

Sicherheitstage SS/09

Verschlüsselung von Daten mit TrueCrypt

TRUECRYPT

FREE OPEN-SOURCE ON-THE-FLY ENCRYPTION

TrueCrypt

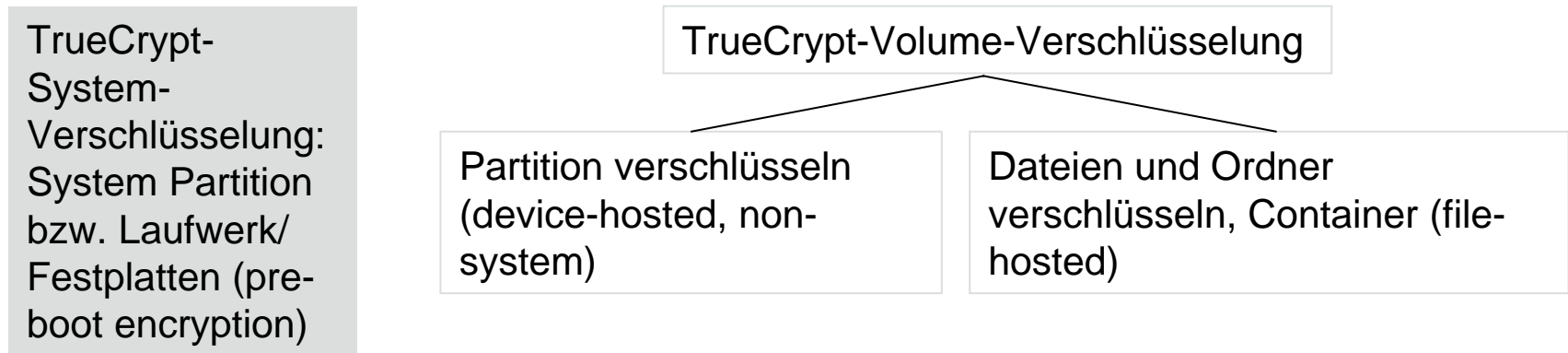
- frei verfügbare, quelloffene Verschlüsselungssoftware für Windows und Linux
- On-the-fly-Verschlüsselung/Entschlüsselung: TrueCrypt entschlüsselt nur für den Arbeitsspeicher/RAM, es werden keine unverschlüsselten Daten auf der Festplatte zwischengespeichert.
- erzeugt eine verschlüsselte Systempartition oder verschlüsselte Volumes, dabei erfolgt die Authentisierung über alphanumerische Kennwörter und Schlüsseldateien, Volumes können im laufenden Betrieb beliebig geöffnet und geschlossen werden
- bietet 3 Verschlüsselungsverfahren an: AES, Serpent, Twofish, diese können einzeln und in allen möglichen Kombinationen eingesetzt werden (Performance!)
- Aktuelle Version 6.2a

TrueCrypt

Punkte, die im Folgenden näher erläutert werden sollen:

- TrueCrypt-System-Verschlüsselung
- „Traveler Mode“
- „Hidden Files“
- Schlüsseldateien

TrueCrypt System-Verschlüsselung



Alle Dateien und Registry-Einträge sind permanent verschlüsselt

Pre-boot Authentifizierung wird realisiert über den TrueCrypt Boot Loader

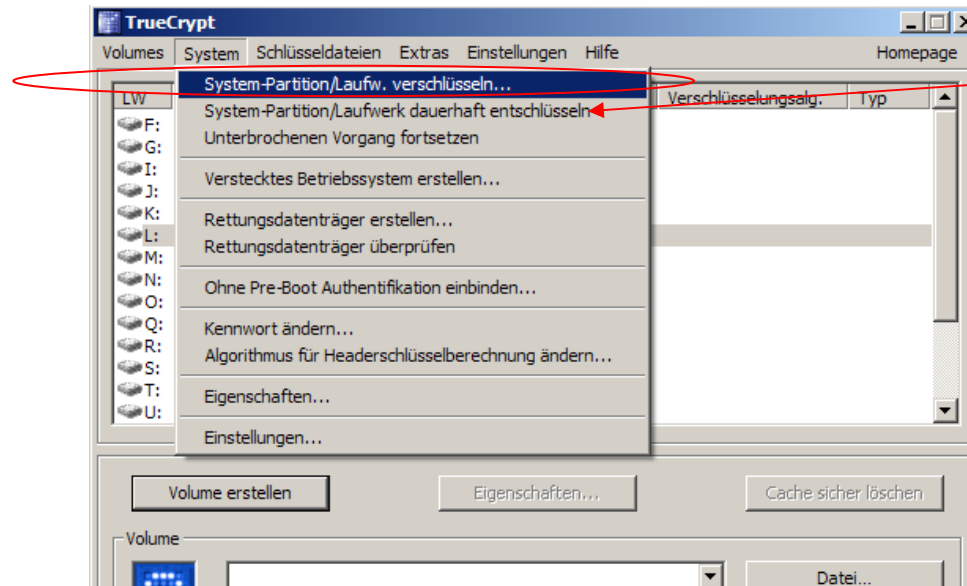
TrueCrypt Rescue Disk für den Fall, dass

- > Der TrueCrypt-Boot-Loader defekt ist oder mit Malware infiziert ist
- > Der Master-Key oder andere kritische Daten defekt sind
- > Windows defekt ist

TrueCrypt System-Verschlüsselung

- Unterstützte Windows Betriebssysteme:
 - Windows XP
 - Windows XP x64
 - Windows Vista
 - Windows Vista x64
 - Windows Server 2003
 - Windows Server 2003 x64

TrueCrypt System-Verschlüsselung



- Absicherung nur mit Passwort, die Funktion „Schlüsseldatei“ wird nicht unterstützt
- Nach Passwortwahl werden Header-Key und Master-Key generiert
- Iso-Image für Rescue-Disk wird erstellt
- Nach Neustart startet der Verschlüsselungsvorgang
- Nach erfolgreicher TrueCrypt-Verschlüsselung meldet sich vor jedem Bootvorgang der TrueCrypt-Boot-Loader und fordert das Passwort

TrueCrypt System-Verschlüsselung



heise Security

Sie sind Gast
[Einloggen](#) | [Registrieren](#)

Suche

[Im Browser einrichten](#)

News

News

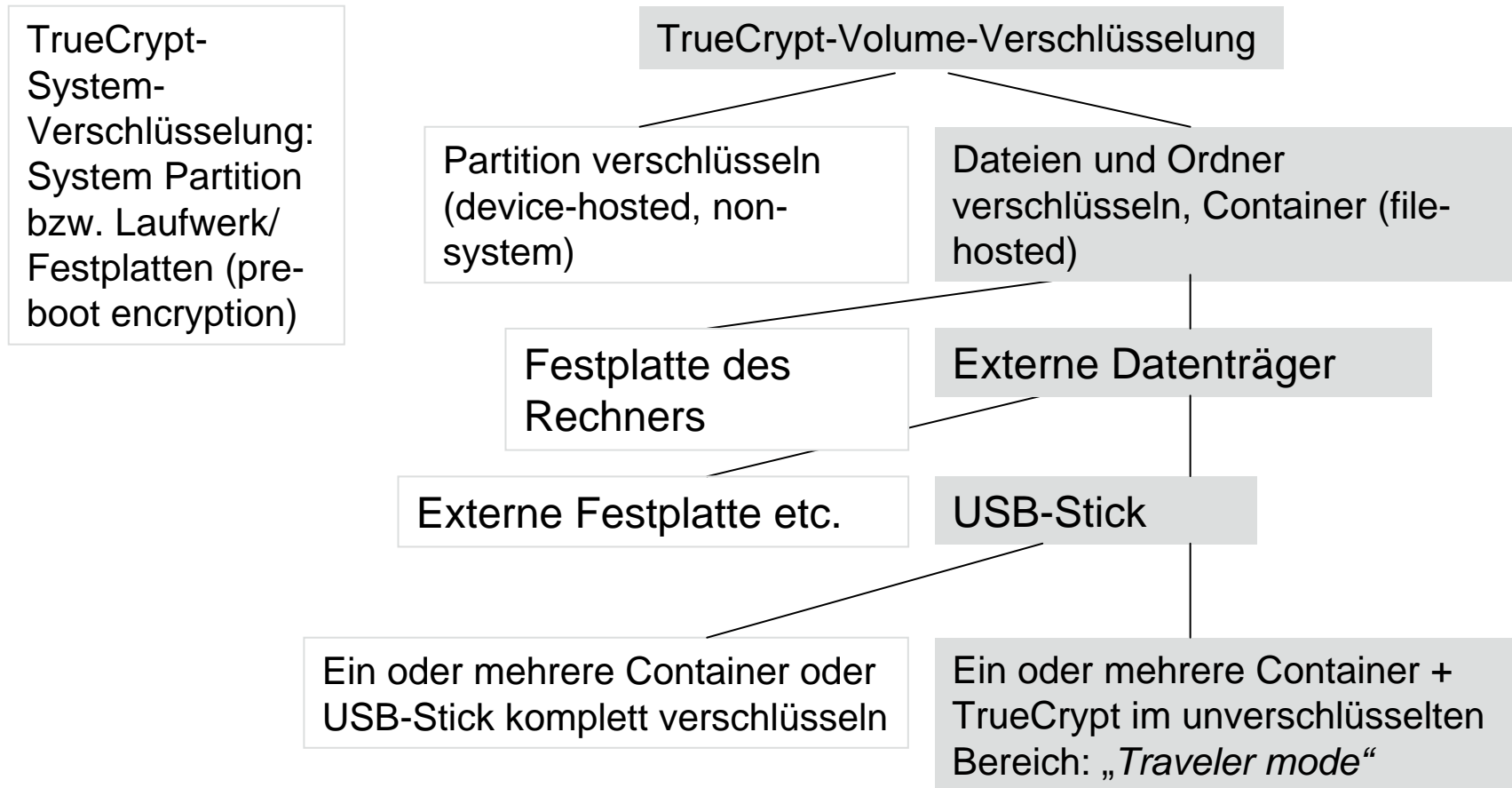
Meldung vom 30.07.2009 10:32

Bootkit hebt Festplattenverschlüsselung aus

Der österreichische IT-Sicherheitsspezialist Peter Kleissner hat au Bootkit namens Stoned demonstriert, das in der Lage ist TrueCryp Systemverschlüsselung auszuhebeln. Bootkits sind eine Kombinati des Schädlings, den Master Boot Record des PC zu modifizieren i Betriebssystem aktiv zu werden.

- 30.07.09: Österreichischer IT-Sicherheitsspezialist stellt sein „Bootkit“ „Stoned“ vor, das diese Systemverschlüsselung aushebelt, indem es sich in den Master Boot Record schreibt, der stets unverschlüsselt ist.
- Für eine Infektion mit „Stoned“ ist ein physischer Zugang notwendig (z.B. CD-Laufwerk)
- Die verschlüsselten Daten sind weiterhin verschlüsselt und können weiterhin nur mit dem TrueCrypt-Passwort entschlüsselt werden.

TrueCrypt „Traveler Mode“



TrueCrypt „Traveler Mode“

- Der TrueCrypt „Traveler Mode“ ermöglicht eine Installation der Verschlüsselungssoftware auf dem USB-Stick. Damit kann der verschlüsselte Inhalt an jedem Rechner entschlüsselt werden. Eine TrueCrypt-Installation auf dem Endgerät ist nicht notwendig.
- Problem dabei ist, dass der Benutzer Admin-Rechte braucht, da auf dem Rechner ein Laufwerk gemountet werden muss.
- Um trotzdem diesen sehr eleganten Modus nutzen zu können, wird im Folgenden eine „Hybrid-Konfiguration“ vorgeschlagen.

TrueCrypt „Traveler Mode“

- USB-Stick
 - TrueCrypt Traveler-Mode im unverschlüsselten Bereich
 - Verschlüsselte TrueCrypt-Container, z.B. dienstlich und privat

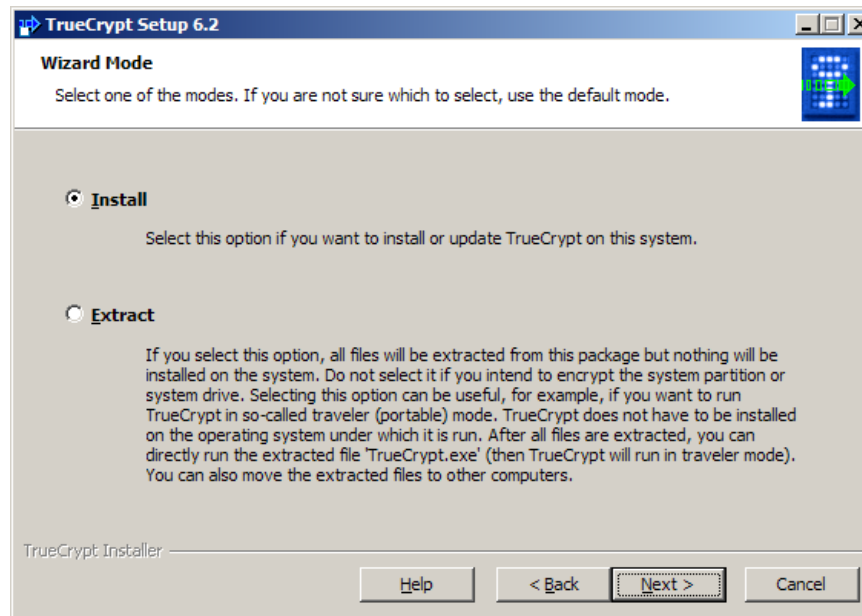


- Arbeitsplatz-Rechner
 - Benutzer mit eingeschränkten Rechten
 - TrueCrypt-Installation auf dem Rechner
 - Optional:
 - Automatisches Mounten des verschlüsselten TrueCrypt-Volumes
 - Bei Rechnerstart wird das TrueCrypt-Passwort abgefragt

- Dienst-Notebook, Privat-Rechner, ...
 - Benutzer hat Admin-Rechte
 - Keine TrueCrypt-Installation notwendig

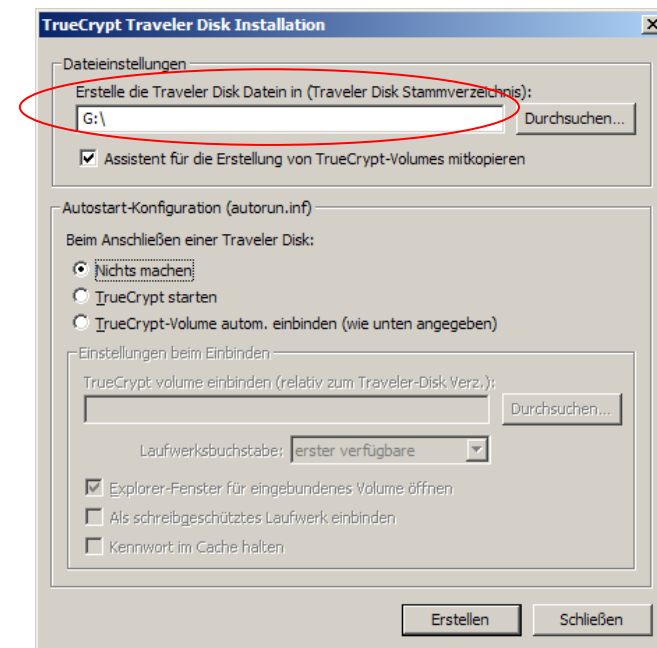
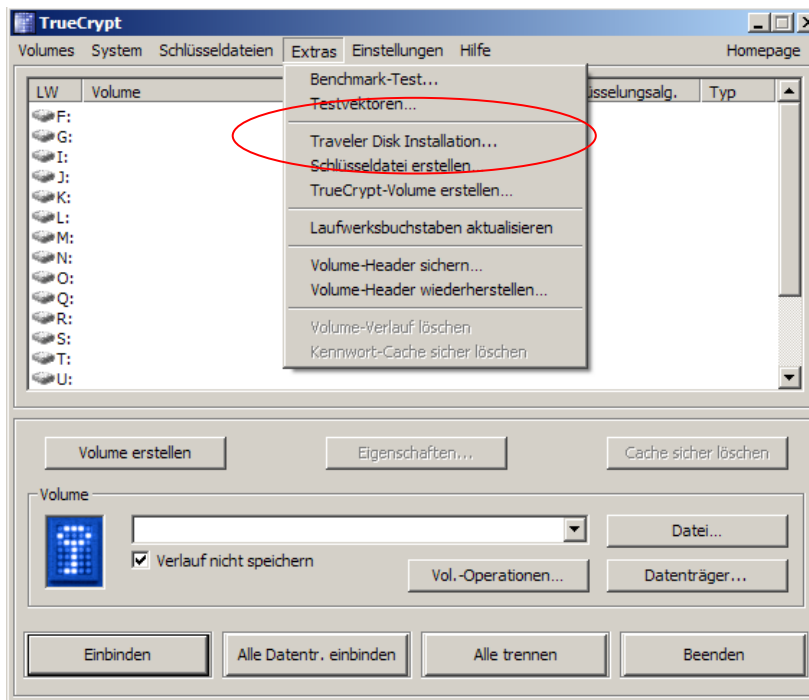
TrueCrypt „Traveler Mode“

- Arbeitsplatz-Rechner (Benutzer mit eingeschränkten Rechten)
 - TrueCrypt-Installation
 1. Admin installiert TrueCrypt auf dem Rechner



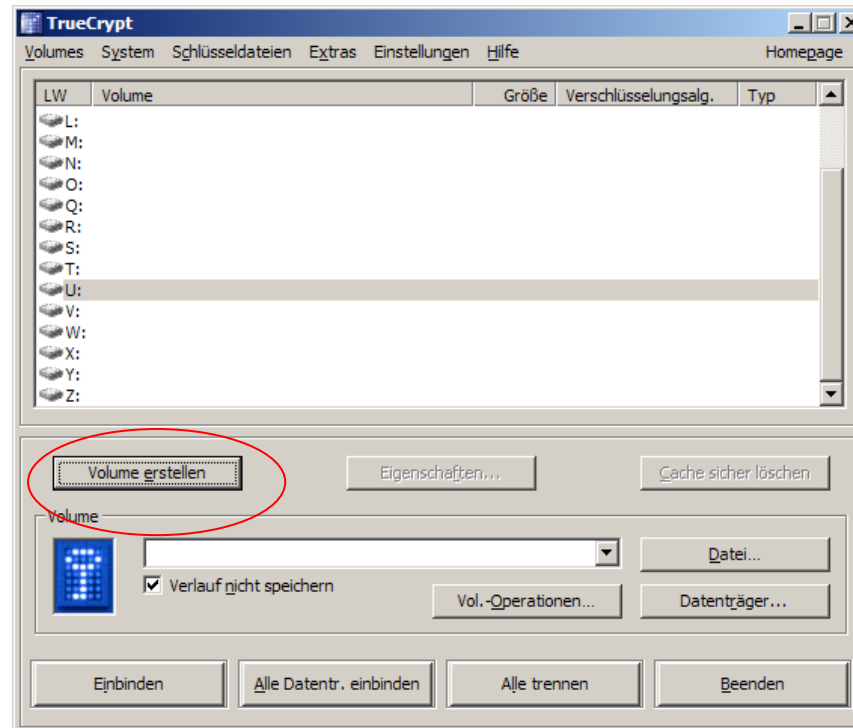
TrueCrypt „Traveler Mode“

- Arbeitsplatz-Rechner (Benutzer mit eingeschränkten Rechten)
 - TrueCrypt-Installation
 2. Admin installiert den „Traveler Mode“ auf dem USB-Stick



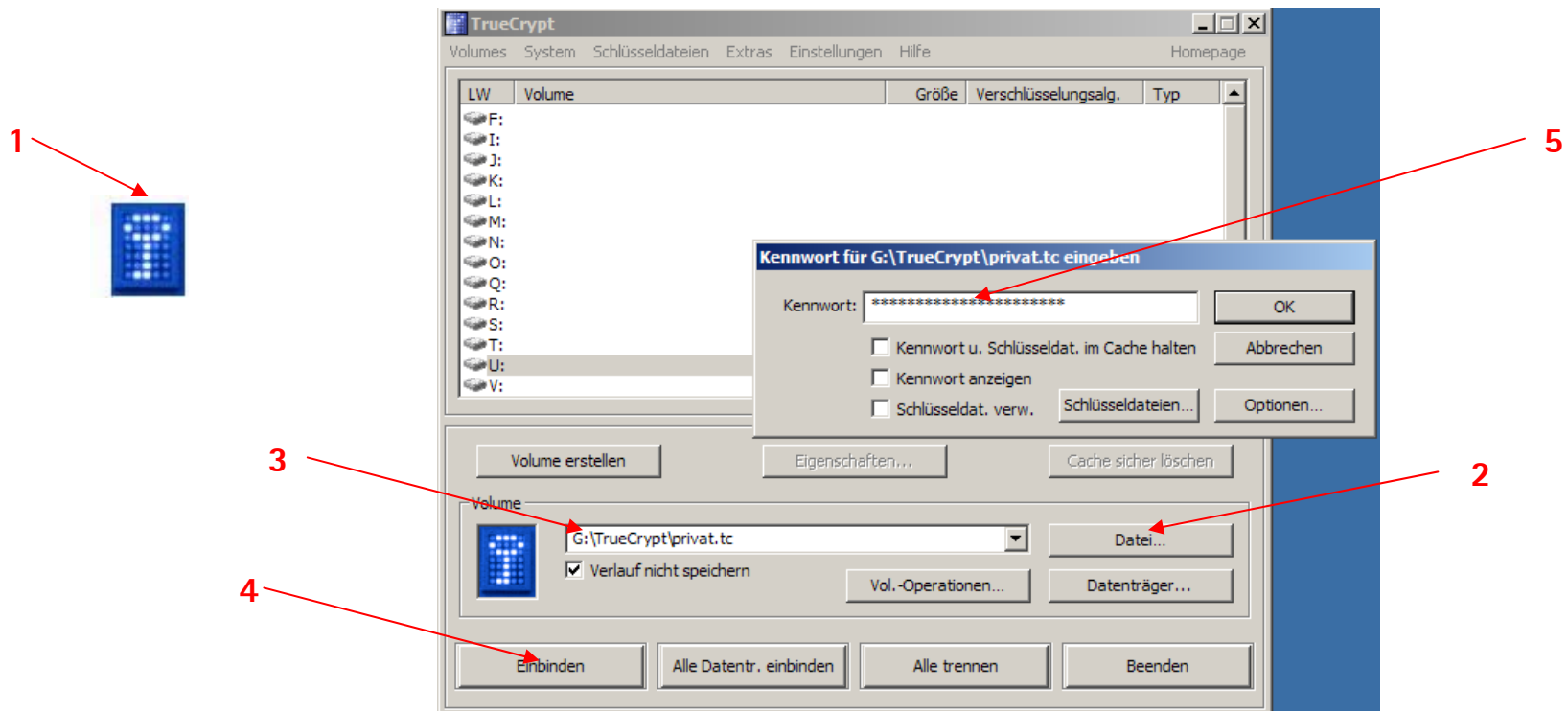
TrueCrypt „Traveler Mode“

- Arbeitsplatz-Rechner (Benutzer mit eingeschränkten Rechten)
 - TrueCrypt-Installation
 3. Admin oder der Benutzer selbst legt ein oder mehrere Volumes auf dem USB-Stick an



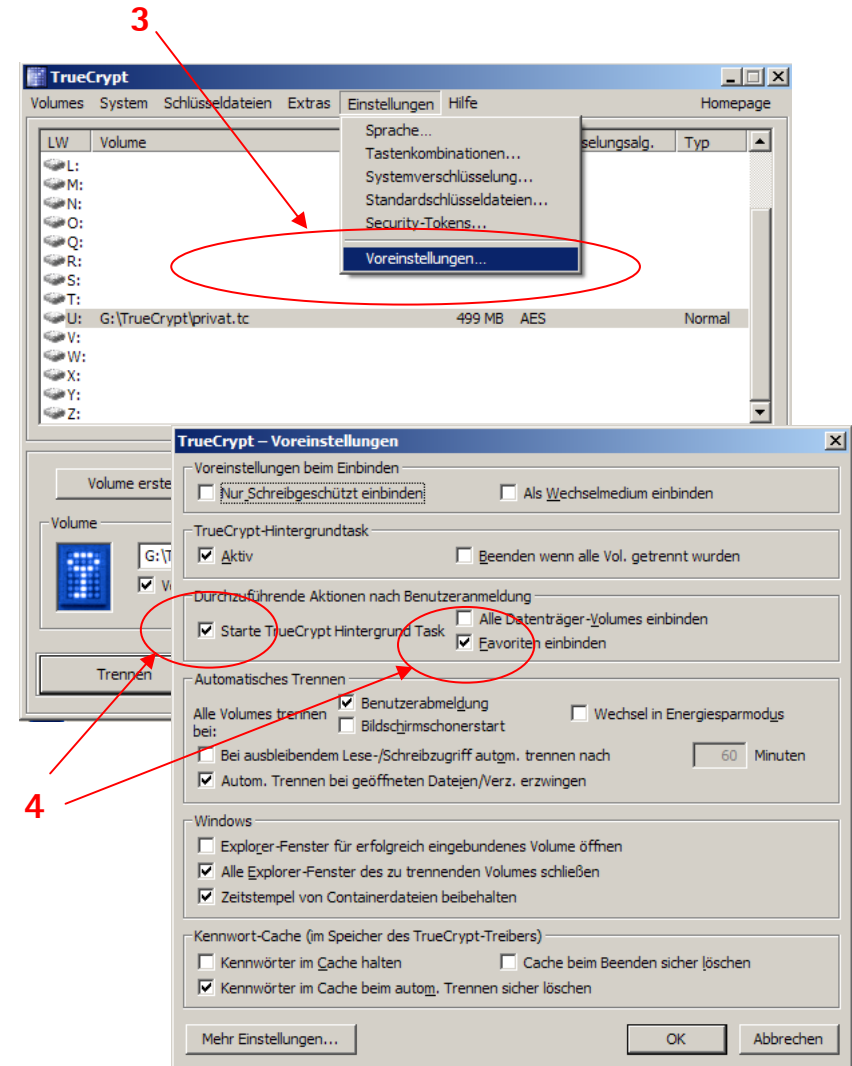
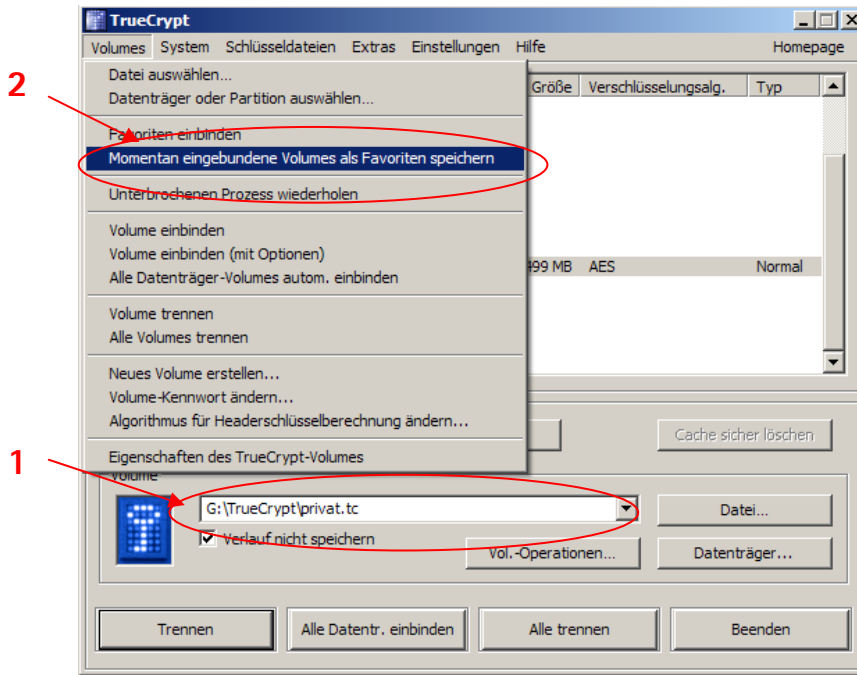
TrueCrypt „Traveler Mode“

- Arbeitsplatz-Rechner (Benutzer mit eingeschränkten Rechten)
 - Arbeiten mit dem verschlüsselten USB-Stick
Variante 1



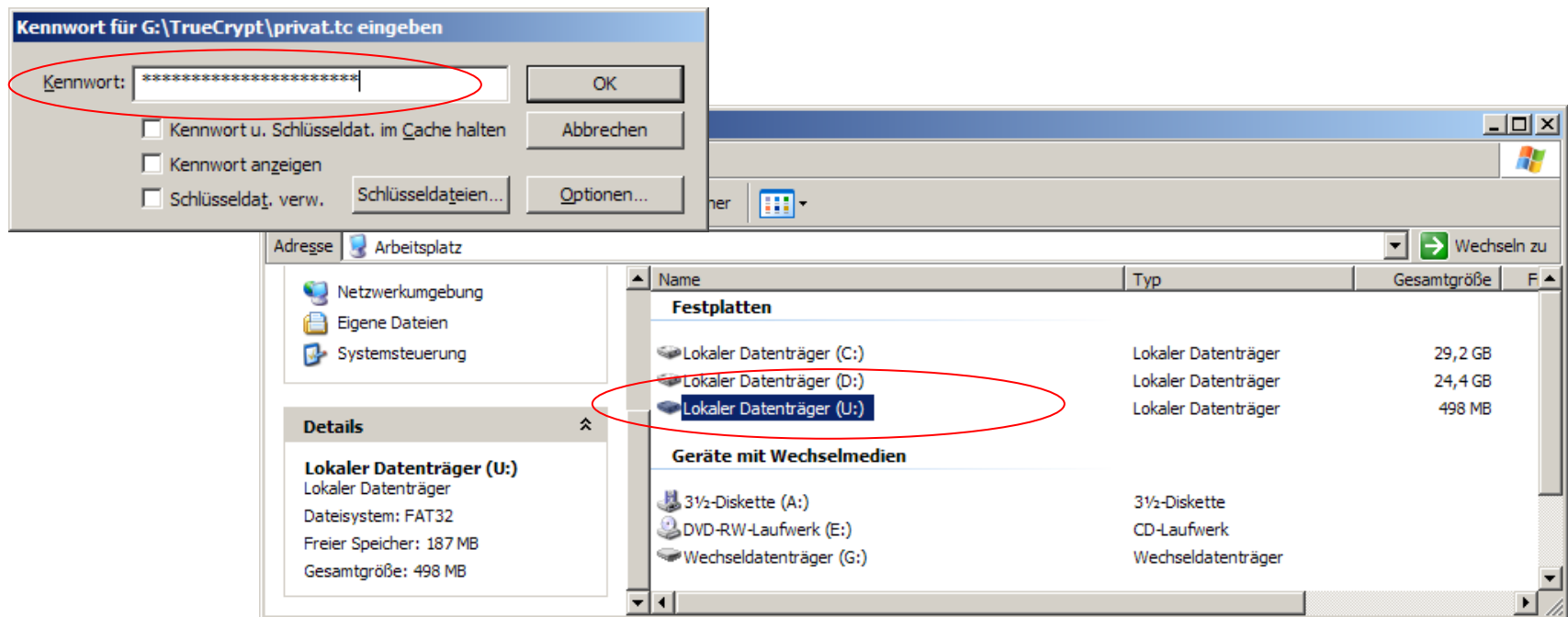
TrueCrypt „Traveler Mode“

- Arbeitsplatz-Rechner (Benutzer mit eingeschränkten Rechten)
 - Arbeiten mit dem verschlüsselten USB-Stick
Variante 2



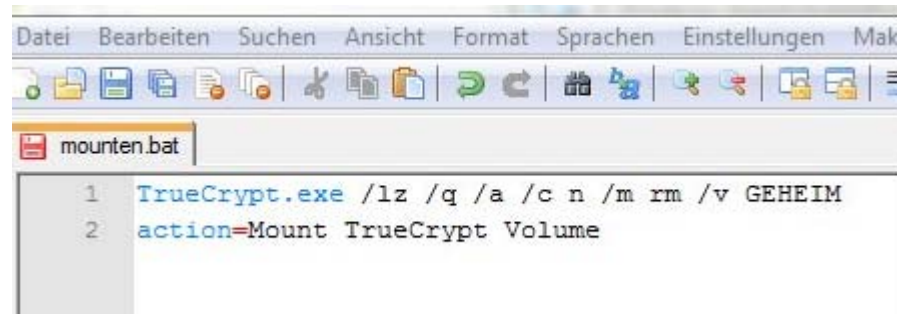
TrueCrypt „Traveler Mode“

- Arbeitsplatz-Rechner (Benutzer mit eingeschränkten Rechten)
 - Arbeiten mit dem verschlüsselten USB-Stick
Variante 2



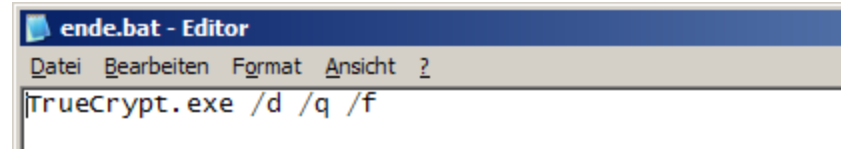
TrueCrypt „Traveler Mode“

- Dienst-Notebook, Privat-Rechner (Benutzer hat jeweils Administratorrechte)
 - Arbeiten mit dem verschlüsselten USB-Stick
 - Start- und Stopdateien auf dem USB-Stick
1. Mounten.bat



```
1 TrueCrypt.exe /lz /q /a /c n /m rm /v GEHEIM
2 action=Mount TrueCrypt Volume
```

2. Ende.bat



```
TrueCrypt.exe /d /q /f
```

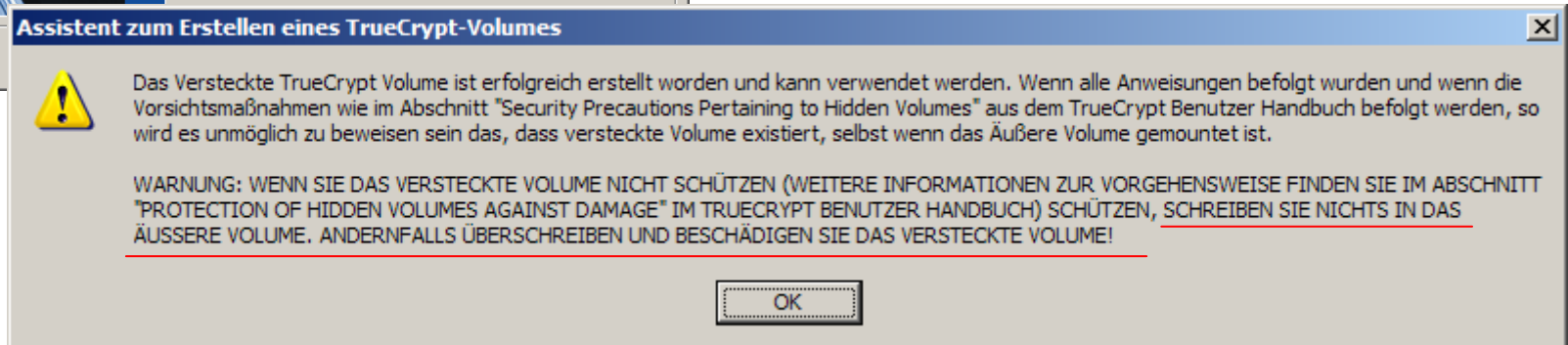
TrueCrypt – „Hidden Volume“

- „Plausible Deniability“
 - „glaubwürdiges Abstreiten der Kenntnis eines Sachverhaltes“
 - hört sich geheimnisvoll an, ist aber nur in bestimmten Fällen sinnvoll



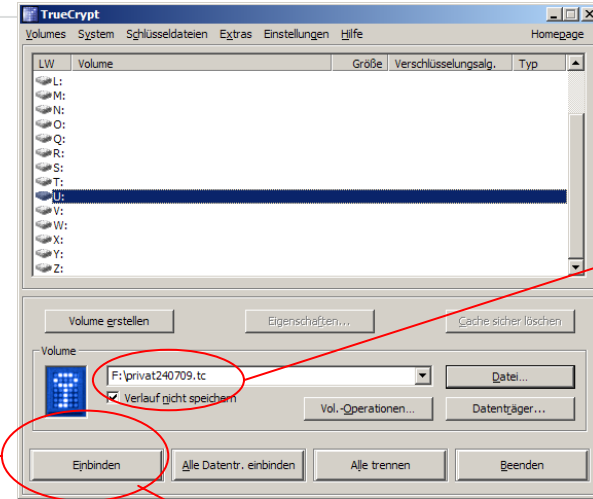
TrueCrypt – „Hidden Volume“

- Hidden Volume erstellen



TrueCrypt – „Hidden Volume“

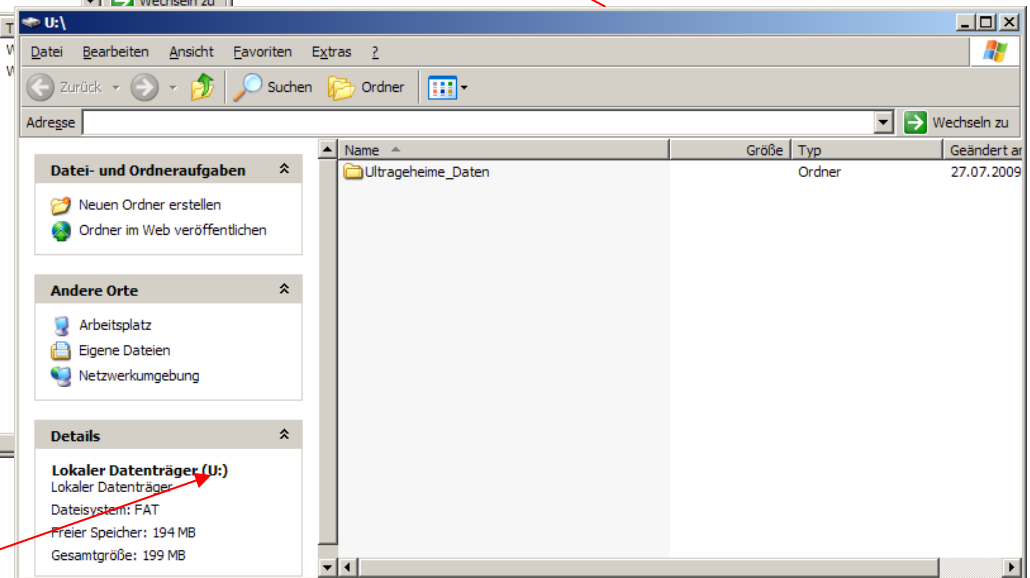
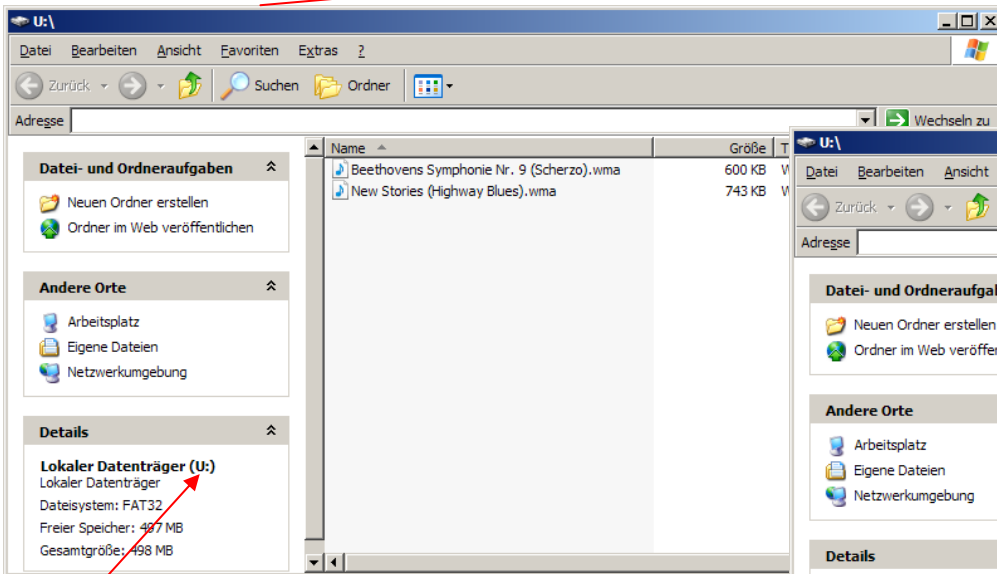
■ Hidden Volume im Einsatz



Container-Datei

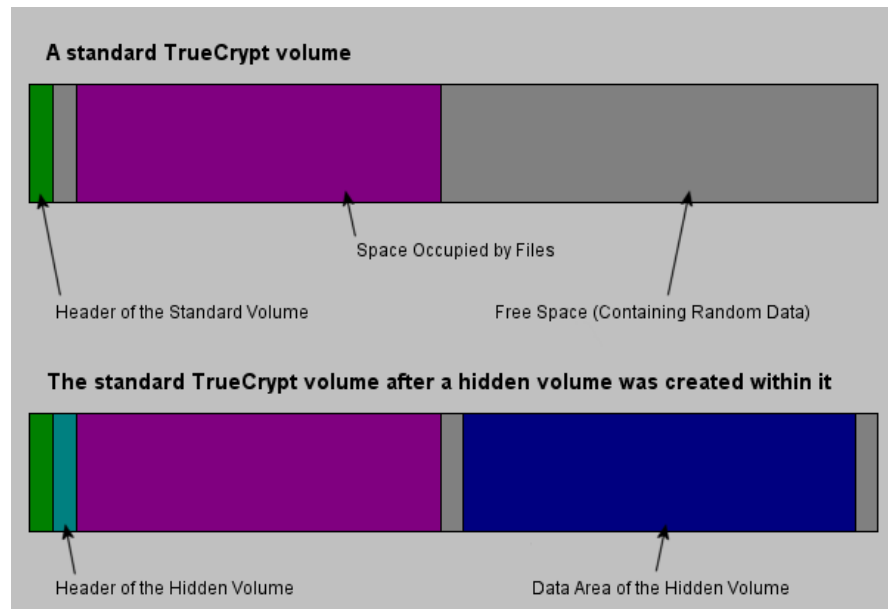
Passworteingabe für äußeres
Volume

Passworteingabe für das
„Hidden Volume“



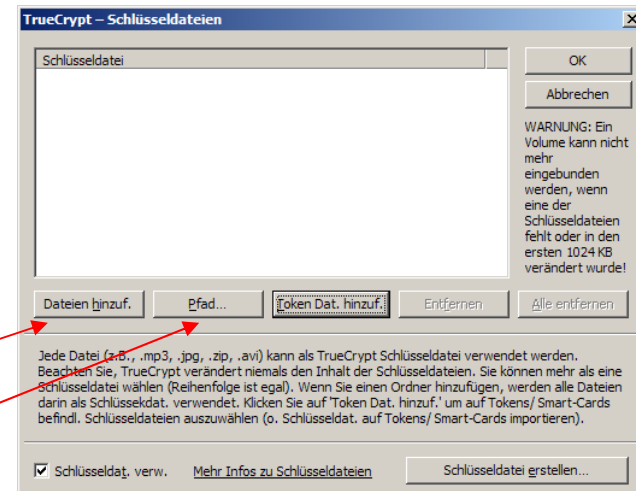
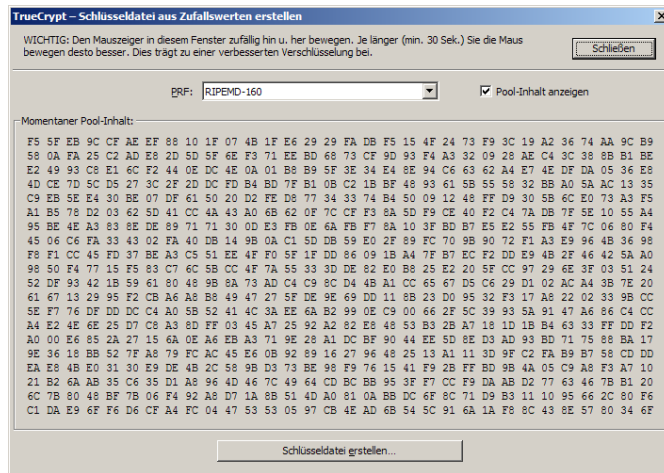
TrueCrypt – „Hidden Volume“

- Hidden Volume, graphische Darstellung



TrueCrypt – Arbeiten mit Schlüsseldateien (Key Files)

- Zusätzlich zum Passwort kann eine oder mehrere Schlüsseldateien verwendet werden, um das verschlüsselten TrueCrypt-Volumes abzusichern.
- Es handelt sich um einen zusätzlichen Schutz vor Keyloggern oder Brute Force Angriffen auf das Passwort.
- Ermöglicht *multi-user shared access*
- Es werden zwei Verfahren zur Bereitstellung von Schlüsseldateien angeboten:
 - Mittels TrueCrypt-Zufallsgenerator (max. Länge 512 bit)
 - Eine existierende Datei oder ein kompletter Pfad



TrueCrypt

- Wiederherstellung/Entschlüsseln der Daten bei PW/Schlüsselverlust

Nicht möglich!!!

Literatur:

- <http://www.truecrypt.org/>
- <http://board.gulli.com/thread/674868-anleitung-tutorial-und-howto-truecrypt-verschlsselung/>