Protection des portables au LAAS
Sauvegarde et Chiffrement

Pourquoi et comment protéger les données sur les portables vis-à-vis de pertes, de casse ou de vol

21/02/13

LAAS-CNRS

Contexte : directive de la direction du CNRS

- Directive demandant le chiffrement des postes de travail janvier 2013
  - https://aresu.dsi.cnrs.fr/spip.php?rubrique99
- Analyse de la **demande**, des **risques**, des **solutions** et des **coûts**
- D'abord les portables :
  - Contenant des données sensibles (perception utilisateur)
  - Nouvelles machines
- Le besoin de sauvegarde prime et est renforcée par l'utilisation du chiffrement
- Solutions existantes au LAAS
  - Offre de sauvegarde complète depuis 2007
  - Offre de chiffrement depuis novembre 2012

Les risques : de quoi se protéger

- De la perte de données
  - Perte du portable, ou vol du matériel
  - Casse du portable
  - Problème matériel (disque HS)

- Du vol de données (sensibles)
  - Par vol du matériel

- *L'objectif n'est pas de se protéger « juridiquement » mais bien d'offrir des outils aux utilisateurs pour assurer la protection de leurs données.*

- Les données peuvent être professionnelles ou personnelles
  - Le portable sert aux 2 utilisations

Les solutions : la sauvegarde

- 3 types de systèmes supportés
  - Windows (XP, 7)
  - Mac OS X (10.6,10.7,10.8)
  - Linux (Fedora, Ubuntu LTS)

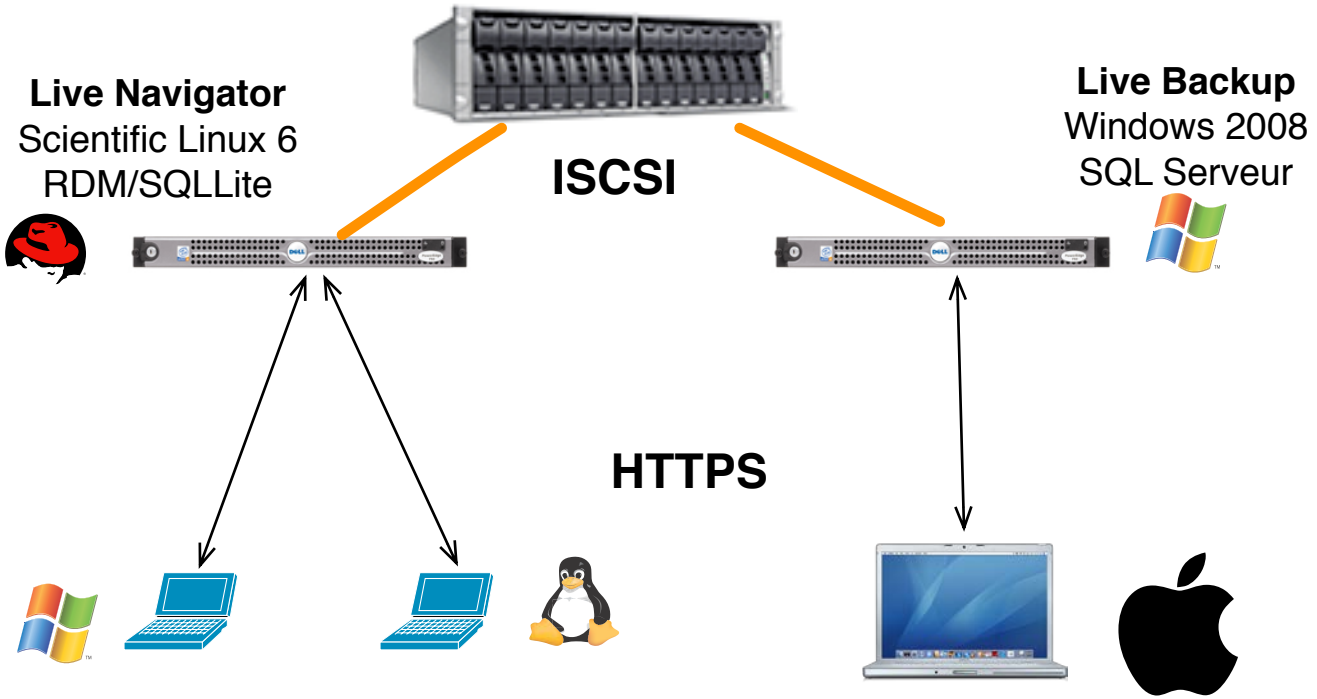
- Cahier des charges
  - Sauvegarde centralisée sécurisée
    - Rétention de 3 mois
  - Sauvegarde et restauration hors-site (mission, domicile…)
  - Sauvegarde déclenchée par le portable
  - Sauvegarde fréquente (CDP)
  - Cache local de sauvegarde

  - Restauration de fichiers effacés
  - Restauration en cas de crash
  - Eventuelle restauration de tout le disque (crash recovery)

Sauvegarde : historique des solutions

- **➔ 2008**
  - Windows : Fichiers hors connexion
  - Mac et Linux : Scripts rsync
- **2008**
  - Windows et Mac : Atempo Live Backup
    - Répond au cahier des charges
    - « Disaster recovery » sur Windows avec restauration de tout le disque
- **2012**
  - Fin de vie de Live Backup
  - Windows et Linux : remplacement par ASG-Atempo Live Navigator
    - Pas de cache de sauvegarde
    - Pas de restauration complète du disque
    - Sauvegarde uniquement les répertoires utilisateurs
  - Mac sous Mountain Lion (10.8) : Time Capsule
    - Insatisfaisant !
  - Pas de solution Windows 8, tablettes, smartphones
- **Présent et futur** : la solution universelle
  - BYOB (Bring Your Own Backup) **DropBox !!!!!**

Sauvegarde Live Backup/Navigator



Coût : quelques dizaines d'euros par poste + serveur puissant + stockage (plusieurs To)

Sauvegarde Live Backup/Navigator

- **Live Navigator**
  - 38 clients Windows
  - 10 clients Linux
  - Espace de stockage : 1 To
  - Volume sauvegardé/restaurable : 10 To

- **Live Backup**
  - 79 clients Mac
  - 100 clients Windows (migration en cours)
  - Espace de stockage : 8,5 To
  - Volume sauvegardé/restaurable : 144 To

Sauvegarde : bilan et évolution

- Mac OS X
  - Changement d'OS obligatoire avec les nouvelles machines
  - Nouvelle version du logiciel
- Linux
  - Changement de noyaux => Recompilation du driver
- Nouveaux matériels
  - Smartphones, tablettes

- Concurrence BYOB
  - Chacun son disque (ex: Time Machine)
  - Chacun son cloud (Apple, Google, DropBox…)

- Besoin réel : synchronisation multi-sites, multi-appareils
  - Bien le distinguer de la sauvegarde

Solutions de chiffrement : critères de choix

- Facilité d'installation pour les ASR
- Facilité d'utilisation pour les usagers
- Pas de dégradation des performances
- Efficacité reconnue de la solution

- Pour gérer quels risques :
  - Empêcher des voleurs de récupérer les données : OUI
  - Empêcher des services de police ou de renseignements étrangers de récupérer les données : NON
  - Empêcher le collègue de bureau de récupérer les données : NON

- Le coût financier doit être nul (et la charge de travail faible)

Chiffrement : nos choix

- Windows 7 : TrueCrypt
  - http://www.truecrypt.org
  - S'applique à des machines existantes
  - Logiciel libre
- Mac OS X (10.7/10.8) : FileVault 2
  - http://support.apple.com/kb/HT4790?viewlocale=fr_FR
  - S'applique à des machines existantes
  - Intégré à l'OS
- Linux : dm-crypt + LUKS
  - http://code.google.com/p/cryptsetup/wiki/DMCrypt
  - Nécessite la réinstallation de la machine
  - Logiciel libre
- Dans tous les cas, on chiffre tout le disque

Choix de TrueCrypt

- Disponible sur Windows
  - BitLocker de Microsoft uniquement sur Windows 7 Entreprise
- Logiciel libre
  - Permet de valider l'implémentation du chiffrement
  - Détection de faiblesses éventuelles
- Fiabilité
  - Reconnu et Certifié (version 6.0a ANSSI)
- Facilité d'installation
  - Peut être appliqué à des machines existantes
- Facile et transparent à l'utilisation
- Recouvrement maîtrisé
- http://www.truecrypt.org
  - Version actuelle 7.1a

Technologie

- Toutes les données écrites sur le disque sont chiffrées (et déchiffrées) à la volée
  - Contenu du disque quasi aléatoire
- XTS-AES-128 : chiffrement bloc 512 octets normalisé pour les périphériques de stockage
  - Perte maximum 16 octets pour 1 bit défectueux
  - http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf
- Clef maître chiffrée par le mot de passe
- Liberté à l'utilisateur
  - De déchiffrer
  - De changer le mot de passe

Chiffrements offerts

- Container chiffré
  - Non, car l'utilisateur n'est jamais sûr de la localisation de ses données sensibles
- Partition système ou disque (une seule partition dans notre cas)
  - On chiffre tout donc on protège tout
  - Très simple d'utilisation
    - Aucune contrainte pour l'utilisateur sauf au démarrage

  - *TrueCrypt Boot Loader* dans le MBR
  - Mot de passe au démarrage de la machine

  - ✖ Pas de mot de passe de recouvrement
  - ✖ Comment gérer une machine multi-utilisateur
    - Mot de passe doit être partagé
  - ✖ Gestion du dual-boot un peu complexe
    - Non testé

Procédure : Installation

- Nous le réservons à Windows 7
  - Mais doit fonctionner avec Windows XP (sauf fichier hibernation)
  - Pas de support Windows 8

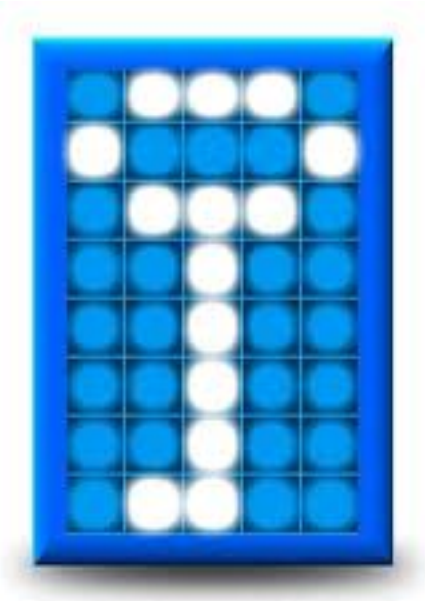
- Nouvelle machine
  - Installation de la machine
  - Ensuite installation de True Crypt et chiffrement du disque
  - Tâche de fond (1 nuit)

- Ancienne machine
  - Installation de True Crypt et chiffrement du disque
  - Tâche de fond (1 nuit)

- Le mot de passe est défini avec l'utilisateur **(Séquestre)**
- Recommandation de ne pas le changer

Procédure : Installation de TrueCrypt

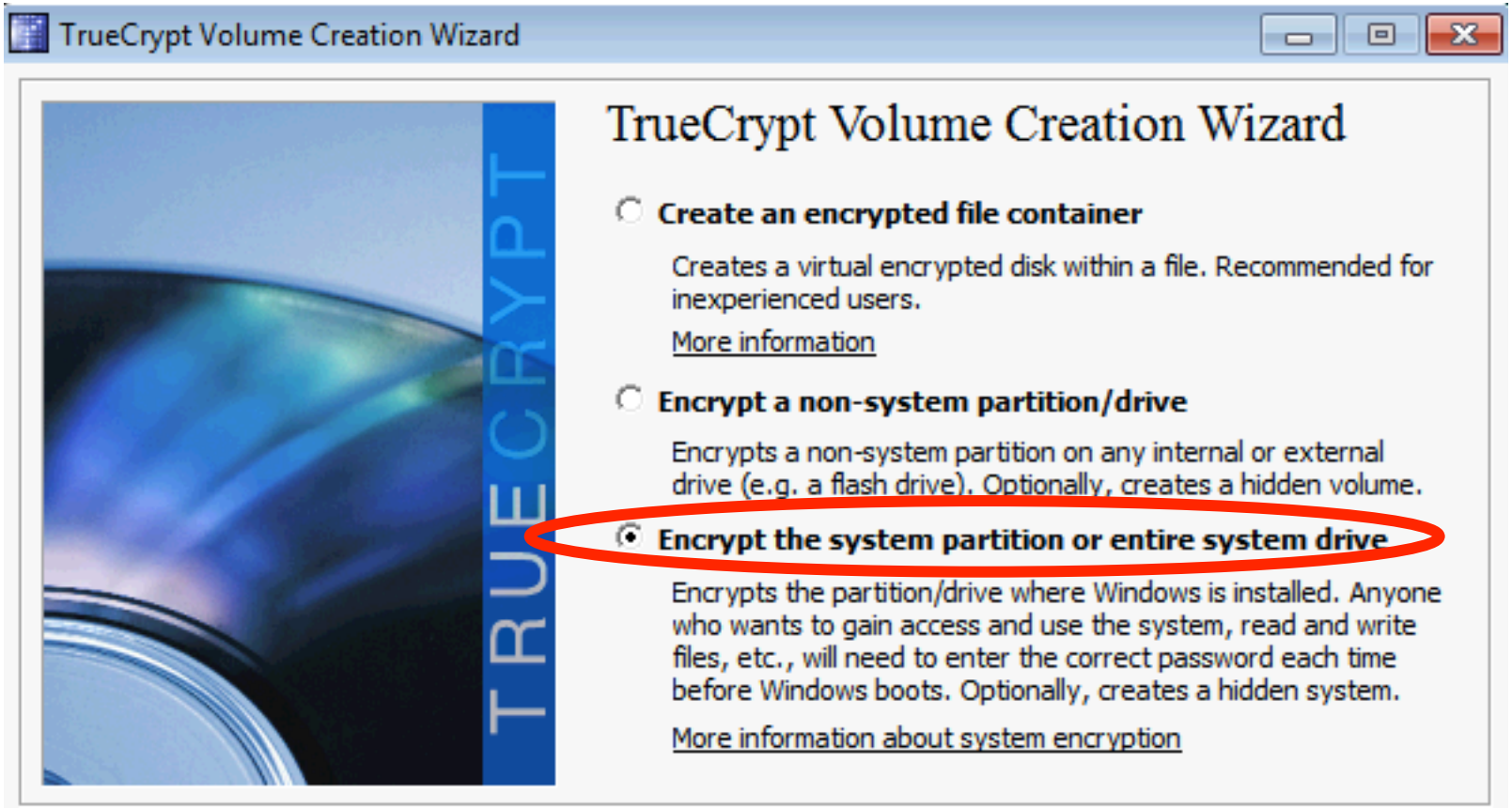
- Télécharger TrueCrypt
  - http://www.truecrypt.org



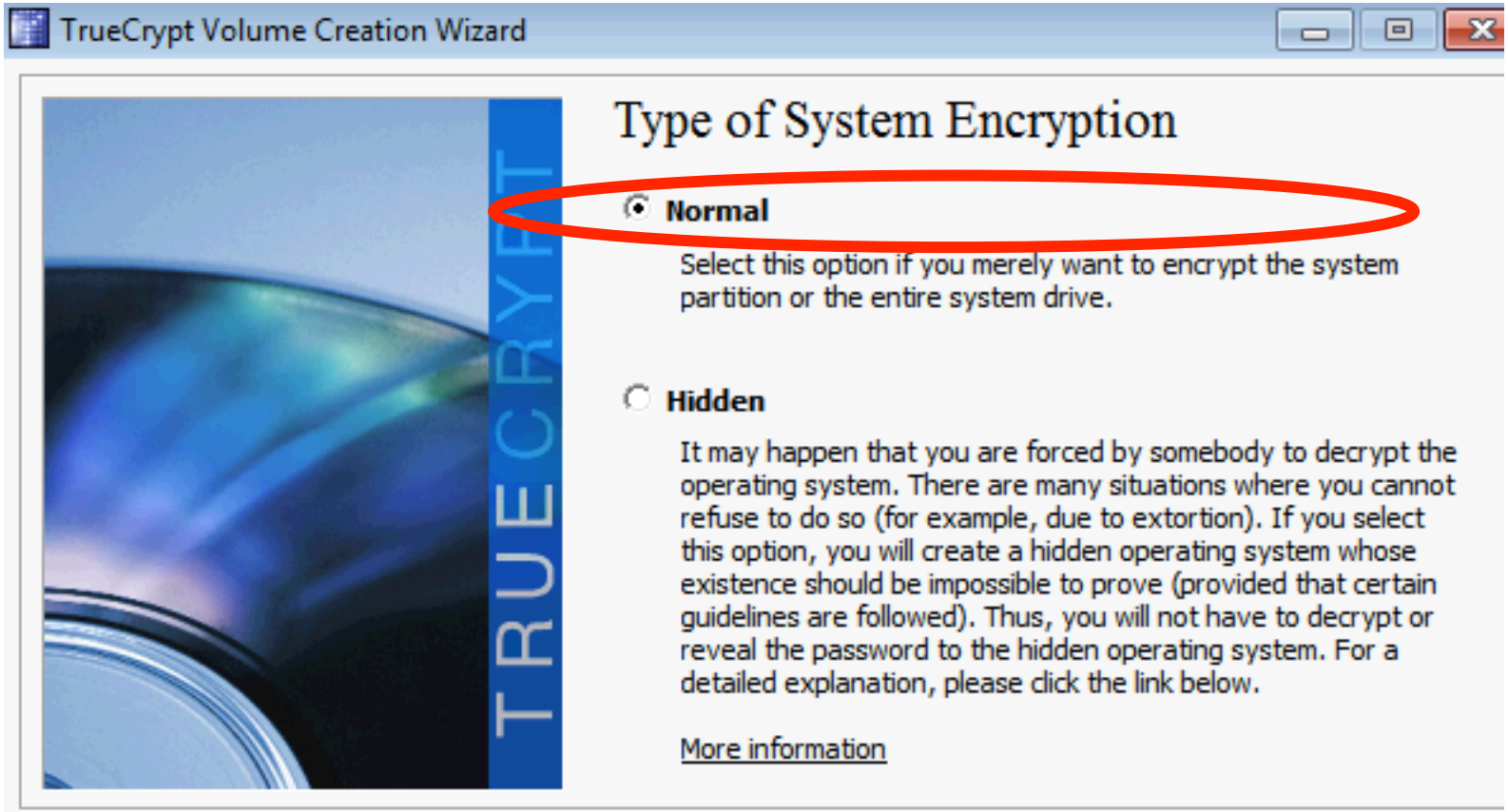
- Next / Next / Next…

Procédure : Chiffrement du disque

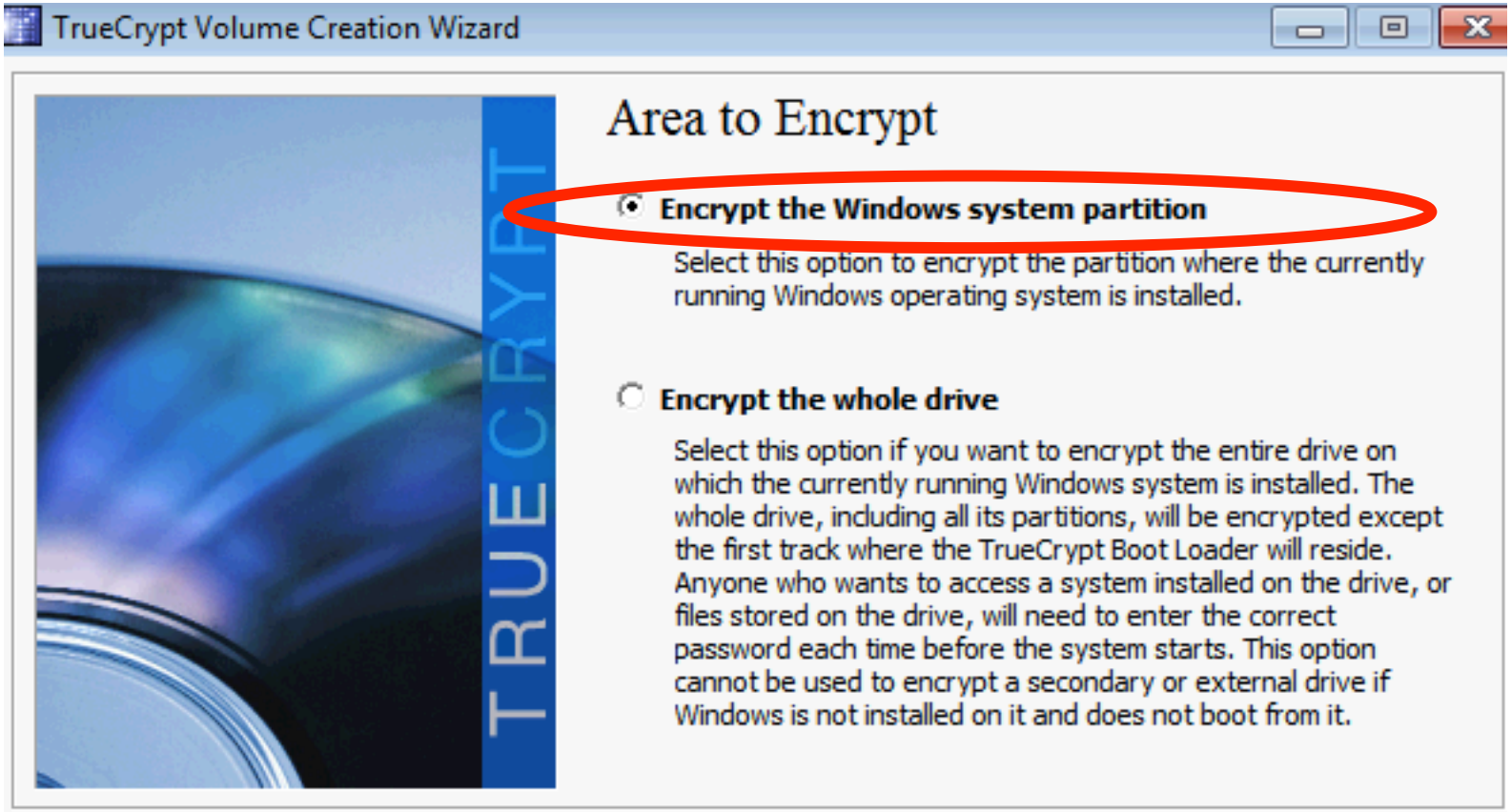
- Ligne de commande : évite de graver le CD de Recouvrement et génère une image ISO
  - **"%ProgramFiles%\Truecrypt\TrueCrypt Format.exe" /noisocheck**



Procédure : Chiffrement du disque

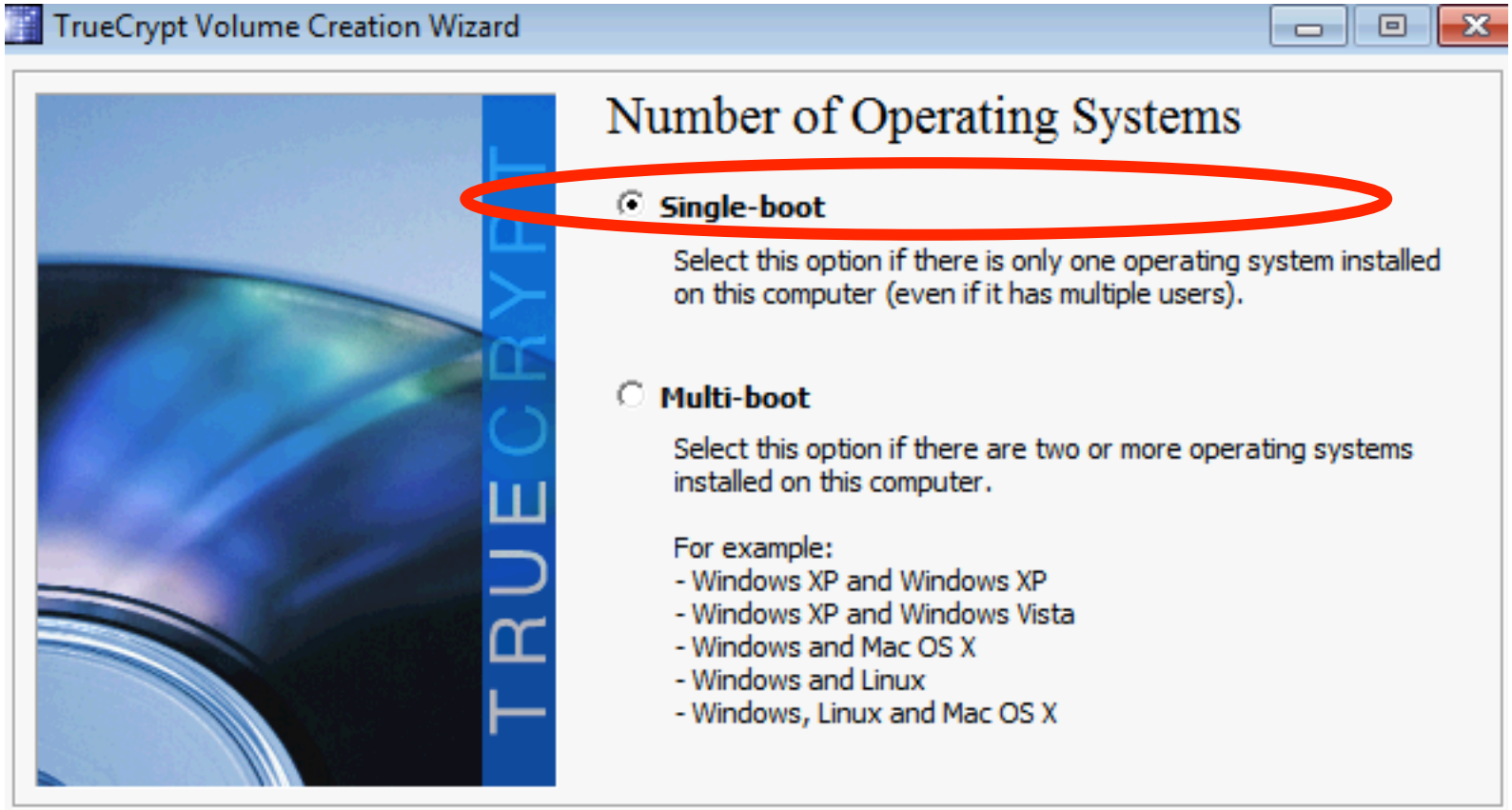


Procédure : Chiffrement du disque

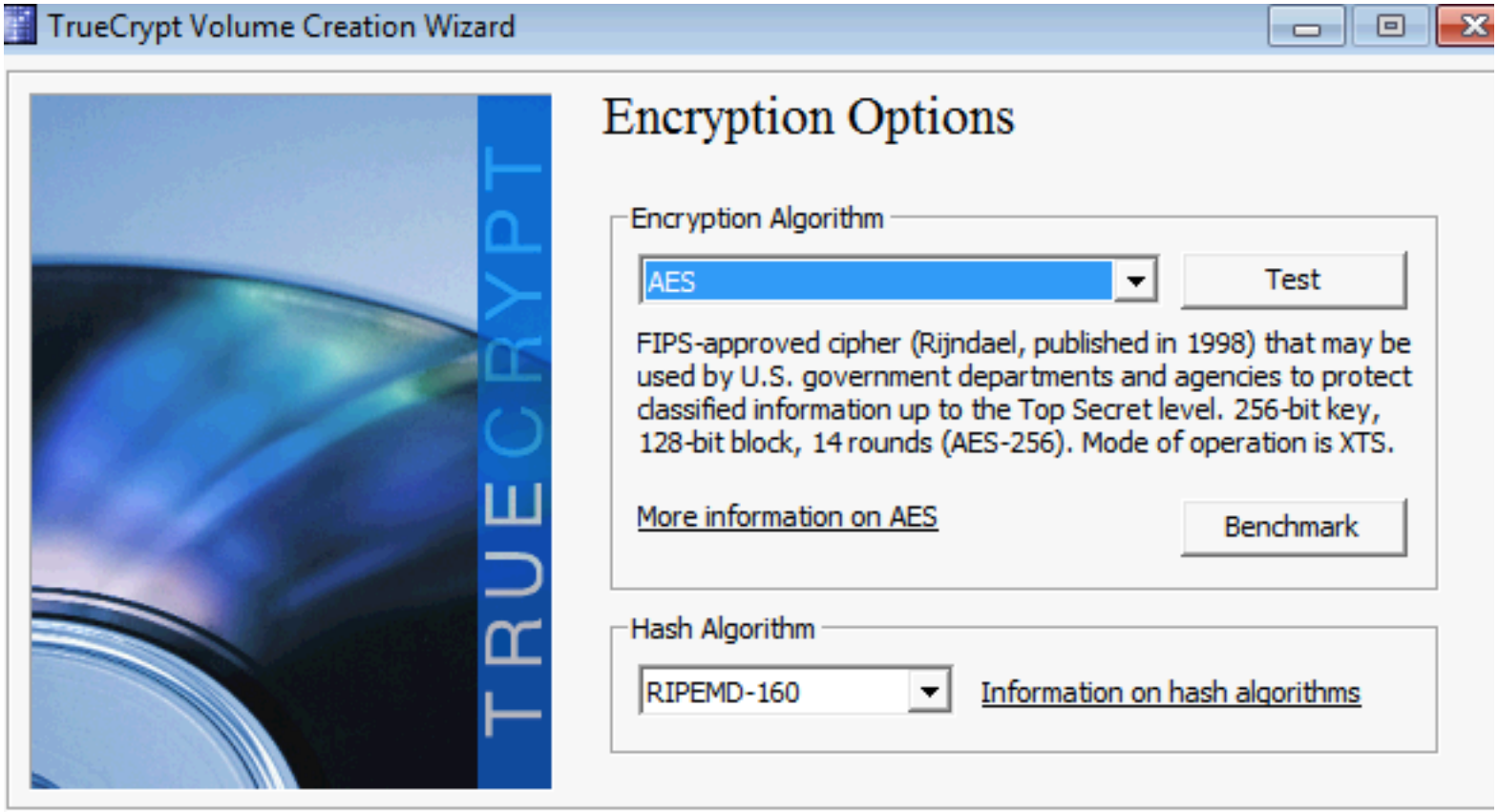


Dans notre cas une seule partition

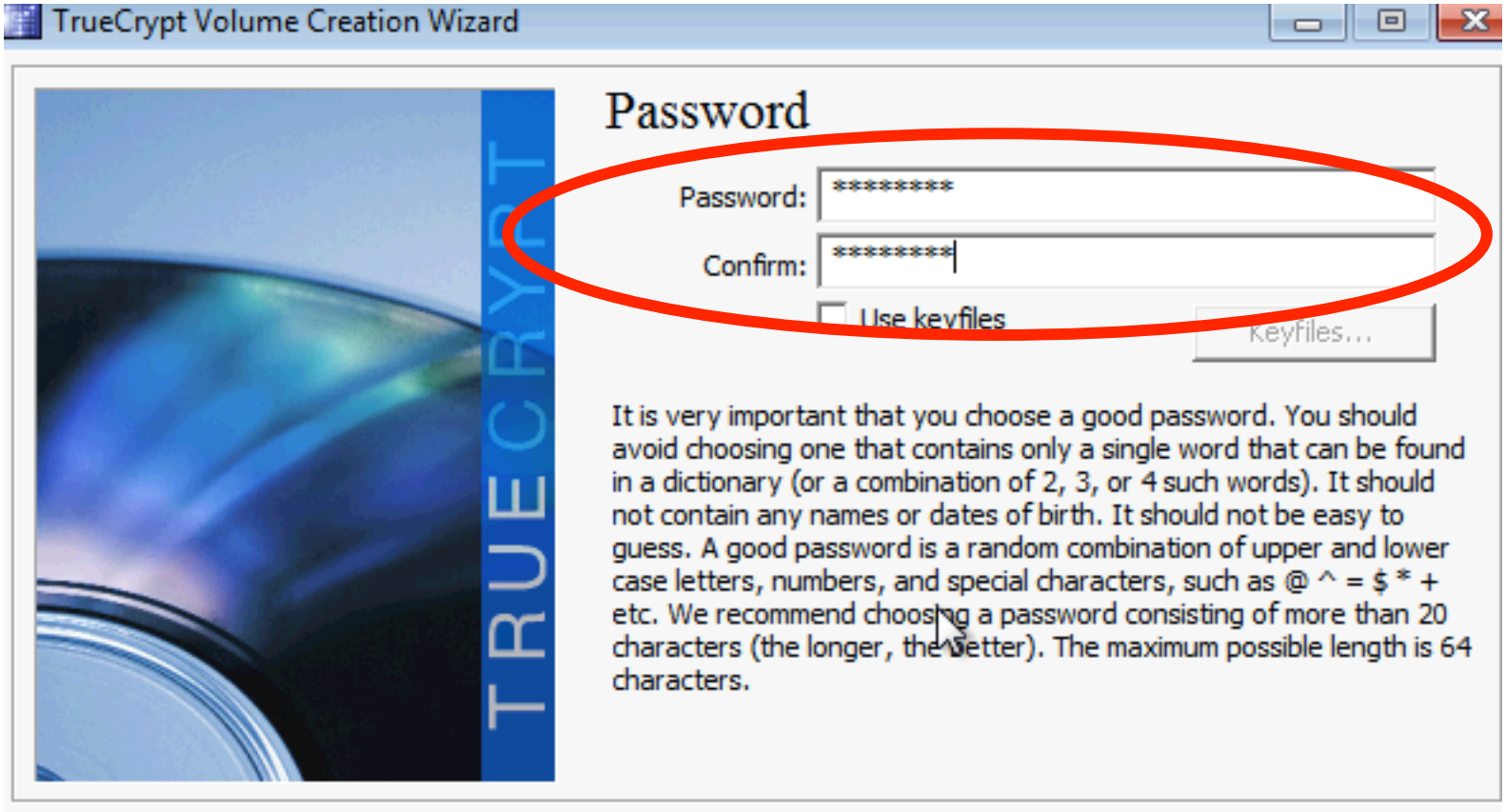
Procédure : Chiffrement du disque



Procédure : Chiffrement du disque

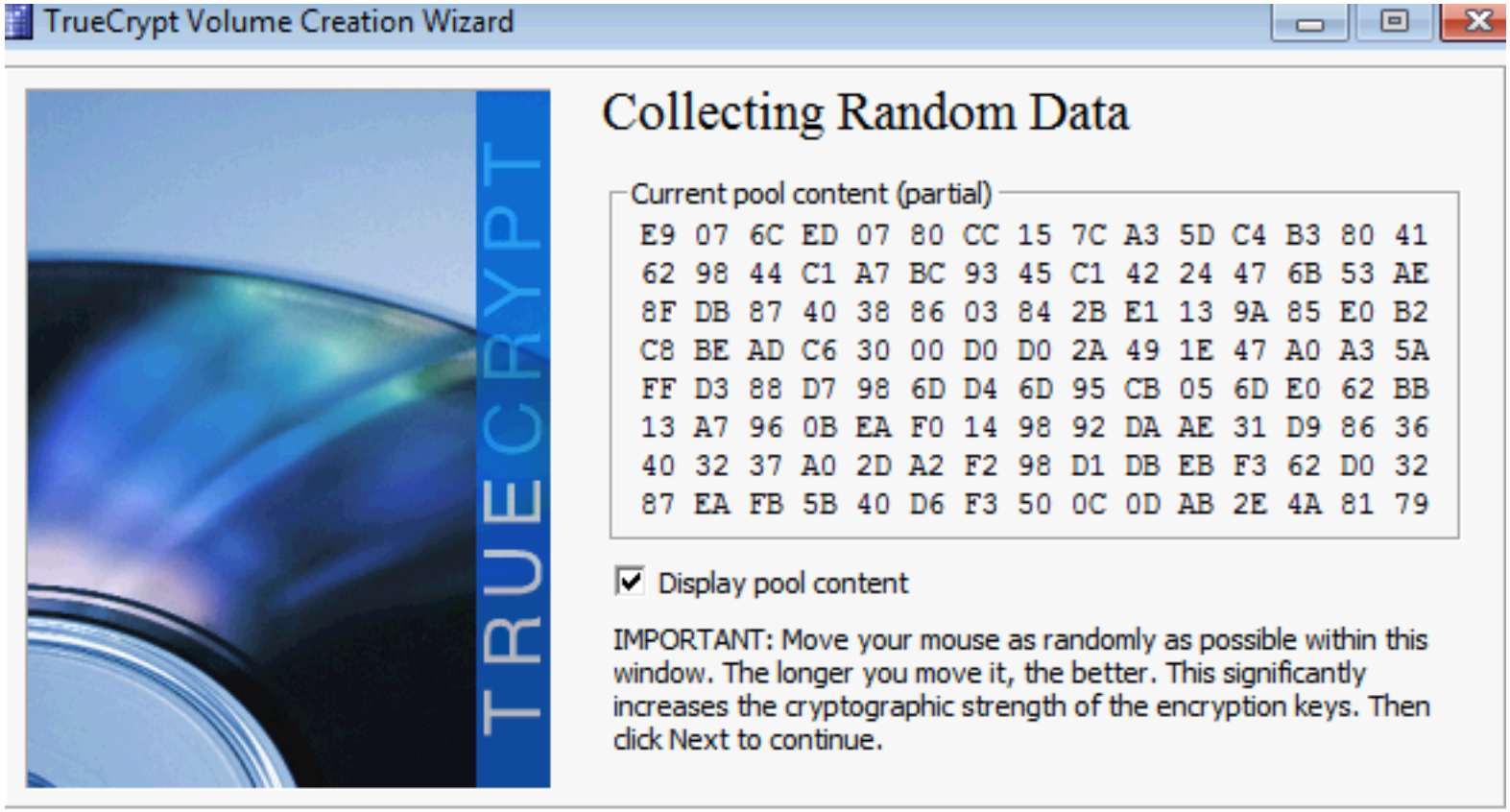


Procédure : Chiffrement du disque

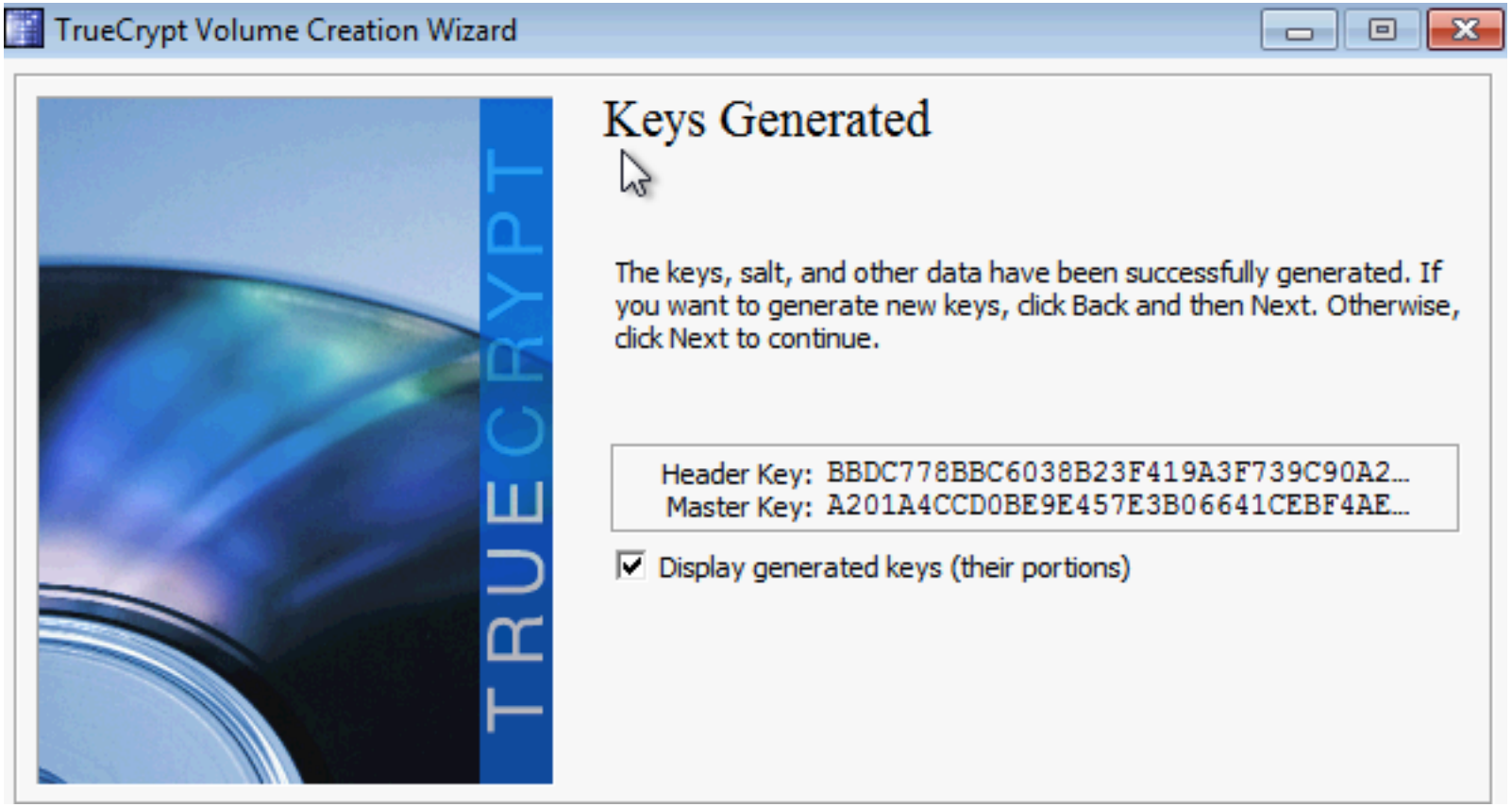


Mot de passe à donner à bien noter et à donner à l'utilisateur

Procédure : Chiffrement du disque



Procédure : Chiffrement du disque



Procédure : Chiffrement du disque

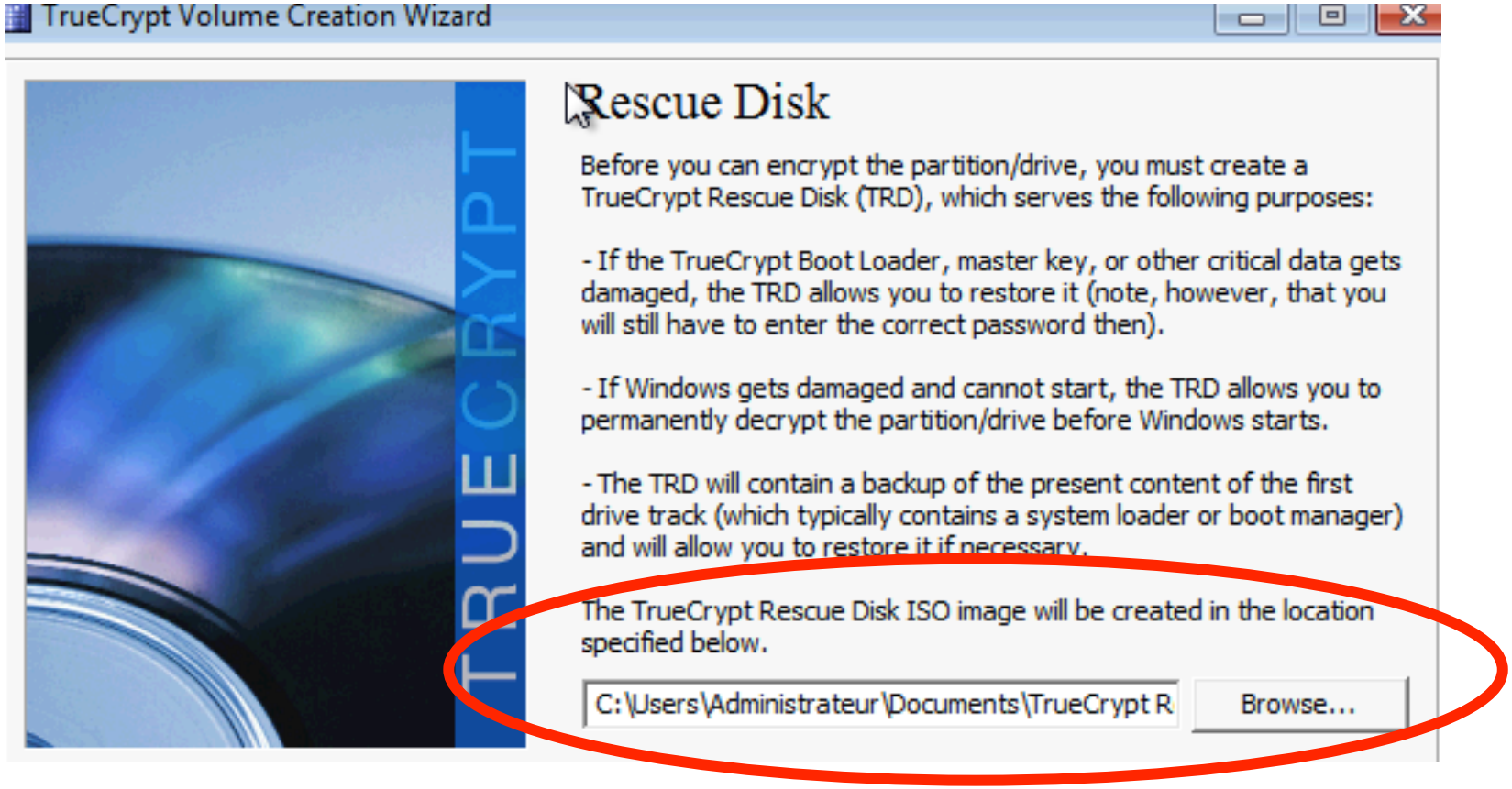
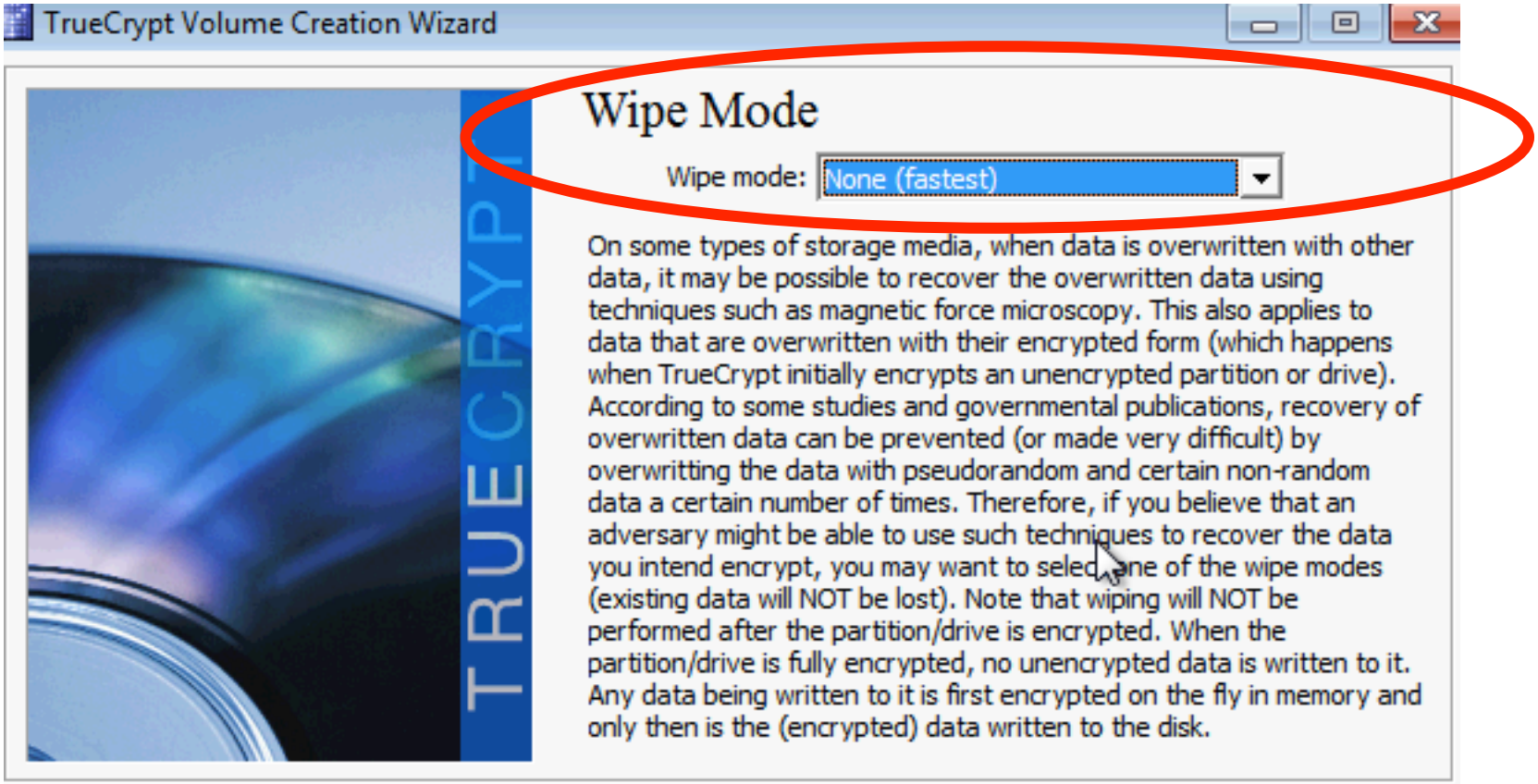


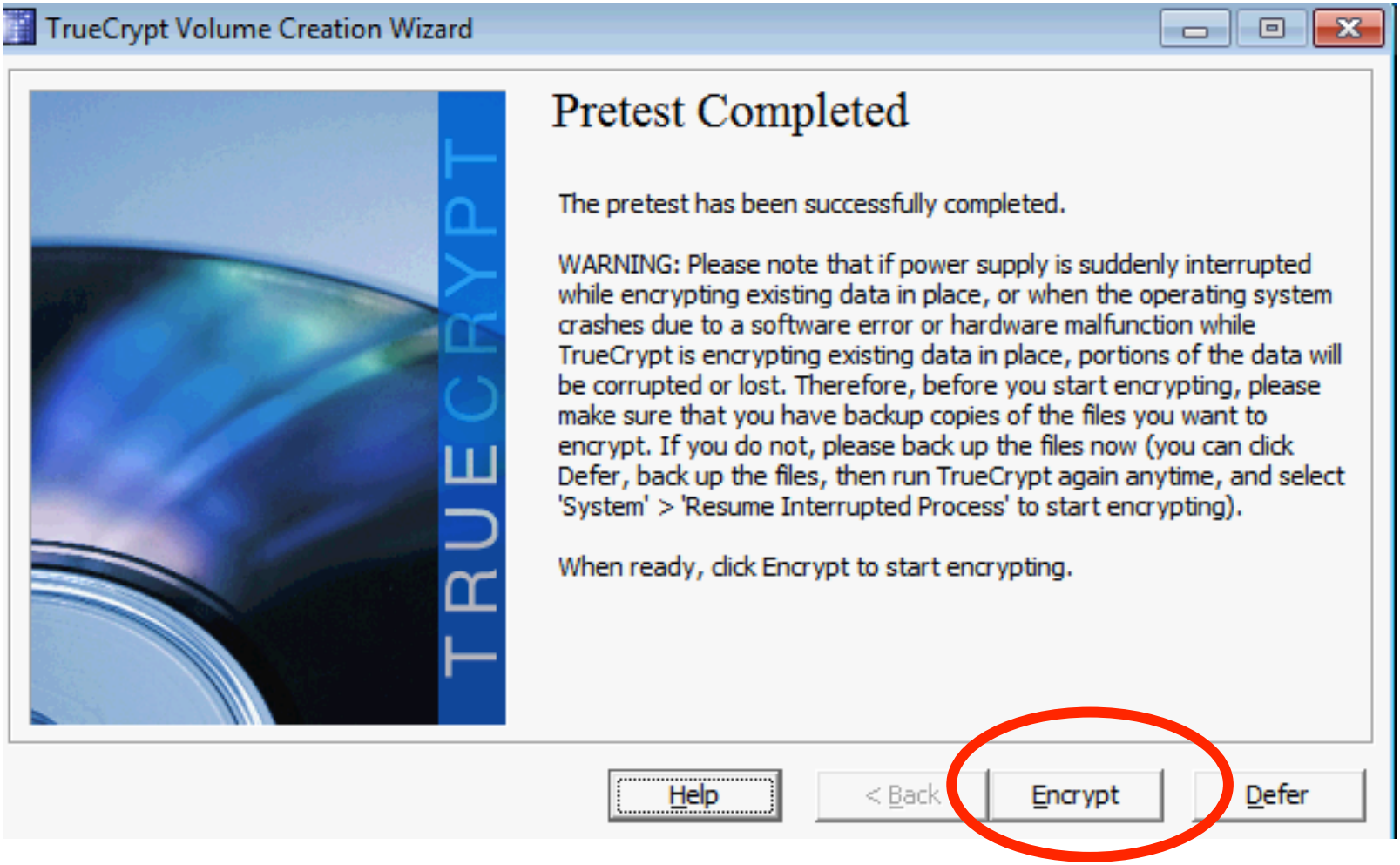
Image ISO à sauvegarder tout de suite sur un autre support

Procédure : Chiffrement du disque

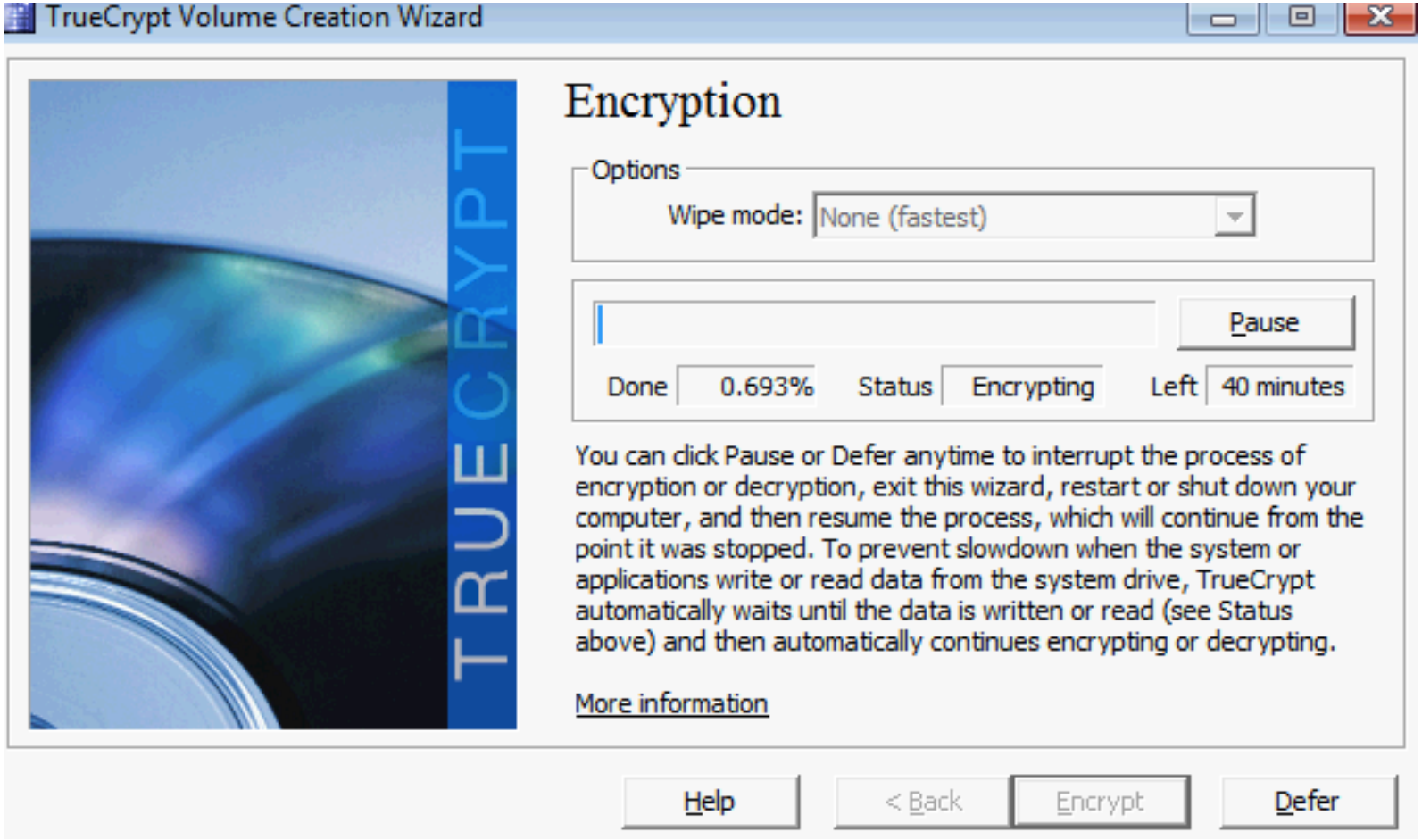


Redémarrage après cela

Procédure : Chiffrement du disque



Procédure : Chiffrement du disque



C'est parti pour quelques heures

Procédure : Séquestre

- On conserver les informations nécessaires au recouvrement dans le séquestre sécurisé

- L'identifiant de la machine
- Le mot de passe
- Le fichier iso du disque de recouvrement (1,8Mo)
  - programme de recouvrement
  - copie TrueCrypt Boot Loader
  - clef maître de chiffrement

- Le fichier ISO sans le mot de passe ne donne aucun droit
  - Ne quand même pas laisser trainer ce fichier !

Recouvrement

- Le plus simple : **mot de passe oublié**
  - Mot de passe sauvegardé précédemment
- **Mot de passe changé et oublié**
  - Démarrer sur le « TrueCrypt Rescue Disk » (image iso sauvegardée)
  - Restaurer la clef maître
- Si le **MBR est abimé**
  - Démarrer sur le « TrueCrypt Rescue Disk » (image iso sauvegardée)
    - Restaurer le MBR
    - Ou Restaurer la clef maître
- **Ordinateur HS**
  - Brancher le disque sur un autre ordinateur et démarrer dessus si ça marche
  - Sinon le monter sur un autre ordinateur où TrueCrypt est installé
  - Sinon restaurer la sauvegarde.
    Parce que vous avez sauvegardé vos portables chiffrés bien sûr.
- **Ordinateur HS et Disque SSD**
  - Restaurer la sauvegarde.
    Parce que vous avez sauvegardé vos portables chiffrés bien sûr.

DmCrypt : Techno

- Device mapper : gestionnaire de devices en mode bloc (disques, partitions) virtuels
- LVM2 : Logical Volume Manager (v2) : gestionnaire de partitions logiques basée sur device mapper
- dm-crypt : chiffrement de devices virtuels en mode bloc
- LUKS : Linux Unified Key Setup : standard de gestion du chiffrement

- **Chiffrement à l'installation de la machine**

DmCrypt : Installation

- Choisir l'installation sur un disque avec volume LVM chiffré
- Spécifier une phrase secrète administrateur **(Séquestre)**
- Après le premier reboot, créer une copie de sauvegarde de l'entête du volume **(Séquestre)**
- Définir une phrase secrète additionnelle pour l'utilisateur

- Commande : *cryptsetup*
  - Permet de faire les différentes manipulations nécessaires

DmCrypt

[!!] Partitionner les disques

Le programme d'installation peut vous assister pour le partitionnement d'un disque (avec plusieurs choix d'organisation). Vous pouvez également effectuer ce partitionnement vous-même. Si vous choisissez le partitionnement assisté, vous aurez la possibilité de vérifier et personnaliser les choix effectués.

Si vous choisissez le partitionnement assisté pour un disque complet, vous devrez ensuite choisir le disque à partitionner.

Méthode de partitionnement :

- Assisté - utiliser un disque entier
- Assisté - utiliser tout un disque avec LVM
- Assisté - utiliser tout un disque avec LVM chiffré
- Manuel

<Revenir en arrière>

DmCrypt : Recouvrement

- Avec la phrase secrète de l'admin
  - Si l'utilisateur a oublié la sienne :
    - Démarrer la machine avec la phrase secrète admin
    - Supprimer le slot correspondant à la clef oubliée (luksKillSlot)
    - Créer une nouvelle phrase secrète (luksAddKey)

- Restauration de l'entête
  - si la clé secrète de l'admin a été supprimée ou si l'entête de chiffrement est vérolée...
    - connecter le disque à une autre machine
    - restaurer l'entête à partir de la sauvegarde avec
    - luksHeaderRestore

File Vault 2

- Prérequis : Mac OS X 10.7 (Lion) ou 10.8 (Mountain Lion)
- Références :
  - https://aresu.dsi.cnrs.fr/IMG/pdf/CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1-0.pdf
  - http://support.apple.com/kb/HT4790
  - Chiffrement XTS-AES-128
- Peut être activé sur une machine déjà installée
- Nécessite la partition cachée de récupération
- Les clefs de chiffrement/déchiffrement sont liés à des comptes utilisateurs, sauf pour la clef principale de recouvrement

File Vault 2 : Installation

- Interface graphique ou ligne de commande sur 10.8 (plus fun)

- **Chiffrement :** Fdsetup
  - *fdesetup enable –user <admin>*
  - Active le chiffrement
  - Génère une clef de recouvrement à conserver (**Séquestre**)

  - Rajouter un utilisateur autorisé à déchiffrer
    - fdesetup add –usertoadd <user>

- Le déchiffrement et le login s'enchainent automatiquement

File Vault 2 : Recouvrement

- Si perte du mot de passe utilisateur
  - Démarrer la machine avec le compte d'admin
  - Changer le mot de passe de l'utilisateur
- Si perte du mot de passe administrateur
  - Avec la clef de recouvrement de la machine
  - au boot, après 3 tentatives de mot de passe infructueuse
  - cliquer sur le triangle jaune, le prompt de la clef apparaît
- Si la machine est cassée
  - Monter la machine ou le disque en « target » sur un autre Mac sous le même OS
  - Utiliser le mot de passe administrateur ou la clef de recouvrement

Autres supports

- Supports amovibles
  - Containers TrueCrypt
- Windows 8
  - BitLocker pour la version professionnelle
- Android et IOS
  - Chiffrement intégré
- Machines en veille
  - Elles sont déchiffrées et le contenu est accessible

Bilan Chiffrement

- 35 postes chiffrés
  - Les nouvelles machines le sont systématiquement
- Pas de ralentissement notable remarqué
- Utilisateurs satisfaits de la simplicité d'utilisation

Protéger les données nomades

- Sur les portables
  - Sauvegarde
  - Chiffrement
- Sur les supports amovibles
  - Pas de version principale sur ces supports
  - Pas de données sensibles
- Cloud public
  - Pas de données sensibles
  - Uniquement des copies
- Cloud privé (chez nous)
  - Sauvegardé et sécurisé