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

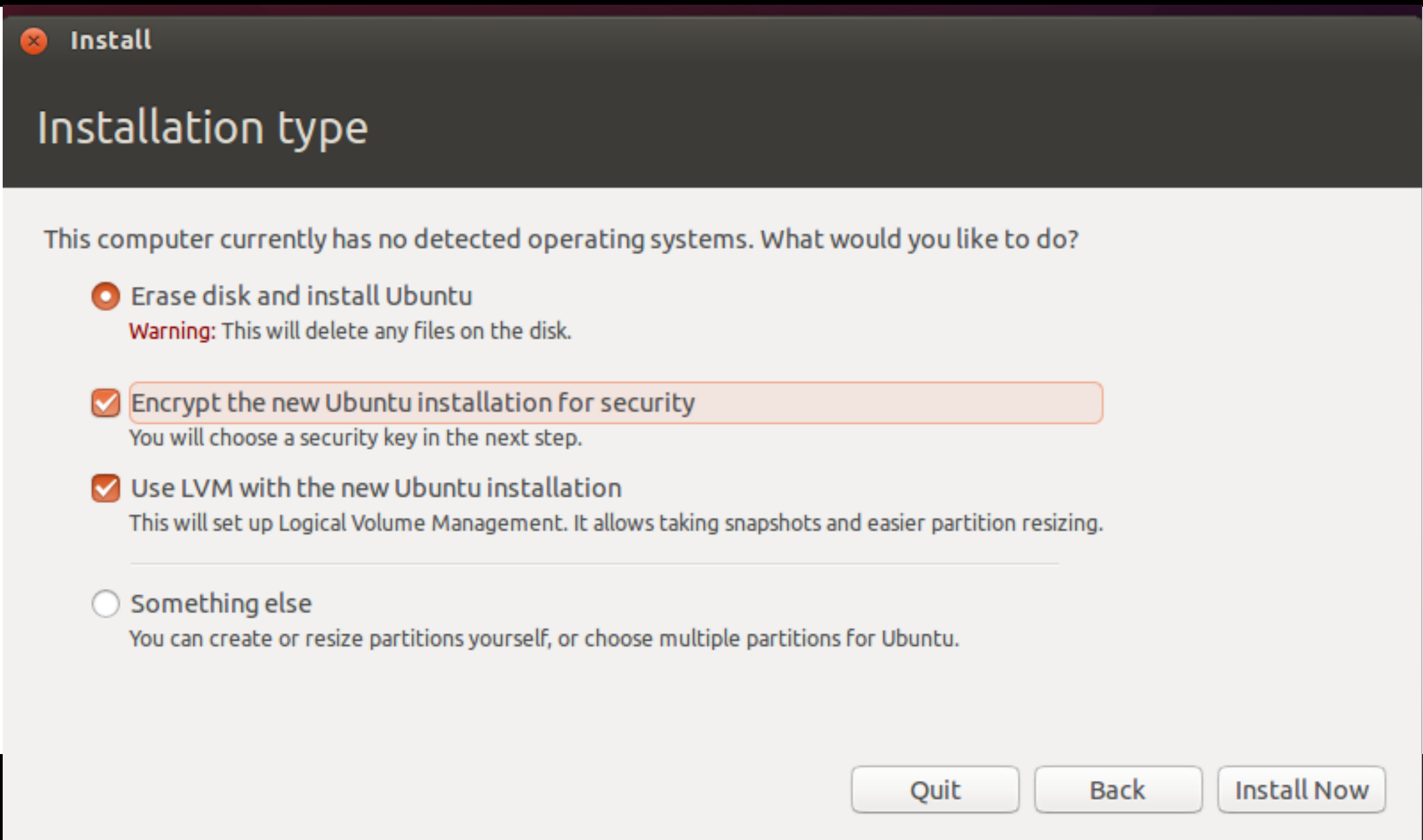
Open Source

- 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

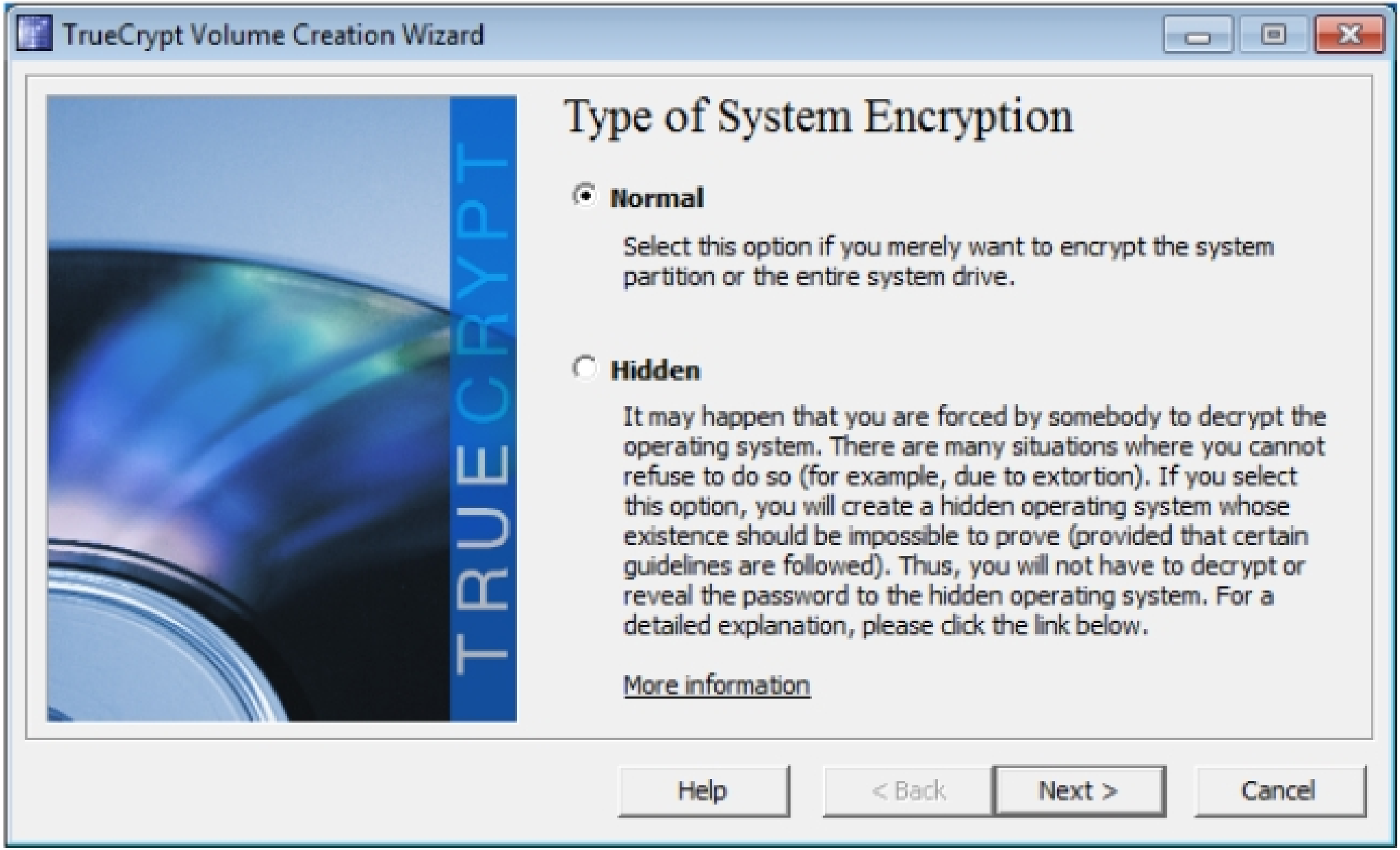
Festplattenverschlüsselung

- 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



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

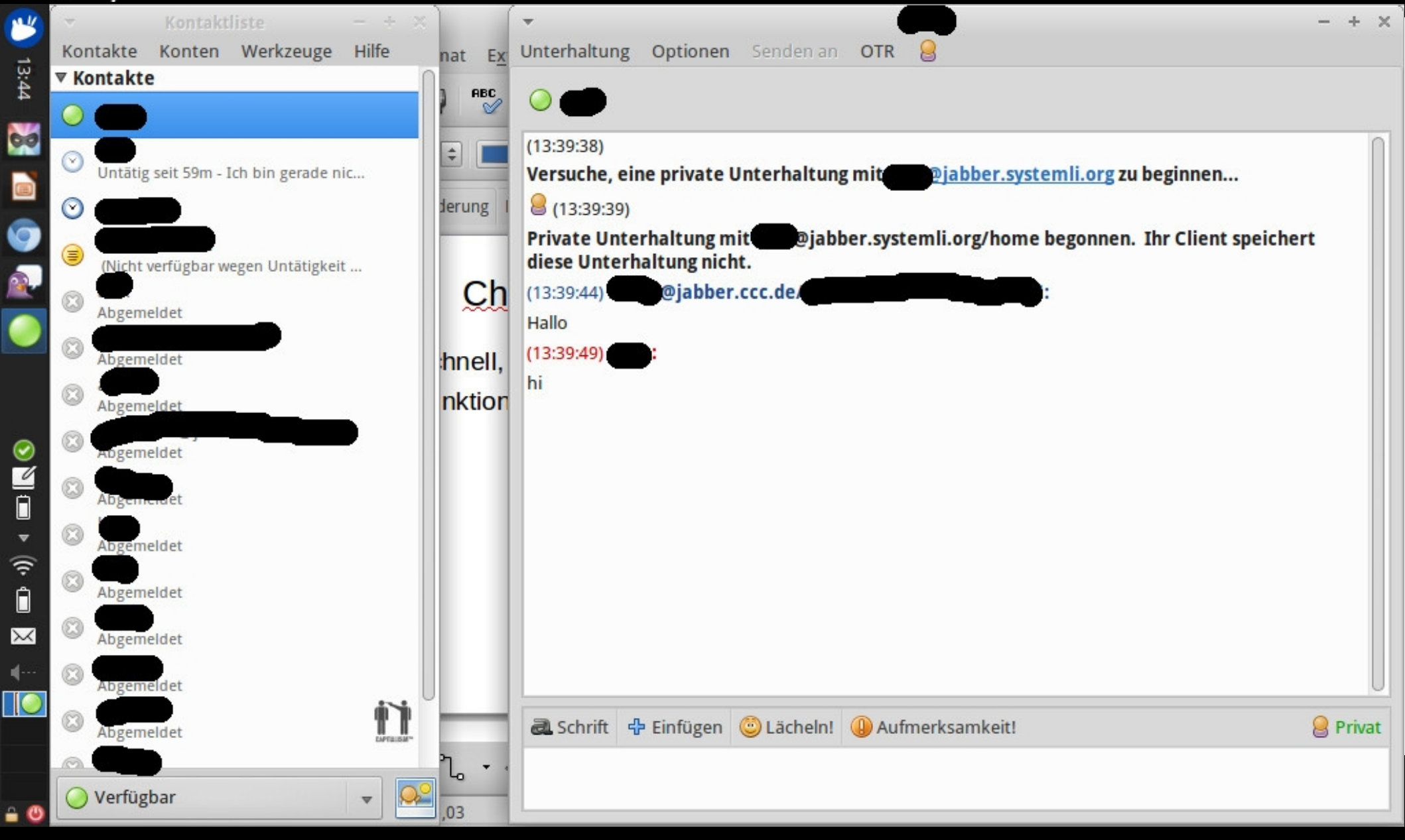
Signieren von Emails (ab 2:35 min)

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

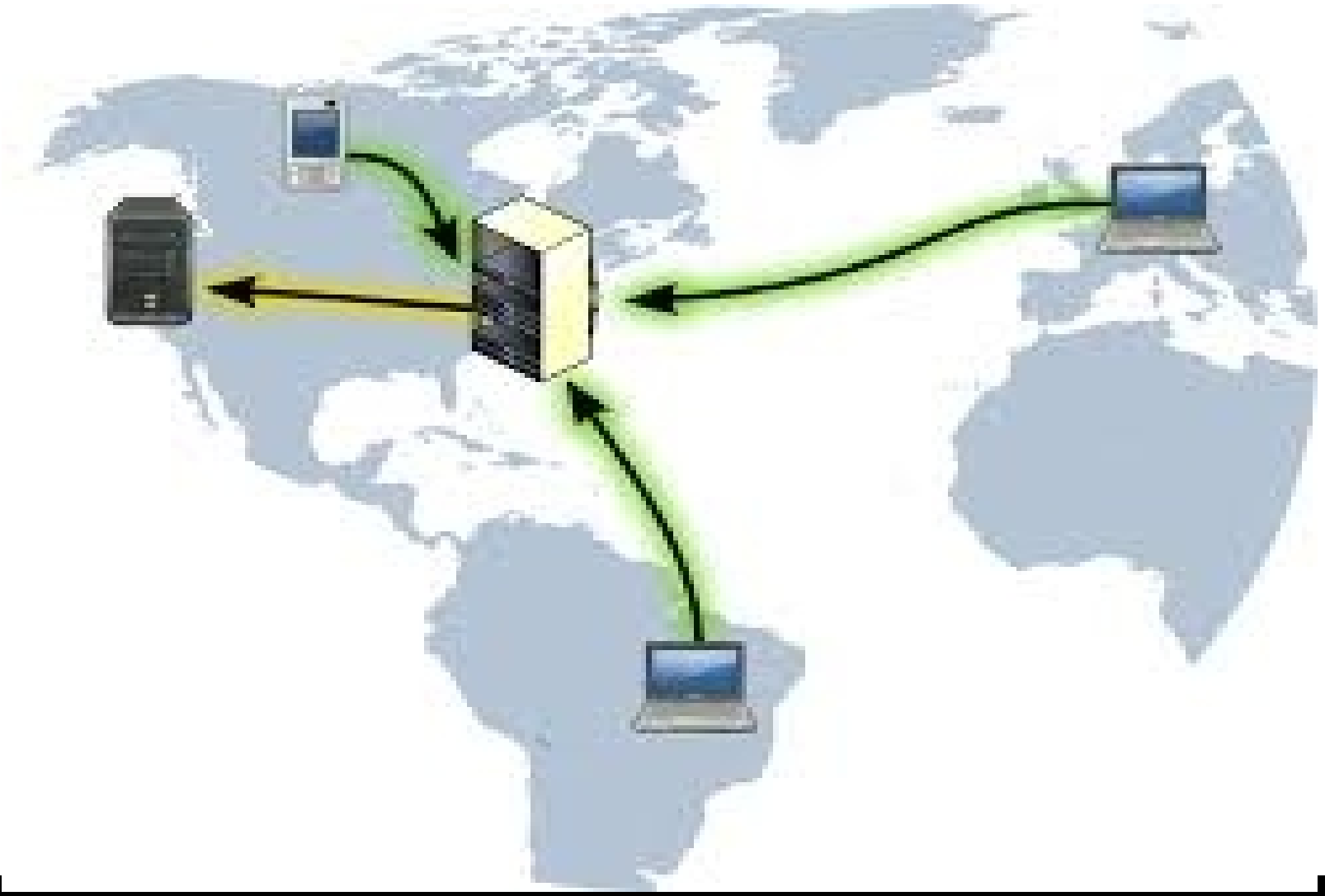
Chatten mit Jabber und otr

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

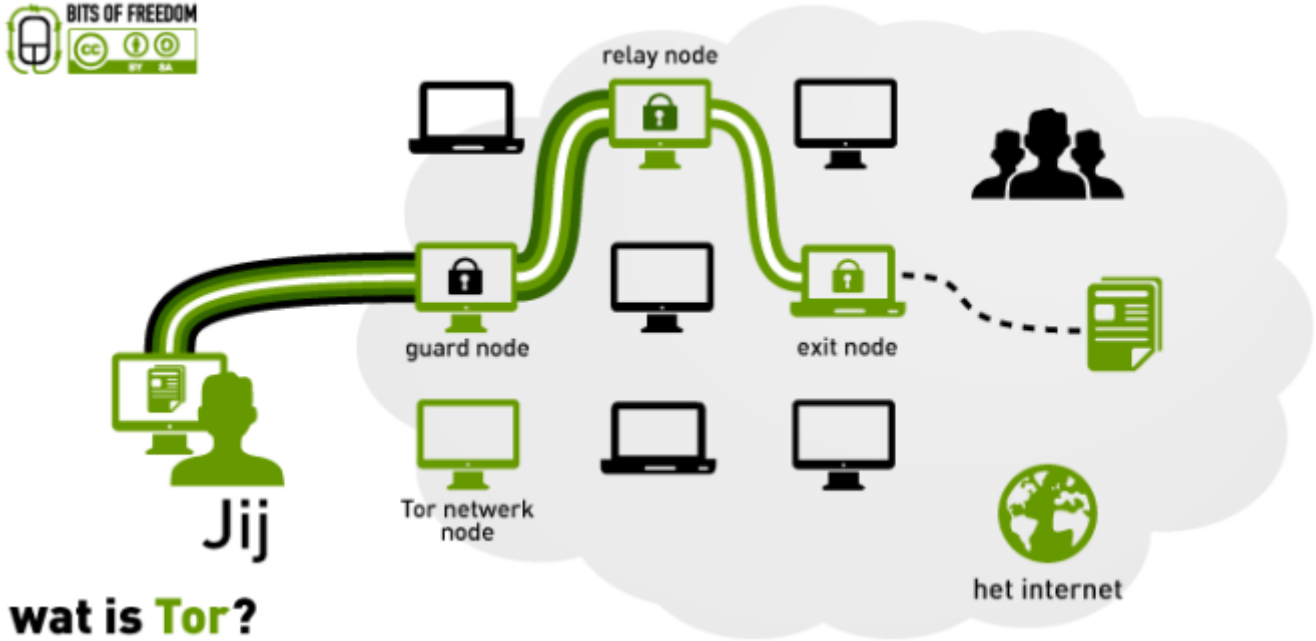
Chatten mit Verschlüsslung

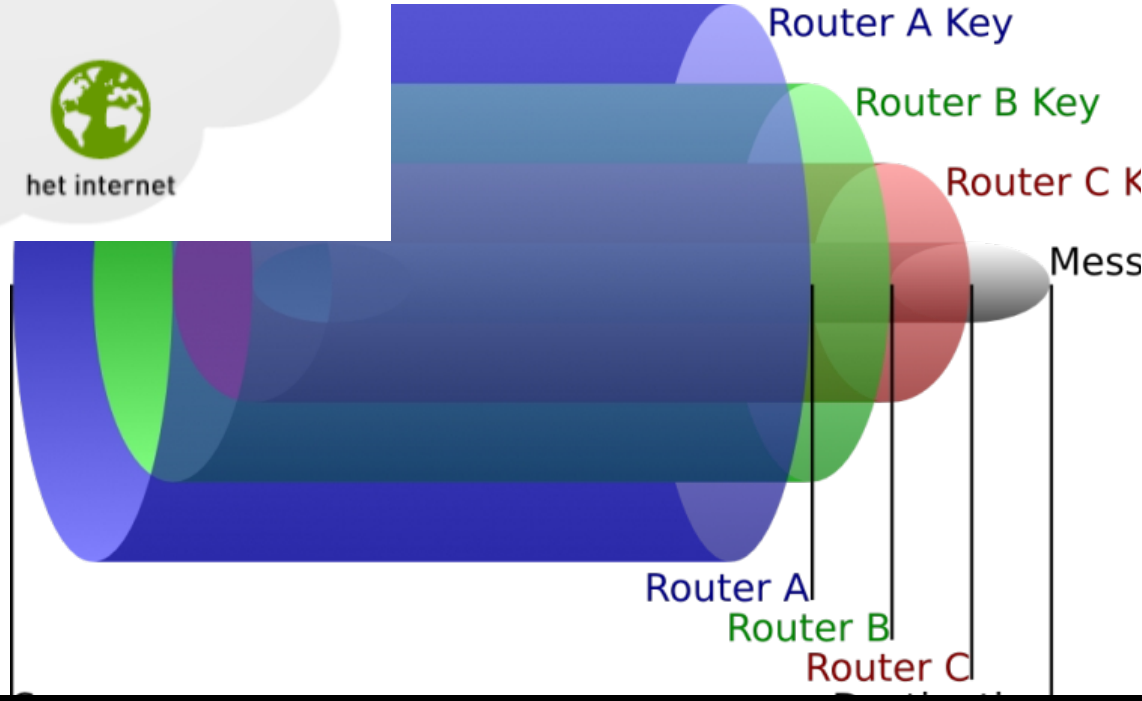


Virtual privat Network (VPN)



the onion router (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!