Sommaire :

VeraCrvpt (remplace TrueCrvpt)	1
Principe	1
Créer un volume	1
Premier montage	7
Réglages	9
Add Mounted Volume to Favorites	9
Settings > Preferences	11
TrueCrypt (ancien)	13
Principe de TrueCrypt	13
Créer un volume pour TrueCrypt	13
Premier montage	
Réglages	20
Save Currently Mounted Volumes as Favorite	20
Settings > Preferences	21
TrueCrypt Traveller pour clef USB, disque externe	22
Notes, FAQ,	23
Peut-on perdre des données ?	23
1	

VeraCrypt (remplace TrueCrypt)

Principe

Les données cryptées sont stockées dans un fichier, à priori inutilisable par quiconque qui ne connait pas votre mot de passe (dans cette doc, le fichier est d:\GT_VeraCrypt\GT.hc).

En fournissant le mot de passe, le contenu de ce fichier est décrypté, et il est "monté" dans un volume (au même titre que C: ou toute autre unité de disque externe ou clef USB. Dans cette doc, le volume est S:). On peut travailler dans ce volume comme dans un volume ordinaire (créer des arborescences, des fichiers de toute sorte, etc...). Quand on "démonte" le volume, tout son contenu est réintégré dans le fichier crypté et redevient inaccessible.

Créer un volume

Cliquer sur Create Volume

(alumna C									
volumes Sy	stem	Favor <u>i</u> tes	T <u>o</u> ols	Settings	<u>H</u> elp			Homeg	gage
Drive Volu M: N: O: P: Q: R:	ime				Size	Encryption Algorithm	n Type		^
U:									
U: U: V: W: Z: Volume	te Volum	ne		Volume	Properti	es	Wip	e Cache	~





	D:\GT_VeraCrypt\GT.hc	∽ Select <u>F</u> ile
	Never save history A VeraCrypt volume can reside in a file which can reside on a hard disk, on a l VeraCrypt container is just like any no example, moved or deleted as any no choose a filename for the container ar you wish the container to be created. WARNING: If you select an existing fil	e (called VeraCrypt container), JSB flash drive, etc. A rmal file (it can be, for rmal file). Click 'Select File' to nd to select the location where e. VeraCrypt will NOT encrypt
VeraCrypt	it; the file will be deleted and replaced VeraCrypt container. You will be able on) by moving them to the VeraCrypt to create now.	with the newly created to encrypt existing files (later container that you are about

Personnellement, je garde les paramètres par défaut :

	Encryption Algorithm	
	AES ~	<u>T</u> est
	used by U.S. government departments and dassified information up to the Top Secret 128-bit block, 14 rounds (AES-256). Mode	d agencies to protect level. 256-bit key, of operation is XTS.
	Hash Algorithm	
VeraCrupt	SHA-512 V Information or	hash algorithms

Donner la taille. On ne pourra pas la modifier ensuite, donc ne soyez pas trop chiche (mais si on veut l'agrandir, il suffira de créer un autre container plus grand et d'y transférer les fichiers, ce n'est pas bien difficile).

	Volume Size
	200 OKB ●MB OGB OTB Free space on drive D:\ is 56.15 GB
VeraCrypt	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 exFAT volume is 424 KB. The minimum possible size of an NTFS volume is 3792 KB. The minimum possible size of an ReFS volume is 642 MB.
	Help < Back Next > Cancel

ServeraCrypt Volume Creation Wizard	- 🗆 × Volume Password
	Volume Password Password: Password: Confirm: Uge keyfiles Display password Uge keyfiles Display password Uge Villes Volume Villes V
VeraCrypt	case letters, numbers, and special characters, such as @ ^ = \$ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 64 characters. Help < Back Next > Cancel

Personnellement, je choisis le format NTFS qui est plus sûr. Balader la souris pour créer un "random pool" aléatoire

	Options Filesystem NTFS	1at Cluster Defau	ilt 🗸 🗌 Dynamic
	Random Pool: /,,, Header Key: *** Master Key: ***	,*+*,**++. **************************	,-,,*/,*,+***** ****************************
	Done	Speed	Abort
VeraCrypt	IMPORTANT: Move you window. The longer yo increases the cryptogr dick Format to create to	ur mouse as rando ou move it, the bett aphic strength of t the volume.	mly as possible within this ter. This significantly he encryption keys. Then
	Randomness Collecte	ed From Mouse Mov	vements

Cliquer sur Format pour terminer



Premier montage

Choisir la lettre de l'unité (Drive) dans laquelle on veut monter les données cryptées (ici S:). Choisir le fichier crypté que l'on veut y monter (ici d:\GT_VeraCrypt\GT.hc).

🐱 VeraCrypt	- 🗆 🗙
Volumes System Favorites Tools Settings Help	Homepage
Drive Volume Size Encryption Algorithm	Туре
U: V: W: Z:	Ŷ
<u>Create Volume</u> <u>Volume Properties</u>	<u>Wipe</u> Cache
D:\GT_VeraCrypt\GT.hc ~	Select File
VeraCrypt Volume Tools	Select Device
Mount All	E <u>x</u> it
Cliquer sur Mount, et donner le mot de passe choisi lors de la création du fich Enter password for D:\GT_VeraCrypt\GT.hc	ier.
Password: ••••••• PKCS-5 PRF: Autodetection	OK Cancel
Use PIM Cache passwords and keyfiles in memory Display password	
Use keyfiles Keyfiles Mour	nt Options

et le fichier est monté dans S:

	C	F	T 1	C				
lumes	System	Favorites	lools	Settings	<u>H</u> elp			Homepa
Drive Vo	olume				Size	Encryption Algorithm	Туре	
M:								
-N:								
0:								
Q:								
	IGTI Ve	raCrynt\GT h	-		100 MR	AFS	Normal	1
U:	101 [10	ider/peraria	-		133110		Horman	
-v:								
-)W:								
Z:								
Z:								
Z:	v 1							
Z:	eate Volu	me		Volume	Propert	ies	<u>W</u> ipe C	àche
Z: Cre Volume	eate Volu	me		Volume	Propert	ies	<u>Wipe C</u>	ache
Z: <u>C</u> re Volume	eate Volu	me	ot\GT.hc	Volume	Propert	ies	Wipe C Select I	ache
Z: Cre Volume	eate Volu	me	ot\GT.hc	<u>V</u> olume	Propert	ies	Wipe C Select	iache Eile
Z: <u>C</u> re Volume	eate Volu D:\c	me GT_VeraCryp ever save his	ot\GT.hc tory	Volume	Propert	ies \ /olume <u>T</u> ools	Wipe C Select I Select De	iache File
Z: Cre Volume VeraCrypt	eate Volu D:\(D:\(me GT_VeraCryp ever save his	ot\GT.hc tory	<u>V</u> olume	Propert	ies 	Wipe C Select I Select De	jie
Z: <u>Cre</u> Volume VeraCrypt	eate Volu D:\c D:\c	me GT_VeraCryp ever save his	ot\GT.hc tory	<u>V</u> olume	Propert	ies	Wipe C Select I Select De	Evit

On peut maintenant utiliser l'unité S:

Réglages

Add Mounted Volume to Favorites

Pour gagner du temps lors de l'utilisation ultérieure, il est bon de sauvegarder les paramètres. Pour cela, après avoir monté votre volume (comme dans le paragraphe ci-dessus), faire "Add Mounted Volume to Favorites". VeraCrypt va mémoriser les fichiers à monter et l'unité où il les monte, ce qui vous fera gagner du temps.

olumes System	Favorites Tools Set	ttings Help		Ho	omepag	
	Add Mounted Vo	lume to Favorites			18	
Drive Volume	Add Mounted Vo	Add Mounted Volume to System Favorites				
N:	Organize Favorite Organize System	Organize Favorite Volumes Organize System Favorite Volumes				
Q:	Mount Favorite V	Mount Favorite Volumes				
S: D:\GT_Ve	D:\GT_VeraCrypt	t\GT.hc	S:	ormal		
U: V: W:						
U: V: W: Z: <u>C</u> reate Volu	me	olume Properties	1	Wipe Cache	±	
U: V: W: Z: <u>C</u> reate Volu Volume D: V	me <u>y</u> GT_VeraCrypt\GT.hc	<u>/olume Properties</u>		Wipe Cache Select File	2	
U: V: W: Z: <u>Create Volu</u> Volume <u>Volume</u> <u>D: W</u>	me <u>y</u> GT_VeraCrypt\GT.hc ever save history	<u>/olume Properties</u> Volume <u>T</u> ools		Wipe Cache Select Eile Select Device	÷	

/eraCryp	ot - Favorite Volum	nes				×
Drive	Label		Volume			
S:			D:\GT_VeraCrypt\GT.hc			
Mo	ove <u>U</u> p Mo	ove <u>D</u> own			<u>R</u> emove	
PKC	S-5 PRF: H	MAC-SHA-512	✓ ☐ TrueCrypt Mode			
Volu	me PIM:	(E	mpty or 0 for default iterations)			
	isplay PIM					
Labe	l of selected favorit	te volume:				
						1
	lse favorite label as	Explorer drive	label			-
	Iount selected volur	me as read-o <u>n</u> ly	y			
M	lount selected volur	me as remo <u>v</u> abl	le medium			
	lount selected volur	me upon log <u>o</u> n				
	lount selected volur	me when its hos	st device gets <u>c</u> onnected			
)pen <u>E</u> xplorer windo	ow for selected	volume when successfully mounted			
	o not mount selecte	ed volume wher	n 'Mount Favorite Volumes' <u>h</u> ot key is j	pressed		
Hele				OK	Grand	

Settings > Preferences

🐱 VeraCrypt		211-1 111-1		×
Volumes System Favorites Tools	Settings	Help	Home	page
Drive Volume	Lan Hot	guage Keys		^
N: O: P:	Syst Syst	em Encryption em Favorite Volumes		
Q:	Perf	formance/Driver Configuration		
S: D:\GT_VeraCrypt\GT.hc	Defa	ault Ke <mark>y</mark> files		
	Def	ault Mount Parameters		
w:	Sec	urity Tokens		
Z:	Pref	erences		~

Je mets les options suivantes (elles me sont utiles pour ma gestion des backups principalement, mais il se peut que pour vous les options par défaut conviennent):

VeraCrypt - Preferences ×
Default Mount Options
Mount volumes as read-only
VeraCrypt Background Task
Enabled Exit when there are no mounted volumes
Actions to perform upon logon to Windows
Start VeraCrypt Background Task Mount all device-hosted VeraCrypt volumes
Auto-Dismount
Dismount all when: User logs off User session locked Screen saver is launched Entering power saving mode
Auto-dismount volume after no data has been read/written to it for 60 minutes
Force auto-dismount even if volume contains open files or directories
Windows
Open Explorer window for successfully mounted volume
Use a different taskbar icon when there are mounted volumes
Preserve modification timestamp of file containers
Make disconnected network drives available for mounting
Don't show wait message dialog when performing operations
Use Secure Desktop for password entry
Password Cache
Cache passwords in driver memory Wipe cached passwords on exit
Temporarily cache password during "Mount Favorite Volumes" operations
☑ Wipe cached passwords on auto-dismount
Include PIM when caching a password
More Settings OK Cancel

Avec ces réglages, TrueCrypt démarre automatiquement à chaque Session Windows. Il n'y a plus que le mot de passe à donner, ou bien il suffit d'ignorer si on ne veut pas décrypter les données.

"Preserve modification timestamp of file containers" est une option cochée par défaut. Il en résulte que le fichier contenant les données cryptées ne change jamais de date. C'est mieux pour la confidentialité, mais personnellement ça me gène d'avoir des données récentes et importantes dans un fichier qui conserve une date ancienne. Pour mes synchronisations et sauvegardes, je préfère décocher l'option.

"Mount volumes as removable media" a plusieurs avantages (à mon sens), décrits ici: <u>http://www.truecrypt.org/docs/?s=volume-mounted-as-removable-medium</u>

TrueCrypt (ancien)

Notes:

- Points de départ sur le web: <u>http://www.framasoft.net/article3931.html</u> et <u>http://www.truecrypt.org</u>
- Normalement, tout ce que je raconte plus bas figure dans la doc. Il suffit de la lire...
- TrueCrypt fonctionne sous plein de systèmes, mais je n'ai testé que Windows.
- La doc a été mise à jour en juin 2009, avec la version 6.2 de TrueCrypt. Depuis il y a de nouvelles versions, et il y a peutêtre quelques nuances dans les menus

Principe de TrueCrypt

Les données cryptées sont stockées dans un fichier, à priori inutilisable par quiconque qui ne connait pas votre mot de passe (dans cette doc, le fichier est D:\GT\TrueCrypt\GT_TC).

En fournissant le mot de passe, le contenu de ce fichier est décrypté, et il est "monté" dans un volume (au même titre que C: ou toute autre unité de disque externe ou clef USB. Dans cette doc, le volume est S:). On peut travailler dans ce volume comme dans un volume ordinaire (créer des arborescences, des fichiers de toute sorte, etc...). Quand on "démonte" le volume, tout son contenu est réintégré dans le fichier crypté et redevient inaccessible.

Créer un volume pour TrueCrypt

Cliquer sur Create Volume

TrueC	rypt								_	<u> </u>
<u>V</u> olumes	System	<u>K</u> eyfiles	T <u>o</u> ols	Settings	Help				Home	page
Drive	Volume					Size	Encryption a	lgorithm	Туре	
≪L: ≪M: ≪N:										
 O: S: T: O: 										
V:										
≪Y: ≪Z:										
	<u>C</u> reate Vo	lume]		/olume Pr	operties,	ļ	₩ipe	Cache	
				1.0			_	Select	<u>F</u> ile	
		<u>N</u> ever sa	ve histor	Ϋ́		Volume <u>T</u> ool	s	Select D	evice	
	Mount		Auto	-Mount De	vices	Dismour	nt All		E <u>x</u> it	
					100					

TrueCrypt Volume Creation Wizard



Create an encrypted file container Creates a virtual encrypted disk within a file. Recommended for inexperienced users. More information Cncrypt 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. Cncrypt the system partition or entire system drive Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.



_ 🗆 X

TrueCrypt Volume Creation Wizard	
	Volume Location
a .	D:\GT_TrueCrypt\GT_TC
	✓ Never save history
	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, copied and 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.
	Help < Back Next > Cancel

Personnellement, je garde les paramètres par défaut :

Encryption Options
Encryption Algorithm
Approved cipner (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 Information on hash algorithms

Donner la taille. On ne pourra pas la modifier ensuite, donc ne soyez pas trop chiche (mais si on veut l'agrandir, il suffira de créer un autre container plus grand et d'y transférer les fichiers, ce n'est pas bien difficile).

TrueCrypt Volume Creation Wizard		- 🗆 🗵
	Volume Size	
	200 С <u>к</u> в 👁 <u>м</u> в С <u>с</u> в	
	Free space on drive D:\ is 73.64 GB	
ш	Please specify the size of the container you want to create.	
	If you create a dynamic (sparse-file) container, this paramete specify its maximum possible size.	r will
	Note that the minimum possible size of a FAT volume is 275 KE The minimum possible size of an NTFS volume is 2829 KB.	i.
	Help < Back Next >	Cancel

	Volume Pass	word	
<u>a</u>	Confirm:	****	
		<u>s</u> e keyfiles isplay password	Keyfiles
	This can import the	ab you ab a set a set of	management Variationald

Personnellement, je choisis le format NTFS qui est plus sûr. Balader la souris pour créer un "random pool" aléatoire

TrueCrypt Volume Creation Wizard	
L	Options Filesystem TFS Cluster Default Dynamic
	Random Pool: 264B4B13B1600828000BA8FB6F371014
	Done Speed Left
TR	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.
	Help < Back Format Cancel

Cliquer sur Format pour terminer



Premier montage

Choisir la lettre de l'unité (Drive) dans laquelle on veut monter les données cryptées (ici S:). Choisir le fichier crypté que l'on veut y monter (ici D:\GT\TrueCrypt\GT_TC).

TrueCrypt			_
e <u>V</u> olumes <u>K</u> eyfiles T <u>o</u> ols Setti <u>n</u> gs <u>H</u> elp			Homep
Drive Volume	Size	Encryption Algorithm	Туре
• J: • L:			
≪M: ≪N: ≪O:			
₽: Q:			
×x:			
Create Volume Volume Proper	ties	<u>Wi</u> pe	Cache
		T Salari	+ File
Image:	Volume <u>T</u> ools	Select [D <u>e</u> vice
Mount Auto-Mount Devices	Di <u>s</u> moun	t All	E <u>x</u> it
juer sur Mount, et donner le mot de passe choisi lors o	de la créatic	n du fichier.	
ter password for D:\GT\TrueCrypt\GT_TC			
	0	C	
Password:	Can		
Password: Cache passwords and keyfil <u>e</u> s in memory	Can	cel	

et le fichier est monté dans S:

<u>v</u> 01	umes <u>K</u> eyfiles	Tools Settings	Help			Home	pag
Drive	Volume			Size	Encryption Algorithm	Туре	
-G:							1
H:							
₽I:							
»]:							
PL:							
₩M:							
N:							
•0:							
₩P:							
₽Q:							
R:							
S:	D: \GI \TrueCry	pt\GI_IC		149 MB	AES	Normal	
# 1: 							
P AL							1
		14	-		(e de	
/olum	Create Volume e D:\GT\7	 TrueCrypt\GT_TC	<u>v</u> olume Pr	operties		cache	1
/olum	<u>C</u> reate Volume e D:\GT\T ☑ <u>N</u> eve	rueCrypt\GT_TC		Volume <u>T</u> ools	Select	t <u>Fi</u> le D <u>e</u> vice	

On peut maintenant utiliser l'unité S:

Réglages

Save Currently Mounted Volumes as Favorite

NOTA: les menus ont changé depuis que j'ai fait la doc ci-dessous. Voir <u>http://www.truecrypt.org/docs/?s=favorites</u> Pour faire bref:

- il y a un nouveau menu "Favorites" dans la barre d'outils
- Pour sauver un volume monté comme favori, faire un clic-droit dessus

Après avoir monté votre volume, faire "Save Currently Mounted Volumes as Favorite". TrueCrypt va mémoriser les fichiers à monter et l'unité où il les monte, ce qui vous fera gagner du temps.

Yolumes System Keyfiles Tools Settings Help Select File Size Encryption algorithm T Select Device Size Encryption algorithm T Mount Favorite Volumes Save Currently Mounted Volumes as Favorite Resume Interrupted Process 199 MB AES Mount Volume 199 MB AES Mount Volume with Options 199 MB AES Auto-Mount All Device-Hosted Volumes Image: Set Header Key Derivation Algorithm Create New Volume Properties Image: Set Header Key Derivation Algorithm Volume Properties Select File	100
Select File Select Device Mount Favorite Volumes Save Currently Mounted Volumes as Favorite Resume Interrupted Process Mount Volume Mount Volume with Options Auto-Mount All Device-Hosted Volumes Dismount Volume Dismount Volume Dismount All Mounted Volumess Create New Volume Change Volume Password Set Header Key Derivation Algorithm Volume Properties Select File	Homegag
Mount Favorite Volumes Save Currently Mounted Volumes as Favorite Resume Interrupted Process Mount Volume Mount Volume with Options Auto-Mount All Device-Hosted Volumes Dismount Volume Dismount Volume Create New Volume Change Volume Password Set Header Key Derivation Algorithm Volume Properties Youme Select File	уре
Save Currently Mounted Volumes as Favorite Resume Interrupted Process Mount Volume Mount Volume with Options Auto-Mount All Device-Hosted Volumes Dismount Volume Dismount Volume Dismount All Mounted Volumes Create New Volume Change Volume Password Set Header Key Derivation Algorithm Volume Properties Volume Select File	
Resume Interrupted Process Mount Volume Mount Volume with Options Auto-Mount All Device-Hosted Volumes Dismount Volume Dismount All Mounted Volumes Create New Volume Change Volume Password Set Header Key Derivation Algorithm Volume Properties Volume Select File	
Mount Volume 199 MB AES Mount Volume with Options Auto-Mount All Device-Hosted Volumes Dismount All Device-Hosted Volumes Image: Constraint of the second se	
Mount Volume with Options Auto-Mount All Device-Hosted Volumes Dismount Volume Dismount All Mounted Volumes Create New Volume Change Volume Password Set Header Key Derivation Algorithm Volume Properties Volume Select File	Iormal
Auto-Mount All Device-Hosted Volumes Dismount Volume Dismount All Mounted Volumes Create New Volume Change Volume Password Set Header Key Derivation Algorithm Volume Properties Volume Select File	
Dismount Volume Dismount All Mounted Volumes Create New Volume Change Volume Password Set Header Key Derivation Algorithm Volume Properties Volume Select File	
Dismount All Mounted Volumes Create New Volume Change Volume Password Set Header Key Derivation Algorithm Volume Properties Volume Set Header Key Derivation Algorithm	
Create New Volume Change Volume Password Set Header Key Derivation Algorithm Volume Properties Volume Select File	
Change Volume Password Set Header Key Derivation Algorithm e Properties Wipe Cad Volume Select File Select File	
Set Header Key Derivation Algorithm e Properties Wipe Cad Volume Properties Select File	
Volume Properties	the
volame ▼ Select File	
Select File	
	e
Volume Tools Select Devi	ice
Dismount All Ex	it



Settings > Preferences

File Volumes Keyfiles Tools	Settings	Help
Drive Volume	Langua Hot Ke Defaul	age :ys It Kevfiles
	Prefer	ences

Je mets les options suivantes:

TrueCrypt - Preferences	×
Default Mount Options	Mount volumes as removable media
TrueCrypt Background Task	when there are no mounted volumes
Actions to perform upon logon to Windows	nt all device-hosted TrueCrypt volumes
Auto-Dismount Dismount all when: User logs off Screen saver is launch Auto-dismount volume after no data has bee Force auto-dismount even if volume contains	ed Entering power saving mode en read/written to it for 120 minutes s open files or directories
Windows Open Explorer window for successfully moun Use a different taskbar icon when there are Preserve modification timestamp of file conta	ted volume mounted volumes iners
Password Cache Cache passwords in driver memory	Wipe cached passwords on exit
More Settings	OK Cancel

Avec ces réglages, TrueCrypt démarre automatiquement à chaque Session Windows. Il n'y a plus que le mot de passe à donner, ou bien il suffit d'ignorer si on ne veut pas décrypter les données.

"Preserve modification timestamp of file containers" est une option cochée par défaut. Il en résulte que le fichier contenant les données cryptées ne change jamais de date. C'est mieux pour la confidentialité, mais personnellement ça me gène d'avoir des données récentes et importantes dans un fichier qui conserve une date ancienne. Pour mes synchronisations et sauvegardes, je préfère décocher l'option.

"Mount volumes as removable media" a plusieurs avantages (à mon sens), décrits ici: <u>http://www.truecrypt.org/docs/?s=volume-mounted-as-removable-medium</u>

TrueCrypt Traveller pour clef USB, disque externe,...

Il existe une option bien pratique qui configure un disque amovible ou une clef USB de manière à posséder une version de TrueCrypt autonome (à la fois le logiciel et les données cryptées sont sur la clef).

🗑 TrueCrypt	
File Volumes Keyfiles	Tools Settings Help
Drive Volume G: H: I:	Benchmark Test Vectors
	Traveller Disk Setup
	Keyfile Generator
	1 011070 1 1

On peut ainsi trimbaler sa clef USB avec des données confidentielles sans aucun risque.

Si on a réglé convenablement les options, on branche la clef dans l'ordinateur hôte, on donne le mot de passe, et hop, les données cryptées sont montées.

Notes, FAQ,...

Quelques remarques en vrac

Peut-on perdre des données ?

Oui, quand le PC plante brusquement sans prévenir (écran bleu de Windows par exemple). Dans ce cas, si un volume TrueCrypt est monté, les données sont en RAM et n'ont pas le temps d'être réintégrées dans le volume. L'expérience montre qu'on peut perdre alors toutes les données de cette session TrueCrypt.

Par contre, dans le mode de fonctionnement normal, TrueCrypt ferme proprement le volume quand on quitte Windows, et il n'est pas nécessaire de démonter le volume avant de quitter Windows (bien que je vous le conseille fortement).

http://www.truecrypt.org/faq

Do I have to dismount TrueCrypt volumes before shutting down or restarting Windows?

No. TrueCrypt automatically dismounts all mounted TrueCrypt volumes on system shutdown/restart.

J'ai réalisé ensuite qu'il existe une option "Mount volumes as removable media". Il semblerait qu'en l'activant, on gagne en sécurité. Mais ce n'est pas très clair...

http://www.truecrypt.org/docs/?s=volume-mounted-as-removable-medium

Volume Mounted as Removable Medium

This section applies to TrueCrypt volumes mounted when one of the following options is enabled (as applicable):

- Tools > Preferences > Mount volumes as removable media
- Mount Options > Mount volume as removable medium
- Favorites > Organize Favorite Volumes > Mount selected volume as removable medium
- Favorites > Organize System Favorite Volumes > Mount selected volume as removable medium

TrueCrypt Volumes that are mounted as removable media have the following advantages and disadvantages:

- Windows is prevented from automatically creating the 'Recycled' and/or the 'System Volume Information' folders on TrueCrypt volumes (in Windows, these folders are used by the Recycle Bin and System Restore features).
- Windows may use caching methods and write delays that are normally used for removable media (for example, USB flash drives). This might slightly decrease the performance but at the same increase the likelihood that it will be possible to dismount the volume quickly without having to force the dismount.
- The operating system may tend to keep the number of handles it opens to such a volume to a minimum. Hence, volumes mounted as removable media might require fewer forced dismounts than other volumes.
- Under Windows Vista and earlier, the 'Computer' (or 'My Computer') list does not show the amount of free space on volumes mounted as removable (note that this is a Windows limitation, not a bug in TrueCrypt).
- Under desktop editions of Windows Vista or later, sectors of a volume mounted as removable medium may be accessible to all users (including users without administrator privileges; see section Multi-User Environment).

Et aussi :

http://www.truecrypt.org/faq

Can I unplug or turn off a hot-plug device (for example, a USB flash drive or USB hard drive) when there is a mounted TrueCrypt volume on it?

Before you unplug or turn off the device, you should always dismount the TrueCrypt volume in TrueCrypt first, and then perform the 'Eject' operation if available (right-click the device in the 'Computer' or 'My Computer' list), or use the 'Safely Remove Hardware' function (built in Windows, accessible via the taskbar notification area). Otherwise, data loss may occur.

http://www.truecrypt.org/faq

What will happen when a part of a TrueCrypt volume becomes corrupted?

In encrypted data, one corrupted bit usually corrupts the whole ciphertext block in which it occurred. The ciphertext block size used by TrueCrypt is 16 bytes (i.e., 128 bits). The mode of operation used by TrueCrypt ensures that if data corruption occurs within a block, the remaining blocks are not affected. See also the question 'What do I do when the encrypted filesystem on my TrueCrypt volume is corrupted?

http://www.truecrypt.org/faq

What do I do when the encrypted filesystem on my TrueCrypt volume is corrupted?

File system within a TrueCrypt volume may become corrupted in the same way as any normal unencrypted file system. When that happens, you can use filesystem repair tools supplied with your operating system to fix it. In Windows, it is the 'chkdsk' tool. TrueCrypt provides an easy way to use this tool on a TrueCrypt volume: Right-click

the mounted volume in the main TrueCrypt window (in the drive list) and from the context menu select 'Repair Filesystem'.