WLAN-Technologien an der HU

1. Technik, Abdeckung, Verfahren
2. Gegenwärtige Sicherheitstechnologien
3. Authentifizierung 802.1x, Verschlüsselung WPA/WPA2
4. Authentifizierung und Verschlüsselung mit IPSec-VPN
5. Authentifizierung und Verschlüsselung mit SSL-VPN
6. Roaming: VPN-CSAG, DFN-Roaming, EDUROAM
7. Vergleich der Zugangstechnologien

Technik, Verfahren

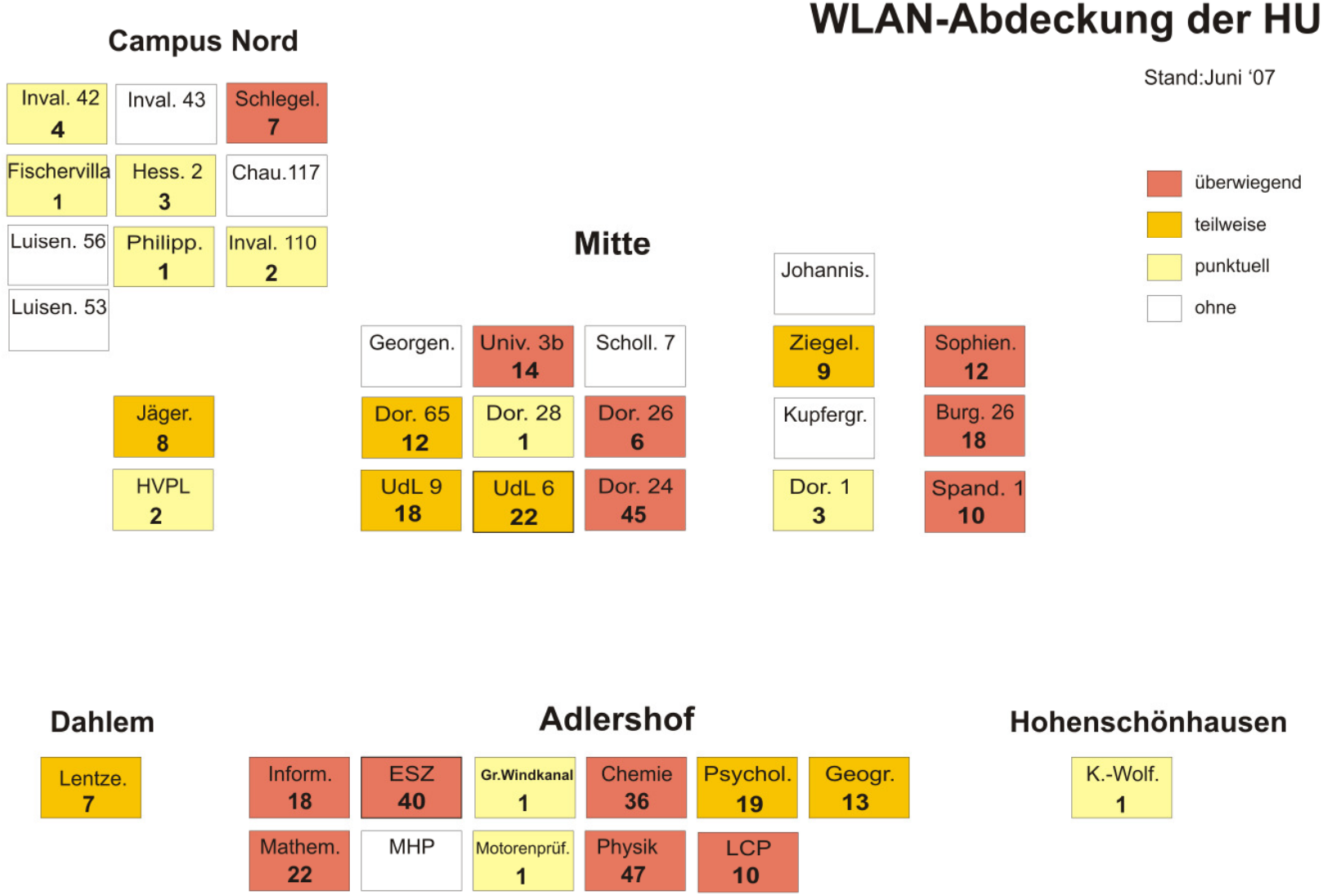
- 413 Accesspoints, davon 207 in Adlershof (2004: 230/175)
- 33 Gebäude mit WLAN-Installationen (2004: 21)
- 9310 registrierte Nutzer (2004: 2200), ca. 350 parallel
- 802.11b (11 Mbit/s), 11g und 11a/h (54 Mbit/s)
- einheitliche Nutzung, zentrales Management
- 2005: 293 Accesspoints Enterasys AP2000 und R2
- Juli 07: komplette Ausstattung Enterasys AP4102
- Multi-SSID erlaubt WLANs mit unterschiedlichen Sicherheitsmechanismen, DFN-Roaming/eduroam

WLAN-Typen

	802.11b	802.11g	802.11a	802.11h
Datenrate Mbit/s	11 ... 1	54 ... 6	54 ... 6	54 ... 6
Frequenz GHz	2,4	2,4	US:5,2-5,8	DE:5,2-5,7
Leistung mW	100	100	US:40/800 DE: 30/60	200/1000
Reichweite		< 11b	< 11h	< 11g
Frequenzbereiche	13/3	13/3	12/12 (4)	19/19
kompatibel zu 11b		ja	nein	nein
Verlust mit 11b		ja	nein	nein
DFS: DynFreqSel			nein	ja
TPC: TraPowCon			nein	ja

WLAN-Abdeckung der HU

Stand:Juni '07



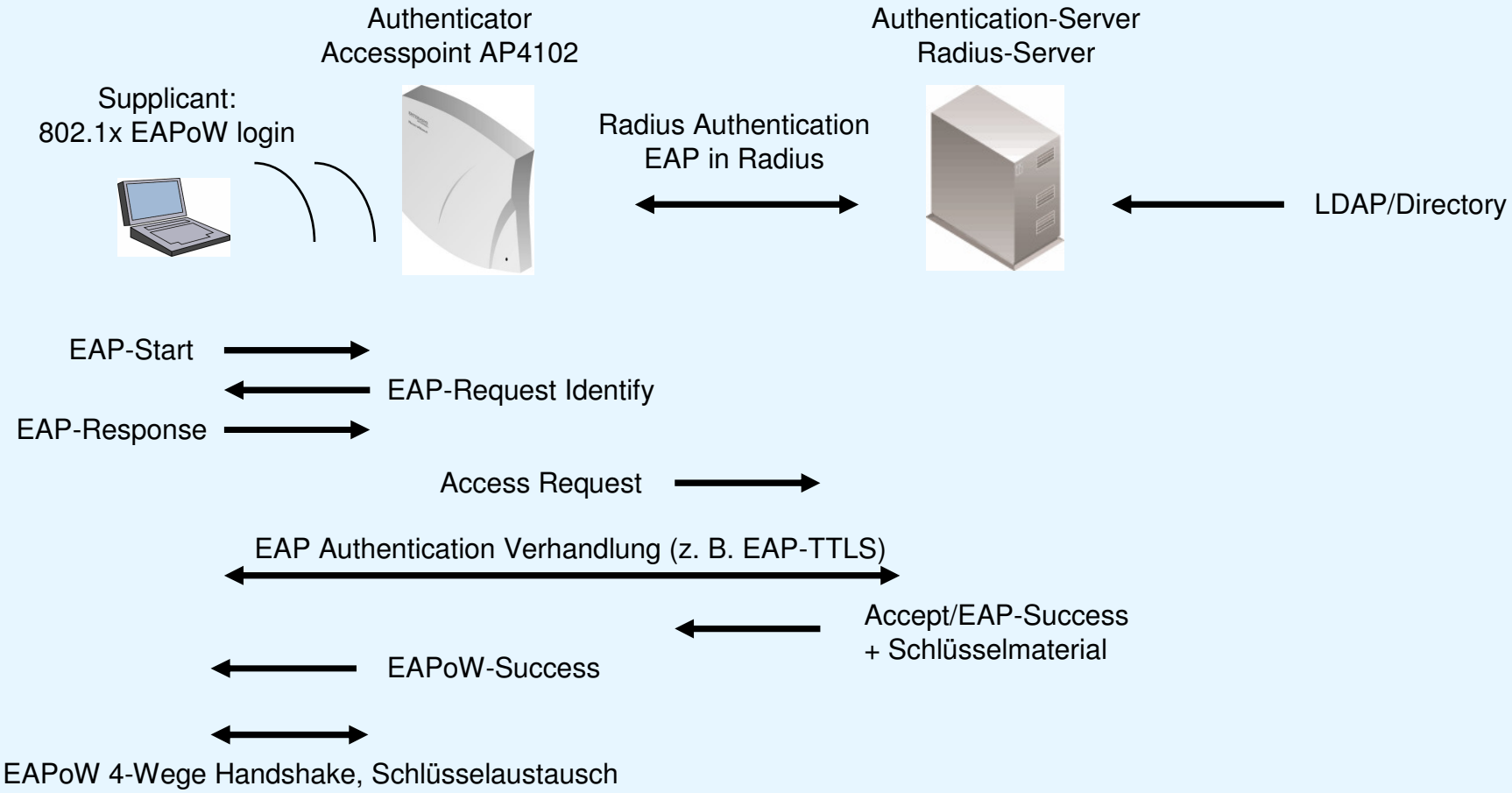
Bisherige Sicherheitstechnologien

- Versteckte SSID
- MAC-Adressfilterung
- 128-Bit-WEP-Verschlüsselung
- Integrity Check Value (ICV)
- VPN optional
- Sicherheit nicht ausreichend!
  - keine Benutzerauthentifizierung
  - zu kurzer Initialisierungsvektor (Schlüsselwiederholung)
  - statische Schlüssel
  - Datenmanipulation (z. B. IP-Adresse) durch offenen ICV

WPA (Wi-Fi Protected Access)

- WPA-Authentifizierung: IEEE 802.1x
  - Benutzername/Passwort oder zertifikatsbasiert
  - Aushandlung Sitzungsschlüssel
- WPA-Verschlüsselung: TKIP (Temporary Key Integrity Protocol)
  - Initialisierungsvektor von 24 auf 48 Bits verlängert
  - Re-Keying: dynamische Schlüsseländerung nach Zeitintervall
  - Per-Packet-Keying: dynam. Schlüsselerzeugung pro Paket (Hash aus IV, MAC und Basisschlüssel)
- WPA-Frame-Integrität: MIC (Message Integrity Check)
  - Prüfsumme mit Benutzung des Schlüssels berechnet
- WPA2 (IEEE802.11i): Verschlüsselung mit AES-128

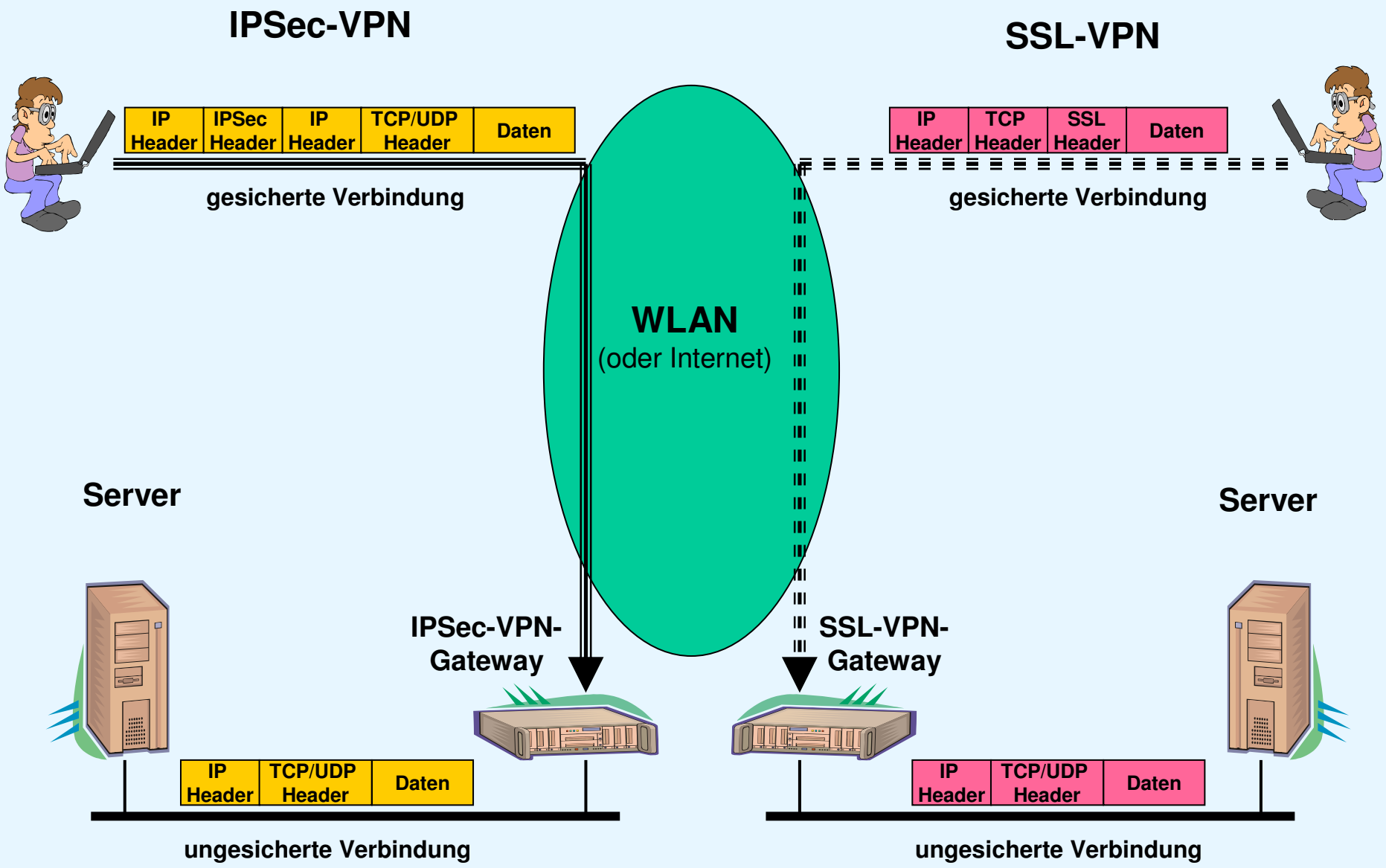
IEEE 802.1x


Authenticator
Accesspoint AP4102
Authentication-Server
Radius-Server
Supplicant:
802.1x EAPoW login
Radius Authentication
EAP in Radius
LDAP/Directory
EAP-Start
EAP-Request Identify
EAP-Response
Access Request
EAP Authentication Verhandlung (z. B. EAP-TTLS)
Accept/EAP-Success
+ Schlüsselmaterial
EAPoW-Success
EAPoW 4-Wege Handshake, Schlüsselaustausch

Virtual Private Network (VPN)

- Verbund privater Teilnetze über öffentliche Leitungen zu einem (scheinbar) privaten Netz
- Remote Access VPN (z. B. WLAN): PC/Laptop = Teilnetz
- Authentifizierung, Verschlüsselung, Datenintegrität, Authorisierung

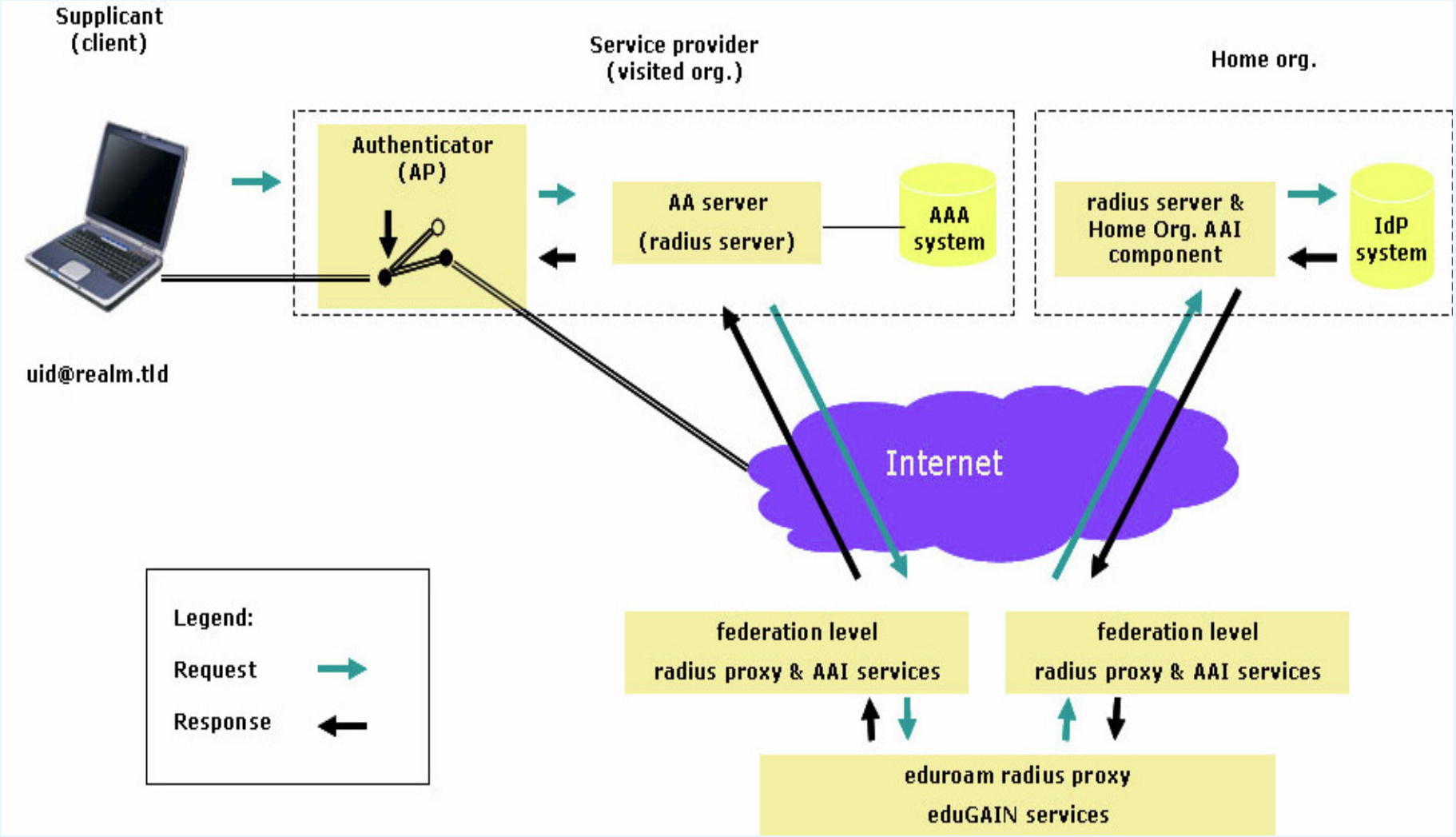
IPSec VPN	SSL-VPN
nicht anwendungsabhängig	anwendungsabhängig
Anw. - TCP/UDP - IP - IPSec - Übertragung	Anwend. - SSL - TCP - IP - Übertragung
keine Authorisierung	Authorisierung für Anwendungen
Tunneling (oder transparent)	kein Tunneling
IP - IPSec - IP - TCP/UDP - Daten	IP - TCP - SSL - Daten
Internet Key Exchange Protocol IKE	SSL Handshake Protocol
Phase 1: SA-Parameter, Schlüsseltausch, Authentifizierung auf Systemebene	ClientHello (Parameter) → ← ServerHello/Zertifikat
Phase 2: IPSec-Parameter, Schlüssel-tausch, Authentifizierung	Key-Exchange Authentifizierung

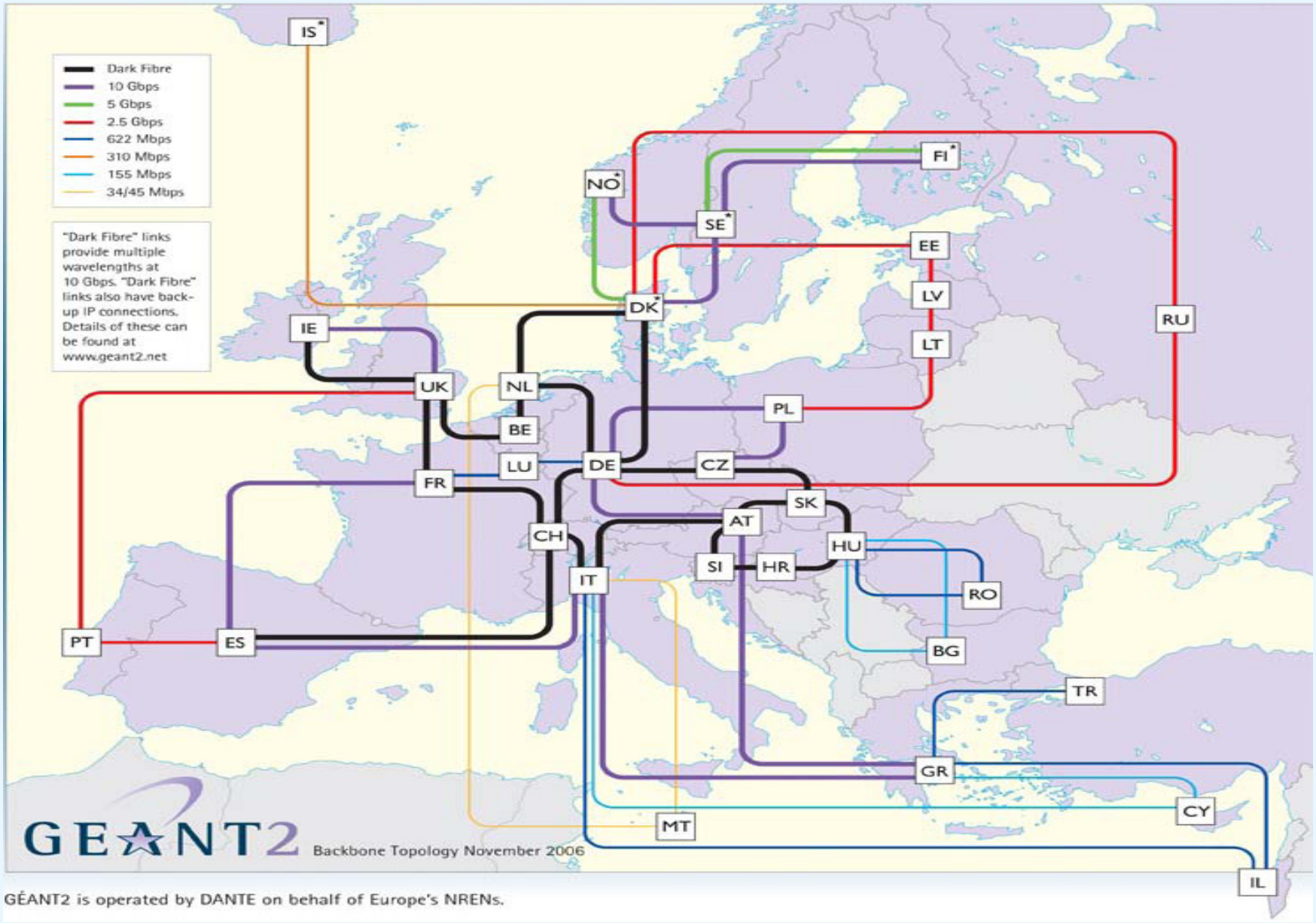

IPSec-VPN
SSL-VPN
IP Header
IPSec Header
IP Header
TCP/UDP Header
Daten
IP Header
TCP Header
SSL Header
Daten
gesicherte Verbindung
gesicherte Verbindung
WLAN
(oder Internet)
Server
Server
IPSec-VPN-Gateway
SSL-VPN-Gateway
IP Header
TCP/UDP Header
Daten
IP Header
TCP/UDP Header
Daten
ungesicherte Verbindung
ungesicherte Verbindung

Roaming mit VPN-CASG

- Controlled Address Space for Gateways
- Zugang zum heimischen VPN-Gateway aus VPN-WLANs der Fremdeinrichtungen
- Adressraum (193.174.167.0/24) für VPN-Gateways der am CASG teilnehmenden Einrichtungen
- Freigabe des Adressraumes und der Ports auf den Routern/Firewalls der teilnehmenden Einrichtungen
- Voraussetzungen: VPN-Client, Fremdeinrichtung im CASG-Verbund (z. B. FU, TU), ansonsten transparent

DFN-Roaming/Eduroam




Dark Fibre
10 Gbps
5 Gbps
2.5 Gbps
622 Mbps
310 Mbps
155 Mbps
34/45 Mbps
"Dark Fibre" links provide multiple wavelengths at 10 Gbps. "Dark Fibre" links also have back-up IP connections. Details of these can be found at www.geant2.net
IS
NO
SE
FI
EE
LV
LT
RU
DK
IE
UK
NL
BE
LU
DE
PL
CZ
FR
SK
AT
CH
HU
SI
HR
IT
RO
BG
PT
ES
TR
GR
CY
MT
IL
GÉANT2
Backbone Topology November 2006
GÉANT2 is operated by DANTE on behalf of Europe's NRENs.

Vergleich der Zugangsverfahren

	802.1x	IPSec-VPN	SSL-VPN
Voraussetzung	**802.1x-WLAN geeign. Radiusinfra.**	**offenes VPN-WLAN IPSec-VPN-Infrastr.**	**offenes VPN-WLAN SSL-VPN-Infrastr.**
Client nötig	ja	ja	nein
Systemabhängigkeit	**ja, wenn nicht XP/Vista+EAP-TLS**	ja	**gering (Browser)**
Aufwand Benutzer	Client	Client	ohne
Aufwand Betreuung	erheblich	mittel	klein
Roaming	**Europa DFN, GÉANT2**	**Deutschland DFN-CASG**	nein
IP-Adr. Heimatnetz	nein	ja	nein
anwendungsabhängig	nein	nein	ja
Authorisierung	nein	nein	ja
Verschlüsselung	**Client – Accesspoint**	**Client - VPN-Gateway**	**Client - VPN-Gateway**