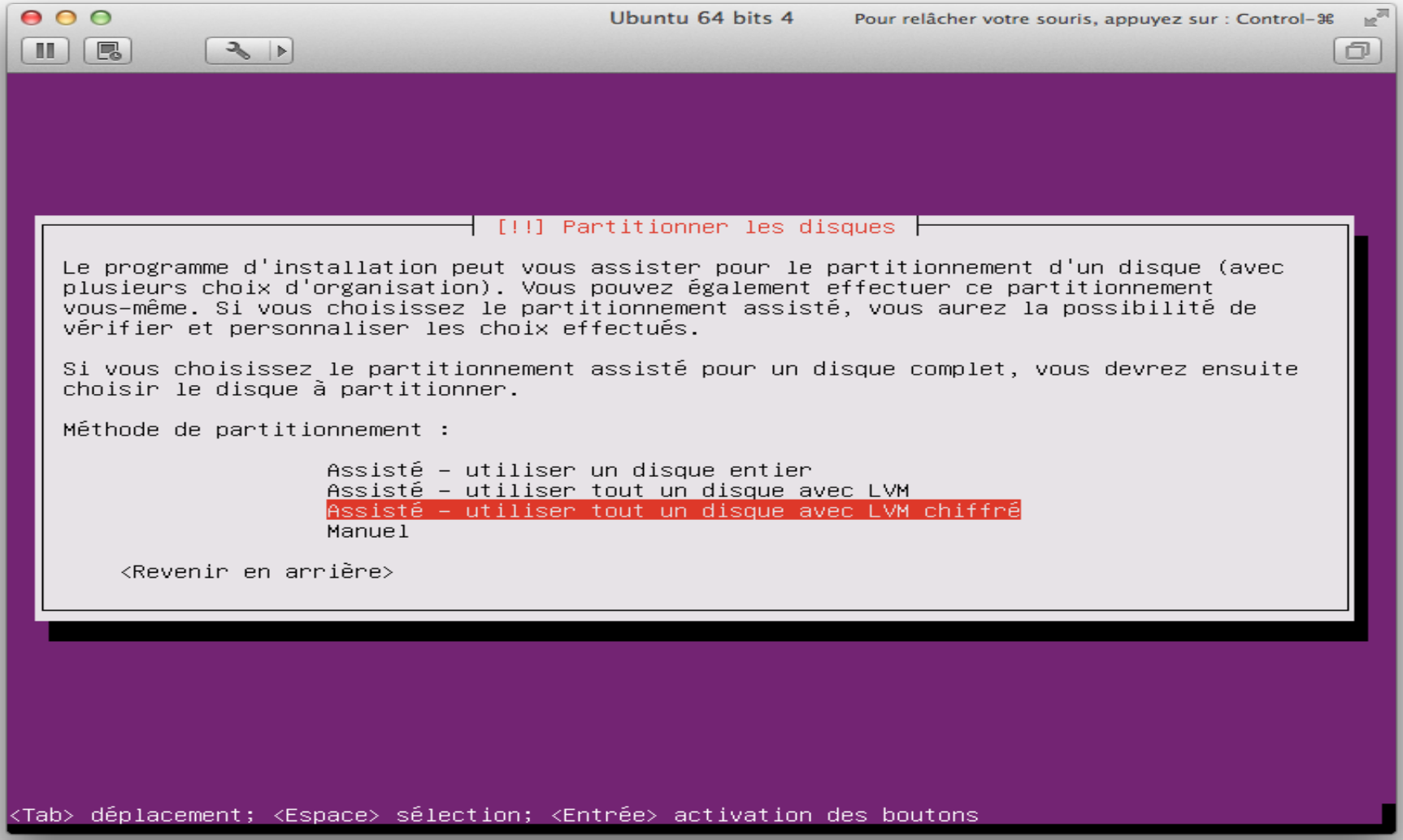
LUKS : Linux Unified Key Setup : standard de gestion du chiffrement



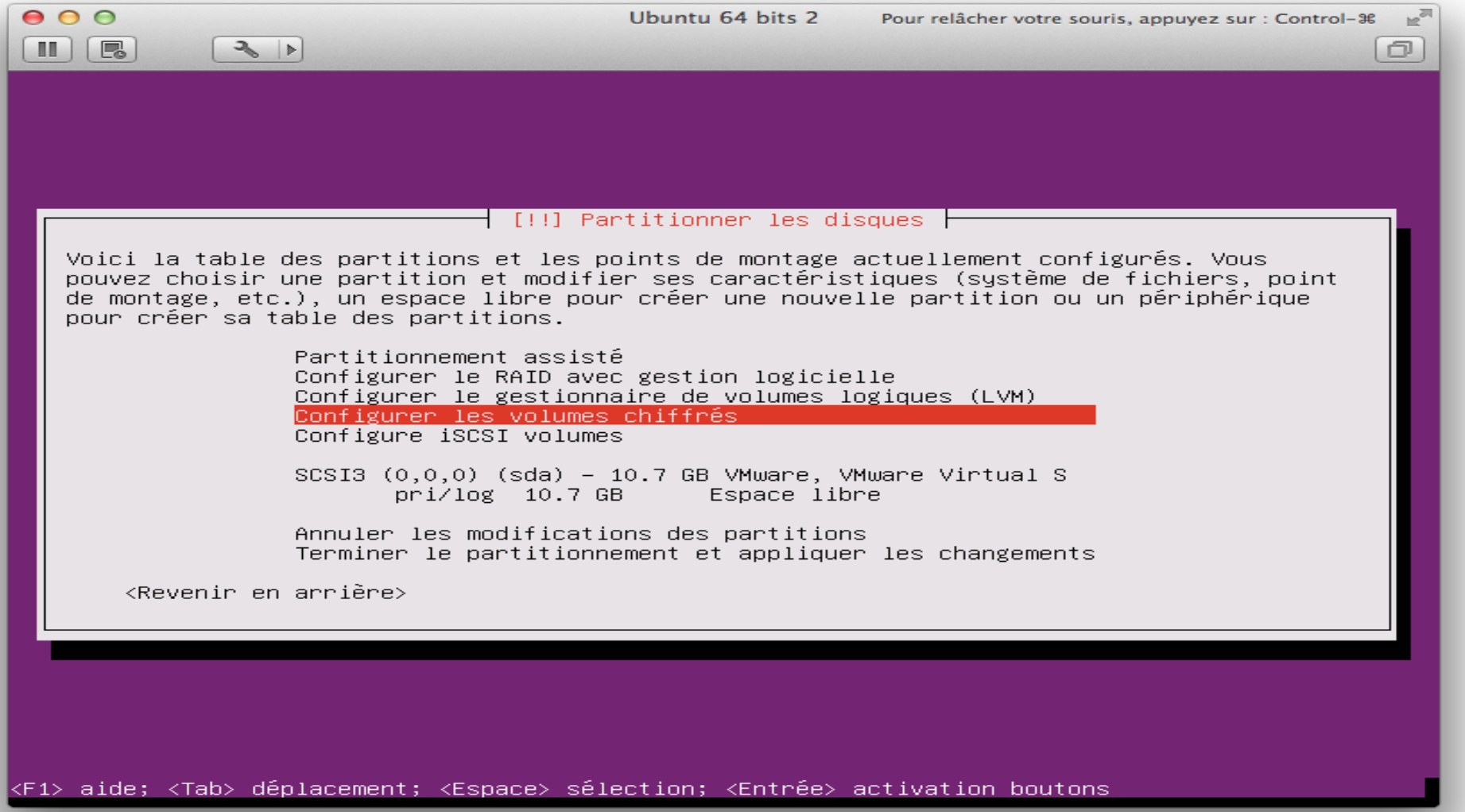
dm-crypt
(debian, ubuntu ...)

- Pendant l'installation de OS
  - Choisir l’installation sur un disque avec volume LVM chiffré
  - Spécifier une passphrase
  - Sauvegarder une copie de l’entête du volume après le 1er reboot
  - Définir une passphrase additionnelle
- L'OS est déjà installé
  - Sauvegarder les données
  - Préparer des partitions chiffrées
  - Restaurer les données

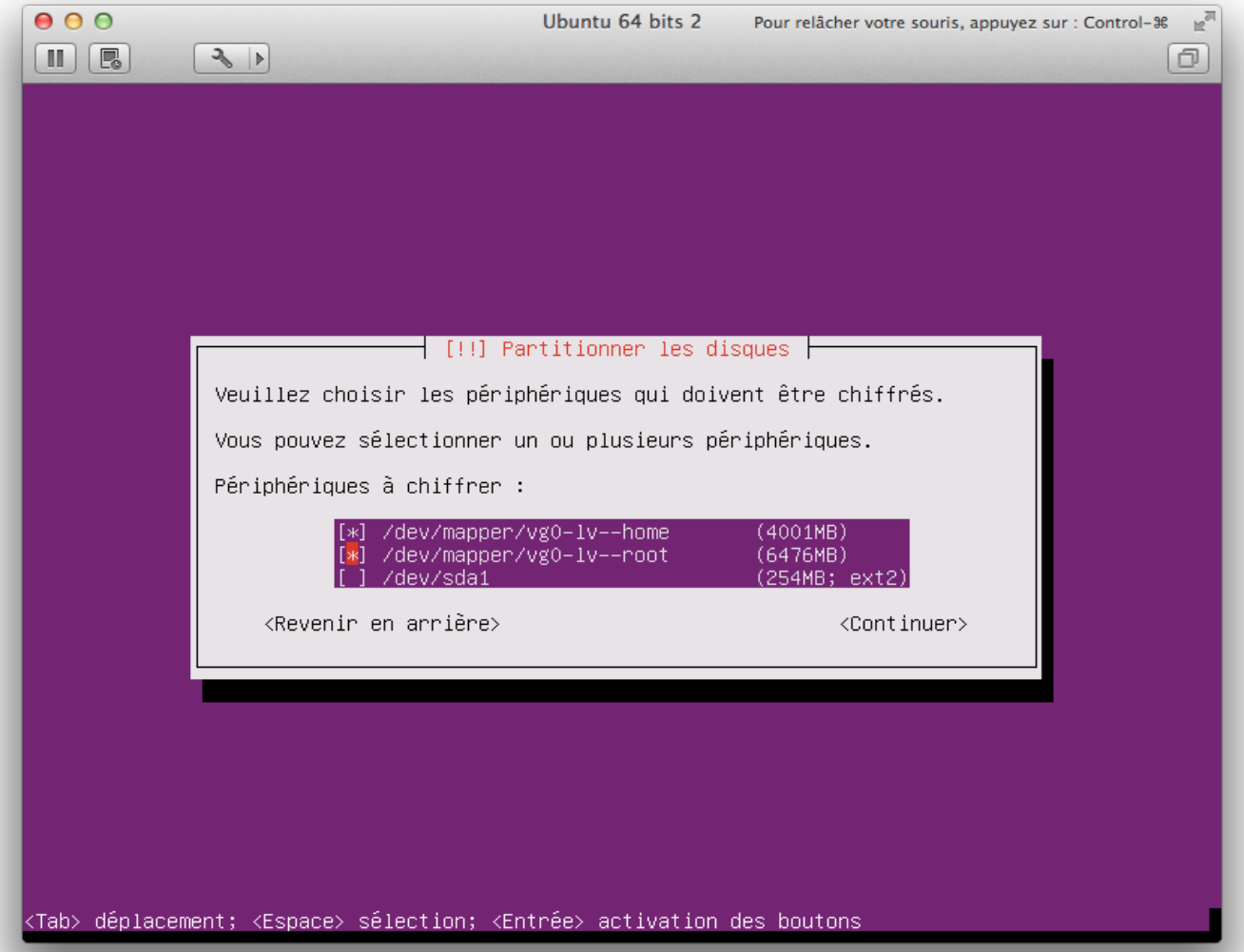
Choisir un disque avec LVM chiffré



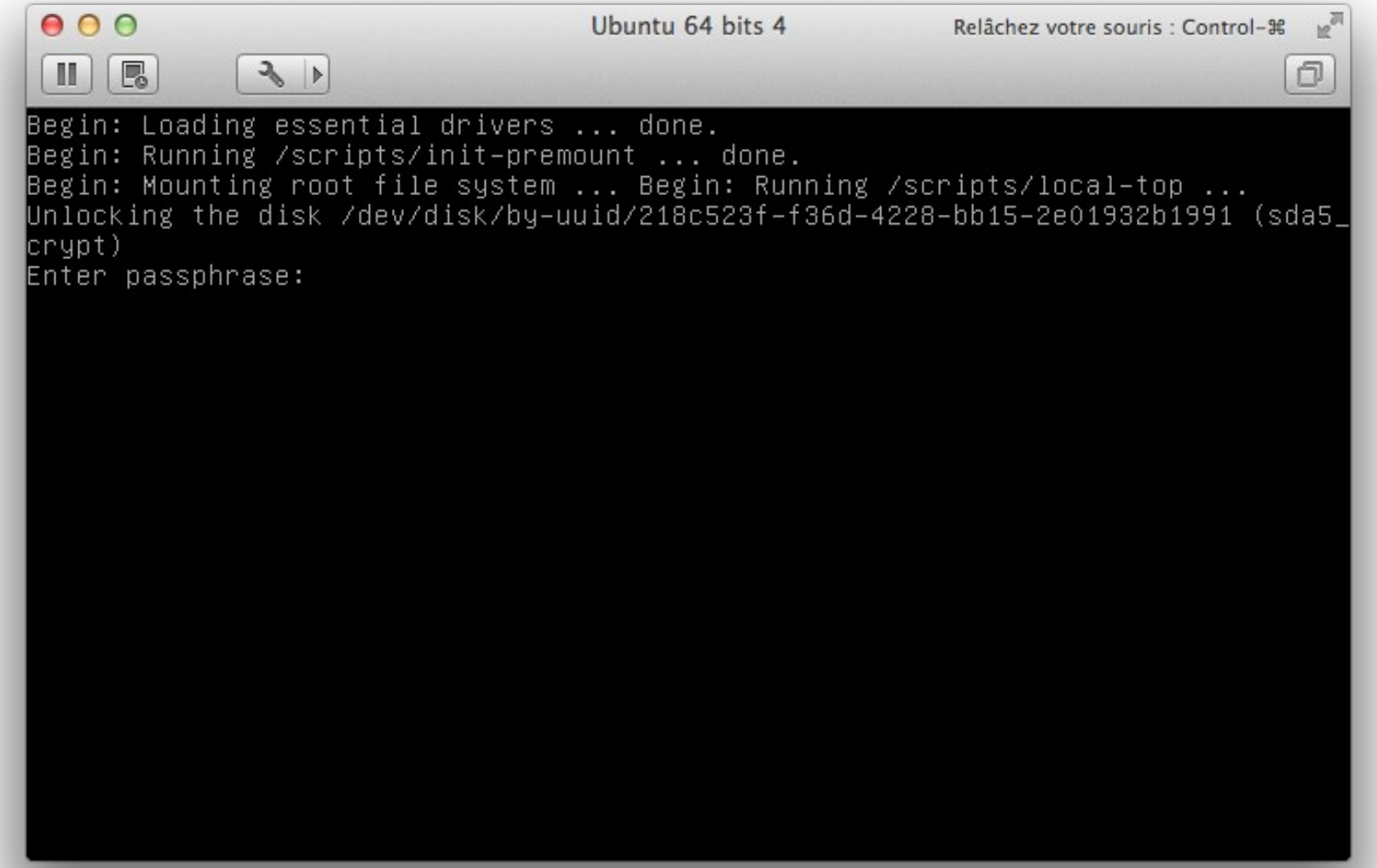
Configurer les volumes



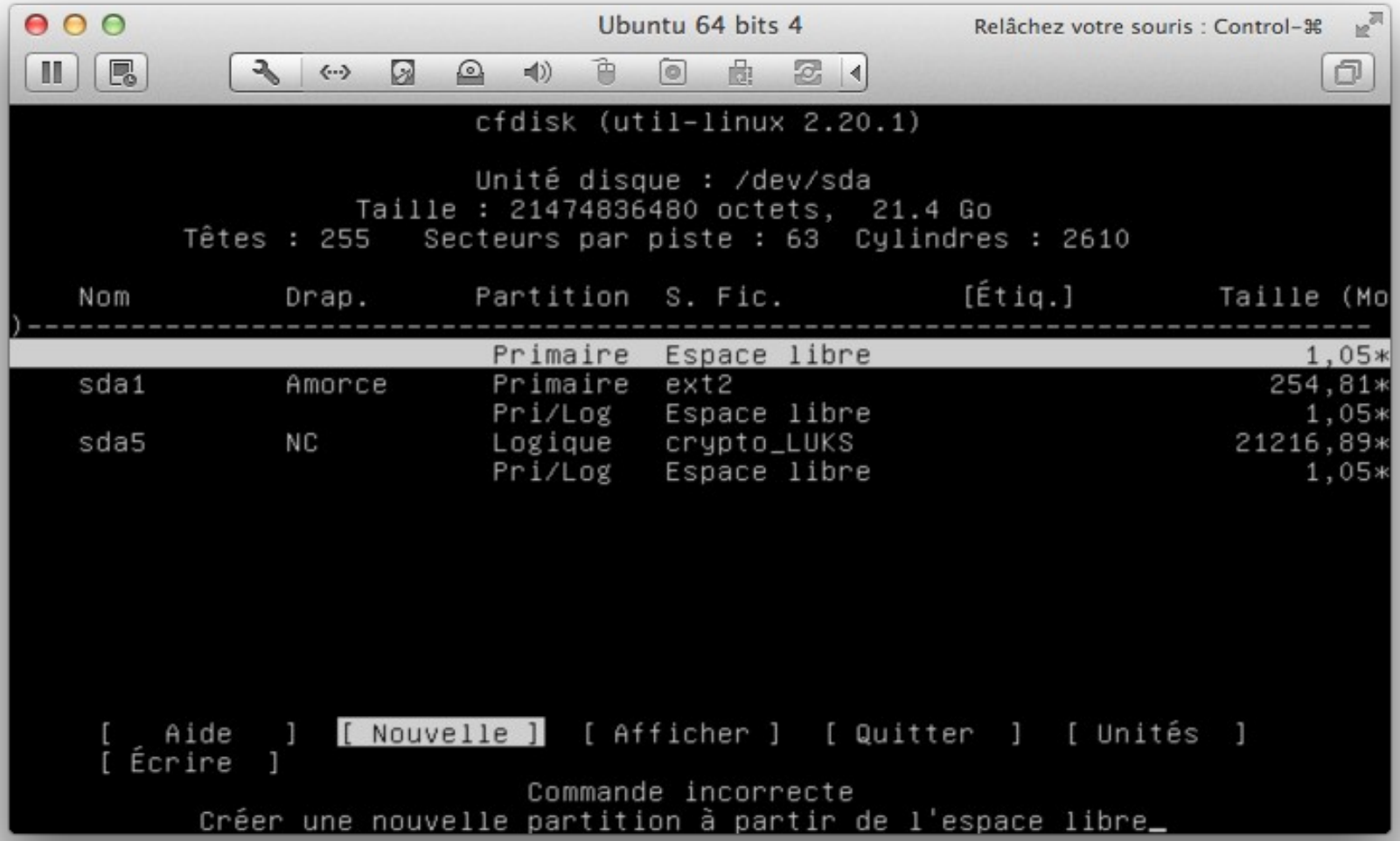
Configurer les volumes chiffrés



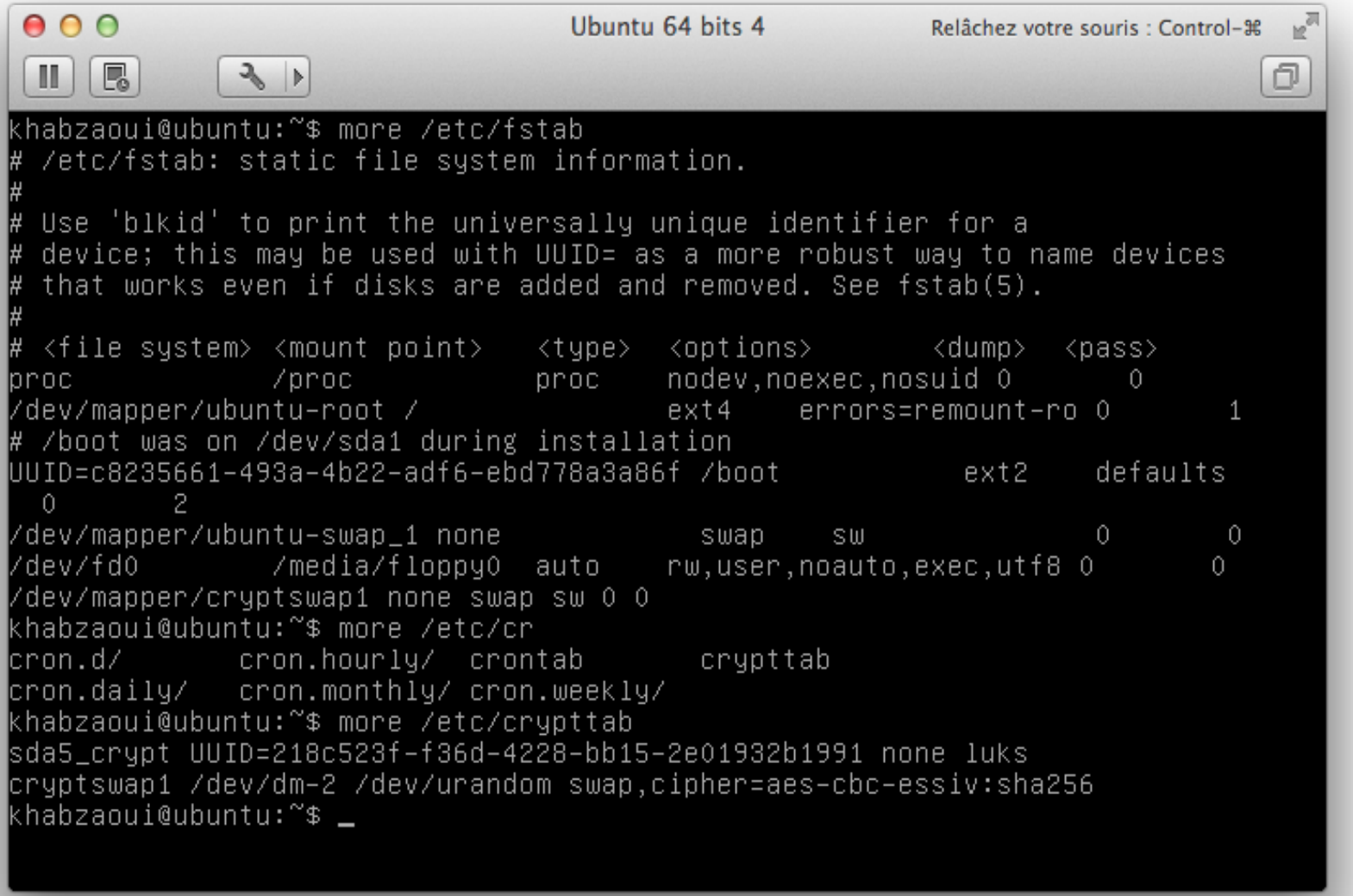
Démarrage du système



Les partitions du disque



/etc/fstab et /etc/crypttab



Gestion des passphrases

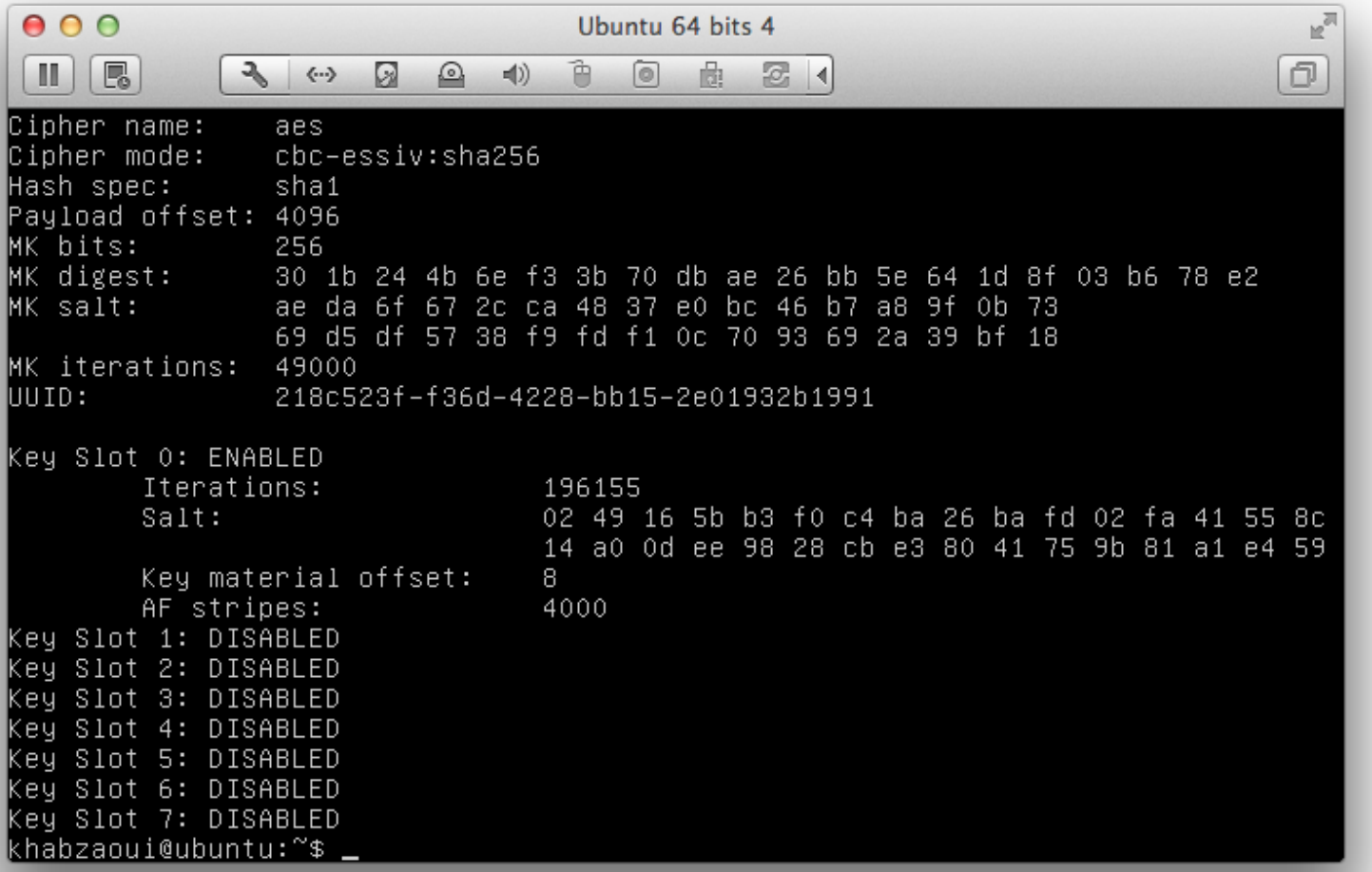
LUKS permet de stocker jusqu’à 8 passphrases

Après le premier reboot ajouter une passphrase pour le service informatique

Si l'entête du conteneur LUKS est endommagé, il ne sera plus possible d’accéder aux données donc il faut sauvegarder la clé de chiffrement en un endroit sûr (coffre-fort)

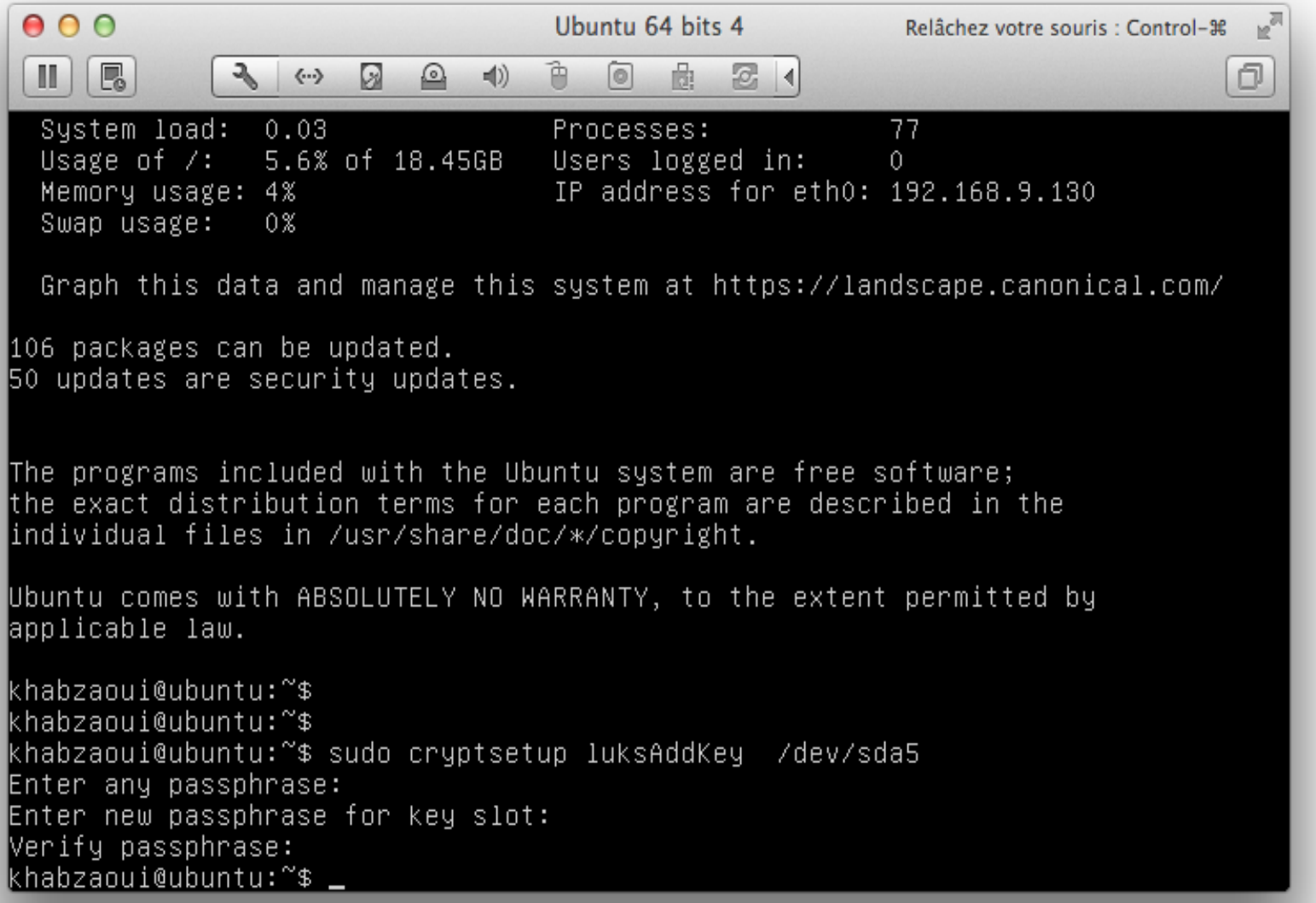
Lister les slots initiaux

sudo cryptsetup luksDump /dev/sda5



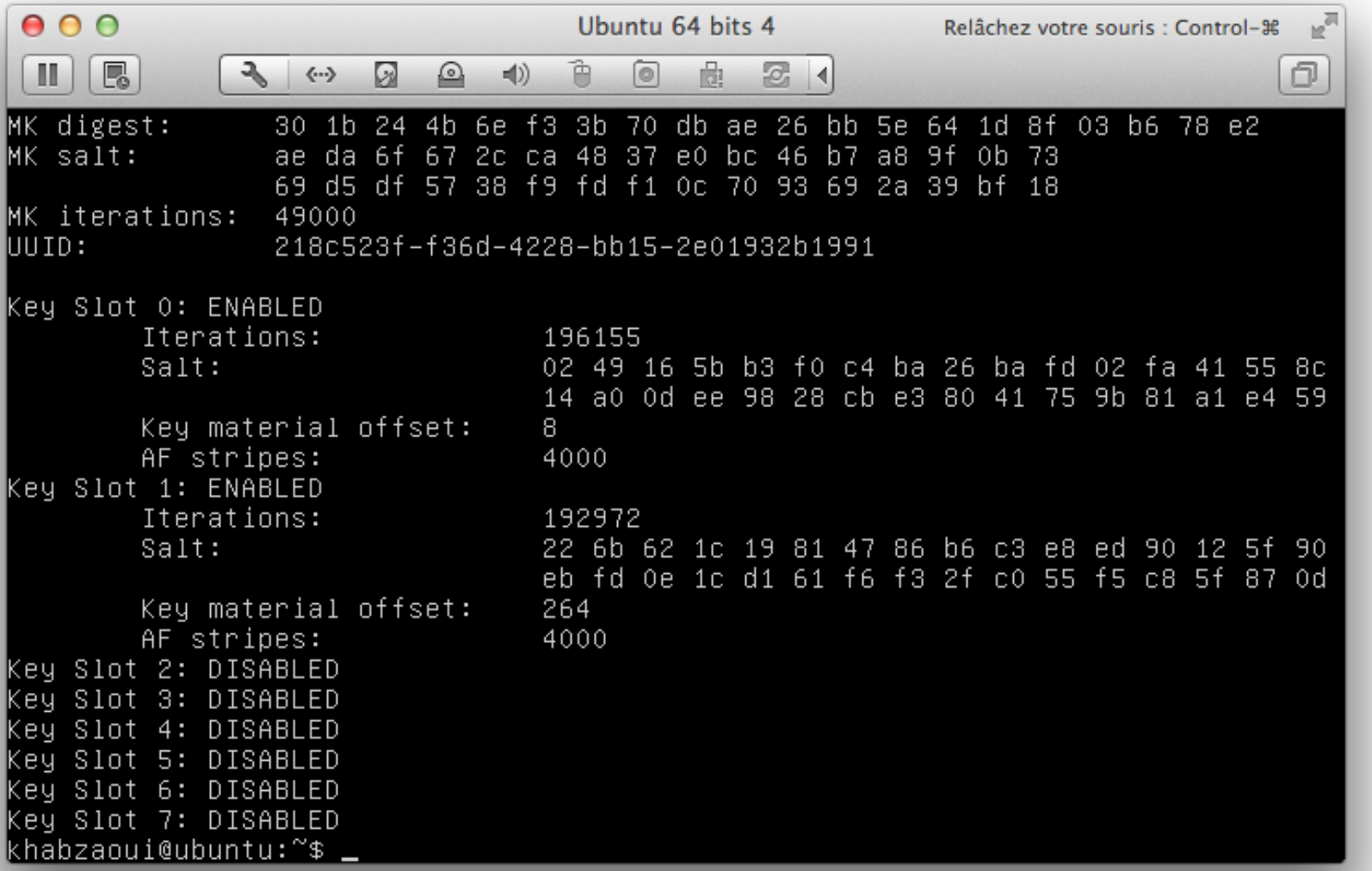
Ajout d'une passphrase

sudo cryptsetup luksAddKey /dev/sda5



Lister les slots

sudo cryptsetup luksDump /dev/sda5



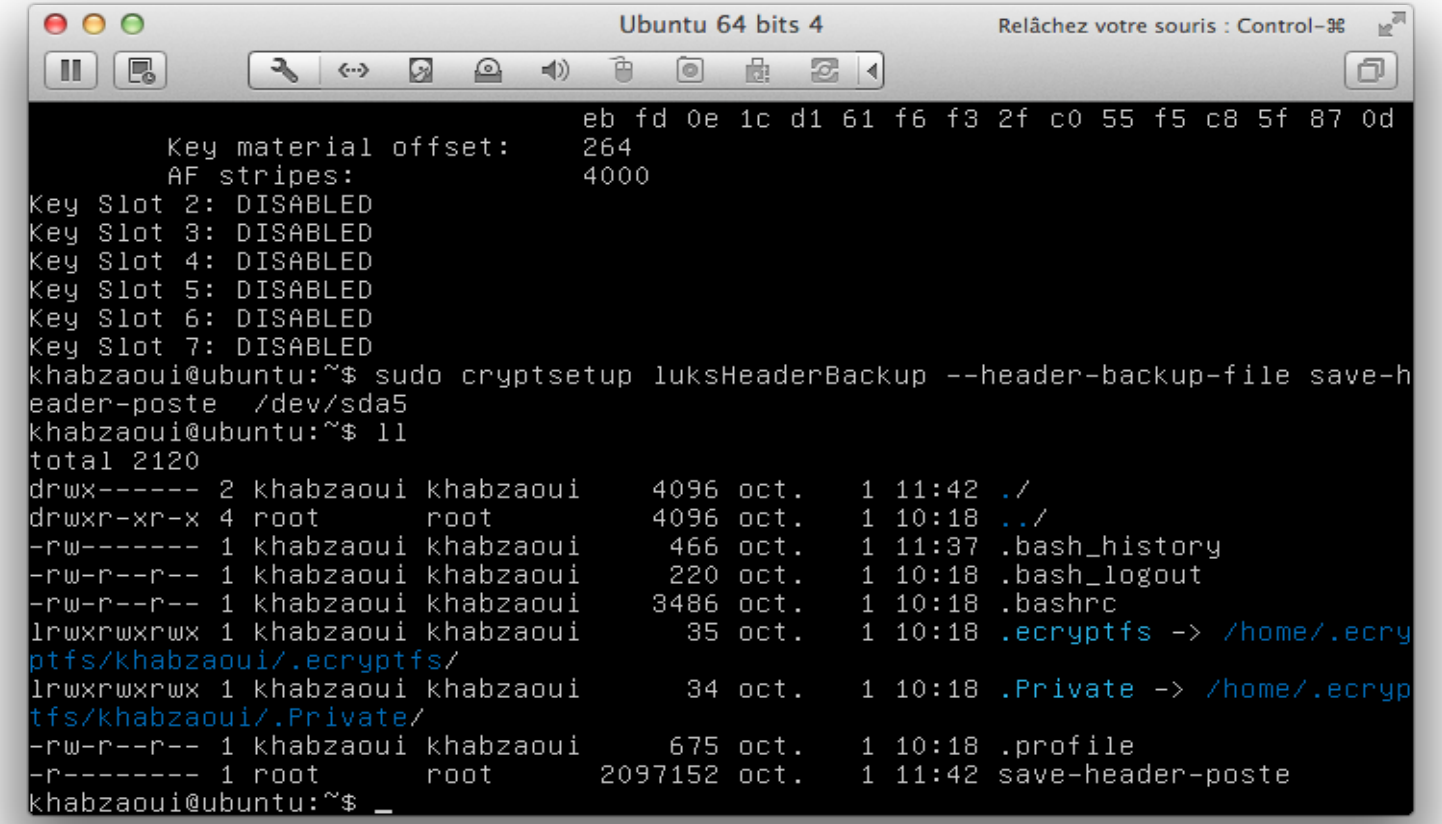
Supprimer une passphrase

Dans cet exemple on supprime la clé présente dans le 2ème slot.

```
sudo cryptsetup luksKillSlot /dev/sda5   2
```

Sauvegarde de l'entête LUKS

cryptsetup luksHeaderBackup --header-backup-file save-header-poste /dev/sda5



Restauration de l'entête LUKS

cryptsetup luksHeaderRestore --header-backup-file save-header-poste /dev/sda5

Recouvrement

Si l'utilisateur a oublié la sienne **(utiliser la passphrase admin) :**

- démarrer la machine avec la passphrase du service informatique
- supprimer le slot correspondant à la clé oubliée (luksKillSlot)
- créer une nouvelle passphrase (luksAddKey)

Si la passphrase de l'admin a été supprimée ou si l'entête de chiffrement est vérolée (**Restaurer l'entête)**

- connecter le disque à une autre machine
- restaurer l'entête à partir de la sauvegarde avec luksHeaderRestore

dm-crypt
Comment crypter un disque
Commandes utiles

Sauvegarder le système complet (un gros tar):

tar cSjf /external/sysbackup.tar.bz2 /bin/ /boot/ /etc/ /home/ /lib/ /opt/ /root/ /sbin/ /selinux/ /srv/ /usr/ /var/

Installer lvm et cryptsetup :

apt-get install lvm2 cryptsetup

Activer le module dm-crypt :

modprobe dm-crypt

On va ensuite créer nos partitions :

- **/dev/sda1 non chiffrée pour le boot (/boot).**
- **/dev/sda2 qui contiendra à la fois la partition système et la partition de swap. Toutes les 2 seront chiffrées**

Supprimer de manière sécurisée ce qui se trouve sur sda :

shred –n 7 /dev/sda

Créer la partition chiffrée sur /dev/sda2 :

cryptsetup -c aes-xts-plain -s 256 luksFormat /dev/sda2

(Cryptsetup demandera alors un mot de passe)

dm-crypt
Comment crypter un disque
Commandes utiles

Monter sda2 sous le nom lvm_crypt par exemple :

cryptsetup luksOpen /dev/sda2 lvm_crypt

Initialiser le volume :

pvcreate /dev/mapper/lvm_crypt

Créer un groupe de volumes qu'on appellera ubuntu :

vgcreate ubuntu /dev/mapper/lvm_crypt

Créer la swap chiffrée... 8 Gb est suffisant pour 4 Gb de RAM (par exemple) :

lvcreate -L8000M -n swap ubuntu

Utiliser le reste de la place du disque pour la partition système (root) :

lvcreate -l 100%FREE -n root ubuntu

Formater les deux partitions :

mkswap /dev/mapper/ubuntu-swap

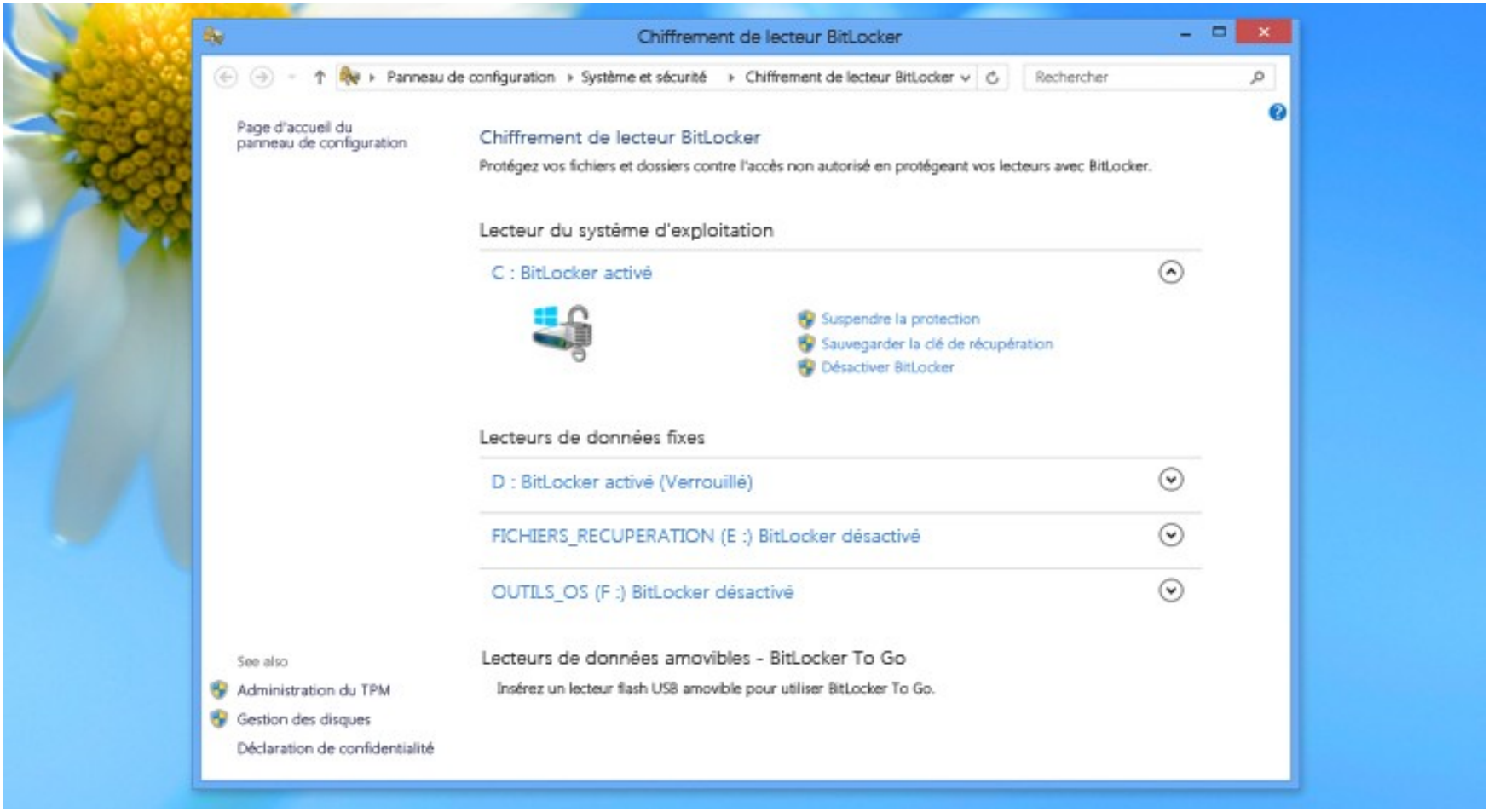
mkfs.ext4 /dev/mapper/ubuntu-root

Chiffrement des portables Windows

- Disque auto-chiffrant
- BitLocker (solution intégrée dans windows 8)
- TrueCrypt

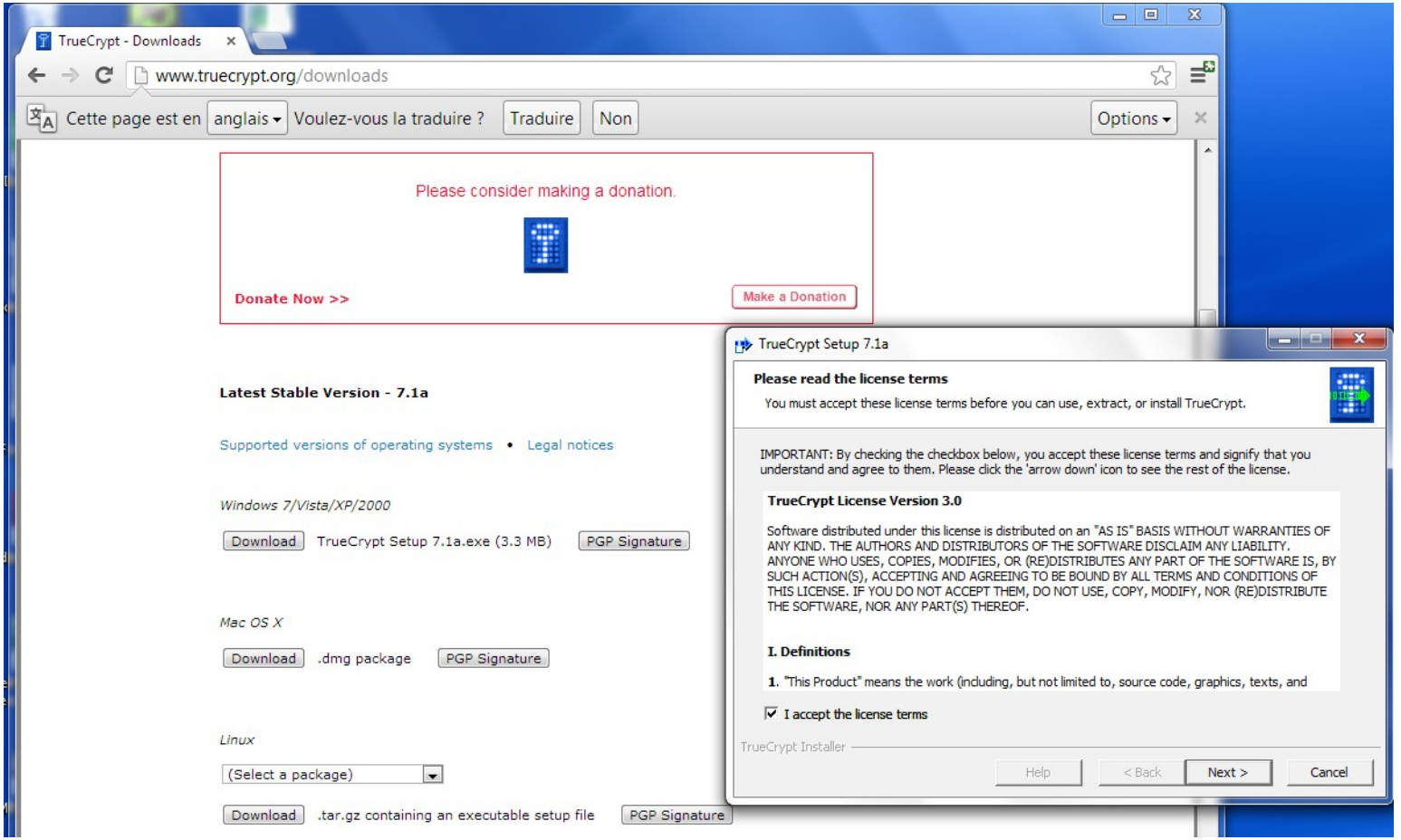
BitLocker

- http://windows.microsoft.com/fr-FR/windows-8/bitlocker

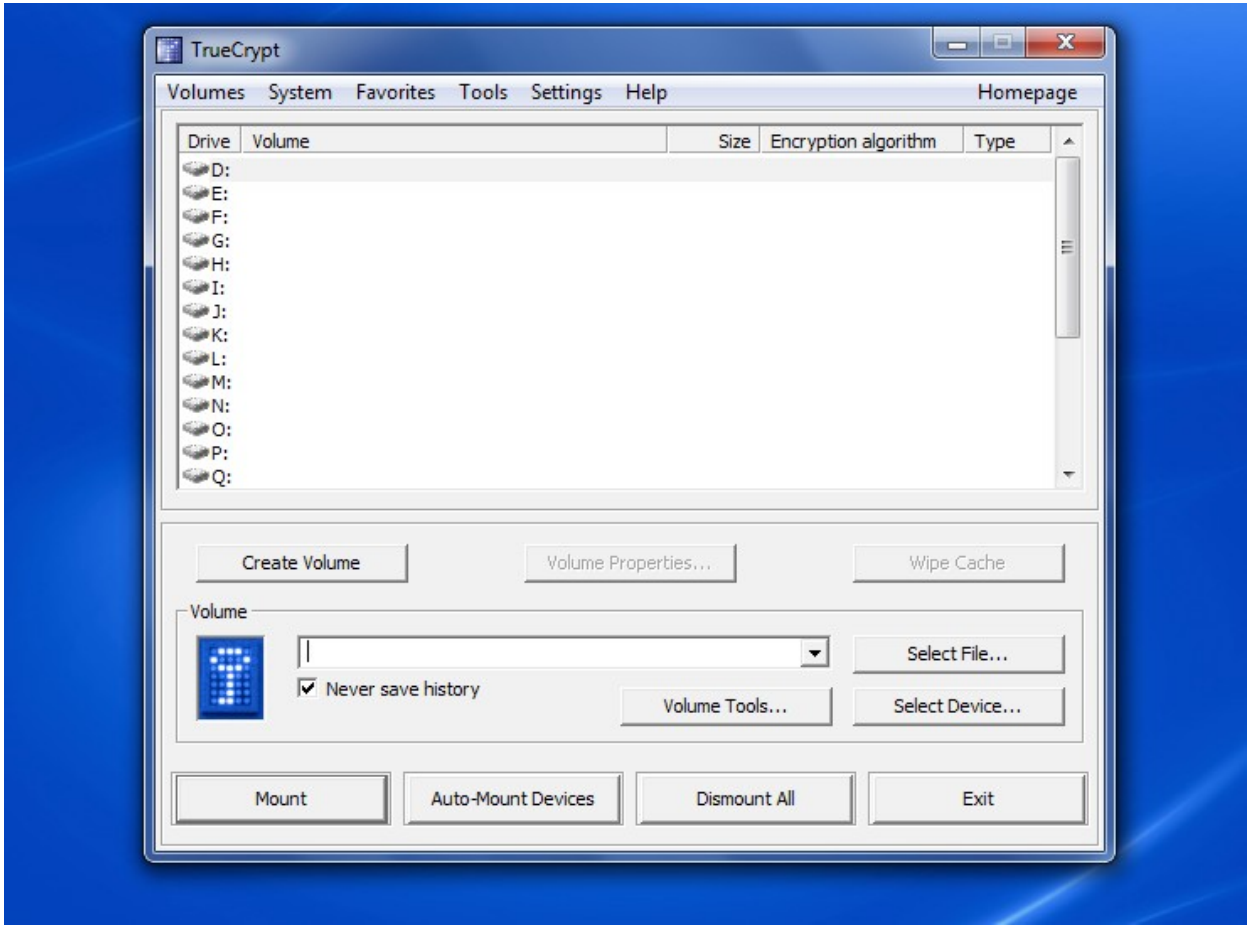


TrueCrypt

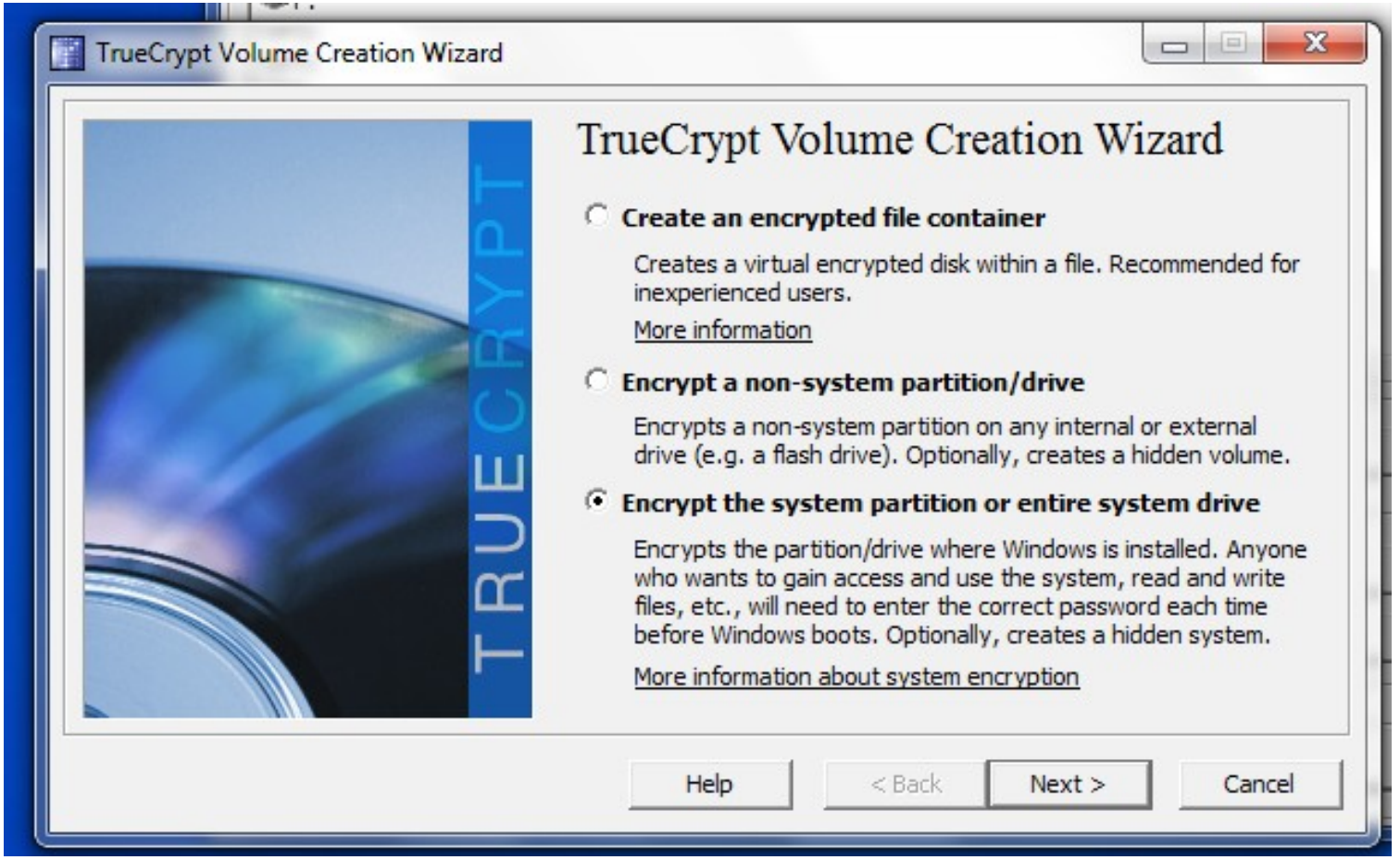
pour Windows (disponible aussi pour mac et linux)



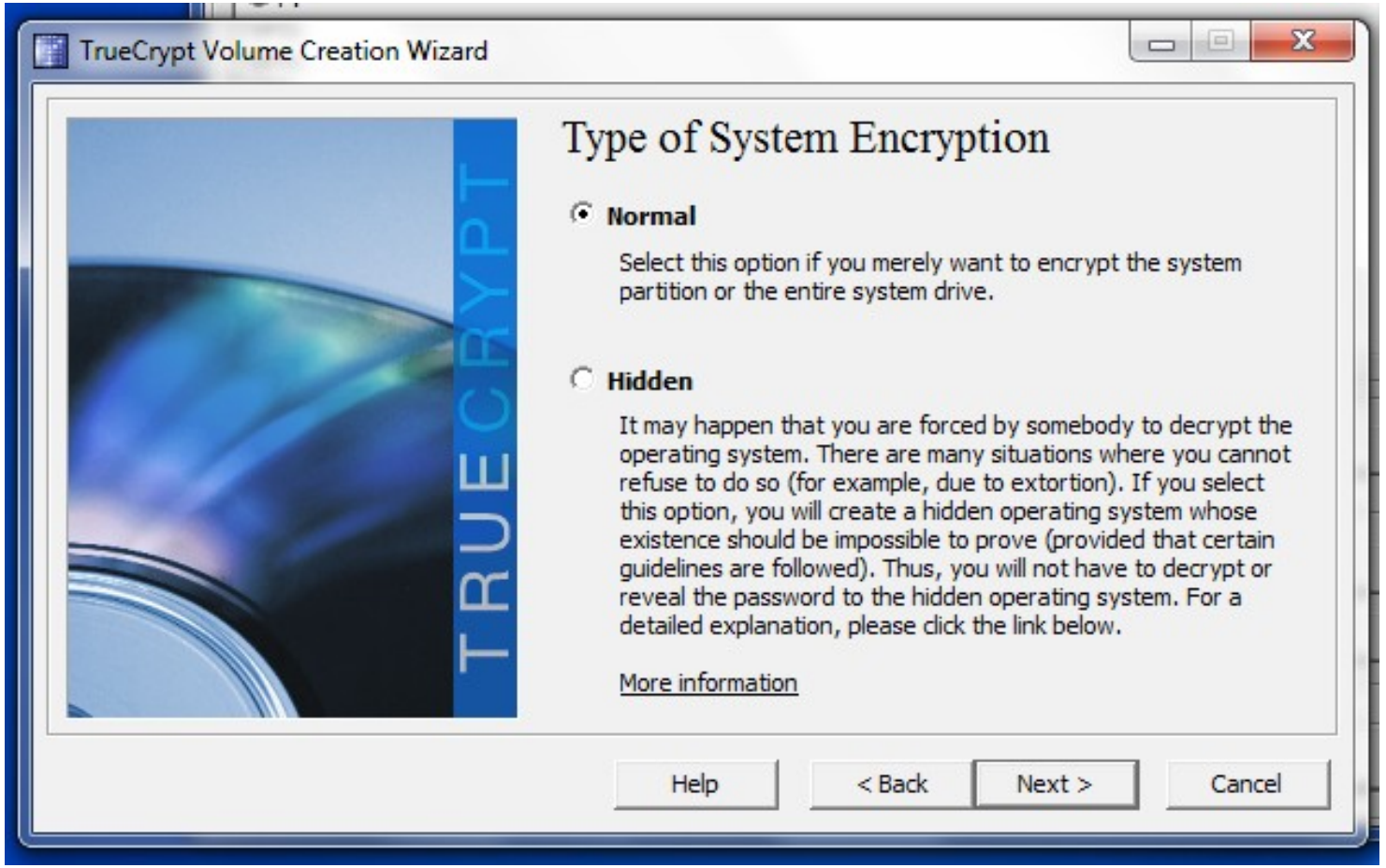
Créer un nouveau volume



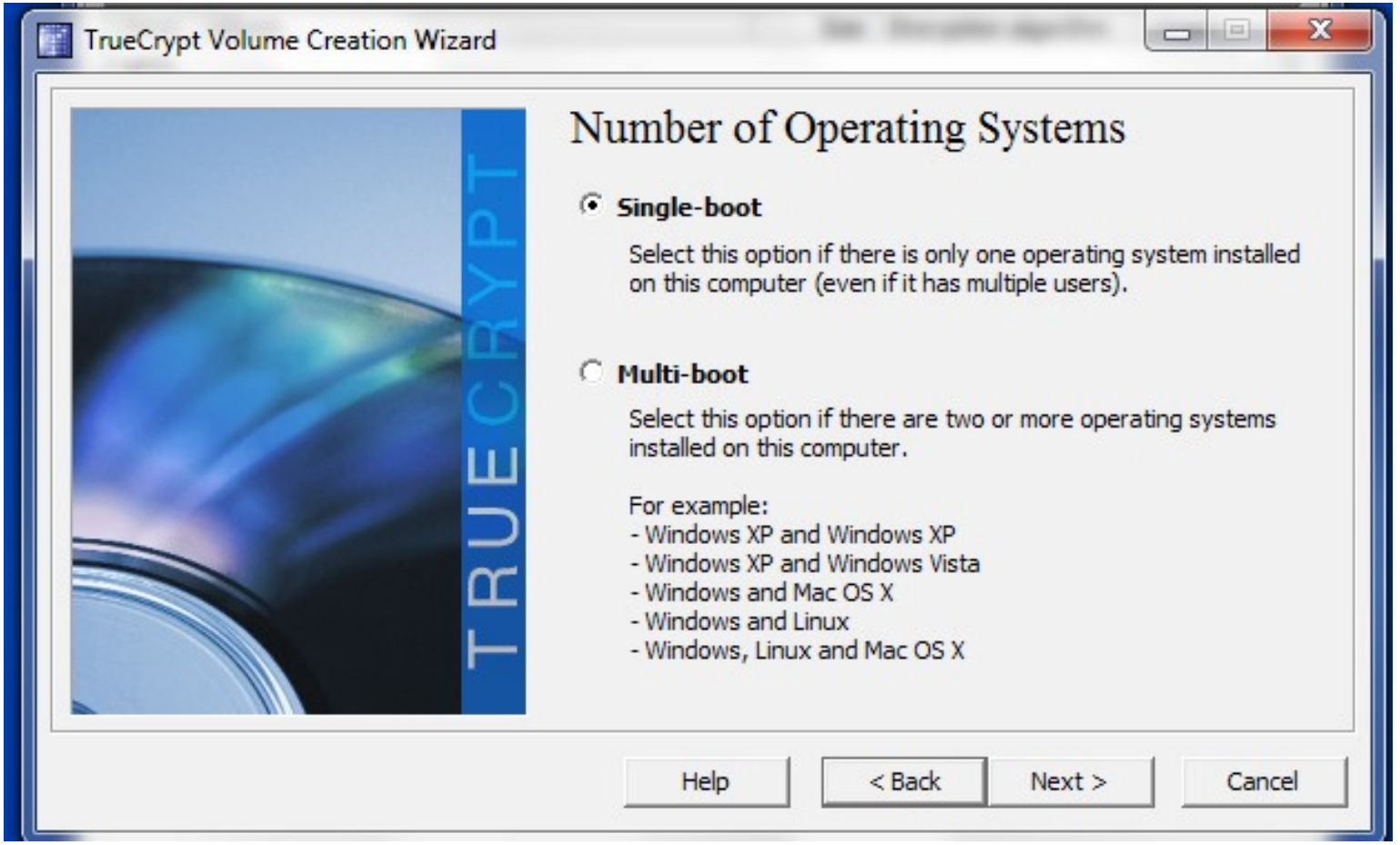
Créer un simple conteneur chiffré, chiffrer une partition qui ne contienne pas d'OS (clé USB) ou une partition /disque système



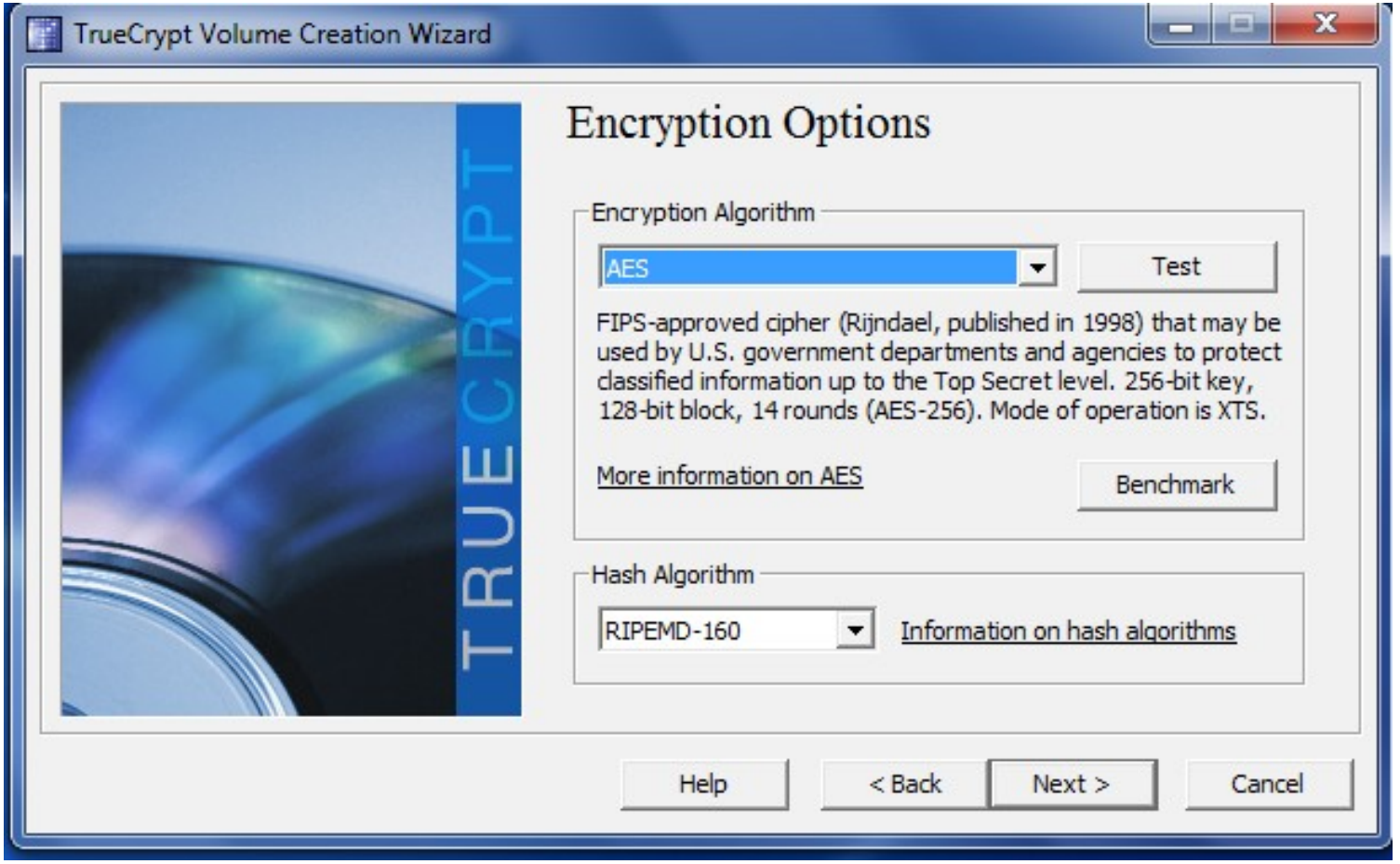
Choisir une partition normale



Un seul OS ou plusieurs (multi boot)



Sélectionner l'algorithme de chiffrement et l’algorithme de hash



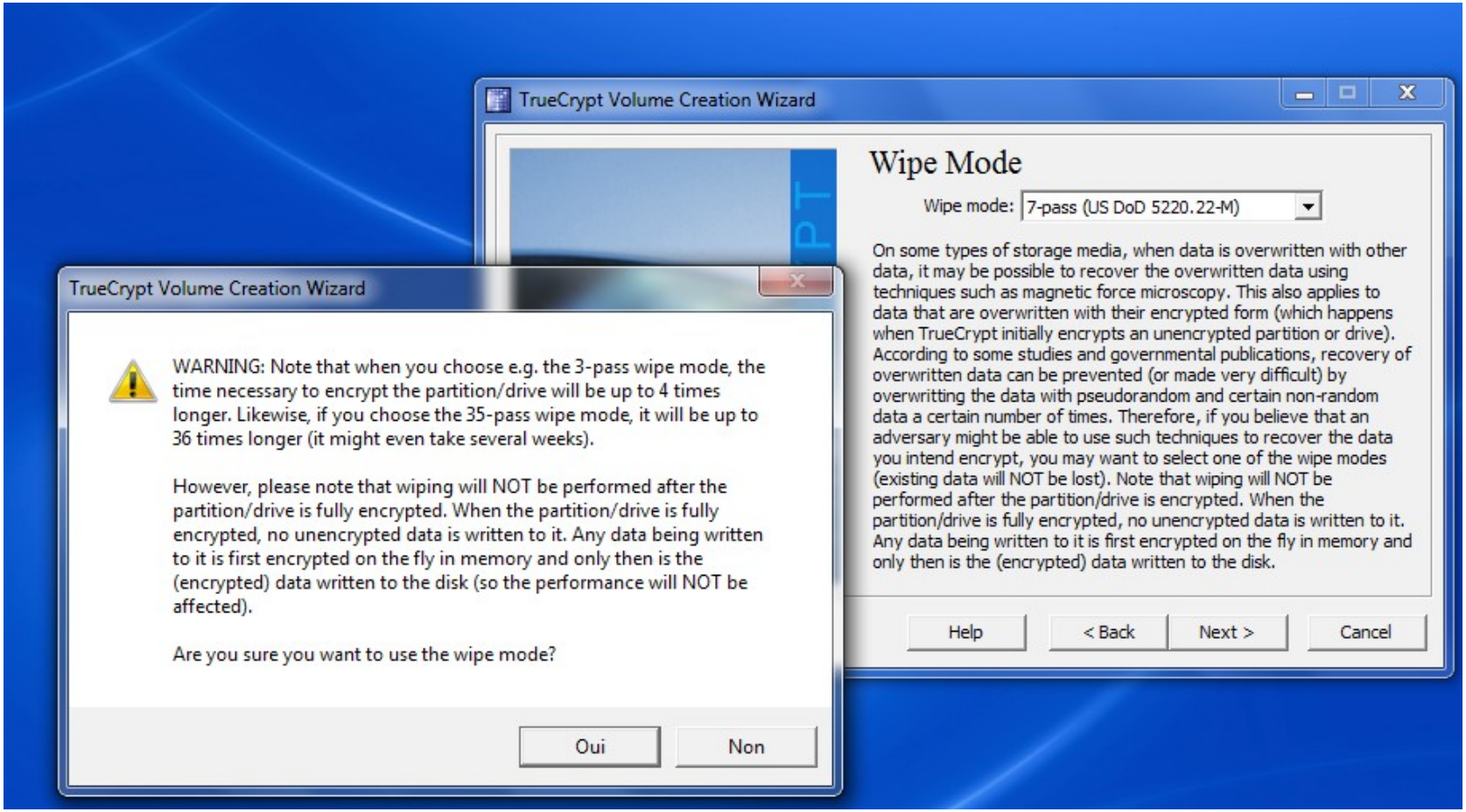
Choisir un mot de passe avec des lettres majuscules, minuscules, et des symboles

Bouger votre souris de manière aléatoire

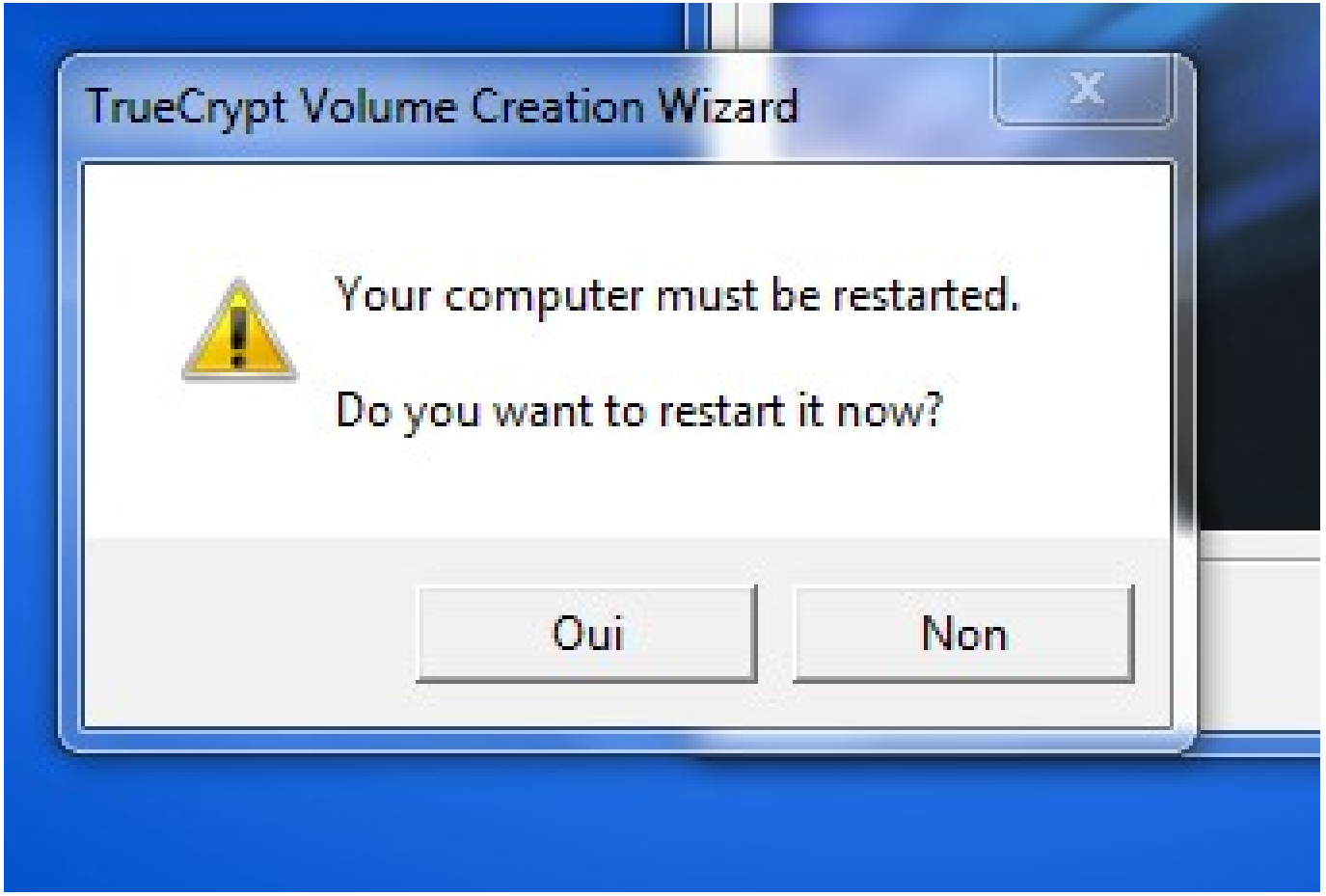

TrueCrypt Volume Creation Wizard
TRUECRYPT
Keys Generated
The keys, salt, and other data have been successfully generated. If you want to generate new keys, click Back and then Next. Otherwise, click Next to continue.
Header Key: B3908048F4BDD9927D9F92F05DE8EC70...
Master Key: D4BF8C9460FE9FC52402524012C82633...
Display generated keys (their portions)
Help
< Back
Next >
Cancel
Dismount All
Exit

Création d'un disque de récupération, il vous faudra obligatoirement un CD vierge ou une clé USB pour l'étape suivante

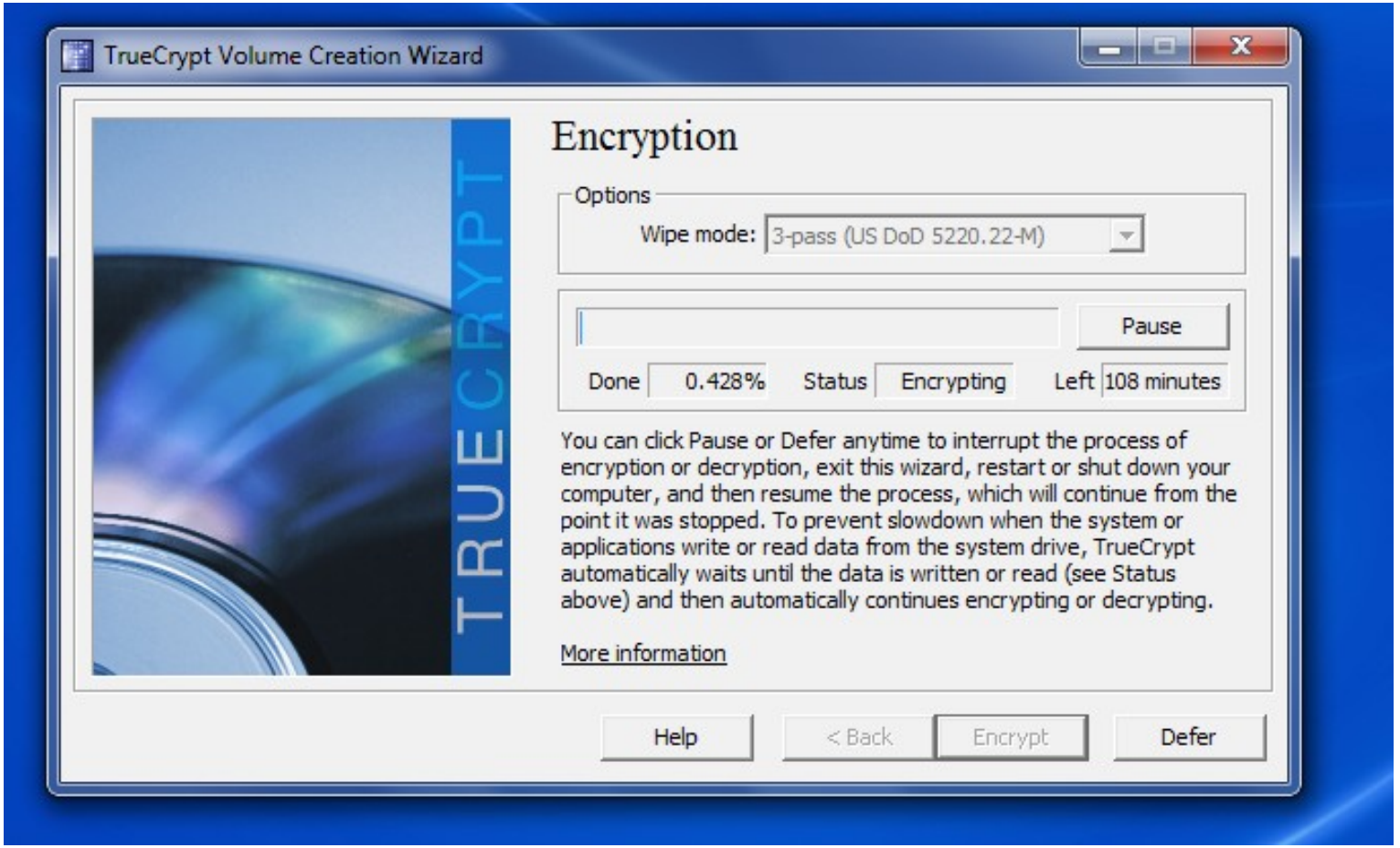
Comment effacer/réécrire les données existantes en évitant que les anciennes soient irrécupérables.



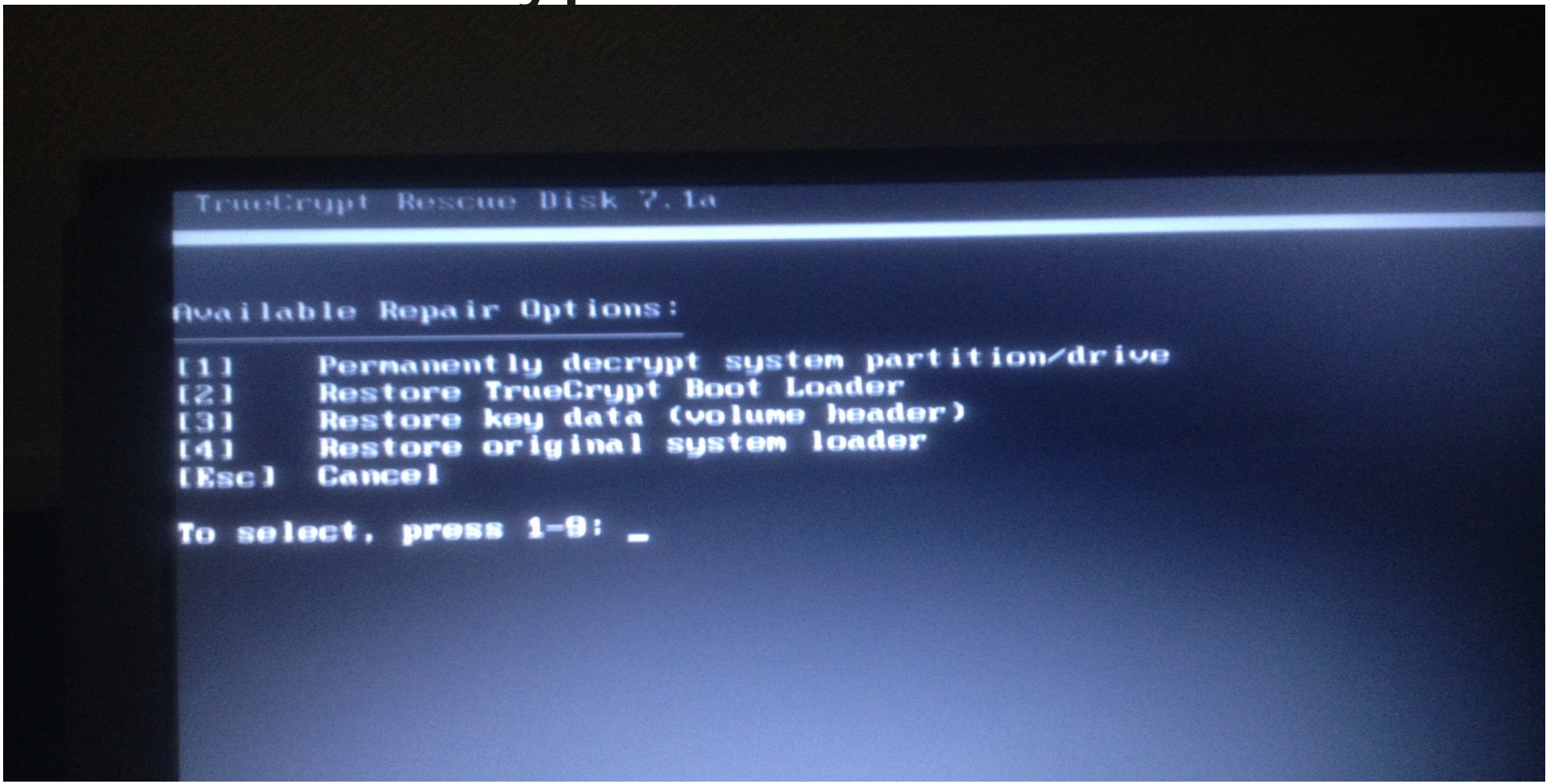
Reboot


TrueCrypt Volume Creation Wizard
Your computer must be restarted.
Do you want to restart it now?
Oui
Non

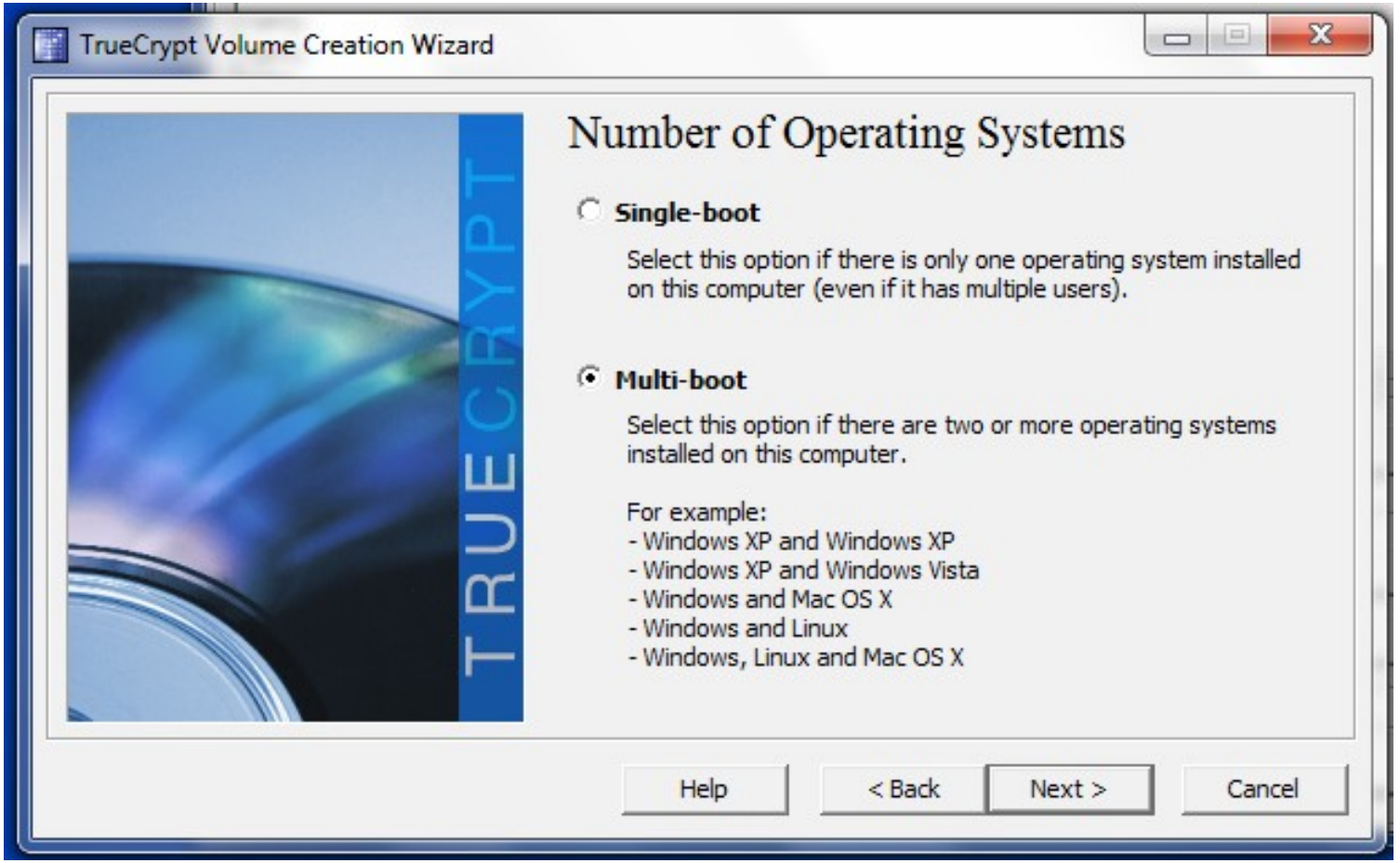
2 heures pour 17GO sur un disque SSD

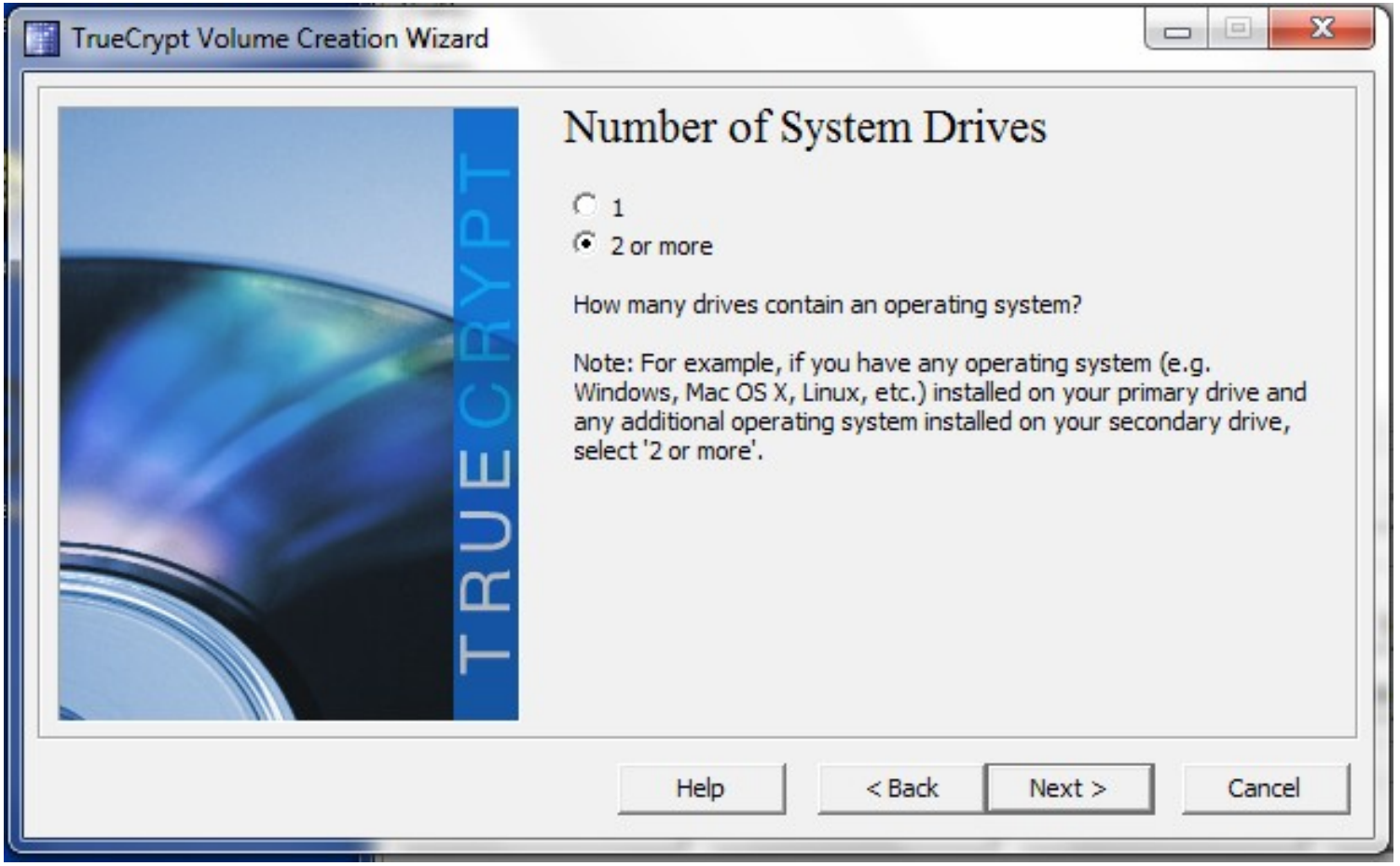


Recouvrement : TrueCrypt Rescue Disk.iso



DUAL BOOT


TrueCrypt Volume Creation Wizard
TRUECRYPT
Number of Operating Systems
Single-boot
Select this option if there is only one operating system installed on this computer (even if it has multiple users).
Multi-boot
Select this option if there are two or more operating systems installed on this computer.
For example:
- Windows XP and Windows XP
- Windows XP and Windows Vista
- Windows and Mac OS X
- Windows and Linux
- Windows, Linux and Mac OS X
Help
< Back
Next >
Cancel


TrueCrypt Volume Creation Wizard
TRUECRYPT
Number of System Drives
1
2 or more
How many drives contain an operating system?
Note: For example, if you have any operating system (e.g. Windows, Mac OS X, Linux, etc.) installed on your primary drive and any additional operating system installed on your secondary drive, select '2 or more'.
Help
< Back
Next >
Cancel

Séquestre de clé de chiffrement

- Dans un coffre fort physique
- Un media de stockage contenant une copie de tous les passphrases et les entêtes ainsi que tous les disques de récupération.
- En format papier si possible (clés de chiffrements)

Conclusion

Chiffrer les portable OK mais à quel Prix !

- *Choix limité : Disque Chiffrant sur portables du marché actuel : SSD 256 =175 euros*
- Est-ce que les *Disques Chiffrants sont* utiles aujourd'hui ?
- Charge de l'ASR (activation, installation, sauvegarde, recouvrement …)
- Un compte de service admin / passphrase admin sur tous les ordinateurs
- Mise en place d'un serveur pour la sauvegarde des portables
- PB : Sauvegarde externe non chiffrée (dropbox et autres)
    - Faire des sauvegarde chiffrées
    - Clé USB chiffrée (matériel ou logiciel)