VPN with Mobile Devices

55. DFN Betriebstagung Oktober 2011 Berlin

Prof. Dr. Andreas Steffen
Institute for Internet Technologies and Applications
HSR Hochschule für Technik Rapperswil
andreas.steffen@hsr.ch

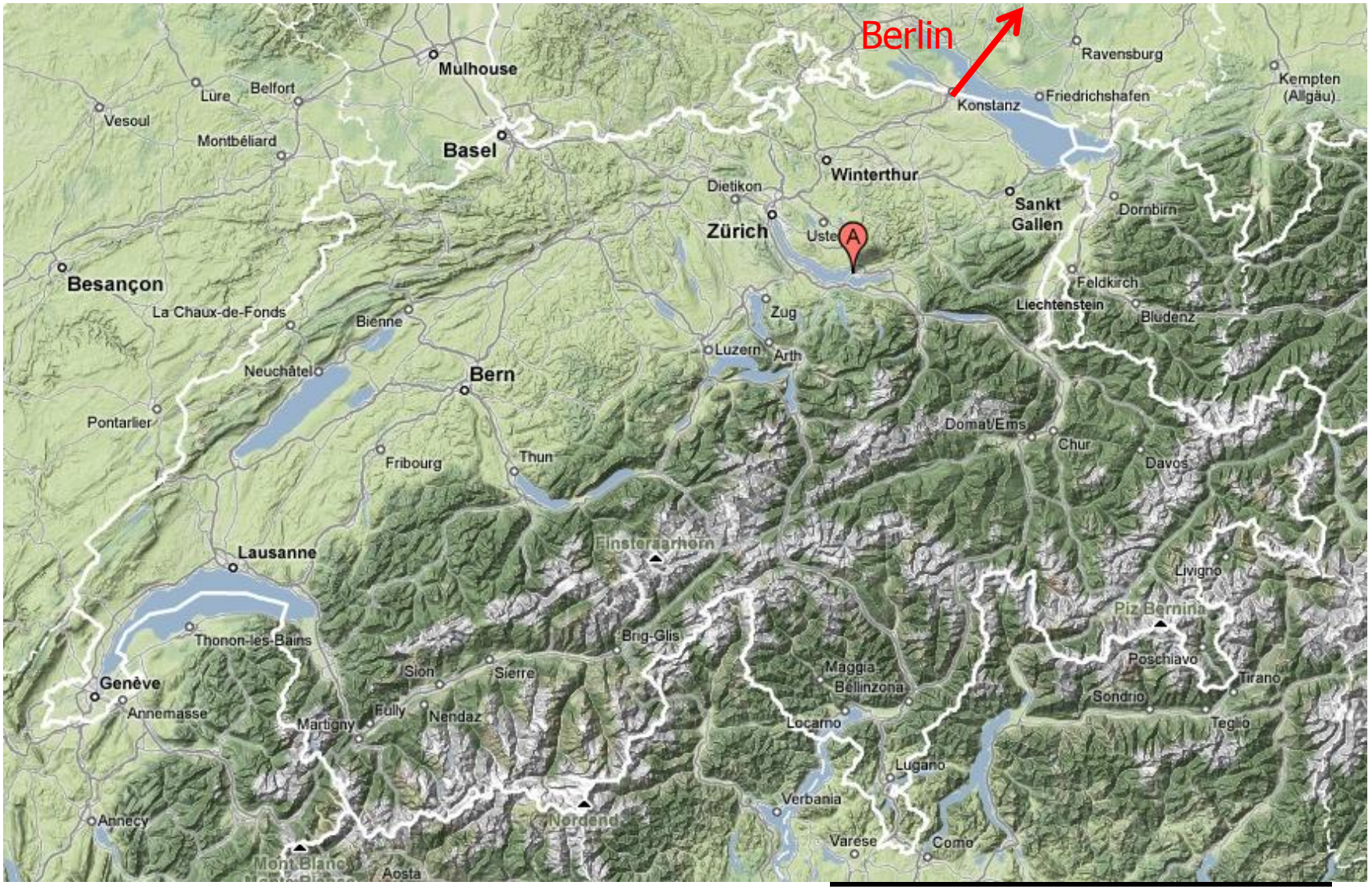
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

strongswan

Wo um Himmels Willen liegt Rapperswil?

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

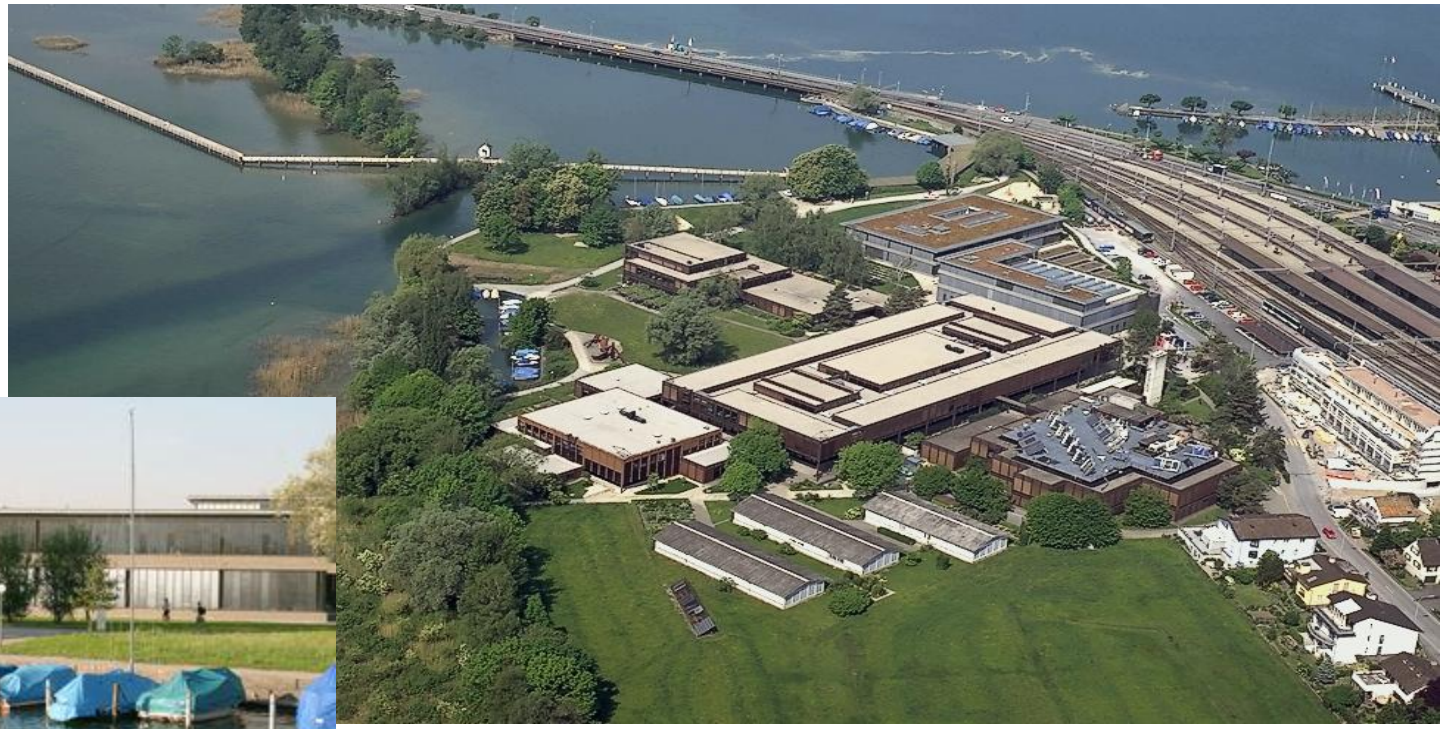
FHO Fachhochschule Ostschweiz



HSR - Hochschule für Technik Rapperswil

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Fachhochschule mit ca. 1500 Studierenden
- Abteilung für Informatik (400 Studierende)
- Bachelorstudium (3 Jahre), Masterstudium (+1.5 Jahre)



VPN with Mobile Devices

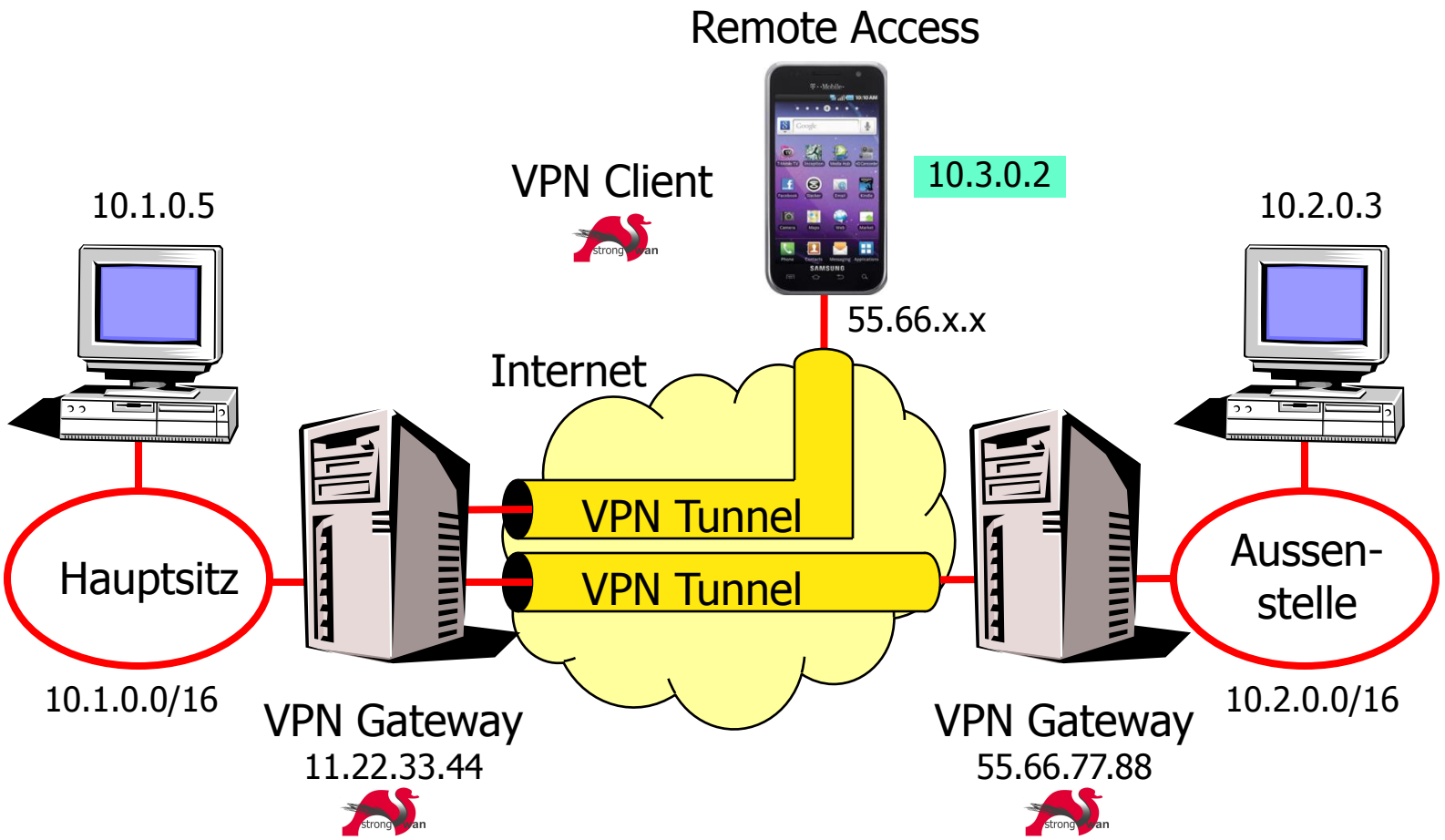
55. DFN Betriebstagung Oktober 2011 Berlin

strongSwan die VPN Open Source Lösung

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

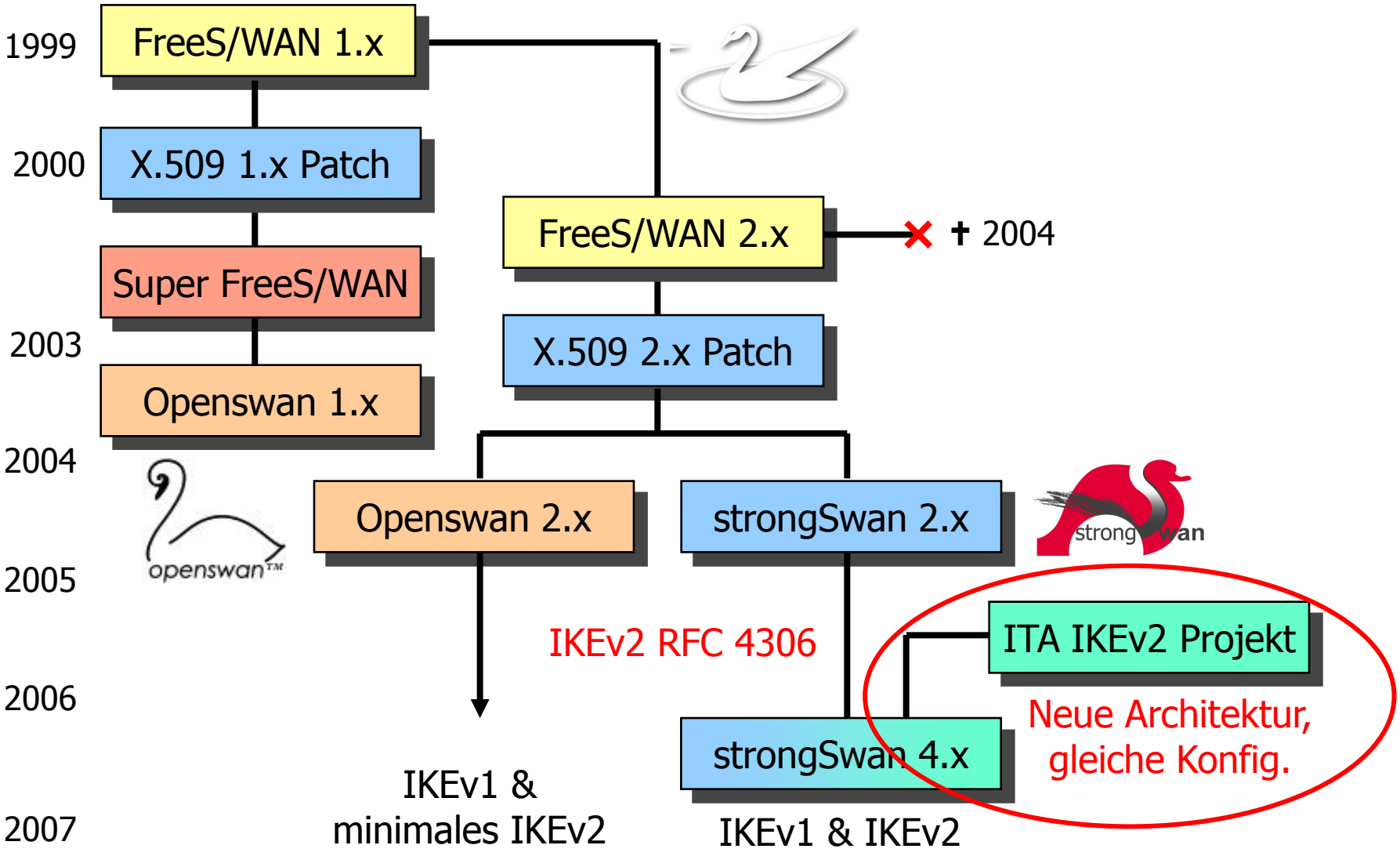
FHO Fachhochschule Ostschweiz

strongSwan Einsatzszenarien



- strongSwan ist ein Internet Key Exchange Dämon, der für den automatischen Verbindungsaufbau von IPsec-basierten VPN Verbindungen zuständig ist.

Der FreeS/WAN Stammbaum



IKEv2 Interoperability Workshops

Frühling 2007 in Orlando, Florida
Frühling 2008 in San Antonio, Texas

- strongSwan funktionierte einwandfrei mit IKEv2 Produkten von Alcatel-Lucent, Certicom, CheckPoint, Cisco, Furukawa, IBM, Ixia, Juniper, Microsoft, Nokia, SafeNet, Secure Computing, SonicWall, und dem IPv6 TAHI Projekt.

strongSwan Schlüsselkunden

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Alcatel-Lucent, Clavister, Ericsson, Nokia Siemens Networks, Ubiquisys
  - Femtocells/Security Gateways für GSM/UMTS/LTE Mobilfunknetze
- Astaro, Karlsruhe
  - Astaro Security Gateway
- Secunet, Dresden
  - SINA Box für Hochsicherheitsanwendungen (BSI, Auswärtiges Amt)
- U.S. Regierung (NSA)
  - Open Source IKEv2/IPsec Referenz- und Test-System für Suite B Elliptische-Kurven-Kryptografie

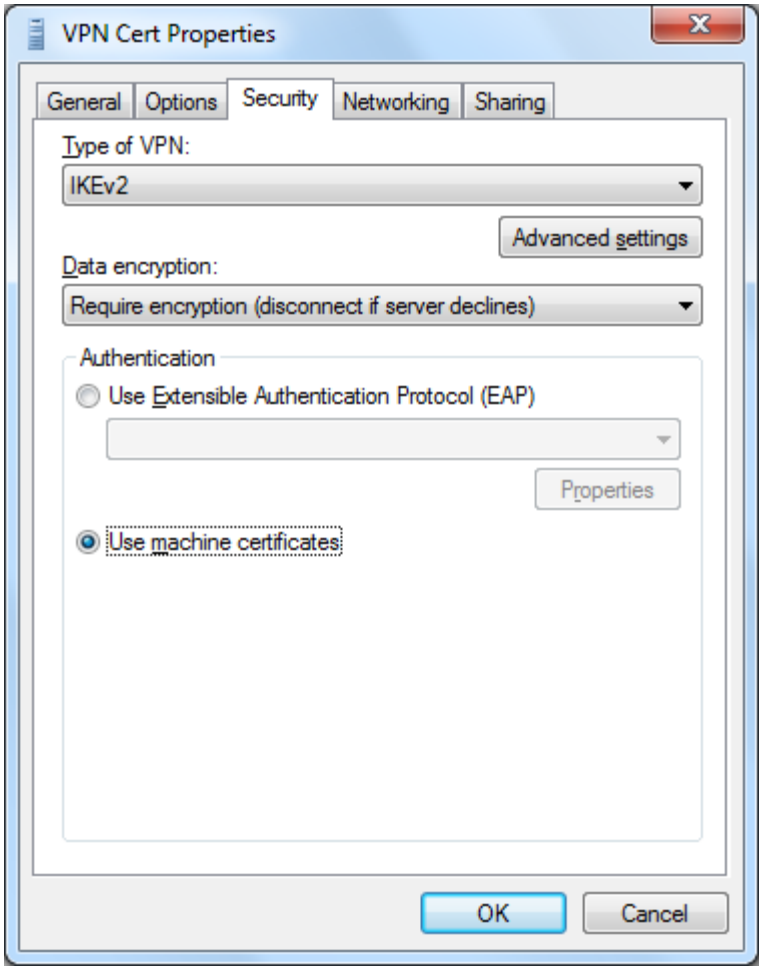
Unterstützte Plattformen

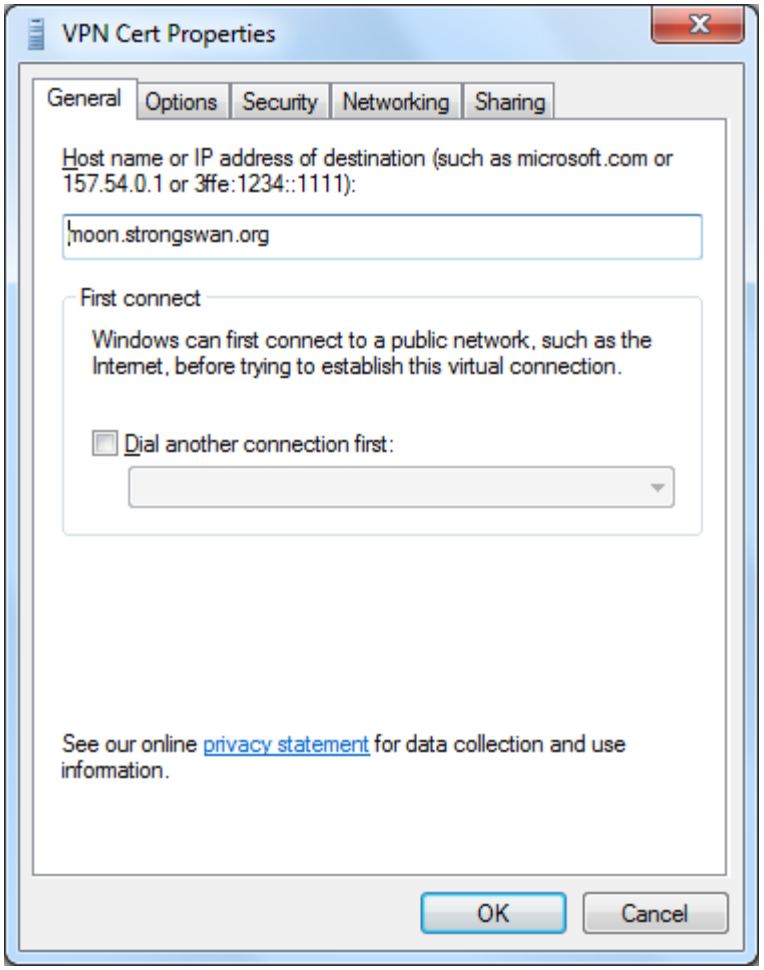
HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Betriebsysteme
  - Linux 2.6 / 3.x
  - Android 2.x
  - FreeBSD 7.x / 8.x
  - Mac OS X 10.5 … 10.7
- Hardware Plattformen (32/64 bit)
  - Intel, Via, AMD
  - ARM, MIPS (z.B. Freescale, Marvell, 16-Core Cavium Octeon)
  - PowerPC
- Netzwerk Stacks
  - IPv4
  - IPv6 (SuSE Linux Enterprise mit strongSwan zertifiziert 2008 durch DoD)
- Portabler Quellcode
  - 100% in C geschrieben, aber mit einem object-orientierten, modularen Ansatz
  - IKE Durchsatz skalierbar durch Verwendung von Multi-Threading

Wie steht es mit Windows?

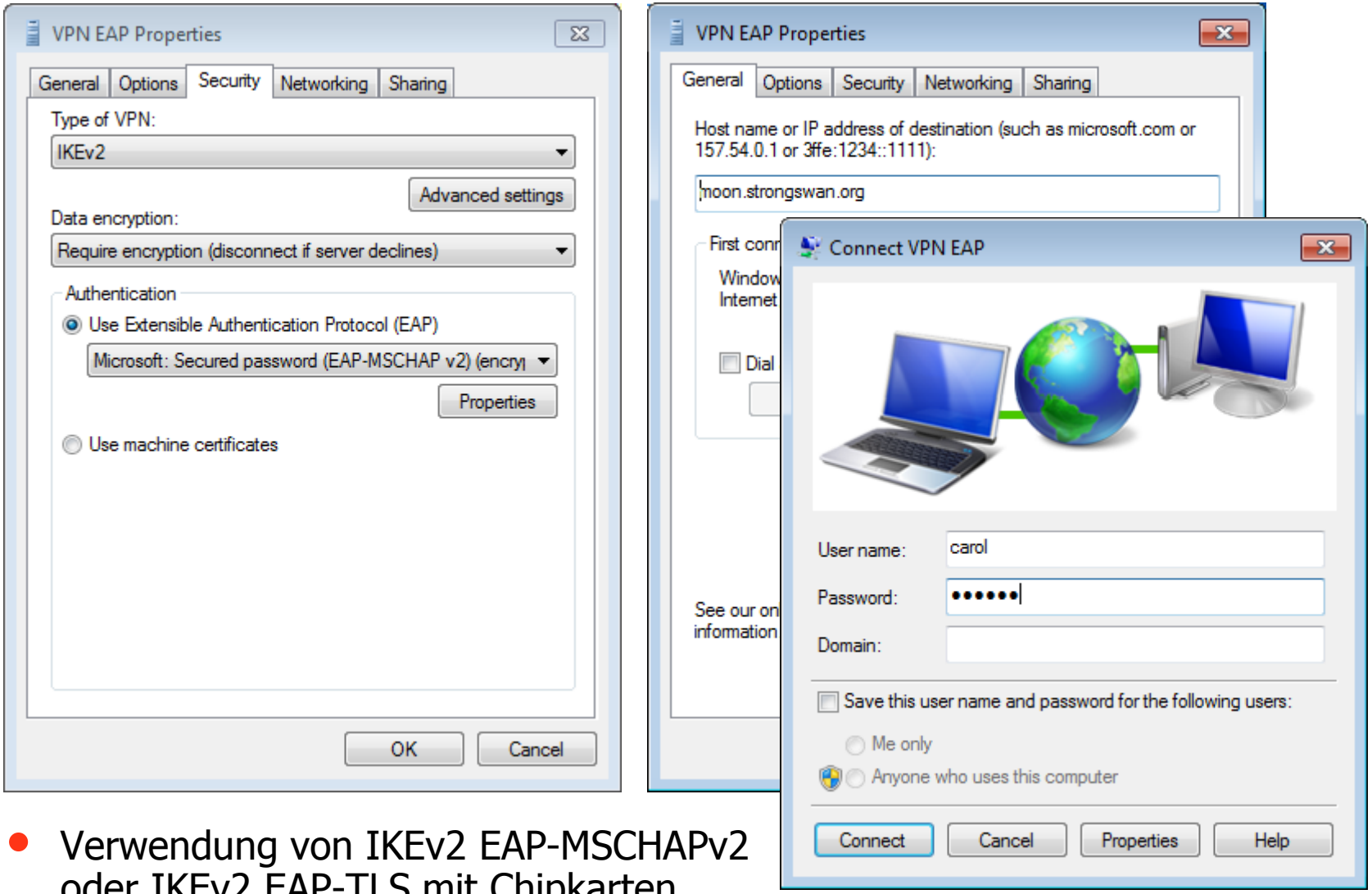
Windows 7 VPN mit Maschinenzertifikaten





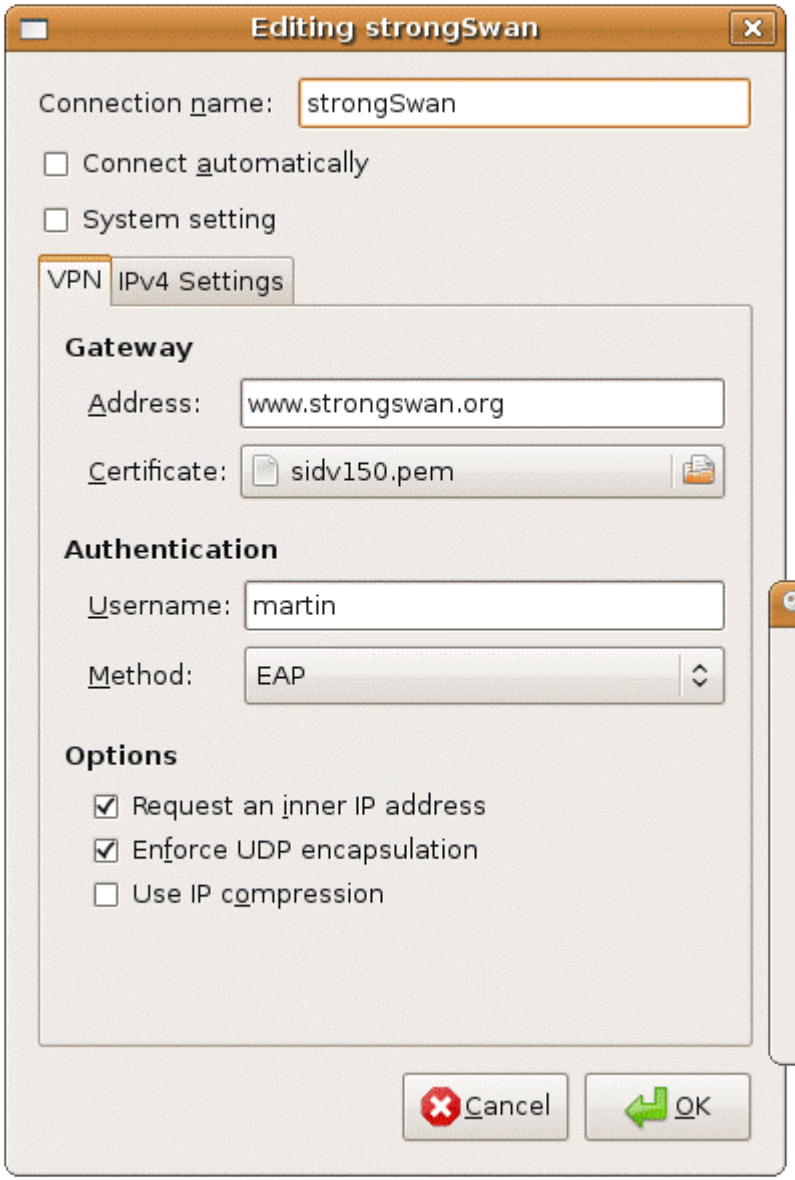
- Microsoft testete die IKEv2 Interoperabilität unter Verwendung von strongSwan bis zum endgültigen Windows 7 Release.

Windows 7 VPN mit EAP Authentisierung



- Verwendung von IKEv2 EAP-MSCHAPv2 oder IKEv2 EAP-TLS mit Chipkarten

strongSwan Applet für den Linux Desktop

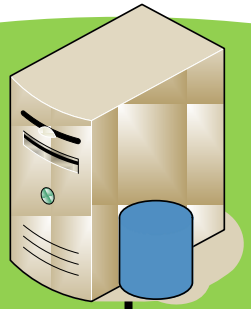


- D-Bus basierte Kommunikation zwischen NetworkManager und strongSwan IKEv2 Dämon.

strongSwan in heterogener VPN Umgebung

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

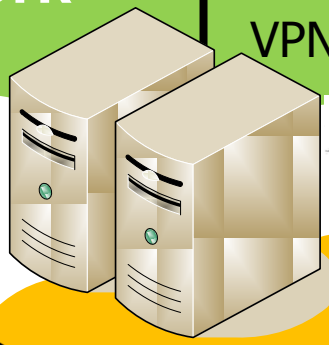
Windows Active
Directory Server

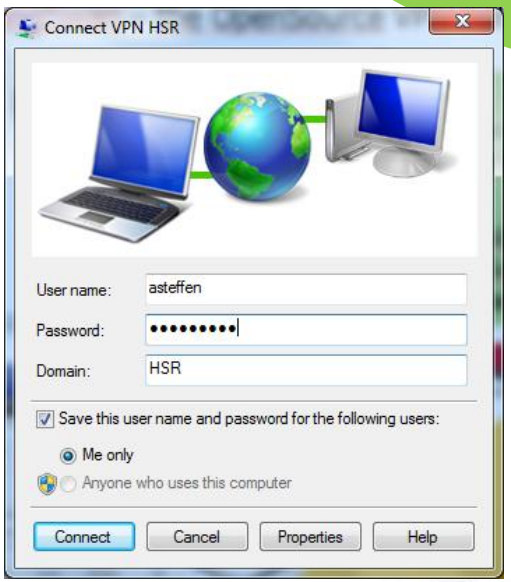


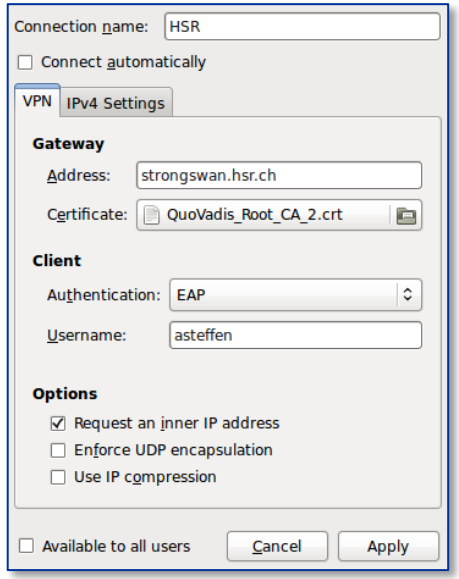
Linux
FreeRadius Server

Corporate
Network

High-Availability
strongSwan
VPN Gateway







Internet

Windows 7
Agile VPN Client

strongswan.hsr.ch

strongSwan
Linux Client

strongSwan IKEv2 Authentisierungsmethoden

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Basierend auf Public Keys
  - X.509 Zertifikate mit RSA or ECDSA Schlüssel
  - PKCS#11 Chipkarten-Schnittstelle
  - CRLs von HTTP/LDAP Server und/oder Einsatz von OCSP
- Basierend auf Pre-Shared Keys (PSK)
  - Beliebige PSK Länge, Vorsicht bei schwachen Passwörtern!
- Based auf dem Extended Authentication Protokoll (EAP)
  - EAP-MD5, EAP-MSCHAPv2, EAP-GTC
  - EAP-SIM, EAP-AKA (GSM/UMTS/CDMA2000)
  - EAP-TLS, EAP-TTLS, EAP-PEAPv0, EAP-TNC (Trusted Network Connect)
- Schnittstelle zu AAA Server
  - EAP-RADIUS
- EAP und TNC Methoden als Plugins implementiert
  - Der strongSwan IKEv2 Dämon lädt die Plugins dynamisch beim Starten

VPN with Mobile Devices

55. DFN Betriebstagung Oktober 2011 Berlin

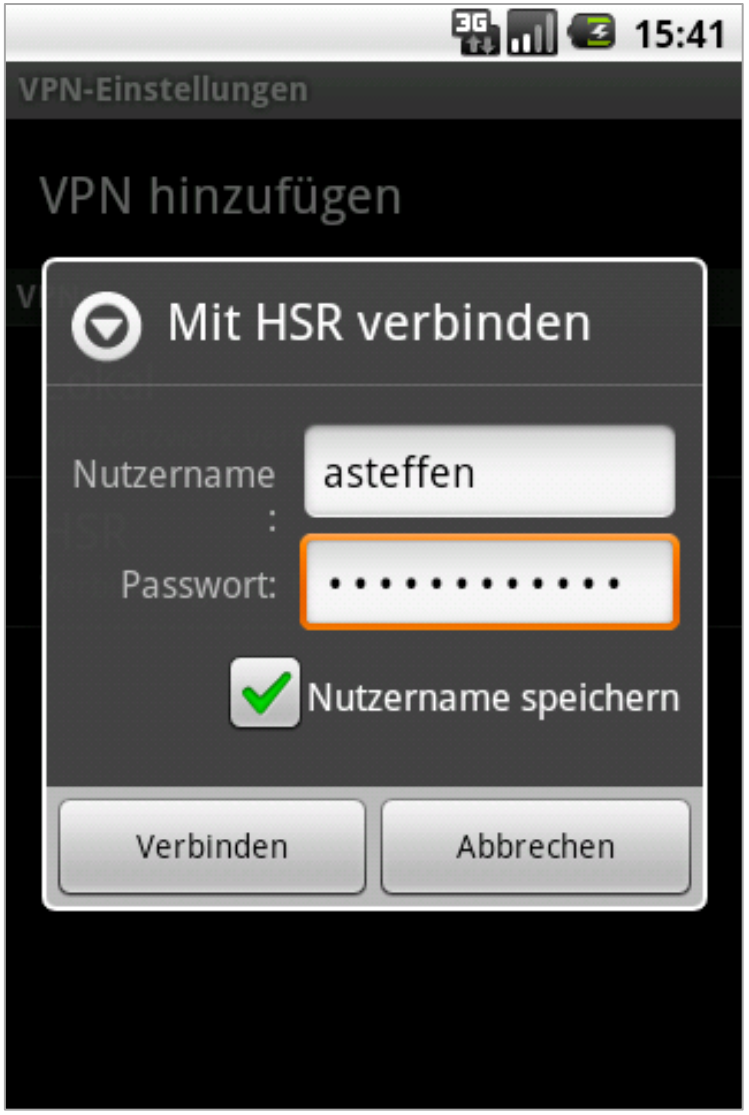
strongSwan unter Android

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

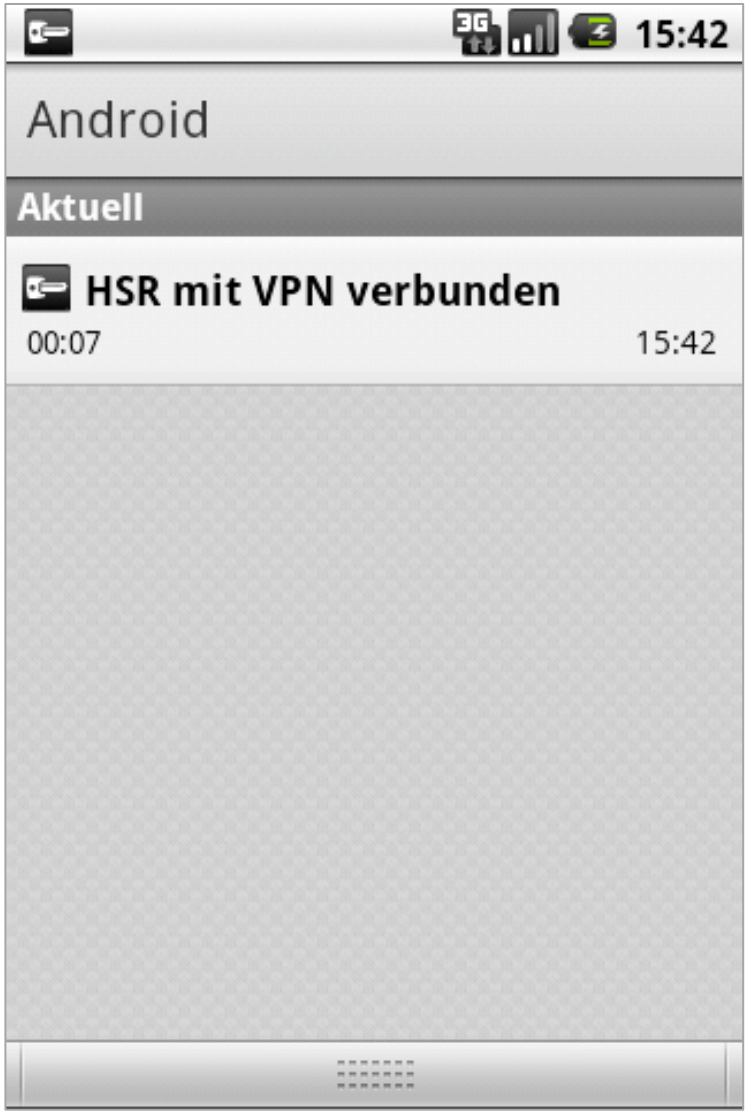
FHO Fachhochschule Ostschweiz

Android VPN Konfiguration

Android VPN Verbindungsaufbau



Android VPN Status



- Android IPsec Erweiterung
  - Damit strongSwan unter Android läuft, muss der Android Kernel um einige IPsec Kernel Module ergänzt werden.
  - Dies bedingt das „Rooten" des Android Geräts.
- Android strongSwan Build
  - Der strongSwan IKEv2 Dämon und die zugehörigen Libraries müssen mit dem Android Emulator gebaut und anschliessend auf das Gerät raufgeladen werden.

strongSwan Roadmap

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Portierung auf neue Android Versionen
  - Android 3.x für Tablet PCs (Samsung Galaxy Tab 10.1)
  - Android 4.0 für Tablet PCs und Smartphones (Google Nexus Prime)
- strongSwan VPN App für Mac OS X
  - Einfaches GUI für die Konfiguration und Starten des strongSwan IKEv2 Dämons (MacBook Air)
- Apple iPhone and iPad
  - Leider sind diese Plattformen völlig geschlossen, so dass die Benutzer mit dem unsäglichen IKEv1 Cisco VPN Client vorlieb nehmen müssen.
- TCG Trusted Network Connect (TNC)
  - IF-MAP 2.0 Interface für die Überwachung von strongSwan Gateways.
- TCG Platform Trust Service (PTS)
  - Überprüfung von Trusted Boot Vorgängen und Messen von Dateien und Anwendungen via TNC (Masterthesis an der HSR)

Danke für Ihre Aufmerksamkeit!

Fragen?

www.strongswan.org