



Crypto-Workshop in der Studivertretung 5. Dezember 2014 ab 14 Uhr

Referat für Datenschutz und
Referat für Politische Bildung

Warum Datensicherheit und Verschlüsselung?

Globale Überwachungs- und Spionageaffäre

- Edward Snowden
- Beispiel Lavabit
- Bewegungsprofile und Soziales Netzwerk (Metadaten)
- “Ich hab doch nichts zu verbergen...”
 - Spiegel Artikel

Open Source

- Definition: Quelltext offen, frei verfügbar
- Keine Kommerzielle Nutzung
 - Keine “Backdoors” von Unternehmen/Staat
 - Aber auch keine regelmäßig finanzierte Überprüfung von Bugs
 - Aber auch keine Anhängigkeit was Updates etc angeht

- Abhängig vom Betriebssystem
- Bei Linux mit luks nur durch neu aufsetzen des Betriebssystems möglich
 - [How-To \(englisch\)](#)
- Bei Windows mit truecrypt auch im laufendem Betriebssystem möglich
 - [How-To \(englisch\)](#)



Ubuntu 14.04 lvm encryption

✕ Install

Installation type

This computer currently has no detected operating systems. What would you like to do?

- Erase disk and install Ubuntu
Warning: This will delete any files on the disk.
- Encrypt the new Ubuntu installation for security
You will choose a security key in the next step.
- Use LVM with the new Ubuntu installation
This will set up Logical Volume Management. It allows taking snapshots and easier partition resizing.

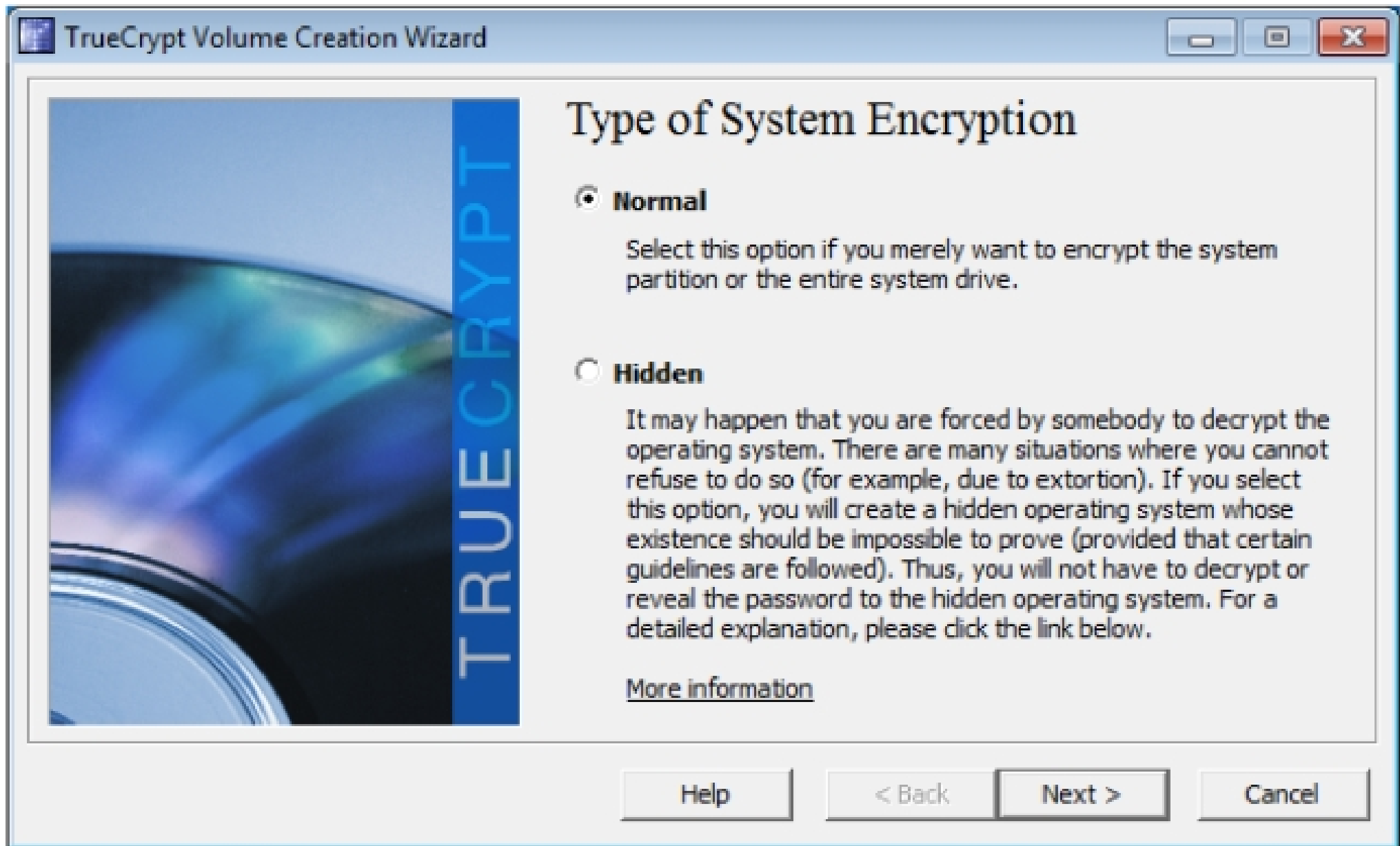
- Something else
You can create or resize partitions yourself, or choose multiple partitions for Ubuntu.

Quit

Back

Install Now

Windows 7 mit truecrypt



Email-Verschlüsselung

- Youtube-Video
- Ein öffentlicher Schlüssel (für andere)
 - Zum Verschlüsseln der Mail an dich
- und ein privater Schlüssel (für dich)
 - Zum Entschlüsseln der Verschlüsselten Mails

- Privater Schlüssel (für dich)
 - Zum Unterschreiben/Signieren
- Öffentlicher Schlüssel (für andere)
 - Zum Überprüfen deiner Signatur



Chatten mit Jabber und otr

- Schnell, sicher und synchron
- Funktioniert wie normaler Chat ist aber cooler!



Chatten mit Verschlüsselung

The screenshot displays a Jabber chat client interface. On the left is a contact list titled 'Kontaktliste' with a menu bar containing 'Kontakte', 'Konten', 'Werkzeuge', and 'Hilfe'. The contact list shows several contacts, many of whom are marked as 'Abgemeldet' (offline). The main window shows a chat conversation with a contact whose name is redacted. The chat history includes the following messages:

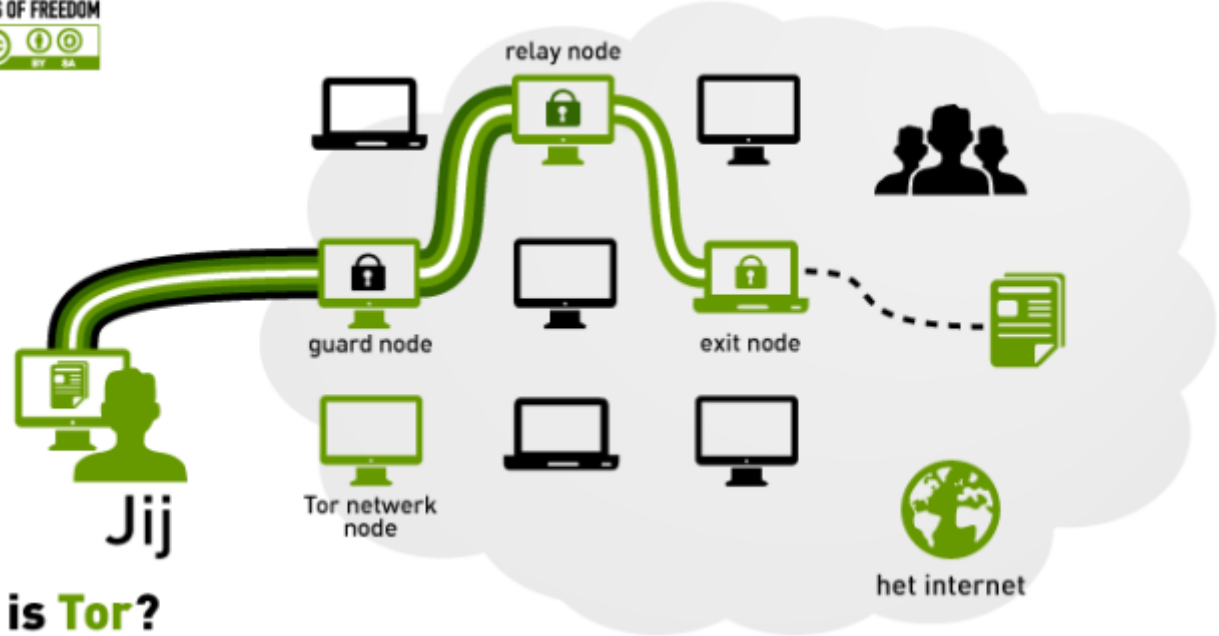
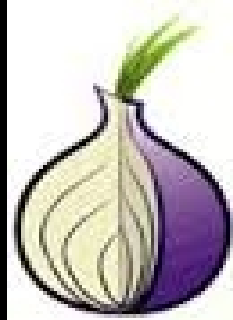
- (13:39:38) **Versuche, eine private Unterhaltung mit [redacted]@jabber.systemli.org zu beginnen...**
- (13:39:39) **Private Unterhaltung mit [redacted]@jabber.systemli.org/home begonnen. Ihr Client speichert diese Unterhaltung nicht.**
- (13:39:44) [redacted]@jabber.ccc.de: [redacted]
- Hallo
- (13:39:49) [redacted]: hi

The bottom of the chat window features a toolbar with icons for 'Schrift', 'Einfügen', 'Lächeln!', and 'Aufmerksamkeit!', along with a 'Privat' status indicator.

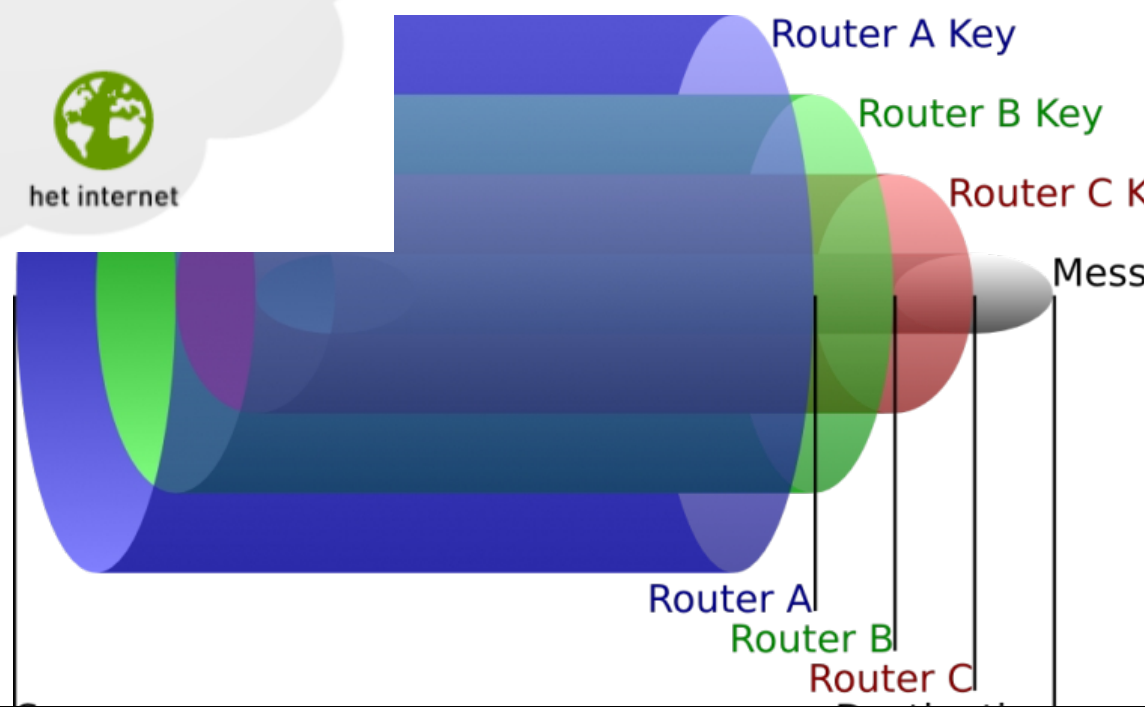
Virtual privat Network (VPN)



the onion router (tor)



wat is Tor?



Workshops

- 1. Slot
 - Email-Verschlüsselung
 - Chat

- 2. Slot
 - Festplattenverschlüsselung
 - Tor und VPN

W-Lan

- Über “eduroam” mit Uni-Account
- Über “WLAN-unifr” mit Uni-VPN
- Über “cryptoparty” passwort: fuckoffNSA



Kontakt

Referat-datenschutz@stura.org

Referat-politische-bildung@stura.org

Don't forget to update, don't forget to back-up!