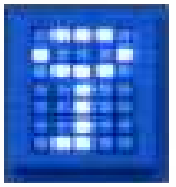
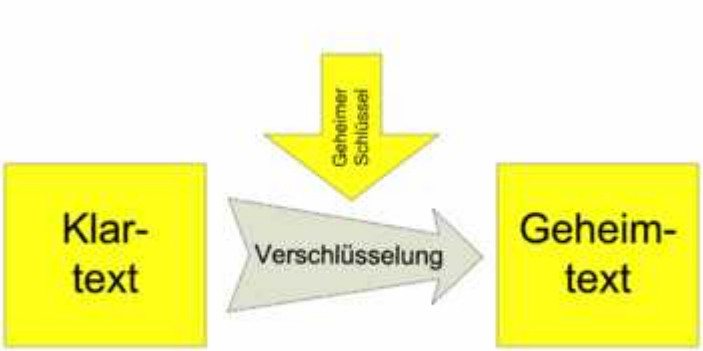
SLT – Schwabacher Linux Tage 2009

Verschluesselung mit Truecrypt





Truecrypt – Verschluesselung

Zusammenfassung Teil 1

- Was ist Truecrypt ?
- Warum Truecrypt ?
- Was macht die Software?
- Verschiedene Varianten
- Anwendungsmoeglichkeiten
- Gundlagen 1, 2 und 3
- Installation

Truecrypt – Verschluesselung

Zusammenfassung Teil 2

- Sichere Passwoerter
- Zukunftsaussichten
- Vorteile / Nachteile
- Alternativen
- LUKS / dm-crypt / cryptsetup
- Webadressen

Truecrypt – Verschluesselung

Was ist Truecrypt?

- Open Source Verschluesselungssoftware
- Grafische Benutzeroberfläche
- Einfache intuitive Bedienung
- Viele verschiedene Einsatzbereiche

Truecrypt – Verschluesselung

Warum Truecrypt?

- Niemand muss meine Daten sehen koennen – Schäuble laesst gruessen
- Daten sind bei physikalischem Zugriff auf den PC geschuetzt
- Daten sind bei Verlust (z.B. Laptop oder USB Stick) geschuetzt (zumindest bis das Passwort geknackt ist, was schonmal bis zu 10 Jahre dauern kann)
- 100 prozentigen Schutz gibt es NICHT

Truecrypt – Verschluesselung

Was macht die Software?

- Durch Kryptografische Tools wie Truecrypt wird Klartext in unleserliche Zeichenfolgen umgewandelt
- Für die Ver- und Entschluesselung muss der gleiche Algorithmus angewendet werden
- Sichere und relativ lange Passwoerter sind das A und O für sichere Verschluesselung

Truecrypt – Verschluesselung

Verschiedene Varianten

- Linux Ubuntu x86.deb oder x64.deb (“dmsetup” muss nachinstalliert werden)
- OpenSuse x86.rpm oder x64.rpm
- MAC OS X 10.5 Leopard oder 10.4 Tiger
- MS Windows 2000/XP/Vista
- Unter Debian Lenny kann das Ubuntu Paket verwendet werden (es muessen noch 3 Programme nachsinstalliert werden)
- Alle verschiedenen Varianten sind untereinander kompatibel

Truecrypt – Verschluesselung

Anwendungsmöglichkeiten

- Komplette Platte oder Systempartition verschlüsseln
- Verzeichnisse / Ordner verschlüsseln
- Einzelne Dateien verschlüsseln
- Spezielle Installation für USB Sticks
- Versteckte Container können seit Version 6.0 eingerichtet werden

Truecrypt – Verschluesselung
Grundlagen I

- **Komplette Partition verschluesseln**
  - Partition muss neu formatiert werden
  - Truecrypt ist immer im Hintergrund aktiv (wenn auf diese Partition zugegriffen wird)

Truecrypt – Verschluesselung
Grundlagen II

- **Verschluesselte Container anlegen**
  - z.B. als Dateien, Verzeichnisse, Partitionen oder auf USB Sticks/Festplatten
  - Geeignet für unverschluesselte Partitionen um verschluesselte Bereiche für sensible Daten anzulegen
  - Muessen ebenfalls formatiert werden

Truecrypt – Verschluesselung

Grundlagen III

- **Booten von Truecrypt Volumes?**
  - Funktioniert leider nicht, da die Bootpartition während des Bootvorganges nicht verschluesselt sein darf
  - Der Bootloader muss den Kern von der Systempartiton in den Speicher laden, damit der Prozessor ihn ausfuehren kann. Ist dieser Bereich verschluesselt, waere dies nicht mehr moeglich

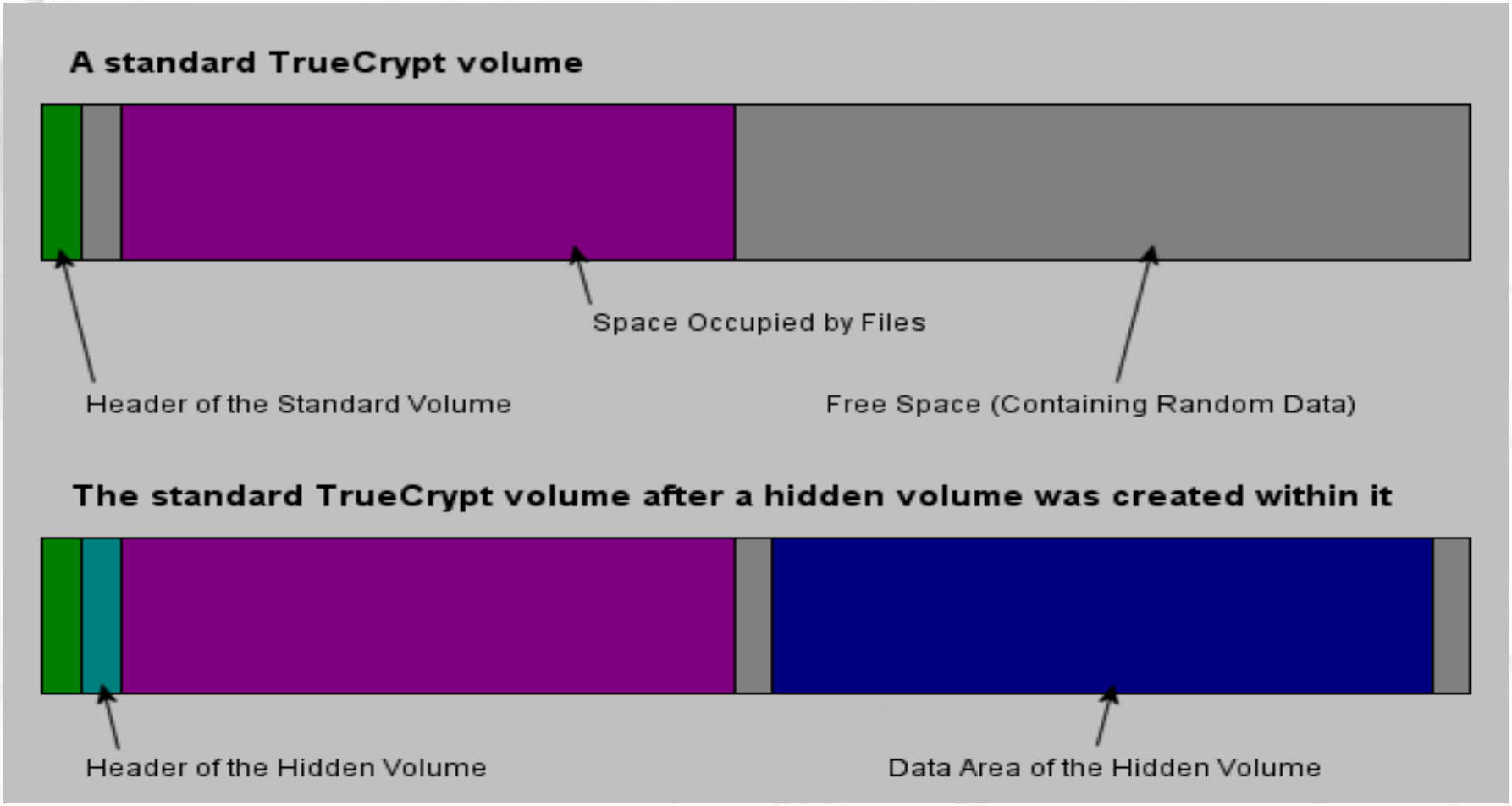
Truecrypt – Verschluesselung

Grundlagen IV

- **Hidden Volumes**
  - Versteckte Truecrypt Container
  - Extra Passwort für Hidden Container
  - Nachteil: Man sollte nicht mehr in den aeusseren Container schreiben
  - Der aeussere Container muss FAT formatiert sein
  - Vorteil: Muss man das Truecrypt Passwort herausgeben, bleiben die Daten im Hidden Container unsichtbar

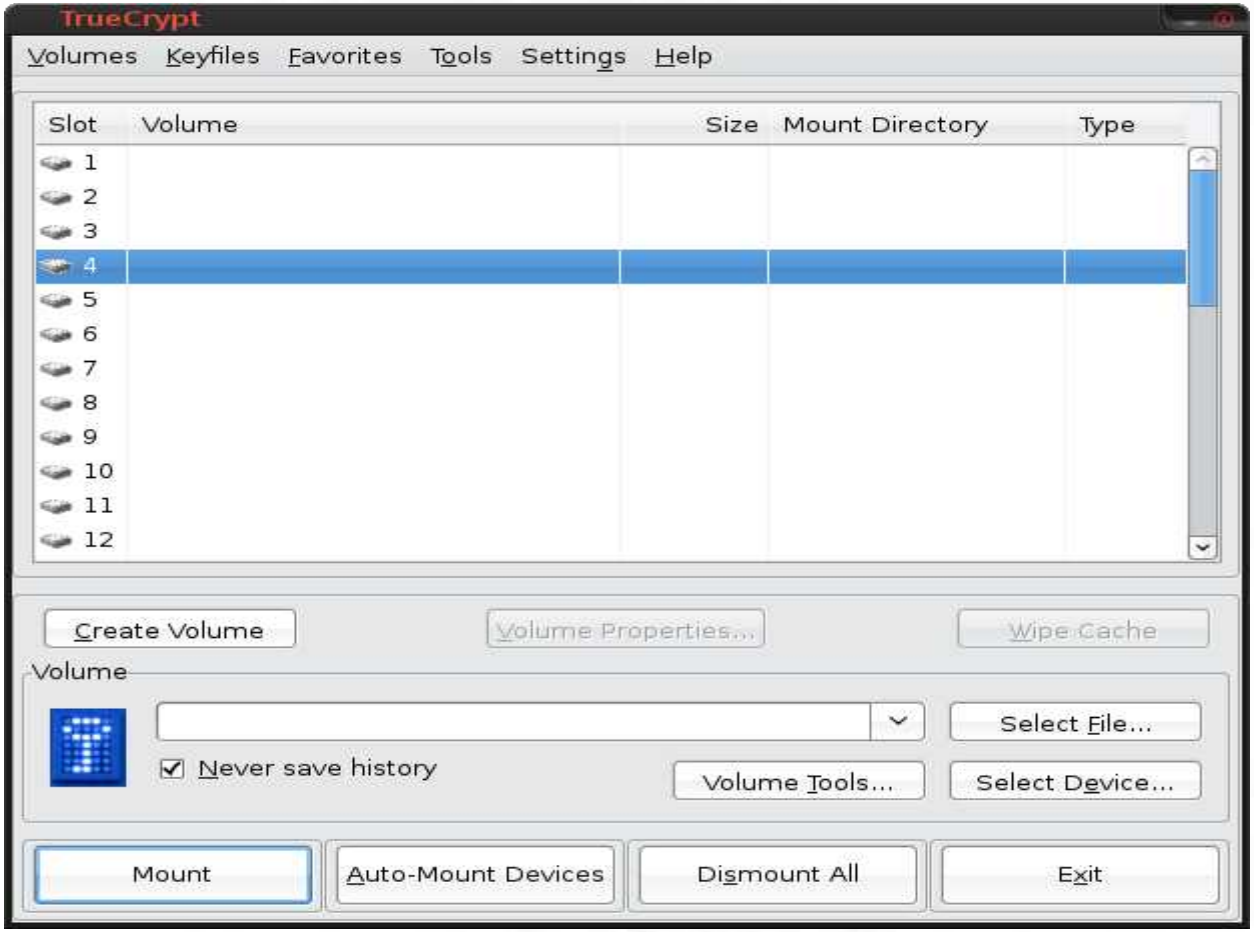
Truecrypt – Verschluesselung

Grafik Hidden Volumes



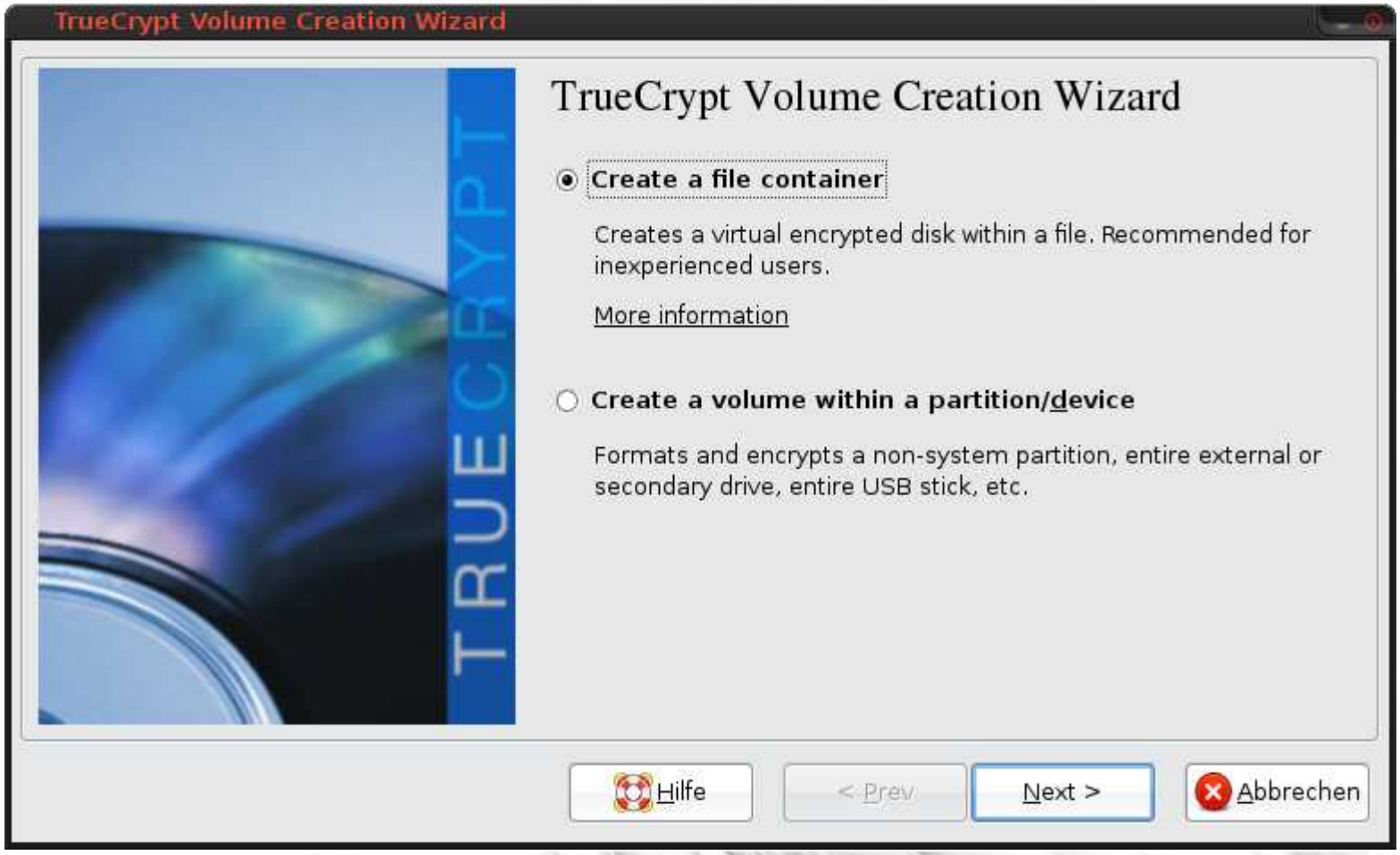
Truecrypt – Verschluesselung

Installation



Truecrypt – Verschluesselung

Installation

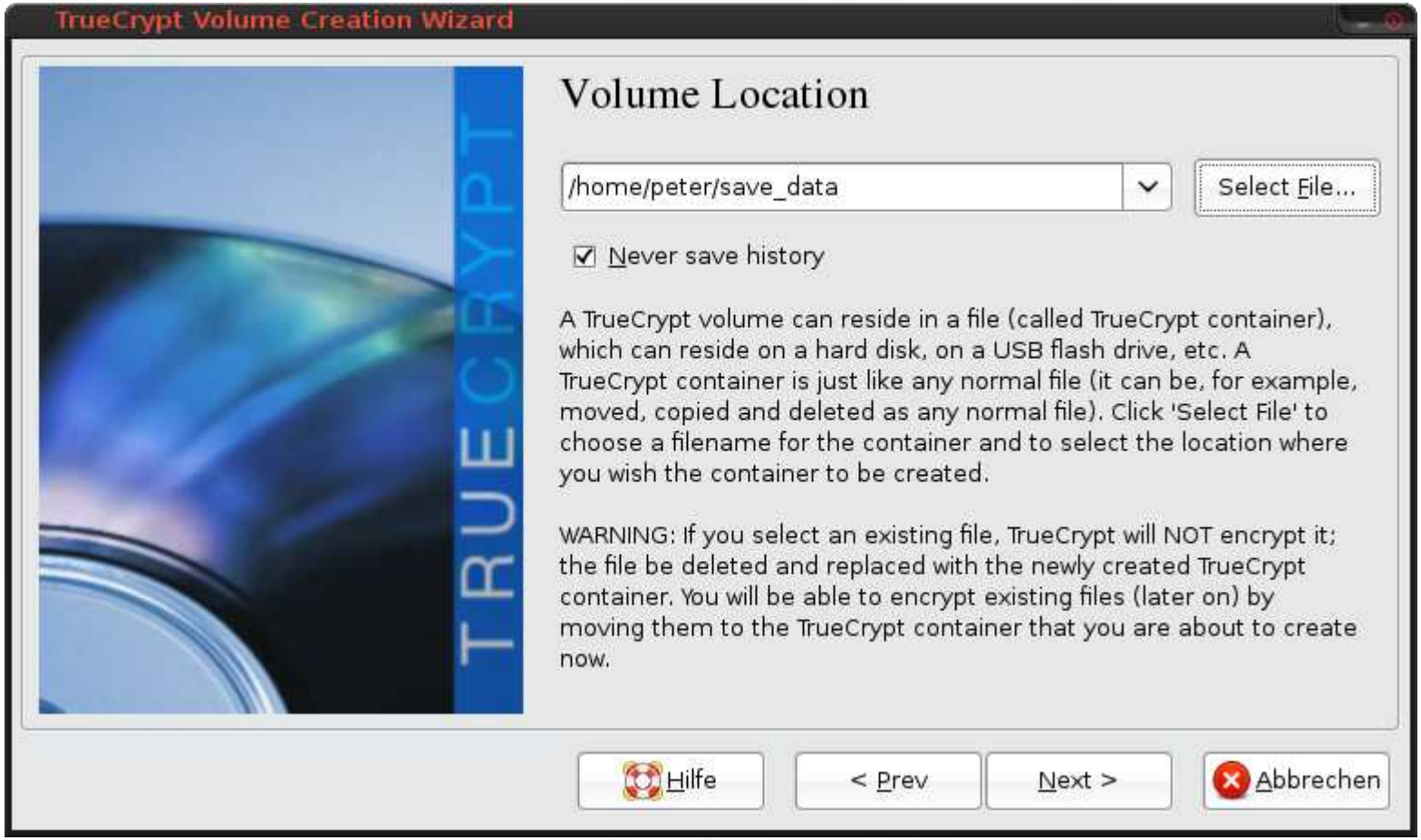


Truecrypt – Verschluesselung

Installation

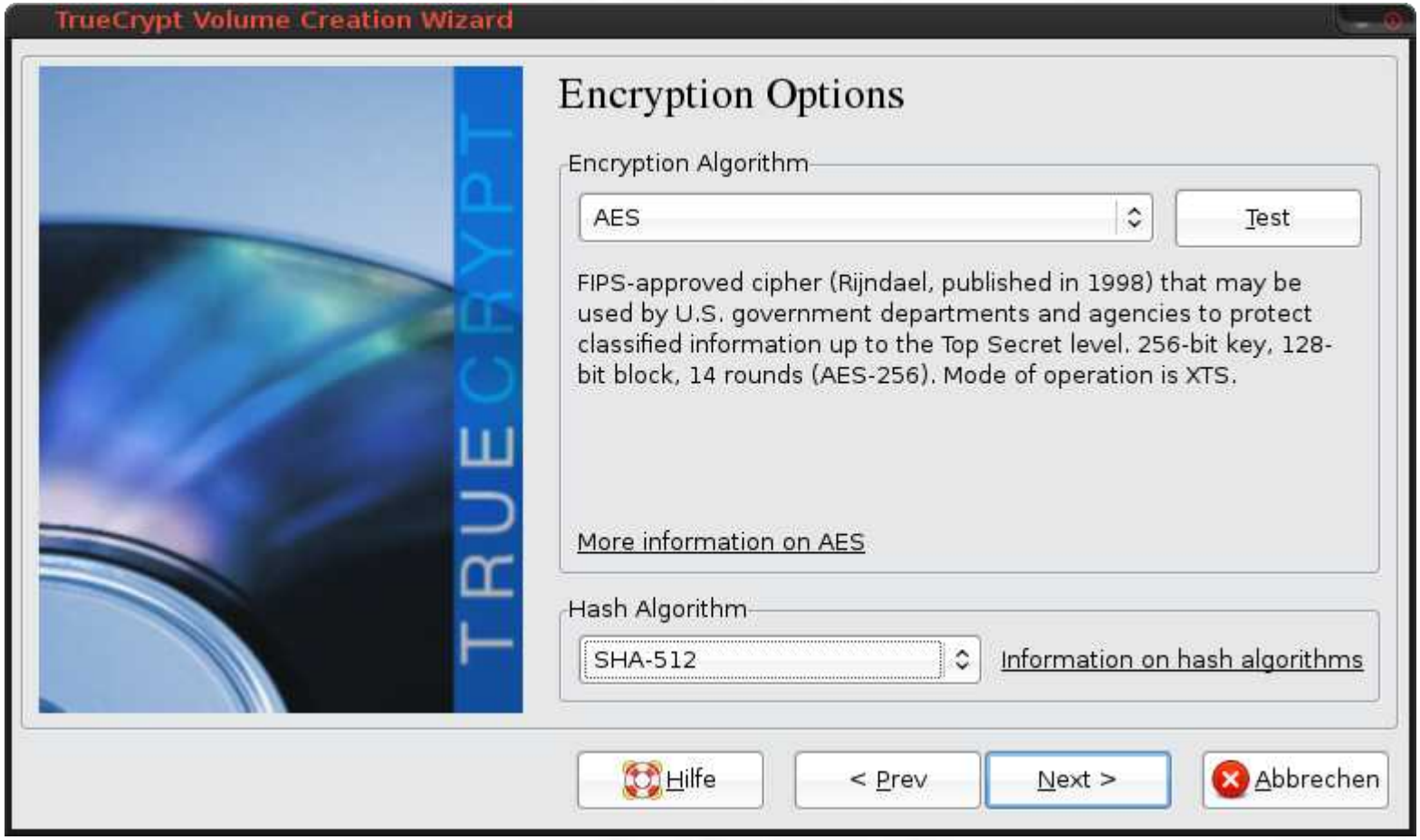
Truecrypt – Verschluesselung

Installation



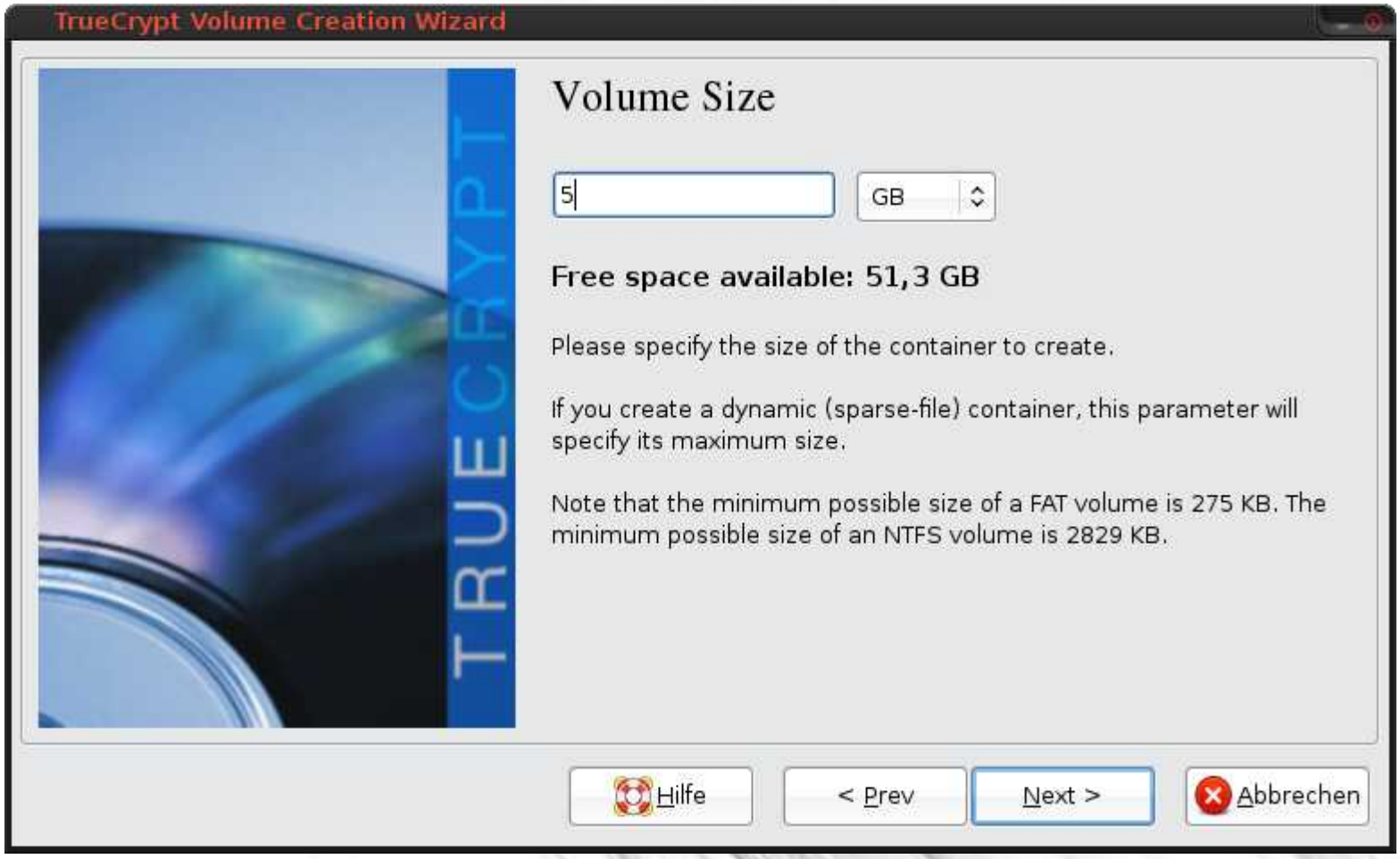
Truecrypt – Verschluesselung

Installation



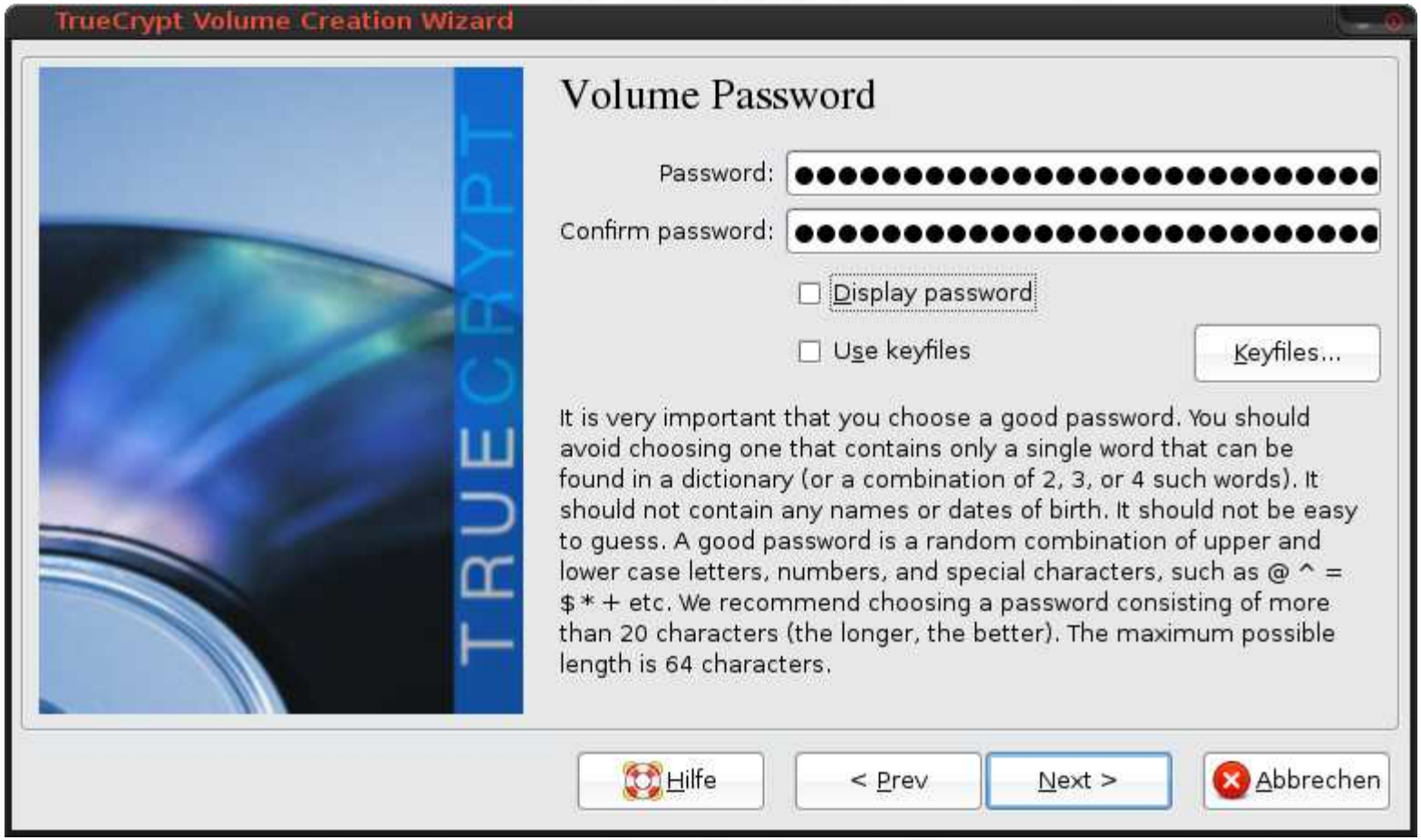
Truecrypt – Verschluesselung

Installation



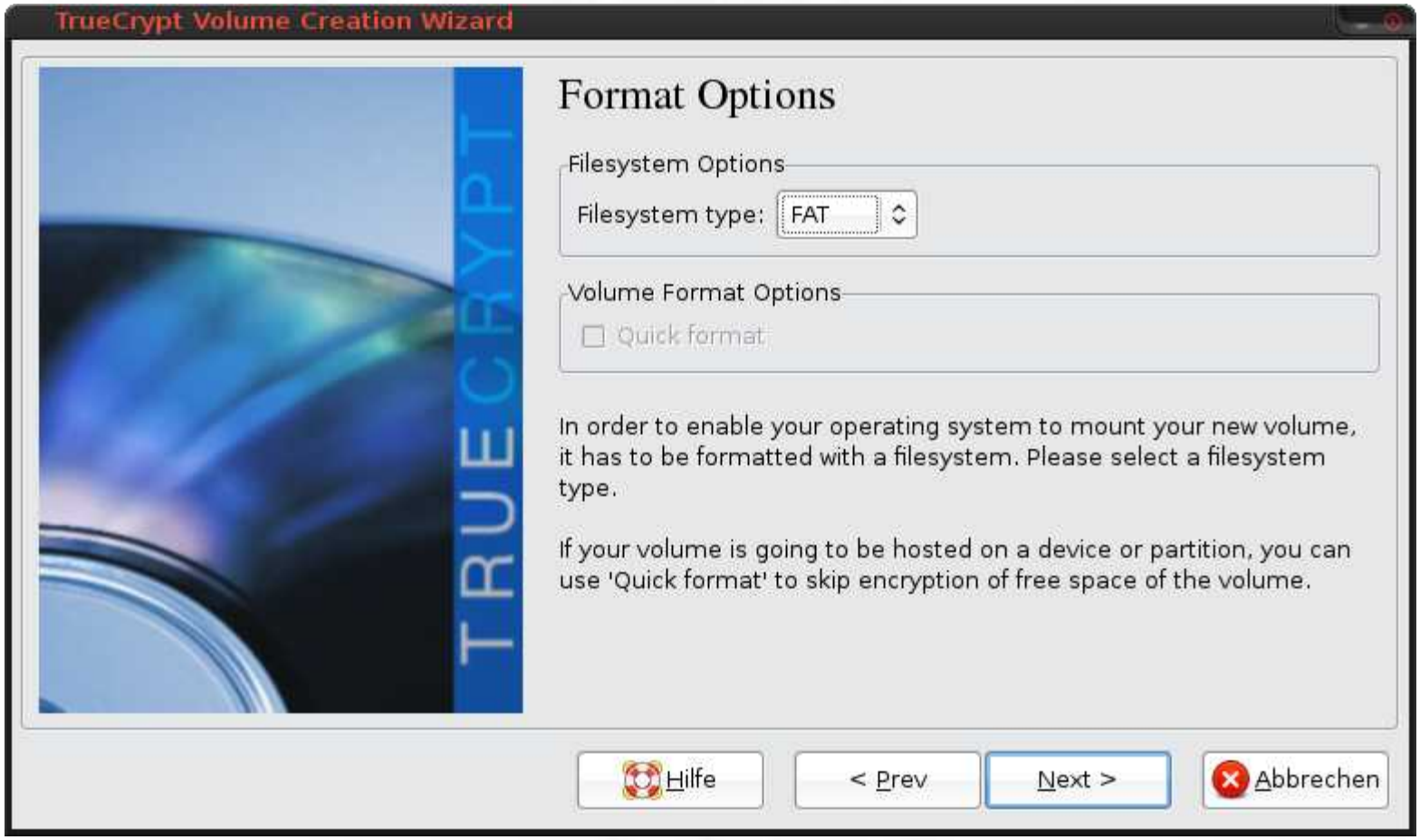
Truecrypt – Verschluesselung

Installation



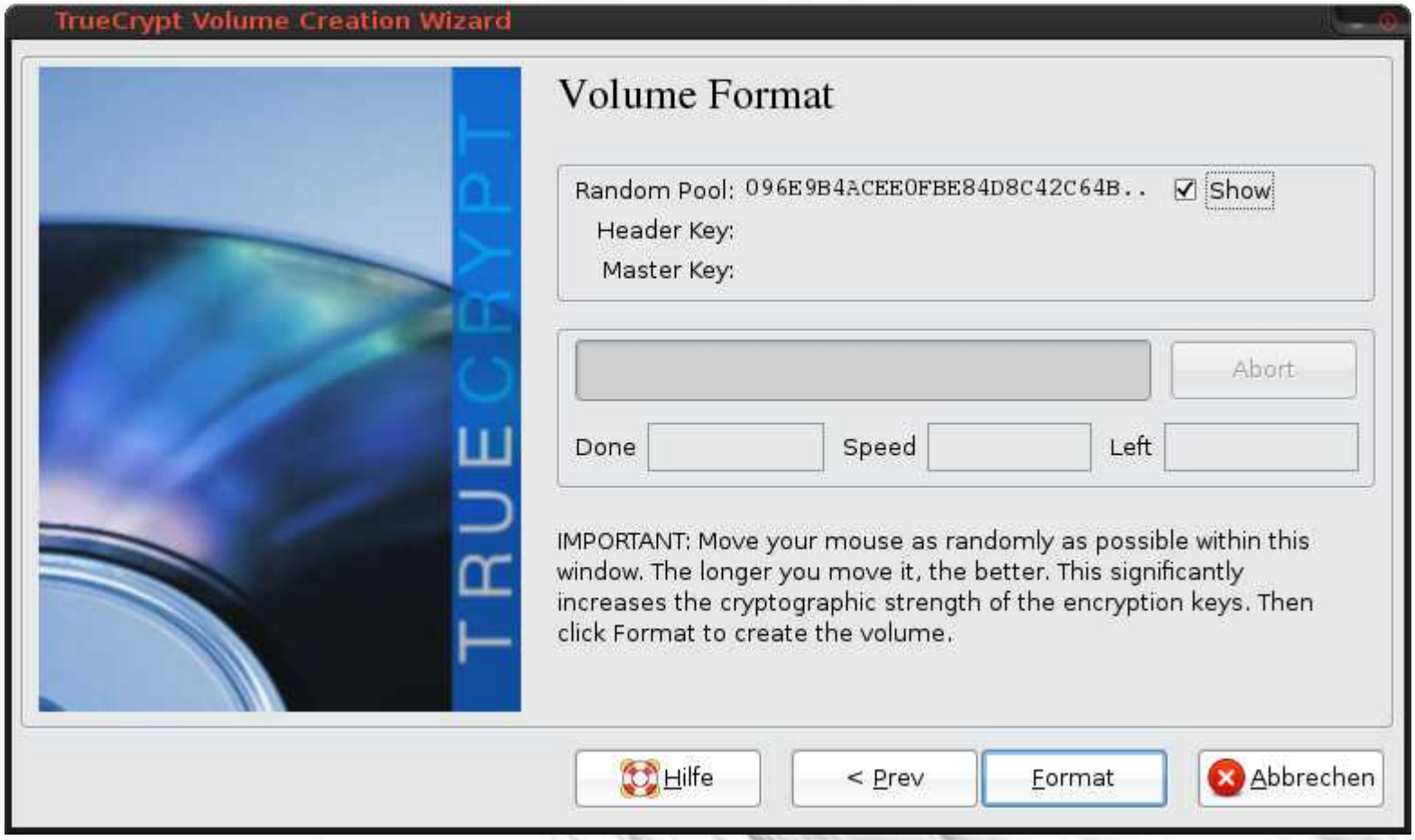
Truecrypt – Verschluesselung

Installation



Truecrypt - Verschluesselung

Installation

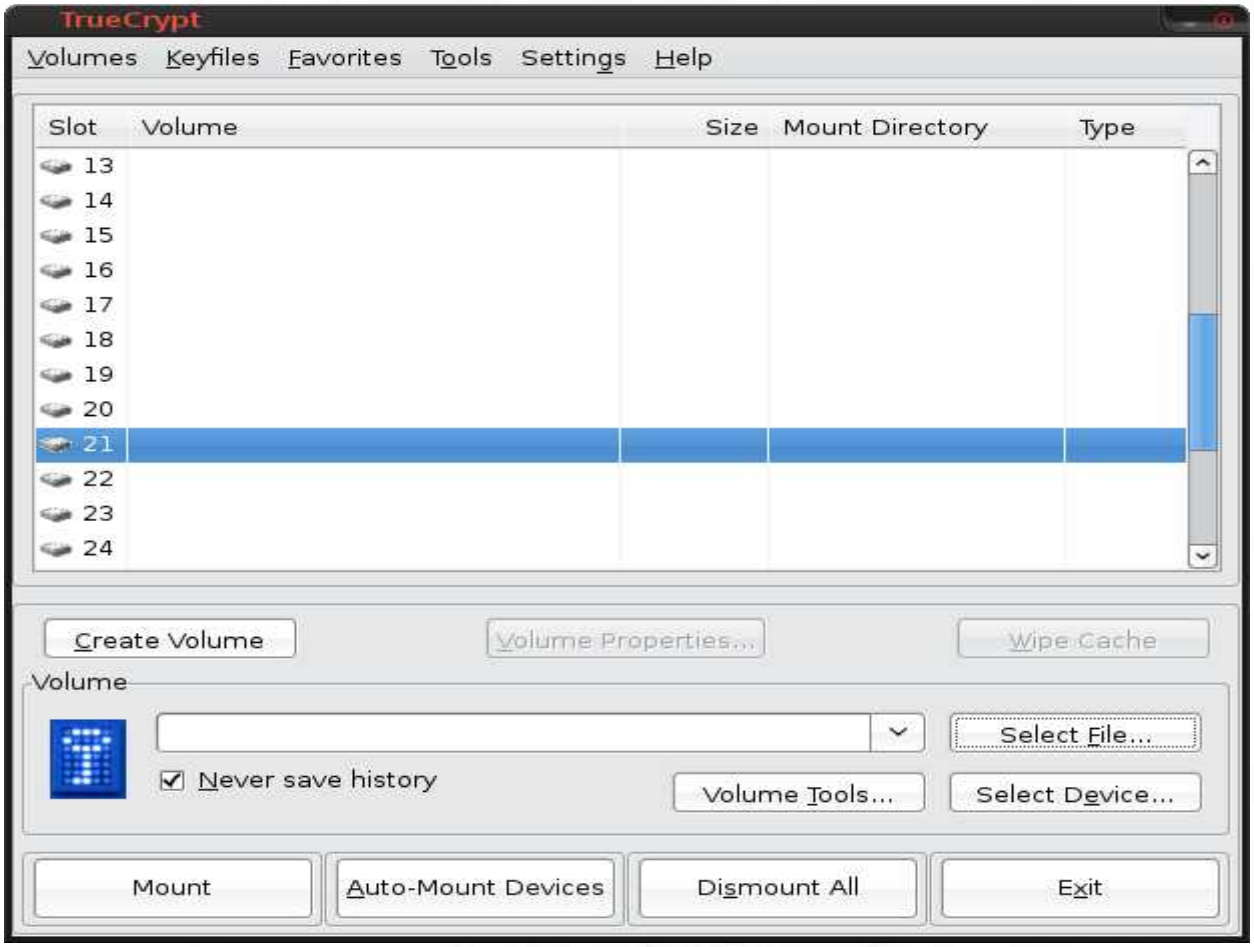


Truecrypt – Verschluesselung

Installation

Truecrypt – Verschluesselung

Installation

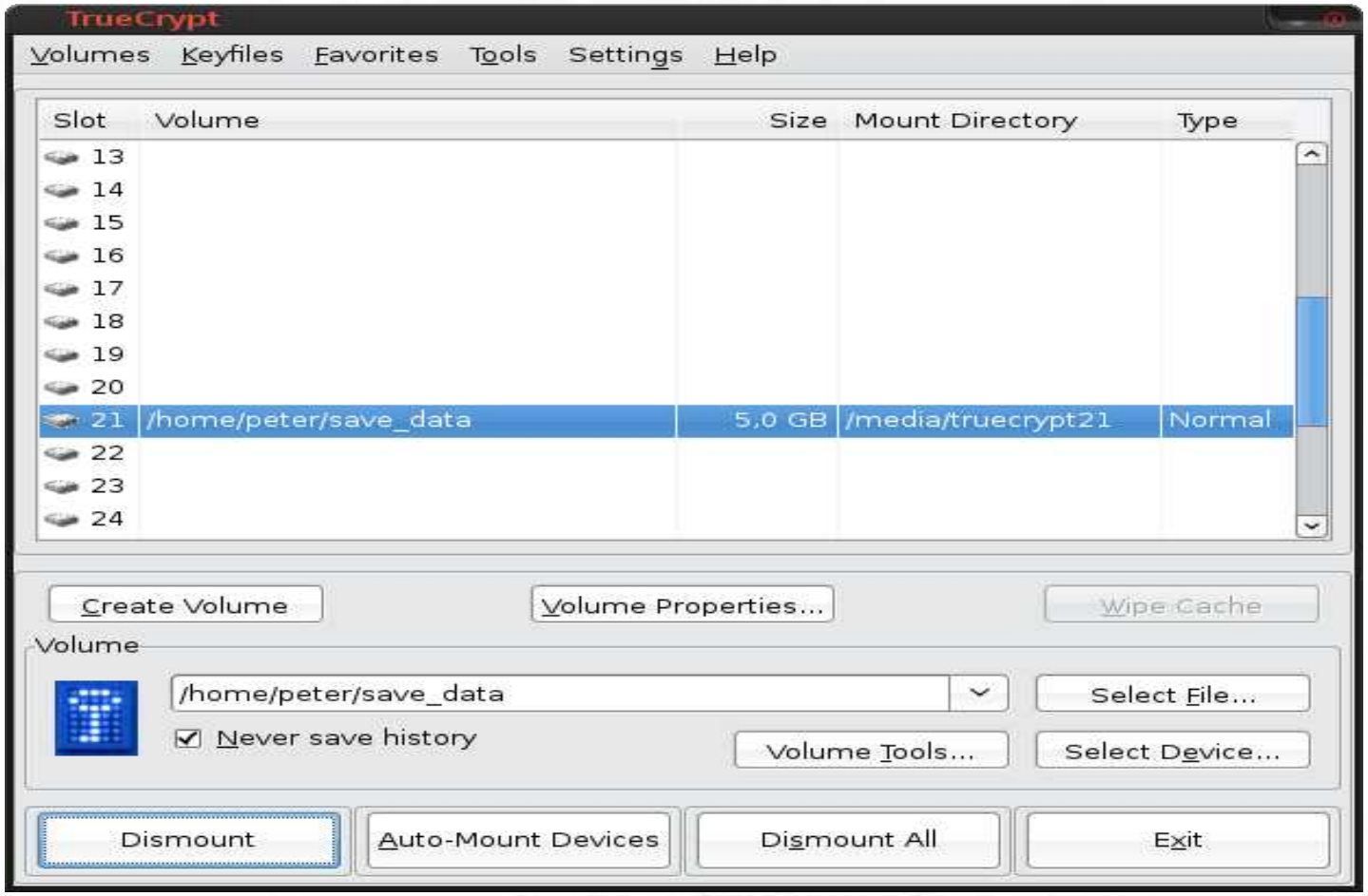


Truecrypt – Verschluesselung

Installation

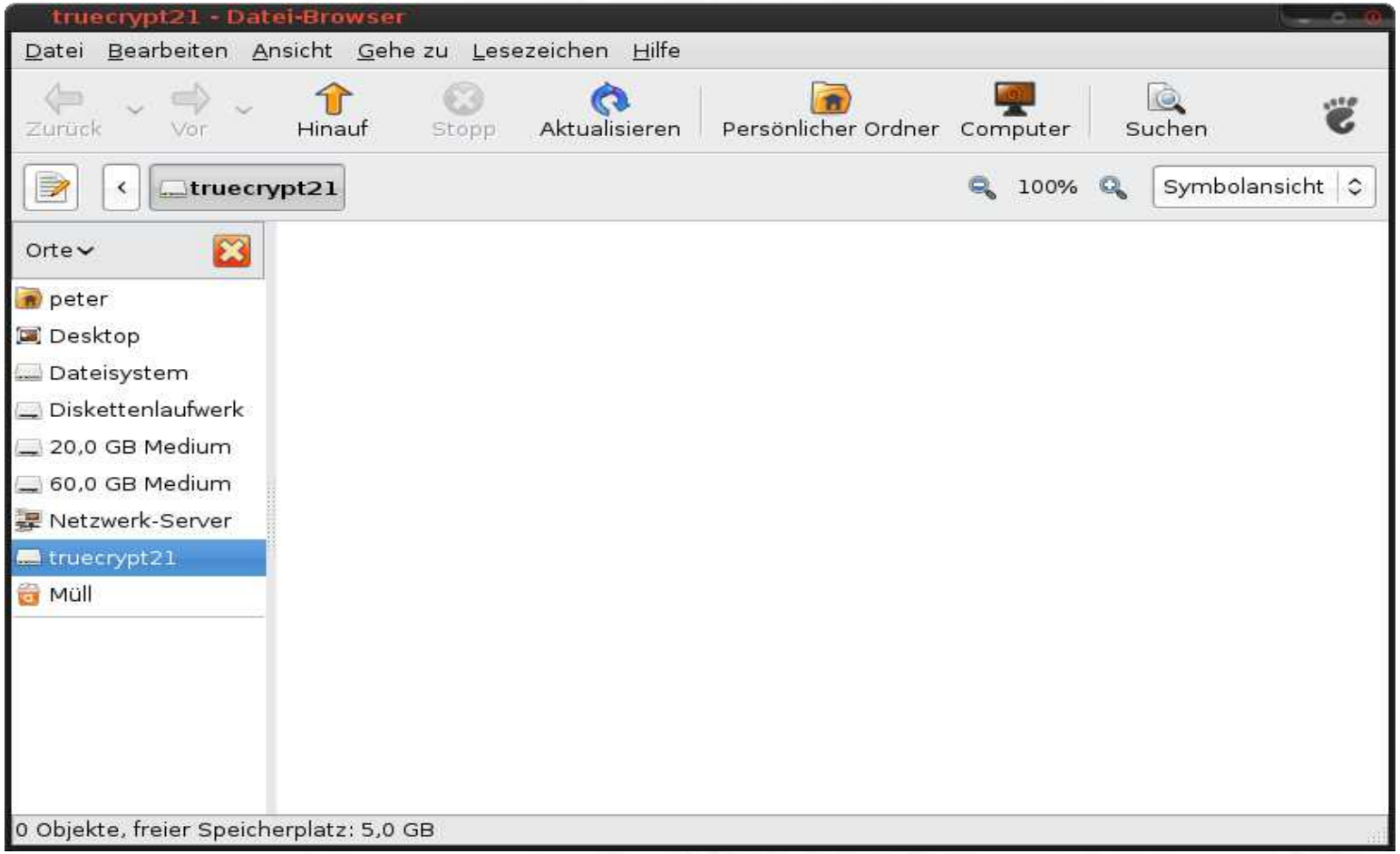
Truecrypt – Verschluesselung

Installation



Truecrypt – Verschluesselung

Installation



Truecrypt – Verschluesselung

Sichere Passwoerter

- Das A und O sind sichere Passwoerter
- Woerterbucheintraege oder Geburtsdaten sind tabu
- Sichere Passwoerter bestehen aus Groß- und Kleinbuchstaben sowie Sonderzeichen
- Je laenger und komplizierter desto besser/sicherer
- Unter Linux mit pwgen Passwoerter erstellen
- Für das OS aus Redmond gibt es auch diverse Passwort Generatoren

Truecrypt – Verschluesselung

Zukunftsaussichten

- z.Zt. Version 6.0 mit Hidden Container und Systempartitionsverschluesselung
- Geplant ist ein Zusatztool welches alle Daten im Hidden Container unter vordefinierten Bedingungen loescht
- Es wird auch daran gearbeitet mit anderen Filesystemen z.B. Ext2 oder Ext3 arbeiten zu koennen
- Verschiedene neuere Verschluesselungs Standards sollen in Zukunft integriert werden

Truecrypt – Verschluesselung

Vorteile Truecrypt

- Software ist Open Source
- Funktioniert Betriebssystem übergreifend
- Einfache und leicht verstaendliche GUI
- Spezielle Tools um USB Sticks/Platten zu verschluesseln
- Hidden Container (unsichtbar für Angreifer)
- Vom Header koennen relativ einfach Sicherungen gemacht werden (**sehr sehr wichtig!**)

Truecrypt – Verschluesselung

Nachteile Truecrypt

- Pakete nur für einzelne Linux Distributionen vorhanden
- Derzeit nur mit FAT und NTFS Dateisystemen kompatibel
- Bei Verlust des Passwortes sind die Daten weg
- Geringerer Datendurchsatz durch Verschluesselung
- Risiko eines Bitfehlers im Header. Danach kann das File nicht mehr geoeffnet werden

Truecrypt – Verschluesselung

Alternativen?

- Die beste Alternative ist LUKS (Linux Unified Key Setup). On-Disk Specification unter Linux, welche den genauen Aufbau des Containers beschreibt
- Enc FS (unter Linux)
- Drive Crypt (unter MS Windows)
- Wirkliche Plattformuebergreifende Alternativen gibt es derzeit noch nicht

Truecrypt – Verschluesselung

LUKS

- **Linux Unified Key Setup**
  - Ermöglicht die Verschluesselung von kompletten Festplatten oder Partitionen unter Linux. Es sollten nicht nur /home, sondern auch die Swap Partition, /tmp, /var sowie Teile des /etc Verzeichnisses verschluesselt werden
  - Durch den Verzicht des Verschluesselns der Partition /boot, kann von diesen Partitionen auch gebootet werden

Truecrypt – Verschluesselung

dm-crypt

- **dm-crypt**
  - Cryptotarget für den device-mapper (dm) im Linuxkernel
  - Device-mapper implementiert u.a. auch Software-Raid oder LVM im Kernel
  - Baut eine zusaetzliche Schicht zwischen verschluesselten Roh Daten und dem Dateisystem auf
  - Ermöglicht die Erstellung von virtuellen verschluesselten Blockgeraeten
  - Ist nicht an einen Verschluesselungsalgorithmus gebunden

Truecrypt – Verschluesselung

cryptsetup I

- **Was ist cryptsetup?**
  - Tool, welches den device-mapper im Kernel „geeignet“ konfiguriert
  - Leitet aus einem Passwort einen kryptographischen Key ab und uebergibt ihn dem Kernel
    - Verfahren PBKDF2 (password based key derivation function 2)

Truecrypt – Verschluesselung

cryptsetup II

- **Zwei wichtige Bereiche**
  - Schluesselgenerierung (wie wird der Schluessel berechnet)
  - Verschluesselungsverfahren (Algorithmus und Modus)

Truecrypt – Verschluesselung

LUKS/dm-crypt/cryptsetup

- Da dies eine sehr komplexe Thematik ist, sollte man sich den Artikel „Geheime Niederschrift“ mal anschauen. Dort wird noch einmal sehr genau auf o.g. Stichpunkte eingegangen
- www.linux-magazin.de/heft_abo/ausgaben/2005/08/geheime_niederschrift

Truecrypt – Verschluesselung

Webadressen

- www.truecrypt.org
- www.truecrypt.de.vu
- www.fixmbr.de/truecrypt-anleitung
- forums.truecrypt.org
- wikipedia.de
- http://alldev.de/59-usb-stick-mit-truecrypt-verschluesseln

Truecrypt – Verschluesselung

Vielen Dank für die Aufmerksamkeit

Noch Fragen?