TRUECRYPT SUR CLEF USB

(Par Sébastien Maisse -09/12/2007)

Voici un petit document concernant d'un espace crypté sur une clef usb en utilisant le logiciel TRUECRYPT. Ce dernier est gratuit et disponible à l'url suivante :

http://www.truecrypt.org

La version à l'heure de la rédaction de ce document est là : 4.3a

Ce logiciel est disponible sur plusieurs systèmes d'exploitation (Windows ainsi que sous Linux).

Cette application permet la création de volume / périphérique crypté afin de permettre la sécurisation, lors du transport, de données sur support amovible (en autres, clef usb).

Dans le cas présent, nous allons voir la mise en place d'un fichier hébergeur (sur clef usb) qui permettra le montage d'un volume virtuel pouvant accueillir des données sensibles.

Après avoir fait l'installation de TRUECRYPT, il faudra si cela n'a pas été déjà fait, le passer en langue Française. Pour ce faire, on procédera ainsi :

Settings Help Language Whot Keys Default Keyfiles Preferences	Size Encryptio	n algorithm	Home Type	page
Language WHot Keys Default Keyfiles Preferences	Size Encryptio	n algorithm	Туре	~
Preferences				
				-
				~
Volume Proper	iej.,		Cache	1
	•	Selec	t <u>F</u> ile	
Lory	/olume <u>I</u> ools	Select [D <u>e</u> vice	
uto-Mount Devices	Di <u>s</u> mount All	[]	E <u>x</u> it	
	tory	tory Volume Tools uto-Mount Devices Dismount All	Volume Properties Wipe Image: Select for y with the select for y withe select for y with the select for y withe sel	Volume Properties Wipe Cache ✓ Select File tory Volume Iools Juto-Mount Devices Dismount All

On clique sur le menu Settings / Language

TrueCrypt - Language 🔀
English Français
- Active language pack
Language pack version:
Translated by:
Download language pack
QK Cancel

Puis là, une fenêtre s'affiche, on sélectionne le choix **Français**.

Si le choix **Français** n'est pas disponible, c'est que l'on a pas installer le language pack. Pour ce faire on clique sur le lien **Download language pack**, ceci aura pour effet de lancer le navigateur internet sur la page contenant les différentes traductions disponibles.

TrueCrypt									
Fichier <u>V</u> olume:	s Fichiers <u>c</u> lé	<u>O</u> utils <u>P</u> a	ramètres	<u>A</u> ide				<u>S</u> ite	Web
Le Volum	e				Taille	Algorithme	de chiffre	Туре	
N: 0: P: 0:				G					
R: S: T: U: V:									W
SX: SY:					1				₩
Créer u Volume	n volume		Prophé	tës du val	ume	-	Videnie	cache	
	 □ Ne jamais e	nregistrer l'hi	storique	Outil	s pour le v	olume	Fich Périphe	ier śrique	
Mont	er 🔤	Montage au	utomatique		Tout dém	onter		Quitter	

Notre logiciel est maintenant en langue française.

Nous allons procéder à la création de notre disque de voyage, à savoir les fichiers qui seront contenu sur la clef usb. Dans le cas présent, j'utilise une clef usb de 4 Go de marque Corsair .

TrueCrypt		_ 🗖 🔀
Fichier <u>V</u> olumes Fichiers <u>c</u> lé	Outils Paramètres Aide	Site Web
Le Volume	Banc de test Test des vecteurs	Igorithme de chiffre Type
M: N: O:	Paramétrer le disque de voyage pénérateur de fichier clé Assistant de création de volume	ES Normal
Q: G B:	Actualiser les lettres de lecteur	-
S: T: U:	Sauvegarder l'en-tête du volume Restaurer l'en-tête du volume	
₩: ₩: X:	Effacer l'historique du volume Vider le cache des mots de passe	
Créer un volume	Propriétés du volume	
Volume	nregistrer Phistorique	Fichier
	Outils pour le v	olume Périphérique
Démonter	Montage automatique Tout dém	onter Quitter

On clique sur le menu **Outils** / **Paramétrer le disque de voyage**.

Paramétrage du disque de voyage TrueCrypt	
Paramètres de fichier	
Créer des fichiers de disque de voyage sur (racine du disque de vo	iyage):
L	Parcourir
Inclure l'assistant de création de volume TrueCrypt	
Configuration de l'autorun (autorun.inf)	
A l'insertion du disque de voyage:	
• Ne rien faire	
C Exécuter TrueCrypt	
C Montage automatique d'un volume TrueCrypt (ci-dessous)	
Paramètres de montage	
Volume l'rueCrypt à monter (par rapport à la racine du disque de v	/oyagej:
	Parcount
Monter le volume avec la lettre 1ère disponible 🔍	
Ouvrir l'Explorateur pour le volume monté	
Monter le volume en lecture seule	
🗖 Mot de passe en cache	
Créer	Fermer

On choisi la destination...

кı	
	<u>^</u>
💷 🐨 🍘 🖅 🐨 🔮 Favoris réseau	~

Paramétrage du disque de voyage TrueCrypt Paramètres de fichier Créer des fichiers de disque de voyage sur (racine du disque de voyage): K:\-I Parcourir... Inclure l'assistant de création de volume TrueCrypt Configuration de l'autorun (autorun.inf) A l'insertion du disque de voyage: Ne rien faire Exécuter TrueCrypt Montage automatique d'un volume TrueCrypt (ci-dessous). Monter le volume avec la lettre 1ère disponible -Ouvrir l'Explorateur pour le volume monté Monter le volume en lecture seule Mot de passe en cache Créer Fermer

On coche (si ce n'est déjà fait) la case **Inclure l'assistant de création de volume TrueCrypt**. Par défaut, lors de l'insertion de la clef, il ne se passera rien. L'option **Ne rien faire** étant sélectionnée par défaut.

Dans le cas présent, ma clef usb est le lecteur K:

Ma clef usb est à présent prête pour accueilir un volume crypté.



Voilà, les quelques fichiers contenus sur cette dernière...

Nom 🔺	Taille	Туре	Date de modification
Language.fr.xml	96 Ko	Document XML	06/05/2007 14:35
TrueCrypt Format.exe	888 Ko	Application	03/05/2007 20:22
TrueCrypt.exe	815 Ko	Application	03/05/2007 20:21
📾 truecrypt.sys	185 Ko	Fichier système	03/05/2007 20:22
🛅 truecrypt-x64.sys	194 Ko	Fichier système	03/05/2007 20:22

Comme on peut le voir, il y a deux programmes l'un servant à la création d'un volume (voir cidessous), l'autre pour le montage de notre volume crypté une fois créé.

Passons maintenant à la création de notre volume. Pour ce faire, il suffit de cliquer sur **TrueCrypt** Format.exe

Kassistant de création de volume True	Crypt 📃 🗖 🔀
	Assistant de création de volume
	Créer un volume TrueCrypt standard
	C Créer un volume TrueCrypt caché
1	Définition d'un volume caché
	Cet assistant va vous aider à créer un nouveau volume TrueCrypt.
<u> </u>	Important: La collecte des données aléatoires a commencé. Les données seront utilisées pour créer la clé principale (master keu), la
	clé secondaire (mode LRW) et le sel (salt) pour le nouveau volume. Les données collectées comprennent les mouvements de la souris
	dans cette fenêtre, les clics, les touches pressées et d'autres valeurs obtenues du système. Les données devraient être aussi aléatoires
	que possible, aussi plus vous déplacez aléatoirement votre souris, meilleur c'est.
	Aide <précédent annuler<="" suivant="" td=""></précédent>

On choisi la création d'une volume standard, si nous souhaitons un volume caché on choisira la deuxième option.

Ici, nous souhaitons créé un fichier volume dans lequel sera contenu nos fichiers cryptés. Si je souhaitais utiliser ma clef entièrement, je choisirais l'option **Périphérique**.

Donc, je clique sur l'option **Fichier** et j'indique le répertoire dans lequel sera créé mon fichier.

Emplacement du volume	
K:\TrueCrypt\DONNEES_PERSO	Fichier
🔽 Ne jamais enregistrer l'historique	Périphérique
 Vous pouvez créer des volumes à fichier héber volumes) ou chiffrer des partitions entières de c disquettes, des clés USB ainsi que d'autres pér stockage. Cliquez sur 'Fichier' pour spécifier l l'emplacement du fichier à créer pour héberger ou cliquez sur 'Périphérique' pour choisir une périphérique à chiffrer. AVERTISSEMENT: Si vous chiffrez une partiti toutes les données présentes seront effacées. 	gé (file-hosted lisques durs, des iphériques de e nom et le nouveau volume partition / on / périphérique
Aide / Précédent Suis	ant Annular

Ici, le fichier sera enregistrer sur la clef (K:\) dans le répertoire **TrueCrypt** et le nom du fichier volume sera **DONNEES_PERSO**. On clique sur le bouton Suivant.

	Options de chiffrement	1
	AES	✓ Tester
	AES Serpent Twofish AES-Twofish AES-Twofish-Serpent Serpent-AES Serpent-Twofish-AES Twofish-Serpent	en 1998) approuvé ces/départements phiquement les le 128 bits, 14 rondes Banc de test
TRI	Algorithme de hachage	jorithmes de hachage

Ci-dessous, nous voilà avec les différents algorithmes de chiffrement...

L	Options de chiffren Algorithme de chiffrement	rent
	AES	▼ Tester
П	par la FIP'S qui peut être utilisé fédéraux américains pour proté informations sensibles. Clé à 25 (AES-256). Le mode opératoire <u>Plus d'information sur AES</u>	par les agences/départements ger cryptographiquement les i6 bits, bloc de 128 bits, 14 rondes est LRW. Banc de test
E	Algorithme de hachage	
	RIPEMD-160	os : algorithmes de hachage
	SHA-1 Whirlpool	1
	And the second s	

Comme, on peut le voir, le choix est vaste. Une description sous l'algorithme de chiffrement choisi permet d'avoir une idée de comment se passe le chiffrement des données.

Dans le cas présent, j'ai choisi d'utiliser un chiffrement offrant un bon rapport chiffrement / vitesse.

F Assistant de création de volume TrueCr	ypt	. 🗆 🖂
	Options de chiffrement	
	AES-Twofish-Serpent	Tester
	Trois chiffrements en cascade opérant en moi bloc est d'abord chiffré avec Serpent (clé de 2 Twofish (clé de 256 bits) et enfin avec AES (c Chaque chiffrement utilise sa propre clé. Toute mutuellement indépendantes. <u>Plus d'informations</u>	de LRW. Chaque 256 bits), puis avec lé de 256 bits). es les clés sont Banc de test
TR	Algorithme de hachage RIPEMD-160	<u>s de hachage</u>
	Aide < Précédent Shiya	nt > Annuler

Ainsi que les différents algorithmes de hachage.

Chiffrement AES-Twofish-Serpent et hachage RIPEMD-160

Concernant la taille du fichier, il fera **1 Go**, ce qui est déjà bien pour y stocker quelques fichiers texte (en autres).

Assistant de création de volume True	Crypt 📃 🗖 🔀
	Taille du volume
	1000 C Ko @ Mo
	L'espace libre sur le disque K:\ est de 3859.32 Mo.
	Spécifiez la taille du conteneur à créer.
	Si vous créez un conteneur dynamique, ce paramètre spécifiera sa taille maximale.
TR	Notez que la taille minimale d'un volume FAT est de 19 Ko. La taille minimale d'un volume NTFS est de 2526 Ko.
	Aide < Précédent Suivant > Annuler

Ci-dessous, nous devons définir un mot de passe de taille correcte et contenant des caractères alphanumérique. Où, si l'on pense oublier le mot de passe, on peut utiliser un fichier qui servira de clef pour pouvoir monter le volume. Le fichier peut-être un fichier son, vidéo, texte, etc... Par contre, il faudra faire attention de ne pas altérer ou perdre le fichier clef en question, sinon le volume ne pourra plus être monter.

Kassistant de création de volume TrueCrypt	_ 🗆 🔀
Mot de	passe du volume
Confir	mer:
	Afficher mot de passe Fichiers clé
Il est très im devriez évite dictionnaire devrait pas pas être fac minuscules comme @ ^	portant que vous choisissiez un bon mot de passe. Vous er d'utiliser un mot simple que l'on trouve dans un (ou une combinaison de plusieurs de ces mots). Il ne contenir de noms ou de dates de naissance. Il ne devrait le à deviner. Un bon mot de passe est une combinaison de et de majuscules, de chiffres et de caractères spéciaux _\$ * + etc.
Il est recom caractères (caractères.	nandé de choisir un mot de passe d'au moins 20 le plus long, le mieux). La longueur maximale est de 64
Ai	de < Précédent Suivant > Annuler

Section de volume TrueC	rypt 📃 🗆 🔀
L	Formatage du volume Options Système FAT Y Cluster Par défa Y Dynamique
	Nb aléatoire: 5CB1A5A43EBECA85D8471D7A66D601AA Clé d'en-tête: 17994510CF09192C03A6D63F8154600E Clé principale: 96D241211A556712E0416A43633E8CC6
TRU	Terminé 91 Mo Vitesse 6.6 Mo/s Reste 2 minutes Ici, paramétrez des options supplémentaires qui affecteront le format du nouveau volume. Consultez la doc pour plus d'infos. Quand vous avez terminé, cliquez sur 'Formater' pour créer votre nouveau volume. Vitesse 6.6 Mo/s Reste 2 minutes Aide Annuler

Formatage du volume en cours...

Patience... Patience.

Kassistant de création de volume TrueCr	ypt 📃 🗖 🔀
L d	Formatage du volume
	Nb aléatoire: 5CB1A5A43EBECA85D8471D7A66D601AA Clé d'en-tête: 17994510CF09192C03A6D63F8154600E Clé principale: 96D241211A556712E0416A43633E8CC6
TRUE	Terminé 503 Mo Vitesse 7.7 Mo/s Reste 64 s Ici, paramétrez des options supplémentanés qui affecteront le format du nouveau volume. Consultez la doc pour plus d'infos. Quand vous avez terminé, cliquez sur 'Formater' pour créer votre nouveau volume.
	Aide < Précédent Eormater Annuler

Notre volume est à présent créé.



On clique sur le bouton **OK**.

F Assistant de création de volume TrueCi	rypt 📃 🗖 🔀
	Volume créé
TRUECH	Le volume TrueCrypt a été créé et il est prêt à l'emploi. Pour créer un autre volume TrueCrypt, cliquez sur 'Suivant'. Sinon 'Quitter'.
	Aide < Précédent Suivant > Suitter

Si nous n'avons pas d'autres volumes a créés, il suffit de cliquer sur le bouton **Quitter** pour fermer l'application.

Voici le contenu de ma clef usb, une fois mon fichier volume créé.

Nom 🔺	Taille	Туре	Date de modification
Eanguage.fr.xml	96 Ko	Document XML	06/05/2007 14:35
TrueCrypt Format.exe	888 Ko	Application	03/05/2007 20:22
TrueCrypt.exe	815 Ko	Application	03/05/2007 20:21
truecrypt.sys	185 Ko	Fichier système	03/05/2007 20:22
truecrypt-x64.sys	194 Ko	Fichier système	03/05/2007 20:22
DONNEES_PERSO	1 024 000 Ko	Fichier	09/12/2007 00:29

Nous allons pouvoir à présent monter notre volume nouvellement fait.

e volume L: M: N:		Taille	Algorithme de	chiffre	Туре
0: P: Q: R: S: T: U: V:					
X: X:					
X: Y: Créer un volume	Propriétés du v	alume]	ļ	Vider le c	ache
Y: Y: Créer un volume /olume K:\TrueCrypt\DONNE	Propriétés du v ES_PERSO	alume 👖		Vidente c Fichier	ache

Il faut cliquer sur le programme **TrueCrypt.exe** qui se trouve sur notre support amovible.

On choisi notre fichier volume grâce au bouton Fichier. Puis on clique sur le bouton Monter.

Là, le mot de passe que nous avons indiquer à la création du volume est requis...

Entrez le mot de passe	e pour K:\TrueCrypt\DONNEES_	PERSO
Mot de passe:	I	ОК
🗖 Mots	de passe et fichiers de clé en cacl	ne Annuler
🗌 Affici	her mot de passe ers clé Fichiers clé	Options

Attention à ne pas se tromper (ci-dessous).



Le V	'olume	Taille	Algorithme de chiffre	Туре	^
 L: M: N: O: K P: Q: 	:\TrueCrypt\DONNEES_PERSO	999 Mo	AES-Twofish-Serpent	Normal	
S T: U: U:					
¥: Y:					*
W: X: Y: Cré	er un volume Propriétés du	volume	Vider I	e cache	-
V: Y: Cré Volume	ier un volumePropriétés du 	volume	Vider I	e cache hier	
V: X: Y: Cré	er un volume Propriétés du K:\TrueCrypt\DONNEES_PERSO Ne jamais enregistrer l'historique	volume	Vider f Ficl volume Périph	e cache hier iérique	·

Notre volume est à présent monter sur la lettre **O**:

Ma clef usb est en dessous le volume crypté ayant été monter en lecteur **O**: Bien entendu, j'aurais pu choisir une autre lettre disponible.



J'ai nommé **PERSO_DEMO** le disque contenant mon volume monté, à vous de choisir le nom qui vous convient.

Lorsque vous avez fini d'utiliser le volume crypté, vous pouvez le démonter de façon simple et rapide. Pour ce faire, il suffit de cliquer sur le bouton **Démonter**. Là, la lettre O: disparaît.

TrueCry	pt			_ 🗆 🕑
ichier ⊻olu	mes Fichiers <u>c</u> lé <u>O</u> utils <u>P</u> aran	nètres <u>A</u> ide		<u>S</u> ite Web
Le Vo	lume	Taille	Algorithme de chiffre	Туре 🔥
SL: M: N: D: K:	\TrueCropt\DONNEES PERSO	999 Mo	AES-Twofish-Serpent	Normal
P: Q: P: S: T: U: V:				
≪W: ≪X: ≪Y:				*
W: X: Y: Crée	r un volume	Propriétés du volume	Viderfe	e cache
V: X: Y: Crée Volume		Propriétés du volume	Vider le	e cathe
V: X: Y: Volume	r un volume K:\TrueCrypt\DONNEES_PER Ne jamais enregistrer l'histo	Propriétés du volume RSO rique Outils pour le	Vider Ir Fich volume Périph	e cache

Si un fichier stocké sur l'espace crypté, il est possible que la boîte suivante s'affiche.



Rien de bien méchant puisque vous pouvez forcer le démontage du volume. Prenez garde à fermer vos documents proprement sous peine dans certaines conditions de les endommagés.

Voilà, vous pouvez à présent, vous baladez tranquillement avec votre support amovible sans craindre qu'on ne vous voles vos données sensibles.

Vous pouvez me contacter par e-mail, si vous avez des questions / problèmes, à l'adresse suivante :

thecyberseb@hotmail.com ou sur le forum : http://forum.monserveurperso.com topic Tutoriels