



**TrueCrypt**

**Chancen und Risiken für  
Sachverständige**



# Grundlagen

- **Ermöglicht Verschlüsselung von Datenträgern**
- **Ermöglicht verschlüsselte Container**
- **Ermöglicht versteckte Datenbereiche**
- **Quelloffene Software**
- **Wählbare Algorithmen**
- **Verfügbar für Linux und Windows**



# Plausible-deniable-Konzept (1)

- **Vorhandensein von Daten kann glaubwürdig abgestritten werden**
- **Versteckte Container innerhalb des freien Speicherplatzes verschlüsselter Container und Partitionen sind möglich**
- **Keine sichtbaren Header**

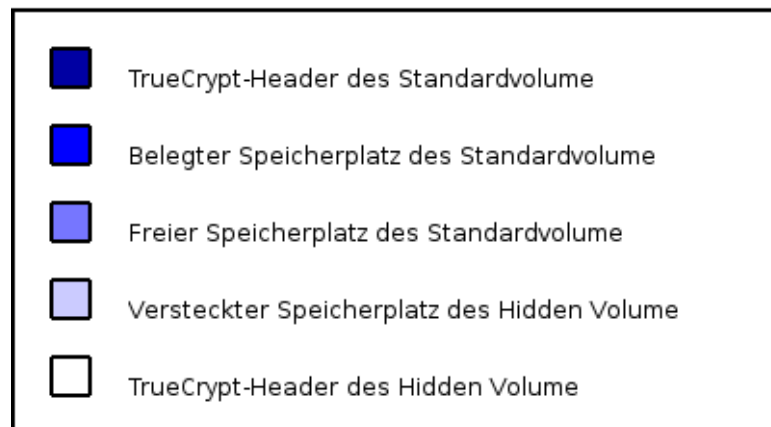


# Plausible-deniable-Konzept (2)

Ein TrueCrypt-Volume



Ein TrueCrypt-Volume mit Hidden Volume





# Anwendungsmöglichkeiten

- **Notebook**
- **Ausgelagerte Sicherheitskopie**
- **USB Stick (Traveller Mode)**



# Probleme für den Sachverständigen

- Selbst bei bekanntem Passwort für ein TrueCrypt Volume können versteckte Daten nicht ausgeschlossen werden
- Forensiktools nicht anwendbar



# Quellen

- <http://www.truecrypt.org/>
- **Linux Howto in deutscher Sprache:**  
<http://privat.heinzelzweg.de/howtos/debian/truecrypt/>
- <http://de.wikipedia.org/wiki/TrueCrypt>