

TrueCrypt

Praxisbeispiel

Erstellen einer verschlüsselten Containerdatei

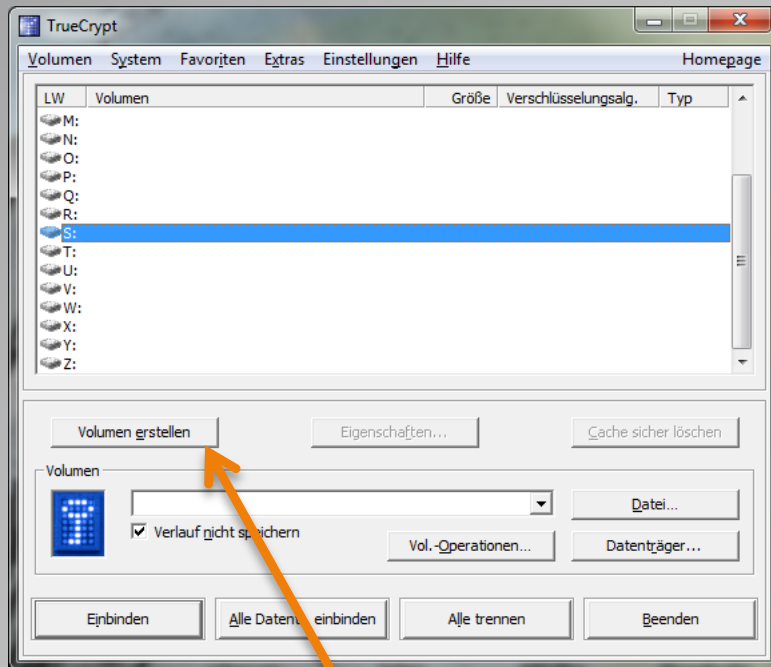
Martin Massat

03. Mai 2011

IAV 10-12

- Aktuelle TrueCrypt Version unter truecrypt.org/downloads downloaden (dieses Praxisbeispiel basiert auf Version 7.0a)
- Installationsdatei ausführen und dem Setup Wizard folgen
- Für eine deutsche Übersetzung kann zusätzlich noch ein Language Pack installiert werden:
<http://www.truecrypt.org/downloads2>

Download & Installation



Ist TrueCrypt gestartet, erhält man eine Übersicht aller verfügbaren Laufwerksbuchstaben. Diese werden später zum Einbinden der verschlüsselten Containerdatei gebraucht.

Zum Erstellen der Containerdatei klicken wir zunächst auf „Volume erstellen“.



Es öffnet sich der TrueCrypt Assistent zum Erstellen eines TrueCrypt Volumes. Wie auch in der Präsentation zu sehen, bietet TrueCrypt hier die Wahl zwischen 3 verschiedenen Verschlüsselungsmethoden. Wir bleiben bei der Standardauswahl „verschlüsselte Containerdatei“.



Im nächsten Schritt kann zwischen einem Standard Volume und einem verstecktem Volume gewählt werden. Wir werden ein Standard Volume erstellen (ein verstecktes Volume integriert ein TrueCrypt Volume in einem anderen).



Nun wählen wir einen Dateinamen sowie den Speicherort für unsere TrueCrypt Containerdatei.

Als nächstes wird der Verschlüsselungsalgorithmus ausgesucht. Dabei kann zwischen AES, Serpent, Twofish oder einer Kaskadierung gewählt werden. Die höchste Sicherheit bietet eine Kaskadierung aller 3 Verschlüsselungsalgorithmen.

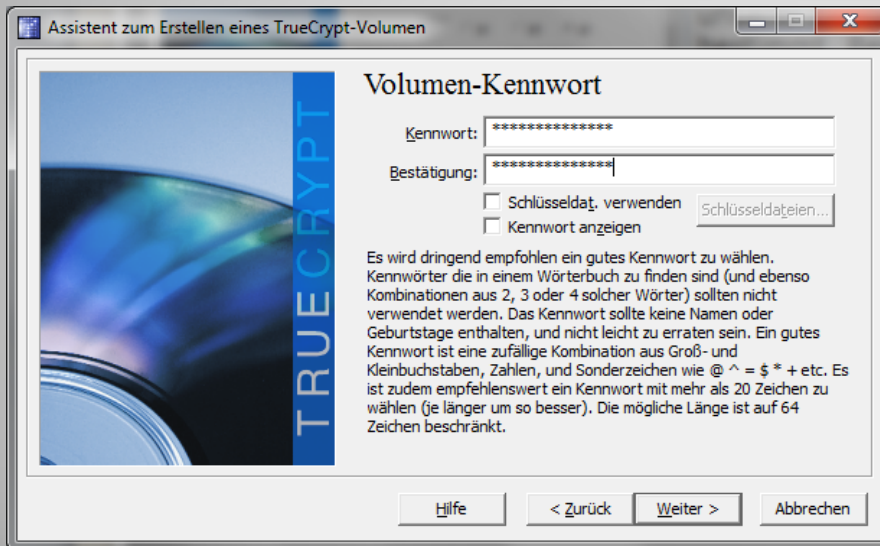


Der Nachteil einer Kaskadierung ist der Geschwindigkeitsverlust. TrueCrypt bietet dafür eine praktische Benchmark Funktion.

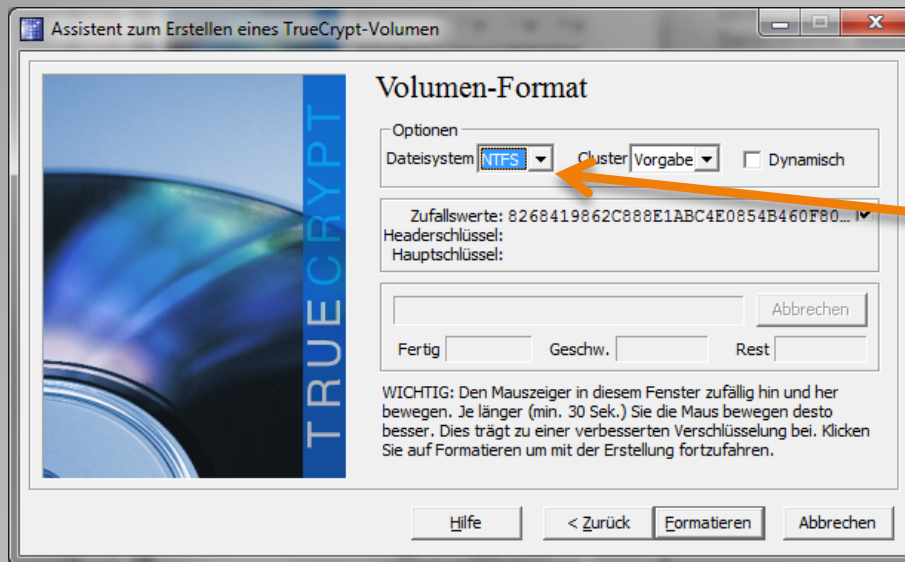
Der Hash-Algorithmus bestimmt den Algorithmus der zur Verschlüsselung des Passwortes verwendet wird. Hat also keinen Einfluss auf die Schreib-/Leseleistung.



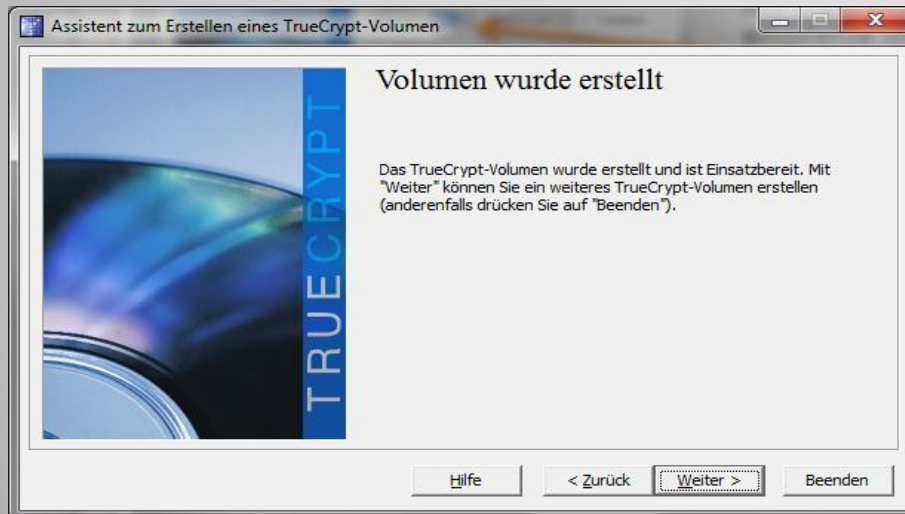
Hier wird nun die Größe der Containerdatei bestimmt. Bedenken Sie das die Größe später nicht mehr veränderbar ist und eine neue Containerdatei erstellt werden müsste.



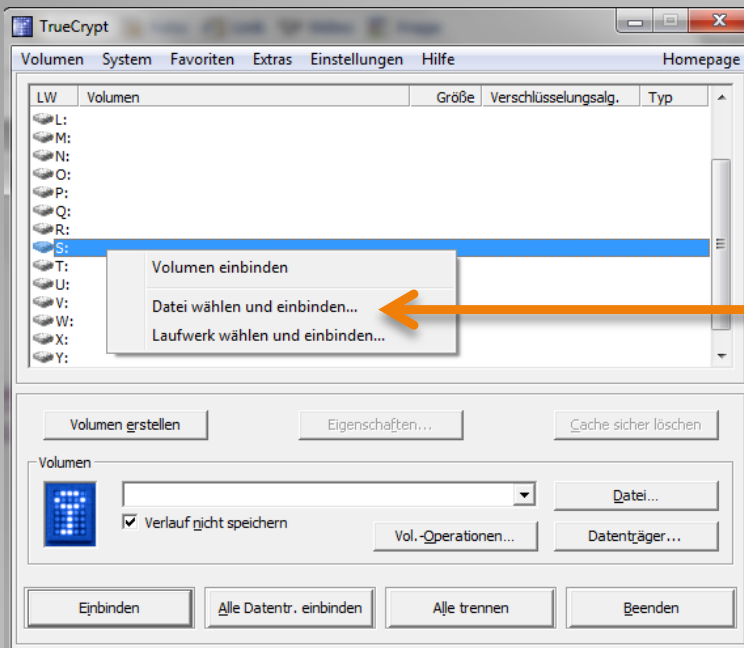
Danach kommt die Passwordeingabe. Ein sicheres Passwort sollte 10 bis 20 Zeichen lang sein und Sonderzeichen sowie Nummern beinhalten. Zusätzlich zu einem Passwort kann hier eine Schlüsseldatei erstellt werden.



Als Dateisystem empfehle ich NTFS, da dieses auch Dateien über 4GB unterstützt.



Nach dem Formatieren ist die verschlüsselte Containerdatei erstellt.



Nun kann per Rechtsklick auf ein freies Laufwerk die verschlüsselte Containerdatei ausgewählt und eingebunden werden.

Eine eingebundene Containerdatei kann danach wie ein virtuelles Laufwerk benutzt werden. Es wird im Arbeitsplatz als eigenes Laufwerk angezeigt und Dateien können on-the-fly gelesen oder geschrieben werden.

Sobald das Volume wieder getrennt wird, liegen die persönlichen Daten sicher verschlüsselt in der Containerdatei.