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
1.1	28/06/2012	François Morris	Intégration des retours, MacOS X Lion, nouveaux
			modèles Dell

Classification	Diffusion CNRS
Référence	manuel.docx
Version	1.1
Date	28/06/2012

Table des matières

Introduction	5
Séquestre et recouvrement	7
Mise en garde	7
Définitions	7
Séquestre d'un mot de passe d'un disque chiffrant	7
Séquestre du mot 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	3
Utilisation des outils de chiffrement	Э
Utilisation d'un disque chiffrant sous Windows10	C
Premier démarrage du PC chiffré10	C
Démarrage du PC chiffré1	1
Oubli du mot de passe14	4
Démarrage de Windows avec un disque système chiffré avec TrueCrypt	5
Utilisation de FileVault sous MacOS X10	6
Création d'un conteneur TrueCrypt sous Mac OS X1	7
Création d'un conteneur (volume) chiffré1	7
Séquestre	3
Utilisation d'un conteneur TrueCrypt Mac OS X 24	4
Montage d'un conteneur (volume) chiffré24	4
Utilisation d'un disque chiffrant sous Linux	C
Démarrage du PC chiffré	C
Changement de mot de passe	0
Oubli du mot de passe	C
Démarrage avec dm-crypt sous Linux	1
Clé USB Corsair Padlock 2	2
Recommandations	2
Initialisation	2
Utilisation	2

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
Parcours pour chiffrer un portable DELL avec disque chiffrant	56
Réception du portable	56
Outil de chiffrement	56
Mise en œuvre	56
Remarques importantes	56
Initialisation d'un disque chiffrant sous Windows	58
Introduction	58
Informations de recouvrement	58
Installation	58
Création d'un utilisateur	65
Installation de TrueCrypt sous Windows	69
Récupération du logiciel	69
Installation de TrueCrypt	69
Installer le français	72
Chiffrement d'un disque système sous Windows à l'aide de TrueCrypt	73
Recommandations	73
Chiffrement du disque système	73
Séquestre	87
Utilisation	87

	Activation du chiffrement sous MacOS X	89
	Chiffrement intégral du disque (Lion)	89
	Chiffrement du répertoire utilisateur	100
	Séquestre	106
	Installation de TrueCrypt sous Max OS X	107
	Récupération du logiciel	107
	Installation de TrueCrypt	107
	Disque chiffrant sous Linux	111
	Généralités	111
	Installation d'une machine en dual boot Windows / Linux	111
	Installation d'une machine sous Linux seul	112
	Chiffrement du système avec dm-crypt sous Linux	113
	Installation de Linux sur une partition chiffrée	113
	Sauvegarde de l'en-tête	114
	Installation de TrueCrypt sous Linux	115
	Installation de TrueCrypt	115
	Modification du fichier /etc/sudoers	115
F٨	AQ	117
	Que faire si le disque tombe en panne ?	117
	Quid des clés USB avec empreinte digitale ?	118
	Pourquoi la mise en veille est-elle désactivée ?	118
	Quelle est la différence entre la protection offerte par un disque chiffrant et un disque v par un mot de passe au BIOS ?	verrouillé 118
	Qu'apportent les nouvelles instructions AES ?	118
	Comment savoir si la machine possède un disque chiffrant ?	119
	Que faire si le mot de passe a été compromis ?	119
	Connexion d'un disque chiffrant externe	119

Introduction

La <u>note</u> 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 <u>PDF</u> ou de <u>pages web</u>.

Il existe une liste <u>chiffrement@services.cnrs.fr</u> 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 <u>https://listes.services.cnrs.fr/wws/subscribe/chiffrement</u>

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 débloquer 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 de 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 débloquer 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'entête. 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 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 <u>installé</u> par une personne possédant les privilèges administrateur.

Lancez TrueCrypt

$\bigcirc \bigcirc \bigcirc \bigcirc$	True	eCrypt		
Slot Slot 1 2 3 4 5 6 7 8 9 10 11 2 12	Volume	Size	Mount Directory	Type
Volume	Never save history	Properties Volu	Wip Sele ume Tools) Select	ct File Close

Cliquez sur « Create Volume »



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



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

000	Specify a New TrueCrypt Volu	me
	Save As: conteneur	
	Where: Documents	•
	Format: All Files	
	Format: All Flies	
		Cancel Save

Choisissez un fichier et cliquez sur « Save »



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

Tru	eCrypt Volume Creation Wizard
	Encryption Options Encryption Algorithm AES Test
	FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.
	More information on AES Benchmark Hash Algorithm
	RIPEMD-160
	? < Prev Next > Cancel

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

Image: Optimized system TrueCrypt Volume Creation Wizard	
	SOQ MB Free space available: 13.1 GB Please specify the size of the container to create. Note that the minimum possible size of a volume is 292 KB.
	(?) (< Prev Next >) (Cancel

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

😝 🕤 🔿 TrueC	Crypt Volume Creation	Wizard
	Volume Passw	vord
	Confirm password:	
		Display password
		Use keyfiles Keyfiles
TRUEO	It is very important should avoid choos that can be found in or 4 such words). It of birth. It should n a random combinat numbers, and speci We recommend cho than 20 characters possible length is 6	that you choose a good password. You ing one that contains only a single word n a dictionary (or a combination of 2, 3, should not contain any names or dates ot be easy to guess. A good password is ion of upper and lower case letters, ial characters, such as $@^{= $ * + etc. posing a password consisting of more (the longer, the better). The maximum 4 characters.
		? < Prev Next > Cancel

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

Image: Second system TrueCrypt Volume Creation Wizard	
	Filesystem Options Filesystem type: FAT Volume Format Options Quick format In order to enable your operating system to mount your new solume, it has to be formatted with a filesystem. Please select a filesystem type. If your volume is going to be hosted on a device or partition, you can use 'Quick format' to skip encryption of free space of the volume.
	(?) < Prev Next > Cancel

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 >** »

True True	eCrypt Volume Creation Wizard
	Volume Format
	Random Pool: 073AD2FDF3BE655D561B6DF768 Show Header Key: Master Key:
U CONTRA CO	Abort
ш	Done Speed Left
TRU	IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
	? < Prev Format Cancel

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

The TrueCrypt volume has been successfully created.
ОК

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 <u>séquestre</u> 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

$\bigcirc \bigcirc \bigcirc \bigcirc$		TrueCrypt		1
Slot A 1 2 3 4 5 6 7 8 9 10 11 12	Volume	Size	Mount Directory	Type
Creat	e Volume V	olume Properties) (Volu evices) Dismo	me Tools) Sele	/ipe Cache

Cliquez sur « Select File ... »

ot 🔺 Volume			Size	Mount Directory	Type
		Select a TrueC	rypt Volum	e	
	Enable: All	Files		•	
		Documents		¢ searc	ih
Réseau		📄 conteneu	ır		
Macintos	sh HD 📃 🕨				
NO NAM	E 🔺 🕨				
Bureau	Þ				
fmo					
À Applicat	ions				- 11
Docume	nts 🕨			Name cont	eneur
Séquenc	es			Size 500	MB
6 Musique		11		Kind Doc	ument av at II
Images			(
New Fol	der			Cancel O	pen
	Υ	Υ	_	Ý	

Choisissez le fichier et cliquez sur « Open »

00 TrueCrypt Slot 🔺 Volume Size Mount Directory Type $\cong 1$ 🥯 2 🥯 3 ₽4 5 6 7 8 9 10 🥯 11 * 🥯 12 Create Volume Volume Properties... Wipe Cache Volume Select File... ÷ 🗹 Never save history Volume Tools... Select Device... Mount Mount All Devices Dismount All Close

Utilisation d'un conteneur TrueCrypt sous Mac OS X

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

😝 🔿 🔿 Enter password for "/Users/fmo/Documents/conteneur"				
Password:	•••••		ОК	
	Cache passwords and key	files in memory	Cancel	
	Display password			
	🗌 Use keyfiles	Keyfiles) O	ptions >	

Entrez le mot de passe et cliquez sur « OK »

Désormais un nouveau disque (NO NAME) est visible



Il est utilisable comme un disque classique.

$\Theta \Theta \Theta$	NO NAME	0
	Q.	
💮 Réseau		
Macintosh HD		
NO NAME 🔺		
NO NAME 🔺		
🔢 Bureau		
fmo í		
Applications		
Documents		
Séquences		
🎸 Musique		
💼 Images		
	Aucun élément, 497,8 Mo disponibles	11.

Démontage d'un conteneur (volume) chiffré

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

00	True	Crypt			
Slot 🔺	Volume	Size	Mount Directory	Туре	
● 1	/Users/fmo/Documents/conteneur	499 MB	/Volumes/NO NAME 1	Normal	
🥯 2					
🥯 3					
🥯 4					
S 🥯					
96					
97					
S 🛸					
9					
✓ 10					
Se 12					
(Create Volume Properties) (Wine Cache					
/olume		operties		be cache	
-0004	/Users/fmo/Documents/conteneur		Sele	ct File	
	Never save history	Volu	me Tools) Selec	t Device	
D	ismount Mount All Devices	Dismo	ount All	Close	

Utilisation d'un conteneur TrueCrypt sous Mac OS X

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

00	1	FrueCrypt		
Slot 🔺	Volume	Size	Mount Directory	Type
● 1				
🥯 2				
🥯 3				
≪ 4				
S				
96				
[™] 7				
™ 8				
9				
10				
Se 11				
· •• 12				
Creat	e Volume Volum	ne Properties)		Wipe Cache
/olume				
-	/Users/fmo/Documents/conteneu	r	•	Select File
	Never save history	Volu	ume Tools S	elect Device
	Mount All Device	s) Dismo	ount All	Close

Utilisation d'un conteneur TrueCrypt sous Mac OS X

Cliquer sur « Close »

Utilisation d'un disque chiffrant sous Linux

Le disque chiffrant doit avoir préalablement <u>initialisé</u> sous Windows par un administrateur.

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 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

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 donnés 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 fabriquant <u>http://www.corsair.com</u>

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 lez code PIN pour vérification.
- 5. Appuyez sur la touche marquée d'une clé et la relâcher 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 tpouche marquée d'une clé et relâcher 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 relâcher 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 lez code PIN pour vérification.
- 7. Appuyez sur la touche marquée d'une clé et la relâcher 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 clé 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 <u>installé</u> par une personne possédant les privilèges administrateur.

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

Assistant de création de volume True	rypt
	Assistant de création de volume
	Create an encrypted file container Crée un disque virtuel chiffré dans un fichier. Recommandé pour los utilizateurs pourses
	Plus d'infos
	C Encrypt a non-system partition/drive
	Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.
	C Chiffrer la partition ou l'intégralité du disque système
	Chiffre la partition/le disque où est installé Windows. Qui veut accéder au système, lire/écrire des fichiers, etc., devra entrer le bon mot de passe à chaque fois que Windows démarre. Crée un système caché (optionnel).
	Plus d'infos sur le système de chiffrement
	Aide < Précédent Suivant > Annuler

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

Assistant de création de volume TrueCryp	ot 🗖 🗖 💌
	Type de volume
	 Volume TrueCrypt standard Sélectionnez cette option si vous voulez créer un volume TrueCrypt normal.
TRUECH	Volume TrueCrypt caché Il se peut que vous soyez forcé par quelqu'un de révéler votre mot de passe. Il y a des situations où vous ne pouvez pas refuser de divulguer le mot de passe (ex: par une extorsion). L'utilisation d'un volume caché vous permet de résoudre de telles situations sans donner le mot de passe de votre volume. <u>Plus d'infos sur les volumes cachés</u>
	Aide < Précédent Suivant > Annuler

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

Assistant de création de volume TrueCr	ypt
	Emplacement du volume C:\Users\fmo\Documents\Conteneur Fichier Ne jamais enregistrer l'historique A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.
TBU	WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.
	Aide < Précédent Suivant > Annuler

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

Assistant de création de volume TrueCo	rypt
CBXP1	Algorithme de chiffrement Algorithme de chiffrement AES Tester Algorithme cryptographique (Rijndael, publié en 1998) approuvé par la FIPS, qui peut être utilisé par les agences/départements fédéraux américains pour protéger cryptographiquement les informations sensibles. Clé à 256 bits, bloc de 128 bits, 14 rondes (AES-256). Le mode opératoire est XTS.
TRUE	Plus d'infos sur AES Benchmark Algorithme de hachage Infos : algorithmes de hachage RIPEMD-160 Infos : algorithmes de hachage Aide < Précédent Suivant > Aide < Précédent Suivant >

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

Assistant de création de volume TrueCrypt	
	Taille du volume 100 C Ko Mo GB Free space on drive C:\ is 195.06 GB Please specify the size of the container you want to create. If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size. Note that the minimum possible size of a FAT volume is 292 KB. The minimum possible size of an NTFS volume is 3792 KB.
	Aide < Précédent Suivant > Annuler

Choisir une taille de volume et cliquer sur « Suivant > »
Assistant de création de volume TrueCrypt			
Mot Mot Il est t devrie diction devra pas êt de mir comme passe maxim	t de passe: ** Confirmer: ** Confirmer: ** très important ez éviter d'utilis nnaire (ou une it pas contenir tre facile à dev nuscules et de e @ ^ = \$ * + e d'au moins 20 nale est de 64 o	e du volume	Fichiers clé,., on mot de passe. Vous trouve dans un de ces mots). Il ne laissance. Il ne devrait e est une combinaison de caractères spéciaux e choisir un mot de e mieux). La longueur
	Aide	< Précédent Suiva	ant > Annuler

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

Assistant de création de volume TrueCr	ypt
	Formatage du volume Options Système FAT ▼ Cluster Défaut ▼ Dynamique Nb aléatoire: F0E0292D20E3E270E47CFA82DA393C51 ▼ Clé d'en-tête: Clé principale: Important: Déplacez votre souris dans cette fenêtre aussi aléatoirement que possible. Plus longtemps vous la bougez, mieux c'est. Cela accroît significativement la force cryptographique des clés de chiffrement. Puis cliquez sur 'Formater' pour créer le volume. Aide < Précédent Eormater Quitter

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 »



Cliquer sur «OK »

Assistant de création de volume TrueCr	ypt
	Volume créé
TRUECEVE	Le volume TrueCrypt a été créé et il est prêt à l'emploi. Pour créer un autre volume TrueCrypt, diquez sur 'Suivant'. Sinon 'Quitter'.
	Aide < Précédent Suivant > Quitter

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 <u>séquestre</u> 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.

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... »

TrueCrypt	
Volumes Système Favorites <u>O</u> utils <u>P</u> aramètres <u>A</u> ide	<u>S</u> ite Web
Le Volume Taille Algorithme de	chiffr Type 🔺
K :	
• • • • • • • • • • • • • • • • • • •	
≪N: ⇔O:	
₩	=
S:	-
V:	
Y:	
See 2:	Ψ
Créer un volume Propriétés du volume	Vider le cache
_ Volume	
C: \Users\fmo \Documents \Conteneur	Fichier
Ne jamais enregistrer l'historique	
Outils pour le volume	Périphérique
Monter Montage automatique Tout démonter	Quitter

Cliquer sur « Monter »

Entrez le mot de passe pour C:\Users\fmo\Documents\Conteneur				
Mot de passe:	*****	*	ОК	
	Mots de passe et fichie	rs dé en cache	Annuler	
	Afficher mot de passe			
	Fichiers dé	Fichiers dé	Options	

Saisir le mot de passe et cliquer sur « OK »

Désormais un nouveau disque (ici X :) est visible

 Disques durs (2) 	
Disque local (C:)	Disque local (X:)
194 Go libres sur 232 Go	98,9 Mo libres sur 98,9 Mo

Il est utilisable comme un disque classique.

				ter, orderes delle	-			x
Colordinat	eur 🕨 Disque local (X:)				▼ + _j	Rechercher dans : Disque	: local (X:)	Q
Organiser 🔻 Inclure	dans la bibliothèque 🔻	Partager avec 🔻	Graver Nouveau do	ossier			•	0
🛧 Favoris	Nom	<u>^</u>	Modifié le	Туре	Taille			
📃 Bureau	📄 Essai.txt		22/02/2011 16:52	Document texte	1 Ko			
Emplacements réce	1							
🌉 Téléchargements								

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.

TrueCrypt	
<u>V</u> olumes Système Favor <u>i</u> tes <u>O</u> utils <u>P</u> aramètres <u>A</u> ide	<u>S</u> ite Web
Le Volume Taille Algorithm	e de chiffr Type 🔨 🖍
Sec: 200 € 100	
Sec.:	
Sec. 10.	
@ 0:	
Sec. 2017	≡
₩V:	
W:	
Y:	Normal
✓ Z:	•
Créer un volume Propriétés du volume	Vider le cache
C:\Users\tmo\Documents\Conteneur	Fichier
✓ Ne jamais enregistrer l'historique Outils pour le volume	Périphérique
Démonter Montage automatique Tout démonter	Quitter

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



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

TrueCrypt				x
<u>V</u> olumes S <u>v</u> stème Favor <u>i</u> tes	<u>O</u> utils <u>P</u> aramé	ètres <u>A</u> ide	<u>S</u> ite	e Web
Le Volume I: J: K: L: M: N: O: R: S: Volume		Taille A	Algorithme de chiffr Type	III III
V: W: X: Y: Z: Créer un volume	Propriét	és du volume	Vider le cache	•
Volume C:\Users\fmo\Docu	uments\Conteneur istrer l'historique	Outils pour le vol	Fichier Fichier Périphérique	
Monter	itage automatique	Tout démor	Quitter	

Cliquer sur « Quitter »

Création d'un conteneur TrueCrypt sous Linux

Introduction

Le logiciel TrueCrypt doit avoir préalablement été <u>installé</u> par une personne possédant les privilèges administrateur.

Les différentes opérations peuvent aussi s'effectuer à partir de lignes de commandes. Nous ne décrirons 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

				TrueC	rypt			(-×
Volume	s Favorites	Tools	Settings	Help					
Slot	Volume				Size	Mount Directo	ory	Туре	
🥪 1									
2									Ξ
S = 0									
i 6									
🧼 8									
🥪 9									
10									
11									
· 12									-
Crea	te Volume		V	olume P	properties		Wipe	e Cache	
Volume									
11112						~	Selec	t File	
	Volume Tools Select Device								
	Mount	Aut	o-Mount D	Devices	Dism	ount All	E	Exit	

Sélectionnez « Tools » \rightarrow « Volume Creation Wizard ».



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

TrueCr	ypt Volume Creation Wizard	
	Volume Type	
	Standard TrueCrypt volume	
	Select this option if you want to create a normal TrueCrypt volume.	
	O Hidden TrueCrypt volume	
TRUEC	It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example due to extortion). Using a so-called hidden volume allows yo to solve such situations without revealing the password to yo volume. <u>More information about hidden volumes</u>	e s e, u bur
	Aide < Prev Next > Annu	uler

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

TrueCi	rypt Volume Creation Wizard			
	Volume Location			
	/home/fm/Documents/Conteneur			
	✓ Never save history			
С С С С С С С	A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.			
TRU	WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.			
	Aide < Prev Next > Annuler			

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

TrueCry	pt Volume Creation Wizard	
	Encryption Options	
	AES	Test
E C B V	FIPS-approved cipher (Rijndael, published in 1998) used by U.S. government departments and agencie classified information up to the Top Secret level. 25 bit block, 14 rounds (AES-256). Mode of operation i	that may be es to protect 56-bit key, 128- is XTS.
	More information on AES	Benchmark
L L		
	Hash Algorithm	
	RIPEMD-160 Information on	hash algorithms
	Aide < Prev Next >	Annuler

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

TrueCi	rypt Volume Creation Wizard	
	Volume Size	
	500 MB \$	
	Free space available: 20,1 GB	
6	Please specify the size of the container to create. Note that the minimum possible size of a volume is 292 KB.	
ш		
E C		
	Aide < Prev Next > Annu	ller

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

TrueCi	ypt Volume Creation Wizard
TrueCr	ypt Volume Creation Wizard Volume Password Password: Password: Output Onfirm password: Display password Use keyfiles Keyfiles It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = \$* + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.
	Aide < Prev Next > Annuler

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

TrueCry	pt Volume Creation Wizard
	Filesystem Options Filesystem type: FAT Volume Format Options Quick format In order to enable your operating system to mount your new volume, it has to be formatted with a filesystem. Please select a filesystem type. If your volume is going to be hosted on a device or partition, you can use 'Quick format' to skip encryption of free space of the volume.
	Aide Annuler

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** > ».

TrueCi	ypt Volume Creation Wizard
	Volume Format
	Random Pool: B50C8A0576E5ED862709ED1829 Show Header Key: Master Key:
	Abort Done Speed
TRU	IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
	Aide < Prev Format Annuler

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

	TrueCrypt 🛛 🗙
9	The TrueCrypt volume has been successfully created.
	Valider

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 <u>séquestre</u> 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.

				TrueC	rypt			(-×
Volume	s Favorites	Tools	Settings	Help					
Clat					c '			-	
Slot	volume				Size	Mount Direct	ory	Туре	_
🧠 1									_
i 2									≡
i i i i i i i i i i i i i i i i i i i									
S									
6									
· /									
S									
9									
- 10 - 11									
- 12									
· 12									\checkmark
Crea	te Volume		V	olume P	roperties		Wip	e Cache	
Volume						×			
	(hanse (free	Decum	anta/Cant				Colo	ct Filo	
	/nome/im/	Docum	ents/Cont	eneur			Sele	ct rile	
	Never s	ave his	tory		Volu	me Tools	Select	Device	
(
	Mount	Aut	o-Mount [Devices	Dism	ount All		Exit	

Cliquez sur « Mount »

📳 Enter p	assword for "/home/fm/Té	léchargements,	/grub-0.97 🗙
Password:	•••••		Valider
	Cache passwords and key	files in memory	Annuler
	Display password	8	
	Use keyfiles	Keyfiles	Options >

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

				TrueC	rypt	2			- X
Volume	s Favorites	Tools	Settings	Help		20			
								_	
Slot	Volume				Size	Mount Direct	ory	Туре	
🧠 1	/home/fm/Do	ocumer	its/Conten	eur	499 MB	/media/truecr	ypt1	Normal	
🧼 2									≡
i i i i i i i i i i i i i i i i i i i									
i 4									
i i i i i i i i i i i i i i i i i i i									
 									
le 7									
8									
i 9									
10									
11 w									
· 12									~
Crea	te Volume		[V	olume P	roperties		Wip	e Cache	
Volume									
	/home/fm/	Docum	ents/Cont	eneur			Sele	ct File	
				erreur					
	✓ Never s	ave his	tory		Volu	me Tools	Select	Device	
	ismount	Aut	o-Mount [Devices	Dism	ount All		Exit	

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

8					t	ruecry	pt1	- Na	nviga	teur	de f	ichi	ers					E	.ox)
Fichier	Édition	Affic	chage	Aller	à	Signet	5 A	ide											
🕼 Pré	cédent	Y °	📎 Suiv	/ant	Ý	\$a		C			5		100%	¢	Vue er	icônes	•	Q	
<	truecry	pt1																	
										*									
0 éléme	nt, espac	e libre	e : 497	,8 Mic)														

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.

Utilisation d'un conteneur TrueCrypt sous Linux

ŧ.				TrueC	rypt 📐				_0
Volume	s Favorites	Tools	Settings	Help	~				
Slot	Volume				Size	Mount Direct	ory	Туре	
a 1	/home/fm/Do	ocumen	ts/Conter	neur	499 MB	/media/truecr	ypt1	Normal	^
🧼 2									
i i i i i i i i i i i i i i i i i i i									
🥪 4									
iii 😳 5									
🧼 6									
li 😳 😳									
li 😳									
🧼 9									
🧼 10									
I1 🥪									
🧼 12									~
Crea	te Volume		N	/olume P	roperties		Wip	e Cache	
Volume									
-005	/home/fm/	Docum	ents/Cont	teneur		<pre></pre>	Sele	ct File	
✓ Never save history Volume Tools Select Device									
D	ismount	Aut	o-Mount I	Devices	Dism	ount All		Exit	

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

i i				TrueC	rypt			(-×
Volume	s Favorites	Tools	Settings	Help					
Clot	Volumo				Sizo	Mount Direct		Tupo	
SIOL	volume				SIZE	Mount Direct	JIY	type	
See 1									
See 2									≡
S 1									
- 6									
~ 7									
· 8				×.					
a 9									
i0									
a 11									
12									~
Cros	to Volumo		5		rapartias		Win	o Cacha	
Clea	te volume			olume P	ropercies		U VVI	e cache	
Volume									
-005	/home/fm	/Docum	ents/Cont	eneur		~	Sele	ct File	
	✓ Never s	ave his	tory		Valu	mo Tools	Colect	Douise	
			2		Volu	ine loois	Select	Device.	
][_
	Mount	Aut	o-Mount [Devices	Dism	ount All		Exit	

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

Parcours pour chiffrer un portable DELL avec disque chiffrant

(S. Accettella, P. Mora de Freitas – SSI/Paris B – juin 2012)

Réception du portable

Vérifier si le disque dur installé dans la machine est bien un disque chiffrant (plusieurs cas d'erreur de fabrication constatés). En cas de doute, appeler le SAV de Dell et, le cas échéant, réclamer auprès du commercial le remplacement du disque.

Outil de chiffrement

Assez souvent l'outil de chiffrement ne vient pas installé d'usine. Dans ce cas, le télécharger sur le site de DELL et l'installer. Dans sa version actuelle il faut installer :

- Data protection (sensiblement similaire à l'ancien Dell Control Point)
- Driver Data protection

Mise en œuvre

Puisque Dell change assez souvent d'outil de chiffrement et de version, une documentation détaillée serait rapidement obsolète. Néanmoins leurs fonctionnements sont très similaires, on se retrouve rapidement avec d'autres versions ou produits adoptés par Dell. Voir la <u>version antérieure</u> du logiciel Dell.

Remarques importantes

• Penser à Activer dans le BIOS la puce TPM, si besoin (taper F2 au démarrage) :

Votre PC contient une puce de sécurité spéciale appelée Trusted Platform Module ou TPM. Pour continuer, vous devez l'activer ou la mettre sous tension via le programme de configuration BIOS de l'ordinateur.

Exemple d'activation d'une puce TPM via le programme de configuration BIOS d'un ordinateur* :

- Redémarrez l'ordinateur et entrez dans le programme de configuration système en appuyant sur [F2] au démarrage (ou pendant le processus d'autocontrôle à la mise sous tension).
- Dans le programme de configuration, ouvrez la catégorie de paramètres « Security TPM » et sélectionnez l'option de menu.
- 3. Définissez l'état de la sécurité TPM sur « On » ou « Enabled ».
- Quittez le programme de configuration en appuyant sur [Echap] et, à l'invite, sélectionnez «Save / Exit» pour sauvegarder les sauvegarder les modifications.

Appuyez sur Annuler pour quitter et terminer cette étape. Au démarrage, cet assistant redémarre.

*Remarque: il s'agit d'un exemple. Consultez la documentation du fabricant de votre PC pour obtenir des détails spécifiques à votre ordinateur.

- Lors de l'écran de connexion du chiffrement le clavier est en QUERTY. N'utilisez pas le clavier numérique (utiliser le shift) et faites attention à certaines lettres placé ailleurs. (pensez à, si possible utiliser, des mots de passe avec des lettres égales en AZERTY et QWERTY)
- Pour changer le mot de passe il suffit que l'utilisateur aie l'option « pouvoir changer son mot de passe » et faire CTL+ALT+SUPP et changer.
- Si l'option dans le chiffrement est « synchroniser les mots de passe », alors le changement est automatique pour le chiffrement

Attention : pour tester à la fin il faut faire « arrêter » et non « redémarrer »

Initialisation d'un disque chiffrant sous Windows

Introduction

Les logiciels fournis par DELL pour gérer les disques chiffrants change au cours du temps. Lors de la rédaction initiale il s'agissait de *DELL Access Control Point* qui intégrait le produit fourni par WAVE. Aujourd'hui Dell utilise Data Protection. Ce chapitre a été néanmoins conservé pour ceux qui utiliseraient d'anciens modèles.

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 versionn 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 :

- <u>Numérique</u>: 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 apparait :



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



Cliquer sur « Suivant > »

Assistant d'initialisation du lecteu	r Trusted Drive d'Emba	ssy ? X		
Le lecteur Trusted Drive est géré par un administrateur de lecteur. L'administrateur de lecteur peut enregistrer d'autres utilisateurs et peut modifier les paramètres du lecteur et de sécurité utilisateur.				
Entrez le nom d'utilisat passe de l'administrateu	eur désiré, puis créez ır du lecteur.	et confirmez le mot de		
Nom d'utilisateur :	administrateur	Sélectionner		
Domaine/Ordinateur :	DSI			
Mot de passe :	•••••			
Confirmer le mot de passe :				
	<	Précédent Suivant >		

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

Assistant d'initialisation du lecteur	Trusted Drive d'Embassy	? ×
IMPORTANT : Sauf si un utilisate passe adéquat pour déverrouiller verrouillé et tous les accès aux d	eur possède le nom d'utilisateur et le mot de le lecteur Trusted Drive, le lecteur restera onnées sur le disque seront bloqués.	
Afin d'éviter tout risque d'identification de l'adm nécessaires au prochair	de blocage, habituez-vous à entrer les d inistrateur Trusted Drive car elles seront a démarrage du système.	onnées
Nom d'utilisateur :	administrateur	
Domaine/Ordinateur :	DSI	
Mot de passe :		
	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 »

Assistant d'initialisation du lecteur	Trusted Drive d'Embassy				
IMPORTANT : Sauf si un utilisateu passe adéquat pour déverrouiller l verrouillé et tous les accès aux do	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 d d'identification de l'admi nécessaires au prochain	de blocage, habituez-vous à entrer les données inistrateur Trusted Drive car elles seront démarrage du système.				
Nom d'utilisateur :	administrateur				
Domaine/Ordinateur :	DSI				
Mot de passe :					
	Vérifier				
	La vérification a réussi. Appuyez sur Suivant.				
	< Précédent Suivant >				

Cliquer sur « Suivant > »

Assistant d'initialisation du lecteur Trusted Drive d'Embassy
REMARQUE IMPORTANTE : Sauvegardez ou imprimez le nom et le mot passe administrateur du lecteur et conservez-les dans un endroit sûr. Vous aurez ainsi toujours accès au lecteur en cas de perte des informations d'identification.
Il est recommandé de stocker la sauvegarde sur une clé USB et de placer la clé dans un endroit sûr. il est déconseillé de conserver une sauvegarde sur un disque dur.
E:\ Si aucune clé USB n'est disponible, choisissez l'option Imprimer ci- dessous et conservez le document dans un endroit sûr.
Imprimer
< Précédent Terminer >

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 suffisemment 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 »



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

Assistant d'initialisation du lecteur Trusted D	Prive d'Embassy
	
Lecteu	r initialise
	Terminé

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 »

Authentification de l'admir	nistrateur du lecteur	? ×
Spécifiez le nom et le Drive Administrator.	mot de passe de l'ad	ministrateur Trusted
Nom d'utilisateur :	administrateur	Sélectionner
Domaine/Ordinateur :	DSI	
Mot de passe :	*******	
		ОК

nètres avancés Trusted Drive	100 100			10.1	8
Gestion Trusted Drive		5VG8WGQ	G ed Drive —		
Sécurité Trusted Drive	Désinitialiser	Numéro de	série	5VG8WGQG	
Mot de passe de récupération Effacement des données	Sauvegarde	Microprog sécurité	ramme de	SeaCOS 4.0 Build 0	
cryptographiques		Microprogr lecteur	ramme de	DED1	
		Volumes d	u lecteur	C:	
Verrouillage de lecteur		Version du	Preboot	3.3.3.104	
Synchronisation de mots de passe					
Connexion unique					
Utilisateurs Trusted Drive	Domaine	Droits	Alias Tru	isted Drive	
administrateur	DSI		7100 110		
Ajouter un utilisateur	Réinitialiser mot	de passe	Change	r de nom	
				Te	rminá
				101	mine

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.

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

Ajouter un util	isateur de lec	teur Trusted Drive	? <mark>X</mark>
Entrez le n passe.	om d'utilisat	teur désiré, puis créez et co	nfirmez le mot de
Nom d'utilis	ateur :	FMO	Sélectionner
Domaine/O	rdinateur :	DSI]
Mot de pas	se :		
Confirmer I passe :	e mot de	******]
🔽 L'utilisate	eur doit change	er son mot de passe lors de s	sa prochaine connexion.
			Ajouter

Cliquer sur « Ajouter »

On obtient donc,

estion Trusted Drive Sécurité Trusted Drive Mot de passe de récupération Effacement des données cryptographiques	Désinitialiser Sauvegarde Effacer	5VG8WG0 Infos Trus Numéro d Microprog sécurité Microprog lecteur	QG ted Drive e série 5VG8WGQG gramme de SeaCOS 4.0 Build 0 gramme de DED1
Verrouillage de lecteur Synchronisation de mots de passe Connexion unique Mémoriser le nom du dernier utilisateur tilisateurs Trusted Drive	V V V	Volumes of Version de	u Preboot 3.3.3.104
Nom de connexion à Windows	Domaine	Droits	Alias Trusted Drive
FMO	DSI	USER	
administrateur Ajouter un utilisateu	DSI r Réinitialiser r	ADMIN not de passe	Changer de nom

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 <u>guide de l'utilisateur</u>.

Installation de TrueCrypt sous Windows

Cette installation demande d'avoir des privilèges administrateur.

Récupération du logiciel

- Télécharger le logiciel TrueCrypt sur <u>http://www.truecrypt.org/downloads</u>
- Vérifier la signature de l'exécutable
 - o Bouton de droite -> Propriétés -> Onglet « Signatures numériques »
 - Sélectionner la signature
 - o 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

Détails de la signature numérique	? 🗙
Général Avancé	
Informations sur la Signature numérique Cette signature numérique est valide.	
Informations sur le signataire	
Nom : TrueCrypt Foundation	
Adresse de messagerie : contact@truecrypt.org	
Date de signature : lundi 23 novembre 2009 20:17:58	-
<u>A</u> fficher le certificat	
Contre-signatures	51
Nom du signat Adresse de me Horodateur	
VeriSign Time St Non disponible lundi 23 novembre 2	
Détails	
Ок	$\langle \rangle$

Installation de TrueCrypt

• Lancer l'exécutable

• Accepter la licence en cochant la case « l accept... » puis en cliquant sur « Accept »

TrueCrypt Setup 7.0a
License You must accept these license terms before you can use, extract, or install TrueCrypt.
IMPORTANT: By checking the checkbox below and clicking Accept, you accept these license terms and agree to be bound by and to comply with them. Click the 'arrow down' icon to see the rest of the license.
TrueCrypt License Version 3.0 Software distributed under this license is distributed on an "AS IS" BASIS WITHOUT WARRANTIES OF ANY KIND. THE AUTHORS AND DISTRIBUTORS OF THE SOFTWARE DISCLAIM ANY LIABILITY. ANYONE WHO USES, COPIES, MODIFIES, OR (RE)DISTRIBUTES ANY PART OF THE SOFTWARE IS, BY SUCH ACTION(S), ACCEPTING AND AGREEING TO BE BOUND BY ALL TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT ACCEPT THEM, DO NOT USE, COPY, MODIFY, NOR (RE)DISTRIBUTE THE SOFTWARE, NOR ANY PART(S) THEREOF.
I. Definitions 1. "This Product" means the work (including, but not limited to, source code, graphics, texts, and
✓ I accept and agree to be bound by the license terms
TrueCrypt Installer

Choisir « Install » et cliquez sur « Next »

Installation de TrueCrypt sous Windows

TrueCrypt Setup 7.0a
Wizard Mode Select one of the modes. If you are not sure which to select, use the default mode.
 Install Select this option if you want to install TrueCrypt on this system.
C <u>Extract</u> If you select this option, all files will be extracted from this package but nothing will be
installed on the system. Do not select it if you intend to encrypt the system partition or system drive. Selecting this option can be useful, for example, if you want to run TrueCrypt in so-called portable mode. TrueCrypt does not have to be installed on the operating system under which it is run. After all files are extracted, you can directly run the extracted file 'TrueCrypt.exe' (then TrueCrypt will run in portable mode).
TrueCrypt Installer

Conserver les valeurs par défaut et cliquer sur « Install »

TrueCrypt Setup 7.0a	
Setup Options Here you can set various options to control the installation process.	
Please select or type the location where you want to install the TrueCrypt program files. If the specified folder does not exist, it will be automatically created.	
C:\Program Files\TrueCrypt\	Browse
 ✓ Install for all users ✓ Add TrueCrypt to Start menu ✓ Add TrueCrypt icon to desktop ✓ Associate the .tc file extension with TrueCrypt ✓ Create System Restore point 	
TrueCrypt Installer	Cancel

Installation de TrueCrypt sous Windows

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.
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

📓 True	Crypt									
<u>V</u> olumes	Système	Favorites	<u>O</u> utils	<u>P</u> aramètres	<u>A</u> ide				<u>S</u> ite	Web
Le H: J: J: K: L: M: N: O: R: S: V: W: X:	Volume					Taille	Algorithme	de chiffr	Туре	
	Créer un vo	lume	registrer	Proprié Thistorique	tés du v Ou	olume	olume	Vider le Fichie Périphé	er	
	Monter		Montage	automatique		Tout dém	onter	Q	uitter	

Sélectionnez « Outils → Assistant de création de volume ».

Assistant de création de volume TrueC	rypt 📃 🗖 🔀
Ty C	Pe du chiffrement du système Normal Choisir cette option si vous voulez simplement chiffrer la partition système ou l'intégralité du disque système. Caché It may happen that you are forced by somebody to decrypt the operating system. There are many situations where you cannot refuse to do so (for example, due to extortion). If you select this option, you will create a hidden operating system whose existence should be impossible to prove (provided that certain guidelines are followed). Thus, you will not have to decrypt or reveal the password to the hidden operating system. For a detailed explanation, please click the link below. Plus d'infos
	Aide < Précédent Suivant > Annuler

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

Assistant de création de volume Tr	ueCrypt 📃 🗖 🔀
	 Cone à chiffrer Chiffrer la partition système Windows Select this option to encrypt the partition where the currently running Windows operating system is installed. Chiffrer l'intégralité du disque Select this option if you want to encrypt the entire drive on which the currently running Windows system is installed. The whole drive, including all its partitions, will be encrypted except the first track where the TrueCrypt Boot Loader will reside. Anyone who wants to access a system installed on the drive, or files stored on the drive, will need to enter the correct password each time before the system starts. This option cannot be used to encrypt a secondary or external drive if Windows is not installed on it and does not boot from it.
	Aide < Précédent Suivant > Annuler

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



Cliquez sur « Suivant > ».

📓 Assistant de création de volume TrueCrypt				
	Nombre de système d'exploitation			
	• Amorçage			
	Sélectionner cette option s'il n'y a qu'un seul système d'exploitation installé sur cette machine (même s'il y a plusieurs utilisateurs).			
	C Amorçage multiple			
	Sélectionner cette option s'il y a au moins deux systèmes d'exploitation installés sur cet ordinateur.			
	Par exemple:			
	- Windows 2000 et Windows XP - Windows XP et Windows Vista			
	- Windows et Mac OS X - Windows et Linux Windows et Linux et Mac OS X			
	- Windows, Ellidx et Mac OS X			
	Aide < <u>P</u> récédent Suivant > Annuler			

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

📓 Assistant de création de volume TrueCrypt			
	Options de chiffrement Algorithme de chiffrement AES Tester Algorithme cryptographique (Rijndael, publié en 1998) approuvé par la FIPS, qui peut être utilisé par les agences/départements fédéraux américains pour protéger cryptographiquement les informations sensibles. Clé à 256 bits, bloc de 128 bits, 14 rondes (AES-256). Le mode opératoire est XTS. Plus d'infos sur AES Benchmark		
TR	Algorithme de hachage RIPEMD-160 Infos : algorithmes de hachage		
	Aide < Précédent Suivant > Annuler		

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

📓 Assistant de création de volume TrueCrypt 📃 🗖 🔀				
	Mot de passe			
	Mot de passe:			
	Confirmer: *****************			
05	Fichiers clé Fichiers clé			
TRUEC	Il est très important que vous choisissiez un bon mot de passe. Vous devriez éviter d'utiliser un mot simple que l'on trouve dans un dictionnaire (ou une combinaison de plusieurs de ces mots). Il ne devrait pas contenir de noms ou de dates de naissance. Il ne devrait pas être facile à deviner. Un bon mot de passe est une combinaison de minuscules et de majuscules, de chiffres et de caractères spéciaux comme @ $^ =$ \$ * + etc. Il est recommandé de choisir un mot de passe d'au moins 20 caractères (le plus long, le mieux). La longueur maximale est de 64 caractères.	:		
	Aide < Précédent Suivant > Annuler			

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

Assistant de création de volume T	rueCrypt	×
T T T	Nombre aléatoire actuel (une partie) 79 13 8E AB EA F2 4A 7B C6 DA 90 4B C2 13 39 B4 A6 11 56 04 08 E8 CF 8C 77 03 B6 8C F0 C0 10 BF 6D AE 0B D0 36 EA CB C0 BF EB D3 58 71 75 78 99 3D C2 2F BF F4 B6 02 E6 9F 80 58 31 64 61 A3 3E 1B 90 47 E0 AD 3A AF 40 C6 03 65	
	09 25 FF 56 23 91 A0 3B D8 16 47 DA BA 49 AA A4 3F 8B 02 4A 41 0B BD 30 05 EF D4 2A 63 7B F6 55 B5 87 BB 88 D9 92 A8 AC 74 9C 65 94 A2 ✓ Afficher le nombre aléatoire	
TR	IMPORTANT: Déplacez votre souris dans cette fenêtre aussi aléatoirement que possible. Plus longtemps vous la bougez, mieux c'est. Cela accroît significativement la force cryptographique des clés de chiffrement. Cliquez sur 'Suivant' pour poursuivre.	
	Aide < <u>P</u> récédent Suivant > Annuler	

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

Assistant de création de volume T	rueCrypt 📃 🗖 🔀
	Clés générées
	Les clés, le sel et d'autres données ont été générés avec succès. Si vous désirez générer de nouvelles clés, cliquez sur 'Précédent' puis 'Suivant'. Sinon cliquez sur 'Suivant' pour poursuivre.
ш	Clé d'en-tête: 698E9D0FFBD0C717F847882AC33AF667 Clé principale: 691FFAEA0665441018B189AE8C779568
TRU	Afficher les clés générées (une partie)
	Aide < Précédent Suivant > Annuler

Cliquez sur « Suivant > ».

📲 Assistant de création de volume TrueCrypt				
Assistant de création de volume	TrueCrypt Disque de secours Before you can encrypt the partition/drive, you must create a TrueCrypt Rescue Disk (TRD), which serves the following purposes: - If the TrueCrypt Boot Loader, master key, or other critical data gets damaged, the TRD allows you to restore it (note, however, that you will still have to enter the correct password then). - If Windows gets damaged and cannot start, the TRD allows you to permanently decrypt the partition/drive before Windows starts. - The TRD will contain a backup of the present content of the first drive track (which typically contains a system loader or boot manager) and will allow you to restore it if necessary. The TrueCrypt Rescue Disk ISO image will be created in the location specified below. C:\Documents and Settions\ono\Mes documents\			
	Aide < Précédent Suivant > Annuler			

Cliquez sur « Suivant > ».

Enregistrement du disque de secours	📓 Assistant de création de volume TrueCrypt 🛛 📃 🗖 🔀				
Image has been created and stored in this file: C:\Documents and Settings\opo\Mes documents\TrueCrypt Rescue Disk.iso Now you need to burn it to a CD or DVD. IMPORTANT: Note that the file must be written to the CD/DVD as an ISO disk image (not as an individual file). For information on how to do so, please refer to the documentation of your CD/DVD recording software. If you do not have any CD/DVD recording software that can write the ISO disk image to a CD/DVD, click the link below to download such free software. After you burn the Rescue Disk, click Next to verify that it has been correctly burned. Télécharger le logiciel de gravure de CD/DVD Aide < Précédent Suivant > Annuler		Enregistrement du disque de secours The Rescue Disk image has been created and stored in this file: C:\Documents and Settings\opo\Mes documents\TrueCrypt Rescue Disk.iso Now you need to burn it to a CD or DVD. IMPORTANT: Note that the file must be written to the CD/DVD as an ISO disk image (not as an individual file). For information on how to do so, please refer to the documentation of your CD/DVD recording software. If you do not have any CD/DVD recording software that can write the ISO disk image to a CD/DVD, click the link below to download such free software. After you burn the Rescue Disk, click Next to verify that it has been correctly burned. Télécharger le logiciel de gravure de CD/DVD Aide Suivant > Annuler			

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

Assistant de création de volume T	rueCrypt 📃 🗖 🔀
TRUECRYPT	Disque de secours vérifié Le disque de secours de TrueCrypt a été vérifié avec succès. Enlevez-le du lecteur et stockez-le en lieu sûr. Cliquez 'Suivant' pour continuer.
	Aide < Précédent Suivant > Annuler

Cliquez sur « Suivant > ».

📓 Assistant de création de volume TrueCrypt 📃 🗖 🔀				
TBUECRYPT	Mode de Aucun (le plus rapide)			
	Aide < Précédent Suivant > Annuler			

Cliquez sur « Suivant > ».

Assistant de création de volume T	rueCrypt 📃 🗖 🔀
TRUECRYPT	 Pré-test du chiffrement système Avant de chiffrer votre partition ou votre disque système, TrueCrypt doit vérifier que tout fonctionne correctement. Après avoir cliqué sur 'Test', tous les composants nécessaires (par exemple, le composant d'indentification du pré-amorçage, c'est-à-dire le chargeur d'amorçage de TrueCrypt) seront installés et votre ordinateur redémarrera. Vous devrez ensuite saisir le mot de passe dans l'écran du chargeur d'amorçage de TrueCrypt qui apparaîtra avant que Windows ne démarre. Après le démarrage de Windows, vous serez automatiquement informé des résultats du pré-test. Le périphérique suivant sera modifié: Disque #0 Si vous cliquez sur 'Annuler' maintenant, rien ne sera installé et les pré-tests ne seront pas effectués.
	Aide < Précédent Test Annuler

Cliquez sur « Test ».

Assistant de création de volume TrueCrypt					
1	Avertissement: À cause de limitations techniques de l'environnement de pré-amorçage, les textes affichés par TrueCrypt dans cet environer (avant que Windows ne démarre) ne peuvent être traduits. L'interface utilisateur du chargeur d'amorçage de TrueCrypt est uniquement en Continuer?				
	<u>Oui</u> <u>N</u> on				

Cliquez sur « Oui ».

1	rueCrypt	×
	IMPORTANT NOTES PLEASE READ OR PRINT (click 'Print'):	^
	Note that none of your files will be encrypted before you successfully restart your computer and start Windows. Thus, if anything fails, your data will NOT be lost. However, if something does go wrong, you might encounter difficulties in starting Windows. Therefore, please read (and, if possible, print) the following guidelines on what to do if Windows cannot start after you restart the computer.	
	What to Do If Windows Cannot Start	
	Note: These instructions are valid only if you have not started encrypting.	
	- If Windows does not start after you enter the correct password (or if you repeatedly enter the correct password but TrueCrypt says that the password is incorrect), do not panic. Restart (power off and on) the computer, and in the TrueCrypt Boot Loader screen, press the Esc key on your keyboard (and if you have multiple systems, choose which to start). Then Windows should start (provided that it is not encrypted) and TrueCrypt will automatically ask whether you want to uninstall the pre-boot authentication component. Note that the previous steps do NOT work if the system partition/drive is encrypted (nobody can start Windows or access encrypted data on the drive without the correct password even if he or she follows the previous steps).	
	- If the previous steps do not help or if the TrueCrypt Boot Loader screen does not appear (before	~
	Imprimer	

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

Assista	nt de création de	e volume TrueCrypt 🛛 🗙
<u>.</u>	Votre ordinateur d Voulez-vous le red	loit être redémarré. Iémarrer maintenant?
	Oui	Non

Cliquez sur « Oui » pour redémarrer l'ordinateur.



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

1	irueCrypt	X
	IF POSSIBLE, PLEASE PRINT THIS TEXT (click 'Print' below).	^
	How and When to Use TrueCrypt Rescue Disk (After Encrypting)	
	I. How to Boot TrueCrypt Rescue Disk	
	To boot a TrueCrypt Rescue Disk, insert it into your CD/DVD drive and restart your computer. If the TrueCrypt Rescue Disk screen does not appear (or if you do not see the 'Repair Options' item in the 'Keyboard Controls' section of the screen), it is possible that your BIOS is configured to attempt to boot from hard drives before CD/DVD drives. If that is the case, restart your computer, press F2 or Delete (as soon as you see a BIOS start-up screen), and wait until a BIOS configuration screen appears. If no BIOS configuration screen appears, restart (reset) the computer again and start pressing F2 or Delete repeatedly as soon as you restart (reset) the computer. When a BIOS configuration screen appears, configure your BIOS to boot from the CD/DVD drive first (for information on how to do so, please refer to the documentation for your BIOS/motherboard or contact your computer vendor's technical support team for assistance). Then restart your computer. The TrueCrypt Rescue Disk screen should appear now. Note: In the TrueCrypt Rescue Disk screen, you can select 'Repair Options' by pressing F8 on your keyboard.	
	II. When and How to Use TrueCrypt Rescue Disk (After Encrypting)	~
	Imprimer OK	

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

Assistant de création de volume Tr	ueCrypt 📃 🗖 🔀
	Chiffrement Options Mode de Aucun (le plus rapide) Bause Fait à 0.374% État Chiffrement Reste 53 minutes You can click Pause or Defer anytime to interrupt the process of encryption or decryption, exit this wizard, restart or shut down your computer, and then resume the process, which will continue from the point it was stopped. To prevent slowdown when the system or applications write or read data from the system drive, TrueCrypt automatically waits until the data is written or read (see Status above) and then automatically continues encrypting or decrypting. Plus d'infos
	Aide < <u>P</u> récédent <u>C</u> hiffrer <u>D</u> ifférer

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.

The system partition/drive has been successfully encrypted. Note: If there are non-system TrueCrypt volumes that you need to have mounted automatically every time Windows starts, you can set it up by mounting each of them and selecting 'Favorites' > 'Add Mounted Volume to System Favorites').	Assista	nt de création de volume TrueCrypt 🛛 🛛 🔀
	(The system partition/drive has been successfully encrypted. Note: If there are non-system TrueCrypt volumes that you need to have mounted automatically every time Windows starts, you can set it up by mounting each of them and selecting 'Favorites' > 'Add Mounted Volume to System Favorites').

Cliquez sur « OK ».

📱 Assistant de création de volume TrueCrypt 🛛 📃 🗖 🔀
ChiffrementOptionsMode de Aucun (le plus rapide)Image: State S
AidePrécédentTerminerDifférer

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

Séquestre

Il faut alors procéder au <u>séquestre</u> 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 c lé 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 c lé symétrique de chiffrement est aussi chiffrée par un dérivé de passe).

La nouvelle version (Lion) de Mac OS X, sortie à l'été 2011 intègre un chiffrement intégral du disque, ce qui est désormais la méthode à employer pour protéger les informations.

Chiffrement intégral du disque (Lion)

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



Cliquer dans « FileVault » :

000 S	écurité et confidenti	alité		
■ Fout afficher			Q	8
Général Exiger le mot de passe imm Pour tous les comptes de cet ord Désactiver l'ouverture de si Exiger un mot de passe d'a Système qui présentent un Déconnexion automatique Afficher un message lorsqu	Vault Coupe-feu édiatement a inateur : ession automatique idministrateur pour a e icône de cadenas v après 60 (‡ min te l'écran est verroui	Confidentialité près la suspension incement de l'écon accéder aux Préfére errouillé nutes d'inactivité llé :	d'activité ou le omiseur d'écran nces	
 Mettre à jour automatiquer Désactiver le récepteur infr L'ordinateur fonctionne avec tou disponible. 	nent la liste de téléc arouge pour télécon te télécommande	hargements sûrs Imande Jumeler		
Pour modifier, cliquez sur le cadena	15.			?

Activation du chiffrement sous MacOS X

Cliquez dans le cadenas pour pouvoir activer FileVault :

000	Sécurité et confidentialité		
■ Tou	t afficher	Q	8
	Général FileVault Coupe-feu Co	nfidentialité	
	FileVault protège les données de votre disque en chiffrement et le déchiffrement de vos fichiers s'e lorsque vous les utilisez.	chiffrant son contenu. Le ffectuent automatiquement	
	ATTENTION : Vous aurez besoin d'un mot de passe de ses clé de secours sera générée automatiquement durant cette votre mot de passe et la clé de secours, vos données seror	sion ou d'une clé de secours. Une e configuration. Si vous oubliez nt perdues.	
	FileVault est désactivé pour le disque « Untitled ».	Activer FileVault	
Pour mo	lifier, cliquez sur le cadenas.		?

Saisissez votre mot de passe et cliquer « Déverrouiller »

	Préférences Système essaye de déverrouiller les préférences Sécurité et confidentialité. Saisissez votre mot de passe pour donner l'autorisation.
Mc	Nom : ssi
	Annuler Déverrouiller

Cliquez alors dans « Activer FileVault »



Annotez, séquestrez la clé de secours et cliquez dans « Continuer » :



Ne jamais stocker la clé de secours dans un tiers. Coucher la case « **Ne jamais stocker la clé de secours auprès d'Apple** » et cliquer dans « Continuer » :



Cliquez dans « Redémarrer » :

000	Sécurité et confidentialité	
I → Tout affic	cher Q	
File	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 Vault est désactivé pour le disque « Untitled ». Activer FileVault	
Pour empêcher	r les modifications, cliquez ici.	?

L'utilisateur peut travailler normalement pendant le chiffrement du disque.

L'utilisation au jour le jour est transparente pour l'utilisateur, le mot de passe pour débloquer l'accès au disque étant le même que celui de l'utilisateur.

ATTENTION

Au moment de « Activer FileVault », si votre Mac possède plusieurs comptes d'utilisateur, vous devrez identifier les comptes d'utilisateur autorisés à déverrouiller le disque chiffré (pour le démarrage de l'ordinateur ou la reprise d'activité après une suspension ou une veille prolongée).

	Chaque utilisateur doit saisir s le disque.	on mot de passe avant de pouvoir déverrouiller
C	apple Admin raid Admin	Activer l'utilisateur e
		Annuler Continuer
Pour	empêcher les modifications, clique	ez iri

Les utilisateurs n'ayant pas l'autorisation de déverrouiller FileVault pourront se connecter au Mac uniquement après qu'un utilisateur doté d'une autorisation a démarré ou déverrouillé le disque.

Voici quelques copies d'écrans récupérées sur internet¹. Cette version est effectivement sortie.

¹ <u>http://www.appleinsider.com/</u>









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

Chiffrement du répertoire utilisateur

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 »

00	Sécurité	
	Tout afficher	Q.
	FileVault FileVault protège votre dossier Départ en chiffrant son con déchiffrage de vos fichiers s'effectue automatiquement lor AVERTISSEMENT : Vos fichiers seront chiffrés en utilisant v session. Si vous oubliez celui-ci et que vous ne connaissez principal, vos données seront perdues. Le mot de passe principal n'est pas défini .	itenu. Le chiffrage et sque vous les utilisez. otre mot de passe de z pas le mot de passe
	de déverrouiller n'importe quel compte FileVault de cet ordinateur.	Le définir
	La protection FileVault du compte est désactivée . L'activation de FileVault peut prendre un certain temps.	. Activer FileVault
	Hot de passe exigé après suspension d'activité l'économiseur d'écran	é ou lancement de
	Pour tous les comptes de cet ordinateur :	
	Désactiver l'ouverture de session automatique	
	Mot de passe requis pour déverrouiller les pré	férences Système sécurisées
	Déconnexion automatique après 60 🗍 m	inutes d'inactivité
	Utiliser la mémoire virtuelle sécurisée	
pou	r empêcher les modifications, cliquez ici.	?

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

	Vous devez créer un mot de pa aux comptes protégés par File sécurité.	asse principal afin de p Vault de bénéficier d'u	ermettre n filet de
	Un administrateur de cet ordinateur pe réinitialiser le mot de passe de n'impo vous oubliez votre mot de passe, vous dossier Départ, même s'il est protégé oublient leur mot de passe de session	eut utiliser le mot de passe p rte quel utilisateur de cet ord pouvez le réinitialiser pour par FileVault. Ainsi, les utilis sont protégés.	rincipal pour dinateur. Si accéder à votre ateurs qui
	Mot de passe principal :		?
	Confirmation :	•••••	
	Indice du mot de passe :		
	Choisissez un mot de passe difficile à sur le bouton d'aide pour en savoir plué conomiseur d'écran	deviner et facilement mémo us sur le choix d'un bon mot	risable. Cliquez de passe.
Pou		Annular	OK

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

00	Sécurité	
	Tout afficher	
	 FileVault FileVault protège votre dossier Départ en chiffrant son cont déchiffrage de vos fichiers s'effectue automatiquement lors AVERTISSEMENT : Vos fichiers seront chiffrés en utilisant vo session. Si vous oubliez celui-ci et que vous ne connaissez principal, vos données seront perdues. Le mot de passe principal est défini. Il s'agit d'un mot de passe "filet de sécurité" qui permet de déverrouiller n'importe quel compte FileVault de cet ordinateur. La protection FileVault du compte est désactivée. L'activation de FileVault peut prendre un certain temps. Mot de passe exigé après suspension d'activité l'économiseur d'écran Pour tous les comptes de cet ordinateur : Désactiver l'ouverture de session automatique Mot de passe requis pour déverrouiller les préfe Déconnexion automatique après 60 \$ mit 	tenu. Le chiffrage et que vous les utilisez. otre mot de passe de pas le mot de passe <u>Modifier</u> <u>Activer FileVault</u> t ou lancement de érences Système sécurisées nutes d'inactivité
pou 👔	r empêcher les modifications, cliquez ici.	?

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.

😝 🖯 Sécurité	
Tout afficher	٩
FileVault FileVault protège votre dossier Départ en chiffrant son cont déchiffrane de voc fichiere c'affectue automationement lore Authentification Tapez un nom et un mot de passe of pour modifier Préférences Systèmes Nom : admin Mot de passe : ••••••• Détails © Control de cet ordinateur :	enu. Le chiffrage et d'administrateur er OK

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

$\bigcirc \bigcirc \bigcirc \bigcirc$	Sécurité
	FileVault nécessite que vous saisissiez un mot de passe pour ce compte utilisateur.
10	File de voir de passe : ••••••
·	se: sion. Si vous oubliez celui-ci et que vous no Annuler o OK
	Le mot de passe principal est défini. Il s'agit d'un mot de passe "filet de sécurité" qui permet de déverrouiller n'importe quel compte FileVault de cet Modifier

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

0 🖯 🖯	Sécurité
	Vous pouvez à présent activer la protection AVERTISSEMENT : Vos fichiers seront chiffrés en utilisant votre mot de passe de session. Si vous oubliez celui-ci et que vous ne connaissez pas le mot de passe principal, vos informations seront perdues.
se pr Le	Une fois FileVault activé, votre session se fermera et l'opération de chiffrage de votre dossier Départ sera lancée. Elle peut prendre un certain temps en fonction de la quantité d'informations dont vous disposez. Vous ne pourrez pas ouvrir de session ni utiliser cet ordinateur tant que FileVault n'aura pas fini.
	Vous ne pouvez pas ouvrir de session sur ce compte depuis un autre ordinateur pour l'utiliser comme partage d'imprimantes ou de fichiers Windows.
?	☑ Utiliser l'effacement sécurisé Annuler Activer FileVault

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.

Nouveau compte :	Standard
Nom :	Jean-Claude
Nom abrégé :	JC
Mot de passe :	•••••
Confirmation :	•••••
Indice du mot de passe : (recommandé)	comme d'habitude
	Activer la protection FileVault
(?)	Annuler Créer le compte

Séquestre

Il est impératif de procéder au <u>séquestre</u> 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

IMPORTANT: By clicking the 'Accept' button below, you accept these license terms and agree to be bound by and to comply with them. Click the 'arrow down' icon to see the rest of the license.	TrueCrypt 7.0a Mac OS X.dmg		
Print Save Decline Accept	IMPORTANT: By clicking the 'Accept' button below, you accept these license terms and agree to be bound by and to comply with them. Click the 'arrow down' icon to see the rest of the license.	TrueCrypt License Version 3.0 Software distributed under this license is distributed on an "AS IS" BASIS WITHOUT WARRANTIES OF ANY KIND. THE AUTHORS AND DISTRIBUTORS OF THE SOFTWARE DISCLAIM ANY LIABILITY. ANYONE WHO USES, COPIES, MODIFIES, OR (RE)DISTRIBUTES ANY PART OF THE SOFTWARE IS, BY SUCH ACTION(S), ACCEPTING AND AGREEING TO BE BOUND BY ALL TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT ACCEPT THEM, DO NOT USE, COPY, MODIFY, NOR (RE)DISTRIBUTE THE SOFTWARE, NOR ANY PART(S) THEREOF. I. Definitions 1. "This Product" means the work (including, but not limited to, source code, graphics, texts, and accompanying files) made available under and governed by this version of this license ("License"), as may be indicated by, but is not limited to, copyright notice(s) attached to or included in the work. 2. "You" means (and "Your" refers to) an individual or a legal metitum (a a compared to the comparison of the source code) Print Save Decline Accept	

Acceptez la licence en cliquant sur « Accept »



Cliquez sur « Continuer »


Cliquez sur « Continuer »

000	🥪 Installer TrueCrypt 7.0a			
Installation simplifiée sur "Macintosh HD"				
 Introduction Sélectionner la destination Type d'installation Installer Terminer l'installation 	Cliquer sur Installer pour effectuer l'installation standard de ce progiciel sur le volume "Macintosh HD".			
	Personnaliser Revenir Installer			

Cliquez sur « Installer »

Authentification			
Programme d'installation vous demande de taper votre mot de passe.			
Nom :	Admin		
Mot de passe :	•••••		
▶ Détails			
?	Annuler OK		

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 <u>http://gna.org/projects/grub4dos/</u>).

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

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 ?				
	Supprimer 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.			
O C	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.			
0 ?	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.

Chiffrement du système avec dm-crypt sous Linux

Saisissez une phrase de passe pour la partition chiffrée				
R	Choisissez une phrase de passe pour vos périphériques chiffrés. Votre phrase de passe vous sera demandée lors du démarrage du système.			
Saisissez une phrase de passe :	•••••			
Confirmer la phrase de passe :	••••••			
		Annuler Valider		

Il est impératif de procéder au <u>séquestre</u> 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 est 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 <u>http://www.truecrypt.org/downloads</u>

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 ddrescue³ 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 SystemRescueCd⁴.

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 *setxkmap 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 <u>http://www.gnu.org/software/ddrescue/ddrescue_fr.html</u>

⁴ <u>http://www.sysresccd.org/Page_Principale</u>

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 complétement 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 agence gouvernementales).

Qu'apportent les nouvelles instructions AES ?

Ces instructions (<u>http://en.wikipedia.org/wiki/AES_instruction_set</u>) 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.

Connexion d'un disque chiffrant externe

Pour connecter un disque chiffrant externe, il faut utiliser un adaptateur eSata. Les adaptateurs USB (ou du moins les modèles testés) ne permettent pas d'envoyer les commande qui permettent de déverrouiller le disque.