

Verschlüsseln sensibler Daten auf einem USB-Stick unter Windows XP mittels TrueCrypt



1. Wozu eigentlich?

Die Entwicklung immer kleinerer, dabei aber gleichzeitig leistungsfähigerer Datenträger ermöglicht uns den mühelosen Transport von Datenunmengen. Ein Datenträger in Lippenstiftgröße ist leicht zu tragen (und zu verlieren) - die Verantwortung für die darauf befindlichen Daten oft schwer. Besonders dann, wenn sich sensible Daten von Drittpersonen darauf befinden. Diese Anleitung soll dabei helfen, auch die Verantwortung leicht tragen zu können.

Apropos Verantwortung: Obwohl diese Anleitung gewissenhaft zusammengestellt wurde, übernimmt der Autor keinerlei Verantwortung für Verluste oder Schäden, die aus dem Vertrauen auf die Richtigkeit der bereitgestellten Inhalte und Informationen resultieren! Es obliegt der Verantwortung des Verwenders, die Richtigkeit, Genauigkeit, Vollständigkeit oder den Nutzen der bereitgestellten Inhalte zu überprüfen. Also ein wenig Verantwortung bleibt Ihnen nicht erspart.

2. Was brauchen wir dazu?

- Freien Speicherplatz auf einem USB-Stick
- Die kostenfreie Software TrueCrypt (<u>www.truecrypt.org</u>)
- Eventuell die deutsche Benutzeroberfläche (www.truecrypt.org/localizations.php)
- Ein paar Minuten Lernbereitschaft ...

3. Die Installation

 Wir laden von <u>www.truecrypt.org/downloads.php</u> die "Latest Stable Version" f
ür Windows Vista/XP/2000 herunter (TrueCrypt Setup.exe)



• Wir starten TrueCrypt Setup.exe, lesen sorgfältig die Lizenz-Bedienungen und akzeptieren sie mittels Klick auf "I accept and agree to be bound by the licence terms" und [Accept].

P TrueCrypt Setup	
License You must accept these license terms before you can use, extract, or install TrueCrypt.	
IMPORTANT: By selecting the first option below and clicking Accept, you accept these license terms agree to be bound by and to comply with them. Click the 'arrow down' icon to see the rest of the lic	; and ense.
TrueCrypt Collective License Version 1,3	~
Software distributed under this license is distributed on an "AS IS" BASIS WITHOUT WARRANTIES OF ANY KIND. THE LIABILITY OF THE AUTHORS AND DISTRIBUTORS OF THE SOFTWARE IS LIMITED.	
ANYONE WHO USES, COPIES, MODIFIES, OR (RE)DISTRIBUTES ANY PART(S) OF A WORK MADE AVAILABLE UNDER THIS VERSION OF THE TRUECRYPT COLLECTIVE LICENSE, IS, BY SUCH ACTION(S), ACCEPTING ALL TERMS OF THE COMPONENT LICENSES (SEE BELLOW) THAT APPLY TO THE CORRESPONDING PART(S) OF THE WORK. IF YOU DO NOT ACCEPT THEM, DO NOT USE, COPY, MODIFY, NOR (RE)DISTRIBUTE THE WORK, NOR ANY PART(S) THEREOF.	
I accept and agree to be bound by the license terms Joseph and agree to be bound by the license terms	
Help < Back Accept	Cancel

• Nun wählen wir für unseren Einsatzzweck zuerst "Extract" aus, dann klicken wir auf [Next].

😰 TrueCrypt Setup	
Wizard Mode Select one of the modes. If you are not sure which to select, click Next.	
← Install	
Select this option if you want to install or update TrueCrypt on this s	ystem.
Extract If you select this option, all files will be extracted from this package I installed on the system. Do not select it if you intend to encrypt the system drive. Selecting this option can be useful, for example, if you TrueCrypt in so-called traveler (portable) mode. TrueCrypt does not on the operating system under which it is run. After all files are extra directly run the extracted file 'TrueCrypt.exe' (then TrueCrypt will ru You can also move the extracted files to other computers.	but nothing will be system partition or J want to run : have to be installed acted, you can Jn in traveler mode).
TrueCrypt Installer	
Help < Back M	Vext > Cancel

• Mittels [Browse ...] suchen wir unseren USB-Stick (z.B. Wechseldatenträger (G:)) und klicken anschließend auf [Extract]

xtraction Options		-222
Here you can set various opt	ions to control the extraction process,	
Please select or type the loc	ration where you want to place the extracted files:	
G:		Browse
If the specified folder does i	not exist, it will be automatically created.	- X
	location when finished	
Onen the destination I		
I✓ Open the destination I		
I✓ Open the destination I		

• Jetzt sollten wir die Meldung "All files have been successfully extracted ..." erhalten und klicken auf [OK]

All files have been successfully ex	tracted to the destination location.	U DE
Extracting G:\TrueCrypt User Gui Extracting G:\License.txt Extracting G:\TrueCrypt.exe Extracting G:\TrueCrypt Format.e Extracting G:\truecrypt.sys Extracting G:\trueCrypt Setup All files have	de.pdf exe nave been successfully extracted to the destination location.	
		÷

• Wir beenden dieses Setup mit einem Klick auf [Finish]

Extraction Complete All files have been successfully extracted to the destination location.		
	•	
Extracting G:\TrueCrypt User Extracting G:\License.txt Extracting G:\TrueCrypt.exe Extracting G:\TrueCrypt Form Extracting G:\truecrypt.sys Extracting G:\truecrypt-x64.s All files have been successfull	Guide.pdf nat.exe sys y extracted to the destination location.	*

• Wir laden von <u>www.truecrypt.org/localizations.php</u> die deutsche Benutzeroberfläche (langpack-de.zip) herunter.

Georgian ქართული	1.0.0	Complete	Download	Kakha Lomiashvili
German Deutsch	0.1.0	Incomplete	Download	Racoon
Greek Ελληνικά	1.0.0	Complete	Download	Βασίλης Κοσμίδης

• Wir entzippen diese Datei und kopieren/verschieben die entzippte Datei "Language.de.xml" zu den anderen, vorher extrahierten TrueCrypt-Dateien.

Name 🔺	Größe	Тур
E Language.de.xml	154 KB	XML-Dokument
License.txt	29 KB	Textdokument
TrueCrypt Format.exe	1.193 KB	Anwendung
📓 TrueCrypt User Guide.pdf	774 KB	PDF-XChange \
TrueCrypt.exe	1.081 KB	Anwendung
truecrypt.sys	219 KB	Systemdatei
truecrypt-x64.sys	225 KB	Systemdatei

4. Anlegen eines verschlüsselten Daten-Containers

• Wir starten das Programm "TrueCryptFormat.exe" (gemischtsprachige Benutzeroberfläche) belassen die Wahl "Create a file-container" und klicken auf [Weiter].



• Wir belassen den Volume-Type bei den voreingestellten Werten und klicken auf [Weiter].

Volume Type
Standard TrueCrypt volume
Select this option if you want to create a normal TrueCrypt volume.
C Hidden TrueCrypt volume
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.
More information about hidden volumes
 Hilfe / Back Weiter > Abbrecher

• Wir klicken auf [Datei ...]

TrueCrypt Volume Creation Wizard	Volume-Speicherort
BUEGBU	 ✓ ORTIME-Speicneroft Datei ✓ Verlauf nicht speichern 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. WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file 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. Hilfe < Back Weiter > Abbrechen

• ... und tragen in das Eingabefeld "Dateiname" einen beliebigen Dateinamen (z.B. "area51") ein. Anschließend klicken wir auf [Speichern] und auf [Weiter].

Dateiname:	area51	•	Speichern
Dateityp:	Alle Dateien (*.*)	•	Abbreche

TrueCrypt Volume Creation Wizard	Volume-Speicherort
TBUEGR	G:\area51 ■ Datei ✓ Verlauf nicht speichern 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. WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file 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.
	Hilfe < Back Weiter > Abbrechen

• Wir belassen die Verschlüsselungseinstellungen bei den voreingestellten Werten und klicken auf [Weiter].

	Verschlüsselungsalgor	ithmus	
	AES		Test
	used by U.S. governr classified information 128-bit block, 14 rour	ment departments and ag up to the Top Secret leve nds (AES-256). Mode of c <u>en über AES</u>	encies to protect el. 256-bit key, peration is XTS. Benchmark
-	Hash-Algorithmus)

• Wir tragen die gewünschte Volume-Größe (z.B. 500 MB) ein und klicken auf [Weiter].

Volume-Größe
500 Скв Смв
Please specify the size of the container to create.
If you create a dynamic (sparse-file) container, this parameter will specify its maximum size. Note that the minimum possible size of a FAT volume is 19 KB. The
minimum possible size of an NTFS volume is 2573 KB.
Hilfe 🛛 < Back Weiter > 🔪 Abbrecher

• Wir geben ein möglichst langes Kennwort ein, bestätigen dieses, indem wir es ein zweites Mal eintragen und klicken auf [Weiter].

Kennwort: ********************
 Bestätigung: ***********************
Schlüsseldat. verw. Schlüsseldateien.
verwendet werden. Das Kennwort sollte keine Namen oder Geburtstage enthalten, und nicht leicht erratbar sein. Ein gutes Kennwort ist eine zufällige Kombination aus Groß- und Kleinbuchstaben, Zahlen, und Sonderzeichen wie @ ^ = \$ * + etc

• Wir belassen entweder die Volume-Format-Einstellungen bei den voreingestellten Werten oder ändern z.B. das Dateisystem auf NTFS und klicken auf [Formatieren].

Volume-Format	
Zufallswerte: A8D608742A7463932E110EE0958EAF09 Headerschlüssel: Hauptschlüssel:	v
Erled. Geschw. Rest	n
IMPORTANT: Move your mouse as randomly as possible within the window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. The click Format to create the volume.	nis en
Hilfe < Back Formatieren Abbre	chei

• Jetzt sollten wir die Meldung "Das TrueCrypt-Volume wurde erfolgreich erstellt" erhalten und klicken auf [OK].

Dateisystem FAT - Cluster Vorgabe - Dynamisch
Zufallswerte: 3461D34E351B852CB7BC974AB74E7339 Headerschlüssel: 04BE8C10B44A349DFCB8FF3C1F42E2D8 Hauptschlüssel: FAE03649F14169D93B35B3BF50BA050D
Abbrechen TrueCrypt Volume Creation Wizard
Das TrueCrypt-Volume wurde erfolgreich erstellt.

 Wir beenden das Anlegen von verschlüsselten Daten-Containern mit einem Klick auf [Beenden].



Alle Schritte bis hierher müssen nur beim ersten Mal durchgeführt werden. Ab jetzt beginnt die normale Arbeit mit dem verschlüsselten Daten-Container und die folgenden Schritte sind jedes Mal durchzuführen.

5. Einbinden (mounten) des verschlüsselten Daten-Containers

• Wir ziehen mit gedrückter linker Maustaste den angelegten Datencontainer (z.B. "area51") auf die Programm-Datei "TrueCrypt.exe" und lassen die Maustaste los, sobald sich der Pfeil über dem Dateinamen "TrueCrypt.exe" befindet.



• Wir wählen einen freien Laufwerksbuchstaben (z.B. "V") und klicken auf [Einbinden].

	rypu						Sand Hard Street	
lumes	System	Schlüsseldateier	i Extras	Einstellungen	Hilfe		Hom	epag
LW	Volume				Größe	Verschlüsselung	gsalg. Typ	
۵L:								1
≦≫M: ≤≫N:								
•P:								
Q; → R;								
• S:								
T: Contra								
٧:	1000							
W:								
- Q.		•						
- ri								6
- ri								jii
• r;	Volume ers	stellen		Eigenschafte	m	Ci	sche sicher lösche	
	Volume ers	stellen		Eigenschafte	n	Ci	ache sicher lösche	an l
Volum	Volume ers	stellen	1	Eigenschafte	n	C	ache sicher lösche	n j
Volum	Volume ers	stellen	ļ	Eigenschafte	n	C	ache sicher lösche Datei	n []
-Volum	Volume ers e G	stellen :\area51 Verlauf nicht spe		Eigenschafte	n		ache sicher lösche Datei Datenträger	29 20
Volum	Volume ers e G	stellen :\area51 Verlauf nicht spe		Eigenschafte	n		ache sicher lösche Datei Datenträger	n]

• Wir geben unser "Volume-Kennwort" ein und klicken auf [OK].



• Wir schließen nun auch diese TrueCrypt-Dialogbox mittels [Beenden].

Truec	rypt							الثالا	×
olumes	System	Schlüsseldateien	Extras	Einstellungen	Hilfe			Home	page
LW	Volume				Größe	Verschlüsse	lungsalg,	Тур	
⇒k: ⇒L;									
≤ M: ≤ N:									
←P:									
⇒Q: SR:									
S:									1
ωŪ:									
	G:\area	51			499 MB	AES		Normal	
۰X:									
Sec. Str. 1									
ω γ:									•
Φ Υ:	Volume er:	stellen	ļ	Eigenschafte	:n		Cache sic	her löschen	•
Y:	Volume er: e	stellen		Eigenschafte	:n		Cache sic	her löscher	
-Volum	Volume er: e	stellen		Eigenschafte	n		,Cache sic	ther löschen stei	
volum	Volume er: e G V	stellen :\area51 Verlauf nicht speic	hern	Eigenschafte	n		Cache sic Da Daten	her löschen stei	

Das Programm selbst wird damit NICHT beendet. Es läuft ab jetzt im Hintergrund und verschlüsselt bzw. entschlüsselt unsere Daten im TrueCrypt-Datencontainer. Kontrollieren können wir das in der XP-Taskleiste bei den Tray-Icons am blauen TrueCrypt-Symbol. (Ein Mausklick darauf würde wieder die soeben geschlossene Dialog-Box öffnen.)



6. Arbeiten mit dem verschlüsselten Daten-Container

- Wir öffnen den "XP-Arbeitsplatz" und sollten hier ein neues Laufwerk (z.B. "Lokaler Datenträger (V:)") finden.
- Dieses neue "verschlüsselte Laufwerk" können wir ab sofort, wie jedes andere normale Laufwerk, zum Speichern und Lesen von Daten verwenden.
- Aber Achtung! Wir sollten nur Kopien von Daten in verschlüsselten Daten-Containern speichern. (Siehe unten die FAQs)

7. Trennen (unmounten) des verschlüsselten Daten-Containers

• Wir klicken in der "XP-Taskleiste" auf das "TrueCrypt-Trayicon"



• Wir markieren mit der Maus das zu trennende Laufwerk, klicken auf [Trennen] und beenden schließlich TrueCrypt mittels Klick auf [Beenden].

LW Volume Grö K: L; M: M: M: N: P: Q: Q: R: S: T: U: V: G:\area51 499 I W: X: Y: 499 I	ße Verschlüsselungsa MB AES	alg. Typ ^
M: N: P: Q: R: S: T: U: V: G:\area51 W: X: Y:	MB AES	E Normal
		•
Volume erstellen Eigenschaften Volume G:\area51		ne sicher löschen
Verlauf nicht speichern VolOper.	stionen	Patenträger

8. Was haben wir nun davon?

- Wir können unseren USB-Stick getrost verlieren, stehlen lassen oder im Garantiefall dem Händler zurückgeben.
- Alle Daten, die im verschlüsselten Daten-Container gespeichert wurden, können nur mehr mit TrueCrypt und unserem Volume-Kennwort gelesen werden.
- Bei Verlust oder Diebstahl haben wir lediglich einen finanziellen Schaden, aber keinen moralischen und können auch nicht gesetzlich belangt werden.
- Wir trinken nun entspannt einen Schluck Kaffee und freuen uns.

9. FAQs

- F: Ich habe das Volume-Kennwort vergessen, wie ... ?
- A: Dann "vergessen" wir auch die verschlüsselten Daten.
- F: Ich habe den USB-Stick unsachgemäß entfernt und die Daten-Container-Datei ist beschädigt, wie ... ?
- A: Dann sind auch die verschlüsselten Daten beschädigt und nicht mehr herstellbar.
- F: Muss man vor dem Entfernen des USB-Sticks mittels "Hardware sicher entfernen" den Daten-Container trennen (unmounten)?

A: Ja.

- F: Muss man vor dem Herunterfahren des PCs den Daten-Container trennen (unmounten)?
- A: Nein. Das macht TrueCrypt bzw. das Betriebssystem automatisch.
- F: Funktioniert das ganze nur auf einen USB-Stick?
- A: Man kann auf jedem Datenträger (PC-Festplatte, Notebook-Festplatte, CD, DVD, etc.) einen verschlüsselten Daten-Container anlegen und einbinden. Auch wenn man anstatt eines USB-Sticks ein beliebiges Laufwerk oder einen beliebigen Ordner z.B. auf der Festplatte wählt, kann man die vorliegende Anleitung verwenden.
- F: Funktioniert das ganze auch ohne Administratorenrechte?
- A: Ja. Allerdings muss der Administrator vorher TrueCrypt "installieren".
- F: Kann man mit einer Kopie oder einem Backup der Daten-Container-Datei arbeiten? A: Ja.
- F: Kann die Daten-Container-Datei über einen UNC-Pfad (z.B. \\meinserver\schule\area51) eingebunden werden?
- A: Ja. Das TrueCrypt-Programm muss aber von einem lokalen Laufwerk (z.B. U:\TrueCrypt\TrueCrypt.exe) gestartet werden.
- F: Sind in dieser Anleitung alle Funktionen von TrueCrypt beschrieben?
- A: Nein, nur ein Bruchteil.
- F: Wo kann ich mein Wissen über TrueCrypt vertiefen?
 A: Mittels der original "TrueCrypt User Guide.pdf" und z.B. auf http://de.wikipedia.org/wiki/TrueCrypt http://www.truecrypt.org/fag.php