# SOLUTION DE CRYPTAGE DISK

TRUECRYPT

Ce guide décrit l'installation de truecrypt sous Windows xp ainsi que la création d'un volume crypté.



Agence Nationale de la Sécurité Informatique



Gestion de document

Version	Date	Modification apportée
0.1	08/06/2009	Première version
0.2	05/02/2010	Maj. de version et de rédaction de guide.

Document Publique

Document Interne

# PLAN

Prés	sentation	3
1.	Installation	3
2.	Création de volume	6
3.	Monter un disque	13
4.	Démonter un disque	18

### PRESENTATION

TrueCrypt est un logiciel libre et gratuit de chiffrement à la volée, fonctionnant sur Microsoft Windows XP/2000/2003/Vista (32-bit et 64-bit), Mac OS X et Linux.

Il permet de créer un disque virtuel chiffré (volume TrueCrypt) contenu dans un fichier et de le monter comme un disque physique réel. TrueCrypt peut aussi chiffrer une partition entière ou un périphérique, comme une disquette ou une clé USB.

Tout ce qui sera stocké dans un volume TrueCrypt sera entièrement chiffré. Il est ainsi possible, par exemple, d'en réparer le système de fichiers avec chkdsk, ou de défragmenter les volumes créés par TrueCrypt une fois montés. Le chiffrement à la volé signifie que le volume chiffré est rattaché à l'arborescence du système de fichiers comme s'il était un disque dur physique (ou un périphérique amovible), rendant ainsi son contenu accessible de la même manière que le contenu des volumes non chiffrés.

Vous pouvez le télécharger depuis son site officiel : <u>http://www.truecrypt.org/downloads</u>

#### **1. INSTALLATION**

- Après avoir téléchargé le fichier « Truecrypt Setup 6.3a.exe » et exécutez-le.

initial (protection of the		
.icense You must accept these license term:	s before you can use, extract, or install TrueCrypt.	line.
IMPORTANT: By checking the check agree to be bound by and to comply	box below and clicking Accept, you accept these license terms and with them. Click the 'arrow down' icon to see the rest of the licen	J ise.
TrueCrypt License Version 2.8		^
ANY KIND. THE AUTHORS AND DIS ANYONE WHO USES, COPIES, MOE SUCH ACTION(S), ACCEPTING AND THIS LICENSE. IF YOU DO NOT ACT THE SOFTWARE, NOR ANY PART(S	TRIBUTORS OF THE SOFTWARE DISCLAIM ANY LIABILITY. DIFIES, OR (RE)DISTRIBUTES ANY PART OF THE SOFTWARE IS, I O AGREEING TO BE BOUND BY ALL TERMS AND CONDITIONS OF CEPT THEM, DO NOT USE, COPY, MODIFY, NOR (RE)DISTRIBUTE I) THEREOF.	BY
I. Definitions		
1. "This Product" means the work (i	including, but not limited to, source code, graphics, texts, and	~
1. "This Product" means the work (i	including, but not limited to, source code, graphics, texts, and by the license terms	~
1. "This Product" means the work (i	including, but not limited to, source code, graphics, texts, and by the license terms	

😰 TrueCrypt Setup 6.3a	_ 🗆 🛛
<b>Wizard Mode</b> 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.	
Extract 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 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 r the extracted file 'TrueCrypt.exe' (then TrueCrypt will run in portable mode).	e or :un
TrueCrypt Installer	Cancel

- Une fois l'interface de l'installation apparaît, vous êtes invité à choisir le chemin de l'installation ainsi que quelques paramètres.

😰 TrueCrypt Setup 6.3a	
<b>Setup Options</b> 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 specified folder does not exist, it will be automatically created.	the
C:\Program Files\TrueCrypt\	owse
<ul> <li>Install for all users</li> <li>Add TrueCrypt to Start menu</li> <li>Add TrueCrypt icon to desktop</li> <li>Associate the .tc file extension with TrueCrypt</li> <li>Create System Restore point</li> </ul>	
TrueCrypt Installer	Cancel
TrueCrypt Setup 6.3a	X

Installing C:\Program Files Installing C:\Program Files Installing C:\WINDOWS\ci	(TrueCryp TrueCryp)	t\truecrypt.sys t\truecrypt-x64. rivers\truecrypt	.sys		
Adding registry entry Soft	;\TrueCryp :ware\Clas	t\TrueCrypt Seti ses\TrueCryptVc	up.exe olume		
Adding registry entry Sol Adding registry entry Sol	TrueCry	pt Setup			
Adding registry entry Sol Adding registry entry Sol Installing TrueCrypt devi	(i)	TrueCrypt has	; been successfully	installed.	5
Starting TrueCrypt devic Adding icon C:\Document	4			eCrv	ot\TrueCrypt.lol
Adding icon C:\Document Adding icon C:\Document			ОК	BCry BCry	pt\TrueCrypt Wi pt\Uninstall True
Adding icon C:\Document. Installation completed.	- <mark>ana 3000</mark>	ngala na ang na	rodayn do erypenn	BCN	peroninistali mue

TrueCrypt est livré avec un manuel d'utilisation en anglais, pendant la première installation réalisé vous serez inviter à lire le manuel.

# 2. CREATION DE VOLUME

TrueCrypt vous permet de :

- ✓ créer un volume virtuel
- $\checkmark~$  chiffrer un périphérique tel qu'une clé USB
- ✓ chiffrer une partition système ou un disque dur entier, c'est à dire une partition ou un lecteur sur lequel Windows est installé.
- Cliquez sur « create volume »

TrueCrypt	
Volumes System Keyfiles Tools Settings Help	Homepage
Drive         Volume         Size         Encryption algorithm           H:         I:         J:         K:         <	Type
Create Volume     Volume Properties     Wipe       Volume     Image: Select sele	: Cache t File Device
Mount All Dismount All	Exit

- Dans notre tutorial nous allons créer un volume virtuel qui sera ensuite monté en étant un disque physique.



- Dans cette étape, vous avez le choix de créer un standard ou un volume TrueCrypt caché. Dans ce guide, nous allons choisir la première option, c'est de créer un volume TrueCrypt standard.

TrueCrypt Volume Creation Wizar	d 📃 🗖 🔀
	Volume Type
	Standard TrueCrypt volume
	Select this option if you want to create a normal TrueCrypt volume.
	C Hidden TrueCrypt volume
RUE C	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 you to solve such situations without revealing the password to your volume. <u>More information about hidden volumes</u>
	Help < Back Next > Cancel

- Nous allons créer notre volume TrueCrypt dans le dossier « C:\Mes Documents\volume crypté » et le nom du volume (conteneur) sera « mon volume » (comme on peut le voir dans la capture d'écran ci-dessous). Notez que le fichier Mon volume n'existe pas encore, Truecrypt le créera.
- IMPORTANT: Notez que Truecrypt ne cryptera pas les fichiers existants. Si vous sélectionnez un fichier existant, il sera écrasé et remplacé par le volume nouvellement créé. Vous serez en mesure de chiffrer les fichiers existants (plus tard) en les déplaçant vers le volume Truecrypt que nous sommes en train de le créer.

Specify Path a	nd File Name				? 🔀
Enregistrer dans :	Colume crypté		• +	🗈 💣 🎫	
Mes documents récents Direau					
Mes documents					
Poste de travail					
Favoris réseau	Nom du fichier :	mon volume			Enregistrer
	Туре:	All Files (*.*)			Annuler

TrueCrypt Volume Creation Wizar		
	Volume Location cuments\volume crypté\ma volume.docx! ✓ Never save history A TrueCrypt volume can reside in a file (calle which can reside on a hard disk, on a USB fla TrueCrypt container is just like any normal fi example, moved or deleted as any normal fi choose a filename for the container and to s you wish the container to be created. WARNING: If you select an existing file, Tru it; the file will be deleted and replaced with to TrueCrypt container. You will be able to enco on) by moving them to the TrueCrypt contait to create now.	Select File  TrueCrypt container), ash drive, etc. A le (it can be, for le). Click 'Select File' to elect the location where eCrypt will NOT encrypt he newly created rypt existing files (later ner that you are about
	Help < Back N	ext > Cancel

- Ici, vous pouvez choisir un algorithme de chiffrement et un algorithme de hachage pour le volume. Truecrypt utilise l'un des algorithmes de cryptage suivants et il peut même combiner entre eux.
  - AES
  - Serpent
  - Twofish

Comme il utilise les algorithmes de hachage afin d'être utiliser pour générer « *Random Number* » plus tard.

- RIPEMD-160
- SHA-512
- Whirlpool

Vous pouvez faire une petite recherche sur internet sur le fonctionnement de chaque algorithme et si vous ne savez pas quoi choisir ici, vous pouvez utiliser les paramètres par défaut et cliquez sur Suivant

	Encryption Options
	AES Test
<b>H</b>	More information on AES       Benchmark
T B C	Hash Algorithm          RIPEMD-160       Information on hash algorithms

 Ici, nous précisons que la taille de notre container Truecrypt soit à 1 mégaoctet.
 Une fois que vous tapez la taille souhaitée dans le champ de saisie cliquez sur Suivant.

TrueCrypt Volume Creation Wizar	d 🔲 🗖 🔀
	Volume Size
	1 C KB @ MB C 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.
L L	The minimum possible size of an NTFS volume is 2829 KB.
	Help < Back Next > Cancel

- C'est l'une des étapes les plus importantes. Ici, vous devez choisir un bon mot de passe pour le volume.
- Lire attentivement les informations affichées dans la fenêtre de l'assistant de ce qui est considéré comme un bon mot de passe.
- Après avoir choisi un mot de passe, tapez-le dans le champ de saisie, puis cliquez sur Suivant.

TrueCrypt Volume Creation Wizard	
TBUEGBH	Volume Password         Password:         ********         Confirm:         Use keyfiles         Display password         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.
	Help < Back Next > Cancel

 Déplacez votre souris de manière aléatoire que possible dans la fenêtre Assistant de création de volumes, pendant au moins 30 secondes. Ceci augmente sensiblement le niveau de chiffrement des clés de cryptage. Ensuite Cliquez sur Format.

TrueCrypt Volume Creation Wizard	d 📃 🗖 🔀
	Volume Format Options Filesystem FAT  Cluster Default  Dynamic Random Pool: 968304BE69D1CCF17159A9D64C5CABCA
	Header Key: Master Key: Abort 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

Cliquez sur OK pour fermer la boîte de dialogue.

-



- Nous venons tout juste réussi à créer un volume Truecrypt.

Cliquez sur Exit afin de fermer l'assistant de « Création de Volume Truecrypt ».



# 3. MONTER UN DISQUE

Dans les étapes suivantes, nous allons monter le volume que nous venons de créer. Nous allons revenir à la fenêtre principale de Truecrypt.

- Sélectionnez une lettre de lecteur dans la liste. Ça sera la lettre de lecteur à laquelle le volume Truecrypt sera monté.

Note: vous pouvez choisir n'importe quelle autre lettre de lecteur disponible.

 Cliquez sur « Select file ». La fenêtre du sélecteur de fichier standard devrait apparaître.

📅 TrueCrypt	
Volumes System Keyfiles Tools Settings Help H	lomepage
Drive Volume Size Encryption algorithm Typ	e 🔼
≪⇒G: ≪⇒H:	
× K:	≡
See 1: See M:	
N:	
See 2013	_
₩ ₩ ₩ ₩ ₩ ₩ ₩ ₩ ₩ ₩ ₩ ₩ ₩ ₩ ₩ ₩ ₩ ₩ ₩	
S:	~
Create Volume Volume Properties Wipe Cache	.
Select File	
✓ Never save history	
Volume Tools Select Device	
Mount Auto-Mount Devices Dismount All Exit	

- Dans le sélecteur de fichier, naviguez jusqu'au dossier contenant le volume, sélectionnez le et cliquez sur Ouvrir.

Select a TrueC	rypt Volume		? 🛛
Regarder dans : Mes documents récents Bureau	volume crypté	• 🗈 😁 💌	
Mes documents Poste de travail			
Favoris réseau	Nom du fichier :	ma volume	Ouvrir
	Fichiers de type :	All Files (*.*)	Annuler

- Dans la fenêtre principale de Truecrypt, cliquez sur Monter. La fenêtre d'invite de dialogue de Mot de passe devrait apparaître.

🎆 True	Crypt										
Volumes	System	Keyfiles	Tools	Settings	Help					Home	epage
Drive G: G: G: G: G: G: G: G: G: G:	Volume						Size	Encryption	algorithm	Туре	
	Create Vo	olume	]		Volume Pr	operties,			Wipe	Cache	
		:\Documer Never sa	its and S ve histor	iettings\jih Y	iene\Mes	document: Volum	s\volun e Tool:	ne cr 💌	Selec Select I	t File Device	
	Mount		Auto	-Mount De	evices	D	ismoun	t All		Exit	

- Tapez le mot de passe dans le champ de saisie de mot de passe.

Enter passv	Enter password for C:\Documents and Setting\ma volume.docx							
Password:	****		ОК					
	Cache passwords and	keyfiles in memory	Cancel					
	🔲 Use keyfiles	Keyfiles	Mount Options					

- Nous venons de montée avec succès le volume comme un disque virtuel « M: » Le disque virtuel est entièrement crypté (y compris les noms de fichiers, les tables d'allocation, l'espace libre, etc.) et il se comporte comme un véritable disque.
- Vous pouvez ouvrir le volume monté, par exemple, en double-cliquant sur la lettre « *M* : » comme il est marqué dans la capture d'écran ci-dessus.
- Vous pouvez également parcourir le volume monté dans « poste de travail ».

umes by	stem K	eyfiles To	ools Sett	ings Help					Home	paç
Drive Vo	lume					Size	Encryption al	gorithm	Туре	1
ise ised at the set of the set										
• I: • 1:										
-K:										
M: C:	\Docume	nts and Se	ttings\ji	(ma volume	.docx	768 KB	AES		Normal	1
N:										
P:										
Q:										
Q: R: S:										
Q: R: S: T:										
Q: R: S: T:										
Q: R: S: T: Cre	ate Volur	ne		Volume	Properties			Wipe	Cache	
Q: R: S: T: Cre	ate Volur	ne j		Volume	Properties			Wipe	Cache	
Q: R: S: T: Cre Volume	ate Volur	ne	and Settin	Volume	Properties		ne cr 💌	Wipe /	Cache File	
Q: R: S: T: Cre	ate Volur  ⊂:\D  ⊽ Ne	ne ocuments	and Settin	Volume Igs\jihene\M	Properties es docume		ne cr 💌	Wipe 1	Cache File	
Q: R: S: T: Cre Volume	ate Volur C:\D I♥ Ne	ne ocuments ever save	and Settin history	Volume Igs\jihene\M	Properties es docume Voli	nts\volur	ne cr 💌 📃	Wipe Select Select D	Cache File	
Q: R: S: T: Cre Volume	eate Volur C:\D V Ne	ne ocuments ever save	and Settin history	Volume Igs\jihene\M	Properties	nts\volur	ne cr 💌 🔤	Wipe - Select Select D	Cache File	



- Vous pouvez copier des fichiers vers et à partir du volume Truecrypt juste comme vous les copiez sur un disque normal. Les fichiers qui sont lus ou copiés à partir du volume chiffré Truecrypt sont automatiquement décryptés à la volée dans la mémoire / RAM.
- De même, les fichiers qui sont écrits ou copiés dans le volume chiffré Truecrypt sont automatiquement cryptés à la volée dans la RAM.
- Notez que : Truecrypt sauve jamais de données décryptées dans un disque. Il ne les stocke que temporairement dans la RAM (mémoire). Même lorsque le volume est monté, les données stockées dans le volume sont toujours cryptée. Lorsque vous redémarrez Windows ou éteignez votre ordinateur, le volume sera démonté et tous les fichiers stockés sur elle ne seront pas accessible.

# 4. Demonter un disque

- Si vous souhaitez fermer le volume et rendre tous les fichiers stockés dedans inaccessible, alors démonter le volume comme suit :

TrueC	rypt				
Volumes :	System Keyfiles Tools	Settings Help			Homepage
Drive G: H: I:	Volume		Size	Encryption algorithm	Туре 🔨
<ul> <li>J:</li> <li>K:</li> <li>M:</li> <li>N:</li> </ul>	C:\Documents and Setting	js∖ji…\ma volume.docx	768 KB	AES	≣ Normal
0: P: Q: R: S: T:	reate Volume	Volume Proc	erties	Wine	Carhe
Volume	C:\Documents and	Settings\jihene\Mes do	ocuments\volur	ne cr 💌 Selec	t File
	Vever save histo	Dry _	Volume Tool	s Select	Device
D	Dismount Aut	o-Mount Devices	Dismour	nt All	Exit