Ein akademisches WLAN:
Vom Aufbau bis zur möglichen Teilnahme an »eduroam«

Master Thesis

zur Erlangung des akademischen Grades

"*Master of Science*", MSc

Universitätslehrgang IKT-Management für Bildungsinstitutionen I

eingereicht am

Zentrum für Bildung und Medien

Abteilung Telekommunikation, Information und Medien

Donau-Universität Krems

von

Dipl.-Ing. Reinfried O. Peter

Graz/Krems, März 2006

Betreuer: Dr. Wilfried Maschtera

Univ.-Prof. Dr. Michael Wagner

Ich, Reinfried O. **Peter**
geboren am 31. Dezember 1962 in Leoben
erkläre,

1. dass ich meine Master Thesis selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfen bedient habe,

2. dass ich meine Master Thesis bisher weder im In- noch im Ausland in irgendeiner Form als Prüfungsarbeit vorgelegt habe,

3. dass ich, falls die Arbeit mein Unternehmen betrifft, meinen Arbeitgeber über Titel, Form und Inhalt der Master Thesis unterrichtet und sein Einverständnis eingeholt habe.

Graz, am 11. März 2006 .....

Ich möchte mich an dieser Stelle beim Leiter des Zentralen Informatikdienstes der Technischen Universität Graz, Herrn Dipl.-Ing. Isidor Kamrat, bedanken, ohne dessen Unterstützung ich diesen Universitätslehrgang nicht besuchen hätte können.

Weiters danke ich meinem Kollegen Ing. Thomas Probst für das Korrekturlesen dieser Arbeit.

Abstract

Im ACOnet, dem österreichischen Forschungsnetz, nimmt – wie auch in vielen anderen Forschungsnetzen – die Verwendung von drahtlosen Netzwerken auf Basis IEEE 802.11* (WLANs) massiv zu.
Im Sinne der Bologna-Deklaration der Bildungsminister von 1999 ist die Mobilität der Forscher in Europa zu fördern. Der unkomplizierte Zugang zu WLANs an Organisationen, die z.B. für Gastvorlesungen besucht werden, ist dabei ein kleiner Teil, der von den nationalen Forschungsnetzen bzw. deren Mitgliedern gezielt gefördert werden kann.
Wie in anderen Forschungsnetzen auch, ist in Österreich der Zugang zu diesen Netzen auf unterschiedliche Art und Weise beschränkt. Die Möglichkeit mit der eigenen Identität bei einer Gastorganisation Zugang zu erlangen – sogenanntes Roaming – wird aber noch nirgends angeboten.
Ziel dieser Arbeit ist es, einen Weg aufzuzeigen, wie ein solches Roaming – zumindest national, wenn möglich aber international – auch in Österreich umgesetzt werden kann.

Many National Research and Education Networks (NRENs) all over the world provide their users with connectivity to the internet via WLANs.
Within TERENA, the Trans-European Research and Education Networking Association, a task force has been installed to find a scalable way for international roaming access to (wireless) LANs.
At the moment there is no roaming infrastructure or roaming policy in Austria, so it is the goal of this work to look for the best way either to install a national solution for ACOnet (the Austrian NREN) or a way to participate in »eduroam«, the roaming solution of TERENA's task force »TF-Mobility Group«.

Inhalt

1 Einleitung

Diese Arbeit entstand im Umfeld der Entwicklung eines WLANs an der Technischen Universität Graz und soll einerseits die Ideen dokumentieren, die dazu geführt haben, wie das WLAN an der TU Graz implementiert wurde, andererseits kann und soll es anderen Universitäten (vor allem in Österreich) eine Hilfe bei den Überlegungen zum Aufbau eines eigenen WLANs vor allem im Hinblick auf eine Teilnahme an interuniversitären Kooperationen geben. Hauptziel der Arbeit ist aber für Teilnehmer an ACOnet einen gangbaren Weg zu beschreiben, wie ein universitäres WLAN Teil einer nationalen oder auch internationalen Infrastruktur werden kann, welche Punkte dabei u.U. schon bei der Planung zu berücksichtigen sind und aufzuzeigen, welche Für und Wider es bezüglich einer Teilnahme zu beachten gibt, wobei die bereits existierenden Lösungen in anderen Ländern als Vergleich bzw. als Lösungsansatz herabgezogen werden.

Im Zuge der Implementierung des Funknetzes an der TU Graz hat es sich gezeigt, dass es zumindest 2 Aspekte auch lokal zu berücksichtigen gilt:

- die einfache Nutzbarkeit
- die sichere Verwendung

An der TU Graz liegen die Aufgaben für beide Bereiche, nämlich

- der Aufbau eines (einfach verwendbaren) Netzes
- die Betriebs- und Netzsicherheit

in der Verantwortung der Abteilung »Kommunikation« des Zentralen Informatikdienstes (ZID), wodurch es organisatorisch relativ einfach möglich war und auch ist, Nutzung und Sicherheit gegeneinander abzuwiegen, da mit Dritten nicht verhandelt werden musste.
Bei den Planungen zum Aufbau einer WLAN-Infrastruktur muss aber sehr wohl immer beachtet werden, dass – wie Vrtala (2005) sagt – das Produkt aus Sicherheit und Bequemlichkeit immer kleiner als eine beliebige Konstante ist, oder anders ausgedrückt (a.a.O.):
Sicherheit und Bequemlichkeit

- schließen einander zum Teil aus
- lassen sich nicht beliebig optimieren

d.h.: es ist i. A. ein Kompromiss zu suchen, wie einfach bzw. wie sicher die Nutzung einer Infrastruktur auszusehen hat.

1.1 Historische Entwicklung

Nachdem das Internet bis Mitte der 90er Jahre des vorigen Jahrhunderts zuerst nur eine von Forschern und Wissenschaftern dominierte Welt war, wurde das Internet ab diesem

Zeitpunkt – fast plötzlich – durch neue Technologien für jedermann zugänglich.
Fast parallel zum entstehenden Internet-Hype (WWW und E-Mail wurden auch für Privatpersonen verfügbar) setzte auch eine Entwicklung ein, das Internet nicht nur technisch einfacher zugänglich zu machen, sondern den Zugriff auf das Medium per Funk auch unabhängig von physikalisch verfügbaren Netzwerkanschlüssen oder anderen örtlichen Beschränkungen zu machen.

1.1.1 IEEE 802.11

Als das Institute of Electrical and Electronics Engineers (IEEE) unter der Nummer 802.11 1997 einen neuen Standard für drahtlose Netzwerkkommunikation verabschiedete (IEEE-SA, 2006), war wohl nicht klar, dass damit einige Jahre später eine weitere Revolution im Internet eingeleitet würde.
Die erste Version des Standards sah eine maximale Bruttobandbreite von 2Mbps vor, verwendete das lizenzfreie und somit gratis verfügbare 2,4 GHz-Band und definierte neben dem MAC-Layer und der physikalischen Schicht des OSI-Referenzmodells mit Wired Equivalent Privacy (WEP) auch bereits einen Standard für eine sichere Kommunikation, weil ja klar war, dass die drahtlose Kommunikation (Radio oder Infrarot) potentiell unsicherer ist als drahtgebundene Kommunikation.

1.1.2 IEEE 802.11a/b/g/h

Der IEEE-Standard 802.11 entwickelte sich mit der Zeit weiter: 802.11b erweiterte die Bandbreite im 2,4 GHz-Band auf (brutto) 11 Mbps, das in Europa erst viel später zugelassene 802.11a auf 54 Mbps im 5 GHz-Band und schließlich wurden mit 802.11g auch 54 Mbps im 2,4 GHz-Band erreicht. 802.11h (IEEE-SA, a.a.O.) passt 802.11a an europäische Gegebenheiten an und erhöht gleichzeitig die sehr geringe Reichweite von IEEE 802.11a[1].

1.1.3 Sicherheit

Aufgrund der bekannten physikalischen Gegebenheiten wie der Ausbreitungscharakteristik elektromagnetischer Wellen war von Anfang an klar, dass das neue Medium stärker abgesichert werden muss als drahtgebundene Kommunikation.
Daher wurde – wie in Kapitel 1.1.1 bereits erwähnt – schon in der ursprünglichen Version des Standards IEEE 802.11 mit WEP eine symmetrische Methode der Verschlüsselung definiert. Zu den Unterschieden zwischen symmetrischer und asymmetrischer Verschlüsselung siehe z.B. Singh, 2000 und Hofherr, 2005.
Leider zeigte es sich jedoch relativ bald, dass WEP schon vom Design her und nicht nur

1 vgl. dazu z.B. auch Koller (2004)

in der Implementierung einige Sicherheitslücken aufweist[2], die im ersten Moment noch nicht so gravierend aussahen, weil man mit einer Kombination aus Zugangsfiltern auf Basis von MAC-Adressen, versteckten SSIDs und WEP doch eine ausreichende Sicherheit zur Verfügung stellen zu können glaubte, die dann nur von Spezialisten ausgehebelt werden könnte.

Ab ca. 2001 erschienen erstmals erschwingliche Geräte – und zwar sowohl in Form von Access Points als auch in Form von Netzwerkkarten – am Markt, fast gleichzeitig nahm die Verwendung von Notebooks zuerst vor allem unter den Studierenden stark zu.

Mit dieser Massenverbreitung nahm auch die Open Source Community an der Entwicklung von Tools im WLAN-Bereich teil und so dauerte es nicht lange, bis es frei verfügbare Programme (Network Device Scanner wie *Airsnort*, *Netstumbler*, *Wellenreiter* oder auch *Kismet*) gab, mit denen es praktisch jedem interessierten Laien möglich wurde, WEP-gesicherten Datenverkehr mitzuhören und auch zu entschlüsseln (Sikora, 2002, Krutak, 2003), wenn nur genügend Datenpakete mitgehört werden können (s.u.). Die Erhöhung der Länge des Schlüssels bringt außerdem bei einer symmetrischen Verschlüsselung im besten Fall einen linearen Zuwachs an Sicherheit.

Die Angriffstechniken, die dabei hauptsächlich zum Einsatz kommen, verwenden einerseits Brute-Force- und Wörterbuchangriffe, die prinzipiell gegen jedes System, das mit User Credentials (Benutzername/Passwort) arbeitet, eingesetzt werden können, andererseits nutzen sie aber auch Schwachstellen im Key-Generator, vor allem, wenn die Keys mittels einer Passphrase generiert werden, was die effektive Schlüssellänge deutlich reduziert, wodurch die Dauer eines erfolgreichen Brute-Force-Angriffs auf wenige Sekunden reduziert wird.

Weitere Angriffsszenarien wie z.B. Re-Injizierung verschlüsselter Pakete, die dann in diversen Tools zum Einsatz kommen, werden von Hofherr (2005, S. 78) beschrieben:

Tool	Betriebssystem	Funktion
Airsnort	*nix, Windows	Angriffe auf WEP-Schlüssel mit dem FMS-Angriff
dwepcrack	BSD, Linux	Angriffe auf WEP-Schlüssel mit dem Improved-FMS-Angriff
Aircrack	Linux, Windows	Angriffe auf WEP Schlüssel unter anderem mit statistischem KoreK-Angriff
WepLab	Linux, BSD, MacOSX	Angriffe auf WEP Schlüssel unter anderem mit statistischem KoreK-Angriff
WepAttack	Linux	Wörterbuchangriffe auf WEP Schlüssel
Aireplay	Linux	Reinjektionsangriff
WEPWedgie	*nix	Reinjektionsangriff

2 vgl. auch Kapitel 2.4.1 und 3.1

Auch die Kombination mit MAC-Filtern kann gegen diese Schwachstellen nicht helfen, da es viele Betriebssysteme gestatten, die MAC-Adresse der Netzwerkkarte frei zu setzen und damit MAC-Adressen einzutragen, die man als berechtigt erkannt hat (MAC address spoofing), außerdem ist die Verwaltung für eine grössere Anzahl von Clients mit vertretbarem Aufwand nicht möglich.

1.1.4 WPA

Nach dem Bekanntwerden der Schwächen von WEP wurde mit 802.11i zwar ein neuer Standard zur Authentifizierung in WLAN-Netz geschaffen, dieser Standard wurde aber erst sehr spät verabschiedet und es war klar, dass dieser Standard mit älterer Hardware nicht realisiert werden kann. Es waren daher schon früher Methoden gefragt, die einen höheren Grad an Sicherheit als WEP erlauben, ohne dass dafür unbedingt neue Hardware notwendig sein sollte. Die Wi-Fi Alliance beschloss deshalb, selbst eine Art Hersteller-Standard auf Grundlage von IEEE 802.11i zu schaffen und nannte diesen Standard »Wi-Fi Protected Access« (WPA), der auf neuerer Hardware später eine Migration nach IEEE 802.11i allein durch Firmware-Upgrades erlauben sollte.
WPA unterscheidet dabei zwischen einem Enterprise-Mode und einem eher wohl nur für SOHO-Benutzer gedachten PSK-Mode (»Pre-Shared Keys«). Im Enterprise-Mode ist WPA eine Kombination aus IEEE 802.1x[3], EAP, TKIP, MIC und RADIUS.
Leider ist WPA nicht für alle Betriebssysteme verfügbar (z.B. BSD) und daher vor allem für ältere Geräte nicht generell einsetzbar, außerdem schreibt Hofherr (2005, S. 133):
“WPA Enterprise (...) bietet uns zwar eine solide Absicherung, stellt uns aber vor die Qual der Wahl bei der Auswahl der Authentifizierungsmethode. Eine falsche Entscheidung an dieser Stelle kann die Sicherheit des gesamten Netzwerkes kompromittieren”.

1.1.5 IEEE 802.11i und WPA2

Wie bereits oben erwähnt, musste bzw. sollte bei der Entwicklung von WPA auf ältere Hardware Rücksicht genommen werden, da WPA ja in erster Linie WEP verbessern bzw. ersetzen sollte, ohne dass neue Hardware notwendig wird. Diese Einschränkung galt für IEEE 802.11i nicht: die Entwickler mussten keinerlei Rücksicht auf bestehende Lösungen nehmen, außer, dass AES verwendet werden sollte. Geräte, die diesen Standard erfüllen, werden von der Wi-Fi Alliance unter der Bezeichnung »WPA2« zertifiziert.
Durch die neuen Anforderungen ist ein Upgrade von WEP zu WPA2 i. A. nicht ohne entsprechenden Hardwaretausch möglich, ob und wie einfach eine Migration von WPA nach WPA2 erfolgen kann, hängt davon ab, wie sehr der jeweilige Hersteller bei der Konzipierung von WPA bereits an IEEE 802.11i gedacht hat.

3 siehe Kapitel 2.4.3

1.2 Implementierung an der TU Graz

Ende 2001 beschloss die Abteilung Kommunikation an der TU Graz dem Zug der Zeit zu folgen und ebenfalls ein WLAN einzurichten, wobei der Fokus auf frei zugängliche Bereiche wie z.B. Foyers gelegt wurde, Hörsäle wurden explizit ausgespart.
Eine Umfrage unter Studierenden ergab keine besondere Präferenzen und daher wurde beschlossen, in möglichst jedem Gebäudekomplex zumindest ein WLAN einzurichten.
Aufgrund der damaligen Verfügbarkeit und Verbreitung wurde vorerst IEEE 802.11b als bevorzugter Standard ausgewählt.
Nachdem zu diesem Zeitpunkt die Schwächen von WEP und MAC-Filtern bereits bekannt waren, wurde mit einigen Hotspotbetreibern und Herstellern von IEEE 802.11b-Netzwerkkomponenten Kontakt aufgenommen, um mehr über Sicherungsmöglichkeiten im WLAN zu erfahren, da wir schon im Virtuellen Campus Graz (»VCG«), dem Netz der Grazer Studierendenheime, die Erfahrung machen mussten, dass unsere Studierenden jede Schwäche auszunutzen versuchen.
Es zeigte sich, dass es noch keinen neuen verfügbaren Standard gab, nur einige proprietäre, nicht kompatible Lösungen. Da wir den Hersteller der Netzwerkkarte unseren Benutzern nicht vorschreiben wollten, mussten wir uns also um eine andere Lösung – wenn möglich nach einem Standard – umsehen.
Unsere Überlegungen waren daher, das WLAN als Netz mit »privaten« IP-Adressen nach RFC 1918 (Rekhter et al., 1996) aufzusetzen und dieses quasi externe Netz mit VPN-Technologie an das Datennetz der TU Graz (»TUGnet«) zu binden, was gleichzeitig die Möglichkeit eröffnete, auch anderen externen Netzen einen VPN-Zugang ins Datennetz der TU Graz zu ermöglichen. Diese Zugangsart birgt zwar die Gefahr, dass ein Benutzer im privaten Netz eine DoS-Attacke gegen einen Access Point starten kann, das wäre aber z.B. mit einem manipulierten oder defekten Mikrowellengerät auf OSI-Schicht 1 auch bei gesichertem Zugang jederzeit möglich, außerdem kann bei dieser Zugangsart natürlich das bekannte VPN-Gateway attackiert werden.

1.2.1 Ausschreibung

Aufgrund der geringen Ausstattung mit Personal und der noch fehlenden Erfahrungen wollten wir die Erstinstallation eines WLANs nicht selbst vornehmen, sondern diese Aufgabe ausschreiben.
Im Juni 2002 wurde somit das WLAN für insgesamt 13 Bereiche in 5 Gebäuden der TU Graz öffentlich ausgeschrieben (Kamrat et al., 2002).
Bei der Angebotseröffnung am 30. August 2002 lagen 6 Angebote mit einer Preisspanne von ca. EUR 11.500 bis EUR 46.000 vor, aufgrund des in der Ausschreibung festgelegten

Best- und nicht Billigstbieterprinzips bekam – nach entsprechender Auswertung der Angebote – die Fa. *Air Access Koller KEG* den Zuschlag.

1.2.2 Betrieb

Das WLAN an der TU Graz wurde bis Ende 2005 dann folgendermaßen umgesetzt und auch laufend erweitert:

- Freier Zugang ins »private« WLAN mit einer IP nach RFC 1918 (172.27.*)
- Erreichbarkeit des ACOnets über den HTTP-Proxy-Servers der TU Graz
- Erreichbarkeit des VPN-Gateways der TU Graz mit Benutzername/Passwort

Durch die Verwendung eines RADIUS-Servers mit Anbindung an die zentrale Benutzer-Datenbank im Informationsmanagementsystem der TU Graz (»TUGonline«), der auch die Verwaltung der Einwahlleitungen übernimmt, war der Aufwand der Einbindung relativ gering, die Verwaltung der Useraccounts in Bezug auf Authentifizierung, Autorisierung und Abrechnung (AAA) ist somit für alle Bereiche und nicht nur das WLAN zentral möglich.

Vorteil:
Wie bereits erwähnt wurde, konnten die Erfahrungen mit VPN auch für den generellen Zugang zum Datennetz der TU Graz genutzt werden.
Da für VPN derzeit keine Sicherheitsbedenken bestehen, kann also davon ausgegangen werden, dass der angemeldete Benutzer wirklich der Benutzer ist, der er laut Anmeldung sein sollte, ansonsten ist der Account als solcher kompromittiert und nicht die WLAN-Verbindung. Die Verfolgung von Fehlverhalten (Abuse) und konsequente Umsetzung und Überwachung der Betriebs- und Benutzungsordnung (Acceptable Use Policy) wird dadurch erleichtert.

Nachteil:
Jeder Benutzer muss den VPN-Client von *Cisco* (oder ein kompatibles Programm) installieren, dieser Client ist aber nicht für jede prinzipiell WLAN-taugliche Komponente verfügbar.

Mit Beginn 2006 wurde das VPN-Gateway aus Sicherheitsgründen und aufgrund von technischen Problemen mit den VPN-Konzentratoren von *Cisco*, die nicht direkt mit dem WLAN zu tun haben, hinter eine Firewall gestellt, was zumindest vorerst keine Auswirkungen auf unsere Installation haben sollte, aber in Hinblick auf das im weiteren betrachtete Roaming noch von Bedeutung sein könnte.

2 Roaming in Österreich

2.1 Begriffsklärung

Mit »Roaming« werden i. A. zwei unterschiedliche Technologien im zellenbasierten Funk (also z.B. GSM, UMTS, WLAN, ...) bezeichnet:

1. der für den Benutzer transparente Wechsel der Funkzelle (besser »Handover«)
2. die Nutzung der Teilnehmeridentität in einem fremden Netzwerk

In Zusammenhang mit WLAN versteht man dann unter »WLAN-Roaming« i. A. Handover, während »Wireless Roaming« die Nutzung der eigenen Zugangsdaten in einem besuchten Netz (Gastnetz, visited Network) bezeichnet.
In der vorliegenden Arbeit wird funktionierendes Handover (also WLAN-Roaming) als gegeben vorausgesetzt; wenn von Roaming gesprochen wird, ist immer Wireless Roaming, also die Nutzung der eigenen Benutzerkennung in einem »visited Network«, gemeint, auch dann, wenn in Zitaten von »WLAN-Roaming« gesprochen wird.

2.2 Historische Entwicklung

Während z.B. in Deutschland im DFN (Bormann et al., 2003, Pattloch und Paffrath, 2003 und Peter, 2003) und bei SWITCH in der Schweiz (Kienholz, 2002) schon ziemlich früh Ideen zum Aufbau einer Infrastruktur geboren wurden, die es erlauben sollten, die mit WLANs und Notebooks mögliche Mobilität voll zu nutzen, blieb es in Österreich lange Zeit nur bei vereinzelten Versuchen, bilaterale Kooperationen zwischen einzelnen Universitäten einzugehen. So gab es schon 2002 E-Mailverkehr zu diesem Thema zwischen dem Autor dieser Arbeit und dem Betreuer (Maschtera, 2002). Auch mit Vertretern anderer Universitäten in Österreich wurden schon 2002 Gedanken ausgetauscht. Es kam aber zu keinem Ergebnis.
Die ersten Gespräche des Autors mit Vertretern von ACOnet bzgl. einer Roaming-Infrastruktur – zumindest im akademischen Bereich Österreichs – fielen zeitlich mit den kommerziellen Plänen, *Greenspot* über die von der ISPA eingerichteten Internet Privatstiftung Austria (IPA) auch in Österreich anzubieten, zusammen (Wein, 2003, Telekom & IT Report, 2003). Da ACOnet an *Greenspot*, einer Clearingstelle für WLAN in Deutschland, gratis teilnehmen können sollte, um die Akzeptanz bzw. die Anzahl der Benutzer von Anfang an hoch zu halten, schien es keinen Bedarf an einer eigenen Lösung für ACOnet zu geben. Die Marktbereinigung im Sektor der österreichischen Hotspot-Betreiber hat aber leider dazu geführt, dass es in Österreich niemals zu einer laufenden Implementierung

von *Greenspot* kam.
Im Rahmen von diversen Sitzungen der Technischen Betriebs- und Planungsgruppe für ACOnet und der ARGE-Secur (der Arbeitsgemeinschaft der Sicherheitsbeauftragten) im ACOnet wurde die Idee einer Zusammenarbeit zumindest im akademischen Rahmen immer wieder diskutiert, konkrete Schritte wurden aber erst 2005 gesetzt.

2.3 Umfrage

In einem ersten Schritt sollte durch den Autor der vorliegenden Arbeit erhoben werden, welche Organisationen im ACOnet überhaupt auf nationaler oder auch auf internationaler Ebene Interesse an einer Teilnahme an einer derartigen (wireless) Roaminglösung haben und welche Technologien im ACOnet eingesetzt werden.

Eine erste informelle Aussendung bzw. Umfrage zu diesem Thema über die Mailinglisten der Technischen Betriebs- und Planungsgruppe und der oben genannten ARGE-Secur blieben so gut wie unbeantwortet, daher wurde dann der Weg eines Webformulars[4] gewählt.
Der Fragebogen wurde an ca. 100 Organisationen versandt, 22 davon, in der Hauptsache wie zu erwarten Universitäten, haben den Fragebogen auch ausgefüllt.
Bei diesen 22 Antworten waren 6 Antworten von Organisationen, die kein Interesse an einem Roaming haben und 16 Antworten, die zumindest an einer österreichischen Lösung Interesse haben und derzeit entweder schon ein WLAN einsetzen oder es für 2006 planen.

Bei den 6 Organisationen, die kein Interesse zeigen, sich aber trotzdem gemeldet haben, verwendet eine Organisation Web Redirect als Zugangslösung, eine andere hat bekannt gegeben, dass aufgrund zahlreicher Tests IEEE 802.1x auf keinen Fall in Frage komme. Soweit beantwortet, werden in keinem WLAN dieser Organisationen Gäste akzeptiert, daher verwenden einige Organisationen auch Kombinationen von MAC-Filtern, versteckten SSIDs und WEP.

Von den 16 Organisationen, die Interesse an einer Teilnahme bekundet haben, verwenden (oder planen) 6 eine VPN-Lösung und eine Organisation strebt eine solche Lösung an, obwohl derzeit Web Redirect verwendet wird.
Von den weiteren 5 Organisationen, die Web Redirect verwenden, plant eine in Richtung IEEE 802.1x, eine verwendet zusätzlich 802.1x, damit ergibt sich folgende Verwendung

4 siehe Anhang 8.1

in den Organisationen, die an Roaming teilnehmen möchten:

Zugangsart	derzeit	geplant
VPN	6	7
Web Redirect	6	4
IEEE 802.1x	5	6
	17	17

Wenn man vor allem die Planung betrachtet, dann zeigt es sich, dass die Nutzung von Web Redirect, das derzeit noch gleich stark wie andere Lösungen genutzt wird, zurückgehen wird, wobei sich aber anscheinend im ACOnet noch keine Präferenz für VPN oder IEEE 802.1x herauskristallisiert hat.

2.4 Beurteilung der einzelnen Lösungen im ACOnet

2.4.1 MAC-Filter, versteckte SSID und WEP

Auf allen gängigen Access Points sollte es möglich sein, Filter (ACLs) zu definieren, die nur Clients mit bestimmten MAC-Adressen, die natürlich zuvor zumeist händisch zu erfassen sind, zulassen.
Weiters sollte jeder Access Point anbieten, die SSID zu verstecken und einen WEP-Key mit zumindest 40 Bit zu vergeben.

Noch vor wenigen Jahren war man der Meinung, dass die Absicherung eines WLANs mit ACLs auf MAC-Adressenbasis zusammen mit versteckten SSIDs und WEP ausreichen müsste. Es wurden zwar sehr bald Sicherheitslücken bei WEP bekannt, doch dachte man zuerst, dass diese Lücken nur von einigen wenigen Spezialisten ausgenutzt werden könnten.
Allzu bald[5] waren aber Werkzeuge frei im Netz verfügbar, mit denen der gesamte Verkehr im WLAN mitgehört werden konnte und mit denen dann die WEP-Verschlüsselung auch ohne Fachkenntnisse sehr schnell geknackt werden konnte.

Die meisten Betriebssysteme, die im WLAN zum Einsatz kommen, erlauben es zusätzlich auch, die MAC-Adresse frei zu setzen und leider hat das inzwischen verbreitetste Betriebssystem (*Windows XP*), wie z.B. Wierenga (2004) schreibt, Probleme mit versteckten SSIDs.

5 vgl. auch Kapitel 1.1.3

Es gilt daher: Die Kombination aus MAC-Filter, versteckter SSID und WEP mag für den privaten Bereich noch ausreichen. Zur Verbindung mit Servern in der Firma oder der Universität sollten abgesicherte Protokolle wie SSH, IMAPS etc. verwendet werden. Für den Zugang zu einem Firmen- oder Universitätsnetzwerk, wo man keinen Einfluss auf den physischen Zugang zum Netz hat, reicht das aber heutzutage bei weitem nicht mehr aus. Vor allem aus Roaming-Sicht scheidet diese Methode daher aus!

2.4.2 Web Redirect

Bei »Web Redirect« (oder »webbased Access«) hat der Benutzer nur einen Browser zu starten und eine beliebige Seite im Internet aufzurufen.
Das Access Control Device (ACD) erkennt, dass dieser Rechner noch nicht berechtigt ist und leitet die Anfrage auf eine Authentifizierungsseite um, die SSL gesichert sein sollte.
Dort sind dann die User Credentials (i. A. Benutzername und Passwort) einzugeben; diese werden überprüft und falls die Berechtigung zum Netzzugang gegeben ist, dann wird das Access Control Device davon in Kenntnis gesetzt: die ACLs werden so umgeschrieben, dass die MAC-Adresse des Rechners freigeschaltet wird.

Vorteil:
Man kann davon ausgehen, dass heutzutage auf praktisch jedem mobilen Device ein Browser zur Verfügung steht, ein weiterer, spezieller Client ist nicht notwendig, der Zugang zum Netz ist daher sehr einfach und auch für absolute Laien möglich.

Nachteile:

- Die Umleitung auf eine Seite, die zur Bekanntgabe von Benutzername und Passwort auffordert, könnte auch von einem rogue Access Point vorgenommen werden
- Die Seite, auf die man umgeleitet wird, könnte kompromittiert sein
- Nach Beendigung der Session könnte die Session von einer anderen Person, die sich die MAC-Adresse angeeignet hat, übernommen werden
- Gäste bekommen eine IP aus dem Netz der besuchten Organisation, kennen dort i. A. die AUP nicht, die besuchte Organisation kennt den Besucher nicht

2.4.3 IEEE 802.1x

Mit 802.1x wurde vom IEEE ein neuer Standard zur Authentifizierung in Rechnernetzen in LANs (IEEE 802) definiert, der es erlauben soll, bereits vor dem Netzzugang – also am physikalischen oder logischen Port im LAN – zu überprüfen, ob Berechtigungen – und wenn ja – welche Berechtigungen für den Netzzugang bestehen.

IEEE 802.1x unterscheidet dabei zwischen dem

- »Supplicant«
  Anwender mit speziellem Client, der authentisiert werden will
- »Authenticator«
  Vermittler, der die Anfrage des Clients an einen Authentifizierungsserver weiterleitet
- »Authentication-Server«
  Die Stelle, die entscheidet, ob Zugang gewährt wird oder nicht

Die Authentifizierung erfolgt dabei logisch am sogenannten unkontrollierten Port, der im Zustand »geschlossen« nur Zugang zum Authenticator erlaubt. Ist die Authentifizierung erfolgreich, so wird der Client transparent an den kontrollierten Port übergeben und es wird ihm dort ein entsprechendes VLAN zugeteilt, über das er dann Zugriff auf die für ihn vorgesehenen Ressourcen erlangt.

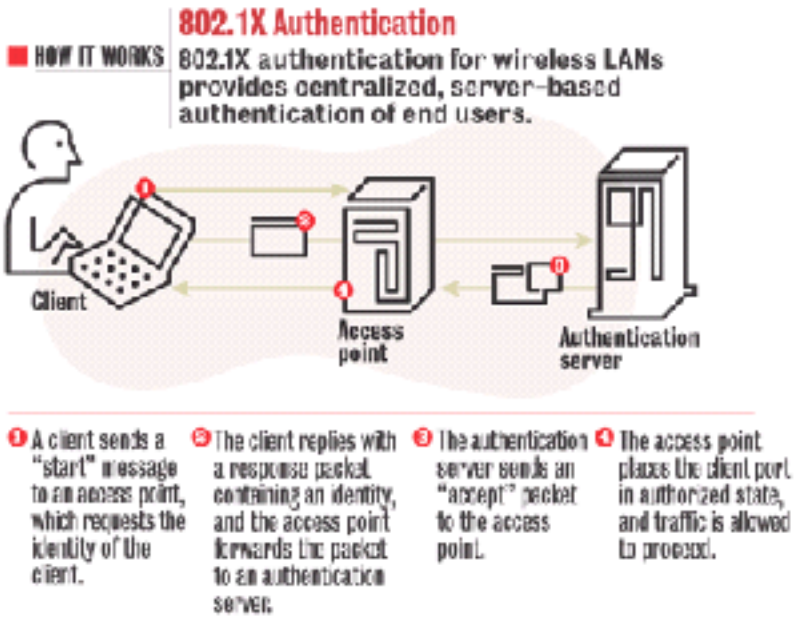

Abbildung 1: 802.1x-Authentifizierung

Der Client schickt dazu eine EAP-Multicast-Anfrage an eine Adresse, auf der alle 802.1x-kompatiblen Authenticatoren lauschen, danach tauschen – je nach EAP-Methode – der Client und der Server so lange Anfragen und Antworten aus, bis der Server entweder entscheidet, ob der Client zugelassen oder ob er abgewiesen wird.

Vorteile:

Clients für diesen Standard gibt es inzwischen in vielen Betriebssystemen, es werden aber auch laufend weitere, teilweise kommerzielle, also kostenpflichtige Clients (z.B. von *Funk*, *Meetinghouse*, *Open1X*, etc.) entwickelt.

Nachteile:

- Wenn für ein bestimmtes Betriebssystem kein Client verfügbar ist, dann ist – wenn keine andere Variante angeboten wird – auch kein Netzzugang möglich
- Gäste bekommen eine IP aus dem Netz der besuchten Organisation, kennen dort i. A. die AUP nicht, die besuchte Organisation kennt den Besucher nicht
- Nicht sicher:
  1. IEEE 802.1x sieht zwar vor, dass sich der Client am Access Point authentisiert, nicht aber, dass der Access Point im Gegenzug seine Identität nachweist, d.h. dass es durch das Einschleusen eines rogue Access Points möglich sein kann, eine Man-in-the-Middle-Attacke (MITM) zu starten, in der dem Client nur vorgegaukelt wird, sich beim echten Access Point anzumelden und damit die Accountdaten des Benutzers zu erlangen.
  2. Nach erfolgreicher Authentifizierung erfolgt keine Zuordnung einzelner Pakete zu einem bestimmten Device, eine Disassociate-Meldung an einen authentisierten Client und die Übernahme dessen Session (»Session Hijacking«) ist somit z.B. durch den Einsatz eines Hubs jederzeit möglich.

D.h.: ohne entsprechende Erweiterungen (z.B. EAP-TLS, CHAP oder LEAP) kann IEEE 802.1x nicht als sicher eingestuft werden, diese Erweiterungen sind aber zumindest teilweise proprietär und somit nicht generell verfügbar. Außerdem verlangen sie teilweise den Einsatz einer PKI:

Bei Verwendung z.B. von EAP-TLS ist die Sicherheit dann zwar als sehr hoch einzustufen, TLS verlangt aber sowohl Client- als auch Serverzertifikate und somit (vor allem, wenn es nicht nur für eine handvoll von Benutzern eingesetzt werden soll) zwingend eine (aufwändige) PKI, aber sogar dabei kann ein Angreifer die Identität des Benutzers ausspähen, was erst durch eine Kombination von EAP-PEAP (oder EAP-TTLS) mit EAP-TLS verhindert werden kann.

Einen Überblick über die verbreitetsten Methoden findet man bei Hofherr (2005, S. 94):

Methode	Authentifizierung	Dynam. Schlüssel	Sicherheit
EAP-MD5	Challenge-Response, nur Server	nein	sehr schlecht
EAP-TLS	Zertifikat, beidseitig	ja	sehr gut
EAP-TTLS EAP-PEAP	Server mit Zertifikat, Client durch andere Methode	ja	Abhängig von nachgelagerter Authentifizierung
LEAP	Challenge-Resonse	ja	mittel

Und er sagt dazu (a.a.O., S. 126): “Bei heterogenen Netzen sollte die Wahl auf EAP-TTLS fallen, da dieses nicht nur EAP-Methoden zur Authentifizierung unterstützt. Da-

mit hält man sich die Wahl einer beliebigen Authentifizierungsmethode offen und kann je nach Anforderung auch mehrere davon parallel einsetzen. An dieser Stelle ist es unmöglich, eine geeignete Methode zu empfehlen, da es bei heterogenen Netzen zu viele unterschiedliche Faktoren gibt, welche die Wahl beeinflussen."

Weiter ist es sehr wichtig zu erwähnen, dass 802.1x nichts mit der Verschlüsselung der Daten, also der Datenintegrität bzw. der Vertraulichkeit, zu tun hat – 802.1x ist für die Authentifizierung und nur für die Authentifizierung zuständig – was danach passiert, das hat mit 802.1x wenig zu tun, einzig eine WEP-Verschlüsselung mit dynamischen Schlüsseln erfolgt. Um nun aber ältere Systeme nicht auszuschließen, sollten nur Schlüssel mit einer Länge von maximal 64 Bit verwendet werden, was aber aus Sicherheitssicht kontraproduktiv ist.

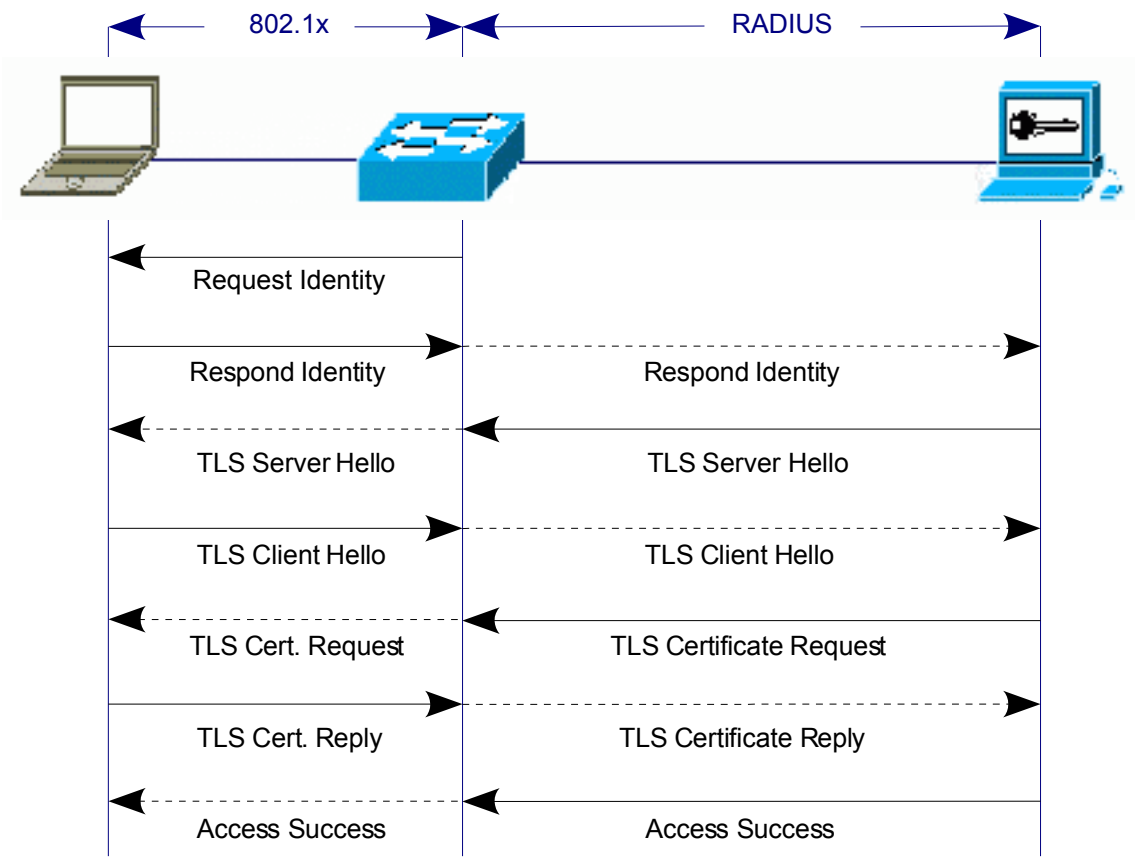

Abbildung 2: Schematischer Ablauf einer EAP-TLS-Authentifizierung

2.4.4 VPN

Bereits seit vielen Jahren werden in Firmen unterschiedliche VPNs eingesetzt, um z.B. Außenstellen mit einer Zentrale über das öffentliche Internet zu verbinden und damit Kosten für teure Standleitungen zu sparen oder um Mitarbeiter in fremden Netzen Zugang zu Ressourcen im eigenen Intranet zu geben.

Virtual Private Networks sind sowohl in Hard- als auch in Software realisierbar, die Technologie ist inzwischen ausgereift und gilt als extrem sicher und zuverlässig.
Eine VPN-Lösung hat heutzutage (wegen der Notwendigkeit des Zugriffs auf Intranetdienste) wahrscheinlich sowieso fast jede Universität im Einsatz; für den Fall, dass auch die Kosten eine Rolle spielen, kann inzwischen auf sehr gute Lösungen mit freier Software auf Standard-PCs zurückgegriffen werden.

Vorteile:

- Die Lösungen sind inzwischen ausgereift und sehr gut getestet
- Clients sind für viele Betriebssysteme, wenn auch nicht für alle, verfügbar
- Sobald man einen Netzzugang hat, hat man Zugang zum eigenen Intranet
- Man bekommt eine IP aus der eigenen Organisation, unterliegt somit i. A. nur der bekannten AUP der Heimatorganisation

Nachteile:

- Wenn man keinen Client für das eigene Betriebssystem findet, dann gibt es keinen Netzzugang, wenn nicht auch Alternativen zur Verfügung gestellt werden
- Da man eine IP aus dem Heimatnetz bekommt, stehen lokale Services der Gastorganisation, wie z.B. Drucker, nicht zur Verfügung
- Daten nehmen u.U. lange Umwege, da selbst lokale Ressourcen immer über das Gateway des Heimatnetzes geroutet werden

2.5 Zusammenfassung

Von den vier im ACOnet derzeit verwendeten und im vorigen Kapitel kurz vorgestellten Methoden scheidet die Variante nur mit WEP und MAC-ACLs sowie versteckter SSID im Zusammenhang mit Roaming aus Sicherheitsgründen sowieso aus, Hofherr (2005, S. 54) sagt dazu: “Die Menge an Schwachstellen zeigt, dass WEP auf ganzer Linie ungeeignet ist, drahtlose Netze wirksam zu schützen. Manche Hersteller haben versucht, einzelne Schwachpunkte von WEP mit proprietären Lösungen zu beseitigen (...), an dem fehlerhaften Design von WEP konnten sie allerdings nichts ändern.”
Für die drei restlichen betrachteten Varianten gilt im Zusammenhang mit Roaming:
Da bilaterale Beziehungen in großem Rahmen auf keinen Fall gut skalieren:

- jedesmal, wenn ein neuer Teilnehmer dazukommt, muss bei allen anderen Teilnehmern eingetragen werden, wo die Berechtigungen überprüft werden können
- Die ACLs oder Firewall-Rules würden bei jedem Teilnehmer linear mit der Anzahl der Teilnehmerorganisationen steigen

muss eine Infrastruktur geschaffen werden, die es erlaubt, die Berechtigung von Gästen zu überprüfen, es gilt also zu überlegen, wie eine solche Infrastruktur auszusehen hat.
Es galt außerdem zu überlegen, welche Punkte besonders wichtig erscheinen, was also die Kriterien sind, nach denen die Lösung ausgesucht werden sollte.
Zumindest in Phase 1 (noch vor der Umfrage) wurden diese Überlegungen in erster Linie von den Mitarbeitern der ARGE-Secur bzw. der CERTs einiger Universitäten bestimmt, was die Gewichtung eindeutig in Richtung auf Sicherheit und nicht in Richtung auf Bequemlichkeit legte.
Die Punkte (unterschieden nach **Muss-** und nach **Soll-**Kriterien):

- die Übertragung von Benutzername/Passwort **muss** so sicher wie möglich sein, da ja immer mehr Universitäten auf Single Sign On (SSO) oder zumindest »Single Credentials« (ein Passwort für alle/viele Dienste wie in TUGonline) setzen und ein kompromittierter Account u.U. Zugriff auf sehr viele Ressourcen ermöglicht
- die relevanten europäischen Rechtsvorschriften (z.B. Urheberrecht, Vorratsdatenhaltung) verschärfen sich zusehends, eine besuchte Organisation bzw. deren CERT **soll** aber nicht für Rechtsübertretungen von Besuchern einer anderen Organisation verantwortlich gemacht werden
- der Benutzer **soll** an der besuchten Universität die gleichen Zugangsprogramme verwenden können wie an der Heimatorganisation
- der Verwaltungsaufwand für die besuchte Organisation **soll** so gering wie möglich sein
- die Daten der Benutzer **sollen** sicher transportiert werden

Es hängt nun vom oben erwähnten Punkt “(...) eine besuchte Organisation **darf** aber nicht für Rechtsübertretungen von Besuchern (...) verantwortlich gemacht werden” ab, welche Lösungen überhaupt in Frage kommen:
Interpretiert man diesen Punkt als **Muss**-Kriterium, so ergibt sich zwingend, dass eine Lösung nur dann erreicht werden kann, wenn dem Benutzer eine IP aus dem Bereich seiner Heimatorganisation zugeteilt wird; das impliziert aber dann auch, dass als Lösung nur eine VPN-Variante in Frage kommt.
Mehrere Ideen zur Umsetzung einer VPN-Lösung wurden dazu im ACOnet diskutiert:

- Ein einziges (u.U. privates) VLAN im gesamten ACOnet.
  Dieses ist in Subnetzen den einzelnen Forschungseinrichtungen zugeteilt, in denen dann sowohl die mobilen Clients als auch die VPN-Server der einzelnen Roaming-Teilnehmern untergebracht sind.
  Vorteil: es wären sogar einfache Lösungen mit PPPoE möglich
  Nachteil: Verwaltung und Routing dieses Netzes nicht einfach

- Es wird zentral eine Liste der VPN-Gateways der teilnehmenden Organisationen gepflegt, über Firewall-Rules wird verhindert, dass die mobilen Clients andere Adressen als diese VPN-Server erreichen.

  Vorteil: Sehr sicher

  Nachteil: kein PPPoE möglich, da kein (V)LAN;
  funktioniert nur, wenn die Liste aktuell gehalten wird;
  Routing-Probleme, falls auch private Netze verwendet werden

Da einige Organisationen inzwischen aber bereits andere Lösungen für den Zugang per WLAN implementiert hatten, sollte überprüft werden, inwieweit sich die unterschiedlichen Varianten vertragen oder ob eine gemeinsame Lösung zu favorisieren ist.
Im Zuge der 31. Arbeitssitzung der Technischen Betriebs- und Planungsgruppe des ACOnets wurde am 2. Juni 2005 an der Donau-Universität Krems dann aber beschlossen, dass man gleich versuchen sollte, sich am europäischen Roaming »eduroam« zu orientieren und – wenn möglich – (auch) dort teilzunehmen.

3 Roaming im DACH-Bereich

Unsere Nachbarn in der Schweiz und in Deutschland betreiben schon länger nationale Roaming-Lösungen, die bei den Überlegungen in Kapitel 2 immer wieder eingeflossen sind. Mitarbeiter der NRENs beider Länder haben nicht unerheblich an der Entwicklung von »eduroam« mitgearbeitet und beide Länder nehmen inzwischen an »eduroam« teil.
Sowohl die nationalen Lösungen SWITCHmobile und DFNRoaming als auch die Art, wie die Teilnahme an »eduroam« umgesetzt ist, kann für ACOnet als Beispiel herangezogen werden, daher werden diese Lösungsansätze dieser beiden Nachbarn im Folgenden sehr detailliert und explizit behandelt.

3.1 SWITCHmobile (Schweiz)

In der Schweiz begannen sich Organisationen bereits 2001 Gedanken über mobilen Zugang zu Netzressourcen und hier natürlich auch zum WLAN zu machen, da schon zu diesem Zeitpunkt immer mehr Universitäten ihren Angehörigen anboten, sich entweder per Ethernet-Steckdose oder per WLAN (basierend auf IEEE 802.11b) ans Netz der Universität anzuschließen.
»SWITCHmobile«, ein Projekt von SWITCH, dem NREN der Schweiz, setzte sich zum Ziel, es den Angehörigen der teilnehmenden Organisationen zu ermöglichen,

1. das Internet zu nutzen
2. Zugriff auf IT-Services der Heimatorganisation zu bekommen
3. einige ausgewählte Dienste im besuchten Campus nutzen zu können.

An und für sich wären diese Ziele relativ einfach dadurch zu erreichen, dass man das »docking network«, das Zugangsnetz, einfach mit dem Backbone der SWITCH-Infrastruktur verbindet.
Es sind aber natürlich einige Einschränkungen zu berücksichtigen:
Einerseits wäre der gesamte Datenverkehr jederzeit anonym und unentdeckt – mit geeigneten Richtantennen sogar über größere Distanzen – abhörbar und dann mit entsprechender Software (wie z.B. *Ethereal* oder *tcpdump*) analysierbar, andererseits ist das in IEEE 802.11 (optional) vorgesehene Verschlüsselungsverfahren WEP mit Tools wie z.B. *Airsnort* in Netzwerken mit viel Datenverkehr sehr schnell zu knacken. Ein weiteres Problem ist, dass bei WEP mit PSK der geteilte Schlüssel von den Geräten an einem Access Point gemeinsam verwendet wird. Nun ist aber – wie Kienholz 2002 schreibt – ein Geheimnis, das tausende Nutzer kennen, kein Geheimnis mehr. Ähnliches gilt auch für versteckte SSIDs, die dann z.T. auf öffentlich zugänglichen Webseiten oder auf jedem zu-

gänglichen Aushängen bekannt gegeben werden.
Erweiterungen zu WEP waren zwar bereits verfügbar, aber untereinander inkompatibel und daher für eine verteilte Lösung unbrauchbar[6].
Ein weiteres Problem, das identifiziert wurde, ist der leider allgegenwertige bewusste oder unbewusste Missbrauch der Datennetzinfrastruktur bzw. generell Verstöße gegen die Betriebs- und Benutzungsordnung (Acceptable Use Policy, AUP), wie z.B. das Versenden von Spam-E-Mails, die Teilnahme an verteilten DoS-Attacken (DDoS) oder sogar strafrechtlich relevante Vorfälle, wie z.B. rufschädigende E-Mails, Datendiebstahl, etc.
Es ist in einem solchen Fall unbedingt notwendig, den Ursacher eindeutig identifizieren zu können und nicht nur das IP-Netz einer Universität zu erkennen. Diese eindeutige Zuordnung ist durch MAC-Adressen nicht möglich, da diese in vielen Betriebssystemen beliebig eingetragen und jederzeit verändert werden können.
Aufgrund dieser Beschränkungen war klar, dass eine Zugangsbeschränkung, bei der Benutzerdaten nur per WEP, MAC-Filter und versteckter SSID geschützt sind, nicht in Frage kommt, man diskutierte daher andere Lösungen und entschied sich 2002 für eine Lösung mit VPN, die jedem Gast eine IP aus seinem Heimatnetz zuweist, den gesamten Datenverkehr zwischen den beiden Endpunkten des VPN-Tunnels sicher verschlüsselt und automatisch mit den Benutzerdaten der Heimatorganisation arbeitet, ohne dass diese anderen Organisationen anvertraut werden muss. Ein weiterer Vorteil der IP der Heimatorganisation ist, dass man dabei natürlich weitgehend der (bekannten) AUP und nicht einer (wahrscheinlich) unbekannten Benutzungsordnung unterliegt.

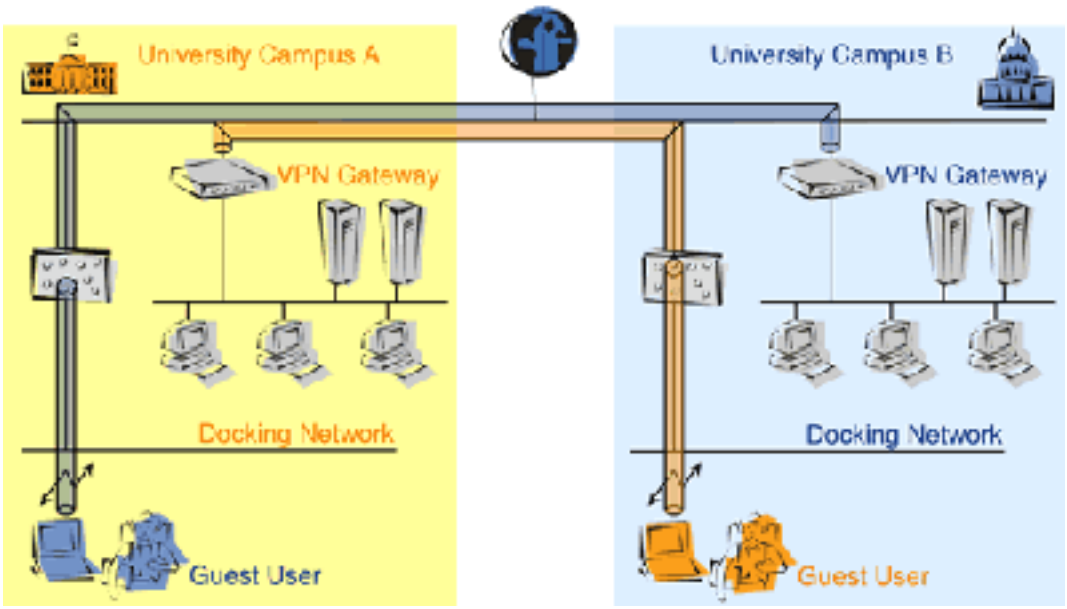

Abbildung 3: Roaming mit VPN

6 vgl. dazu auch Kapitel 1.1.3 und 2.4.1

Ein Angehöriger der Organisation A, der gerade Universität B besucht, bleibt logisch im Netz der Universität A, während ein Angehöriger der Universität B, der z.B. gleichzeitig die Universität A besucht, logisch in seinem Heimatnetz, also B, bleibt.
Problem Nr. 3 – ausgewählte Dienste auch lokal zur Verfügung zu stellen – kann mit VPN aber nicht gelöst werden, da man logisch ja gar nicht lokal vor Ort ist.
Ein weiteres Problem ist, dass für VPN i. A. die Installation eines speziellen Clients – der allerdings unabhängig vom Gastnetz ist: er muss nur mit dem VPN-Gateway im Heimatnetzwerk abgestimmt sein – notwendig ist, was für Laien u.U. nicht einfach oder vielleicht sogar untersagt ist. Daher wurde z.B. an der Universität Lausanne, wie Al-Atassi (2004) beschreibt, für die eigenen Benutzer eine einfachere Methode entwickelt und zwar wahlweise über Web Redirect oder clientless VPN (eine Art ASP über HTTPS) Zugang zu Ressourcen zu bekommen.
Die Angehörigen der (damals) 13 anderen Teilnehmer an SWITCHmobile müssen aber VPN verwenden und können auch nur einen jener Endpunkte erreichen, die in einer von SWITCH gewarteten Liste stehen.

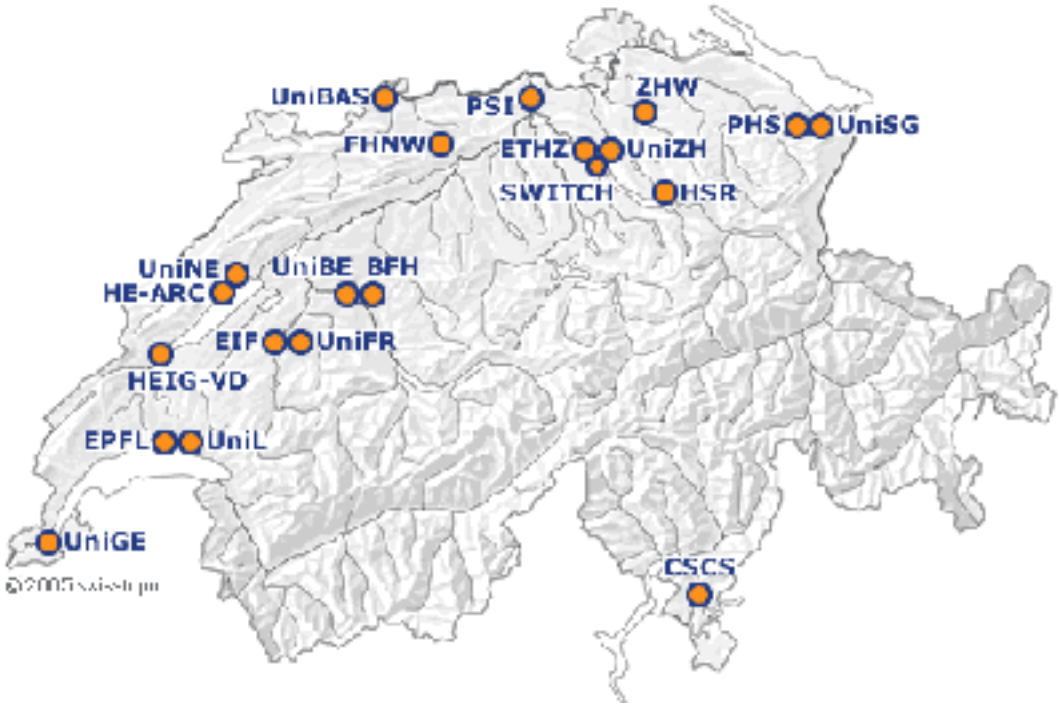

Abbildung 4: Roamingstandorte in der Schweiz, 14. Jänner 2006

Im Rahmen eines Pilotprojektes, das im Juli 2005 gestartet wurde, ist SWITCHmobile (inzwischen auf 20 Teilnehmer angewachsen) – ähnlich, wie es mit *Greenspot* in Österreich geplant war[7] – nun auch von ca. 700 Hotspots von 3 führenden WISPs der Schweiz aus erreichbar.

7 vgl. Kapitel 2.2

Born (2005a, S. 22) sagt dazu: “Ziel unserer e-Academia ist es, unseren Kunden laufend weitere Roamingnetzwerke zur Verfügung zu stellen, von denen aus sie sich bei ihrer Heimorganisation einwählen können. Mit dem Versuchsbetrieb erreichen wir genau das. (...) Wir suchten nach einer Möglichkeit, verschiedene Netze kostenneutral miteinander zu koppeln. Unsere Partner haben sich bereit erklärt, ihre Netze während der Versuchsphase von den Hochschulen zum Nulltarif mitbenutzen zu lassen. Im Gegenzug stellen die Hochschulen symmetrisch deren Netze für die Kunden der Partner zur Verfügung. Das Resultat ist eine klassische Win-Win-Situation, jeder profitiert von jedem.”
Und er erläutert weiter (a.a.O., S. 23): “Das System sollte in der Benutzung völlig transparent zu SWITCHmobile sein. Das war eines der wichtigsten Designziele. Das bedeutet, dass das Vorgehen beim Einwählen mit dem bestehenden Dienst von SWITCHmobile identisch ist.”
Ein Anfrage bezüglich einer ähnlichen Zusammenarbeit in Österreich bei den Betreibern *aon*, *ONE* und *T-Mobile* brachte zumindest vorläufig leider kein Ergebnis: *aon* hat derzeit Hotspots nur in wenigen Orten und “*ONE* setzt”, wie Schmidt (2005) schreibt, “in Zukunft auf UMTS bzw. Nachfolgetechnologien im Bereich Mobiles Breitband. In Richtung WLAN ist kein weiterer Ausbau geplant.” Von *T-Mobile* ist eine Antwort noch ausständig.

3.2 DFNRoaming (Deutschland)

Auch im Deutschen Forschungsnetz (»DFN«) wurde bereits sehr früh intensiv über Lösungen nachgedacht, wie Angehörige der Forschungseinrichtungen Zugriff zu ihren Daten im Intranet erhalten könnten. So schreibt schon Kahler (2001, S. 4): “Wissenschaftler, die sich von zu Hause aus ins Hochschulnetz einwählen, haben in Ermangelung interner IP-Adressen auf eine Vielzahl von Angeboten keinen Zugriff und sind unter Umständen selbst von den Ergebnissen ihrer eigenen Arbeit abgeschnitten. Regelmäßig Probleme bereiten die Zugriffsbeschränkungen auch dort, wo es um die Nutzung von Campus-Software oder den erweiterten Zugriff auf Bibliotheken oder interne Datenbanken geht. (...) Um den Mitarbeitern wissenschaftlicher Einrichtungen und Studenten ihre tägliche Arbeit zu erleichtern, aber ebenso auch um Lehrern und Professoren die Möglichkeit zur effektiveren Nutzung des Mediums Internet zu geben, hat sich der Verein zur Förderung eines Deutschen Forschungsnetzes e.V. zum Ziel gesetzt, flächendeckend eine Einwahl ins Internet bereitzustellen, mit der die Nutzer einen gesicherten und kostengünstigen Zugang auch zu den internen Rechnernetzen ihrer Hochschulen und Wissenschaftseinrichtungen haben. Für jede der teilnehmenden Hochschulen wird hierbei ein Virtual Private Network aufgebaut, in das sich die Studierenden und Mitarbeiter der Hochschulen von jedem beliebigen Ort in Deutschland aus in das Intranet ihrer Hoch-

schule einwählen können. (...) Die Vergabe der IP-Adressen erfolgt bei DFN@home auf Basis eines Virtual Private Networks (VPN). Durch eine Kombination verschiedener Komponenten der Netzeinwahl wird das physische Hochschulnetz virtuell bis zu den privaten Rechnern der Nutzer ausgeweitet. (...) Technisch wird hierbei das das (sic!) L2TP Protokoll (sic!) (...) verwendet. (...) Charakteristisch für DFN@home ist, dass die Authentifizierung der Nutzer aufgrund der Regeln der angewählte Wissenschaftseinrichtung erfolgt. Die Überprüfung der Zugriffsrechte der Benutzer erfolgt nach einer Vor-Authentifizierung mit Hilfe hochschuleigener Daten. Dadurch lassen sich die Rechte jedes Anwenders spezifisch festlegen. Durch die Kombination Tunnel und Authentifizierung ist es bei einem Maximum an individueller Sicherheit möglich".

Zu diesem Zeitpunkt wird also bereits auf VPN über Einwahlleitungen als gemeinsame Zugangsinfrastruktur gesetzt, Nestvogel und Hoelzner (2002) erwähnen in ihrem Artikel, dass der DFN-Verein sogar an ein internationales Roaming für DFN@home denkt.

Auch Ullmann (2001, S. 6) beschreibt den »nomadischen User«, als "reisender Wissenschaftler mit Zugriffswunsch auf seine gewohnte Arbeitsumgebung über das Netz der Gasteinrichtung" und er definiert: "Eine erste Aufgabenstellung für den DFN-Verein und seine Anwender ist der Aufbau einer „Roaming" - Infrastruktur. Mit dieser Infrastruktur soll erreicht werden, daß (sic!) man von einer beliebigen Wissenschaftseinrichtung im DFN Bereich durch Zugriff über das dortige lokale Netz (...) auf seine Arbeitsbasis sowie auf öffentlich verfügbare Dienste wie z.B. Druckserver der gastgebenden Einrichtung zugreifen kann. (...) Eine Realisierungsoption wäre über eine einheitlich organisierte Radiusstruktur denkbar."

Den Begriff des »reisenden Wissenschaftlers« verwendet auch Paffrath (2002, S. 12) und er schreibt, dass er "von Orten außerhalb seines Heimat-LANs in der Regel keinen Zugriff auf die internen Ressourcen" hat und dass spätestens für diesen Benutzer ein Dienst notwendig wird, "den man im Allgemeinen als „Roaming" bezeichnet".

Er hält fest, dass die immer höheren Sicherheitsanforderungen neue Probleme für die Benutzer produzieren – so erwähnt er beispielsweise, dass das Versenden von E-Mails i. A. ohne ein ständiges Anpassen der Einstellungen im E-Mail-Client nicht möglich ist. Weiter sagt er (a.a.O.): "Die Mechanismen der Datenübertragung über das Internet bieten zahlreiche Möglichkeiten, Informationen im Rahmen eines Roaming-Dienstes sicher über das Netz zu übertragen. (...) Wichtig ist hierbei, dass diese Dienste eine End-zu-End Sicherheit gewährleisten müssen, wobei dies für den Anwender transparent sein muss."

Als eine Variante einer solchen sicheren Datenübertragung schlägt er IPSEC vor und schreibt (a.a.O., S. 13): "Besonderer Vorteil des IPSEC ist es, dass es die Sicherheit der Daten auf der Netzwerkschicht weit unterhalb der Anwendungsschicht garantiert, so dass keine Sicherheitsmechanismen zum Schutz der übertragenen Daten explizit in die IP-An-

wendungen integriert werden müssen. (...) Auf lange Sicht ist der Einsatz von IPSEC für die Realisierung eines sicheren Roamings eine geeignete Lösung, da dieser Ansatz umfassend ist."

Als zweite Variante untersucht er SSH-2, also ein Produkt, das im Gegensatz zu IPsec nicht sehr tief im OSI-Referenzmodell angesiedelt ist, sondern – ganz im Gegenteil – auf höchster Ebene, der Anwendungsschicht, ansetzt. Der große Vorteil von SSH ist seine weite Verbreitung und die einfache Installation. Paffrath plädiert daher für die Verwendung von SSH (in der sicheren Version 2) mit Public-Keys, weil hier unsichere Protokolle (wie z.B. POP3) wirksam und einfach abgesichert werden können. Auf die Probleme einer entsprechenden Infrastruktur (Wie erlange ich Netzzugang?) geht er hier noch nicht ein.

In einem weiteren Artikel (Pattloch & Paffrath, 2003, S. 4) ergänzt er aber: "In diesem Bild fehlte bislang noch das Puzzleteil, wie das Wissenschaftsnetz unterwegs schnell, unkompliziert und frei von laufenden Entgelten erreicht werden kann. (...) Grundlegendes Konzept für DFNRoaming ist ein verteiltes Authentifizierungssystem. Um als Nutzer von DFN-Roaming registriert zu sein, genügt es, sich genau einmal in seiner eigenen Einrichtung eine Kennung zu beschaffen.(...) Technologisch wird DFNRoaming als verteilte Struktur von RADIUS-Servern realisiert. Als Protokoll kommt das international standardisierte Protokoll IEEE 820.1X zum Einsatz."

Peter (2003, S. 3) sagt ergänzend: "In den letzten Jahren wurde an nahezu jeder Hochschule ein flächendeckender W-LAN Dienst aufgebaut. Zugangsberechtigt sind im Regelfall alle Hochschulangehörigen. (...) Die sicherheitstechnischen Verfahren, mit denen unberechtigte Nutzer von einem Zugriff abgehalten werden, sind bekannt und werden wohl überwiegend eingesetzt. (...) Angehörige von Mitgliedseinrichtungen des DFN bekommen über W-LAN Zugang zum Netz der Fremdhochschule und werden zu ihrer eigenen Hochschule durchvermittelt. Technisch ist dies kein Problem, sofern sich die Hochschulen auf ein gemeisames (sic!) Zugangsverfahren einigen. Vorschläge hierzu werden vom DFN erarbeitet und allen Mitgliedshochschulen angeboten."

Die weitere Entwicklung von DFNRoaming beschreibt Paffrath (2004, S10) dann folgendermaßen: "Die Liste der DFNRoaming Standorte vom Oktober 2004 zeigt ein eher bescheidenes Zwischenergebnis im DFNRoaming, denn von den ca. 600 DFN Mitgliedseinrichtungen sind bisher 7 Einrichtungen, die konkret einen 802.1X bzw. einen webbasierten Zugang anbieten, aufgeführt" und er gibt u.a. als Gründe für die zögernde Annahme verschärfte Sicherheitskonzepte und Befürchtung von rechtlichen Konsequenzen im Fall eines Missbrauchs an. Als Migrationslösung (z.B. für ältere, nicht IEEE 802.1x-kompatible Hardware) wurde in der halbjährigen Pilotphase von DFNRoaming auch eine SSL abgesicherte webbasierte Zugangskontrolle entwickelt, die aber diese Gründe na-

türlich erst recht nicht entschärft. Er schreibt dort auch: “Hingegen nicht zu empfehlen, (sic!) ist bei Verdacht eines Missbrauchs, selbst tätig zu werden”, was aber aus Sicht einer u.U. notwendigen sofortigen Reaktion eigentlich unmöglich umzusetzen ist.
Um den Aufbau und die Installation DFNRoaming-Infrastruktur zu vereinfachen, entwickelt der DFN-Verein ein eigenes KNOPPIX ISO-Image, das sowohl die 802.1x- als auch die webbasierte Lösung beinhaltet und das unter GPL frei verfügbar ist. Mitte 2005 (Wissenschaftsnetz in Zahlen) beteiligen sich dann 15 Einrichtungen mit insgesamt ca. 450 Access Points an DFNRoaming.
Ein Jahr später ergänzt er (Paffrath, 2005, S. 24): “Im Rahmen von DFNRoaming bekommt jedoch der Anwender in der Regel nach erfolgreicher Authentifizierung eine IP-Adresse aus dem Gast-Netz, in dem er sich befindet”, wodurch der Zugriff z.B. auf lizenzpflichtige Software oder Dienste versagt bleibt. Als Lösung für dieses Problem schlägt er dann wieder VPN, inzwischen aber nicht mehr SSH-2 sondern auf Basis von *OpenVPN*, vor. *OpenVPN* baut unter Verwendung von statischen Schlüsseln oder Zertifikaten einen SSL-verschlüsselten Tunnel über einen einzigen Port auf und für *Windows*-Benutzer gibt es (nicht unwichtig) natürlich ein grafisches Front-End, ein GUI.
Explizit weist er darauf hin, dass der VPN-Server extra gehärtet werden muss, was für VPN-Gateways, die ja den Zugangspunkt zum Intranet bilden, generell der Fall sein sollte – egal, ob das nun ein spezieller Zugangspunkt nur für Roaming oder generell für VPN-Dienste aus dem Internet sein soll. Es gibt es dann auch wenig Grund diese Infrastruktur zu verdoppeln: hier ist immer mit höchster Sicherheitsstufe zu arbeiten! Falls also wie von Paffrath vorgeschlagen sogar eine softwarebasierte Lösung zur Anwendung kommen soll, dann ist auch das Betriebssystem des Servers zu härten, d.h. bis auf SSH und *OpenVPN* sollten alle Dienste deaktiviert sein. Zur einfachen Nutzung vor allem für *Windows*-Benutzer schlägt er zusätzlich vor, dass mit geeigneter Software vorkonfigurierte, selbstinstallierende Pakete vorbereitet werden.

3.3 Zusammenfassung

Sowohl in der Schweiz als auch in Deutschland gab es bereits gut funktionierende Lösungen vor »eduroam«. Diese Lösungen werden auch nach wie vor eingesetzt und man sollte daher auch im ACOnet darüber nachdenken, ob es – unabhängig von »eduroam« – eine nationale Lösung geben soll, die auch von ACOnet-Teilnehmern genutzt werden kann, die nicht (voll) an »eduroam« teilnehmen wollen oder können.
Nach Meinung des Autors sollte zumindest ein CASG installiert werden (was ja auch den Überlegungen in Kapitel 2.5 entspricht) – egal, ob dieser dann mit den CASGs anderer NRENs verschaltet wird oder nicht.

4 Die Entwicklung von »eduroam«

Bereits 2002 machte Maschtera, der Betreuer dieser Arbeit, die Mitglieder der Technischen Betriebs- und Planungsgruppe für ACOnet (TBPG) – aufgrund von ersten Diskussionen zur Installation von WLANs an einzelnen Universitäten in Österreich – auf eine Initiative von TERENA aufmerksam, in der es darum ging, eine Infrastruktur für Wireless Roaming im europäischen Forschungsbereich zu installieren.
Zum damaligen Zeitpunkt ging es den meisten Universitäten in Österreich aber darum, erst einmal ein funktionierendes WLAN lokal aufzubauen, trotzdem wurde immer wieder (auch auf Initiative des Autors) über Roaming zumindest innerhalb von ACOnet diskutiert.
Wie am Ende von Kapitel 2.5 erwähnt, wurde im Juni 2005 beschlossen, dass ACOnet an »eduroam« teilnehmen sollte und es sollte erhoben werden, unter welchen Bedingungen das erfolgen kann.
Neben der in Kapitel 2.3 bereits behandelten Umfrage sollte ein Papier erstellt werden, das den aktuellen Stand von »eduroam« den Mitgliedern der TBPG und den Mitgliedern der ARGEsecur im ACOnet näher bringen sollte. Diese Aufgabe war eine der Ursachen für die Entstehung der vorliegenden Arbeit.
Grundlage von »eduroam« ist die Idee, die Grenzen, die der Mobilität der Forscher und Studierenden im europäischen Raum durch Zugangsbeschränkungen gesetzt sind, soweit wie möglich aufzuheben. Bormann et al. (2003) schreiben dazu (S. 12): “Allerdings ist die alleinige Existenz von WLANs in vielen Hochschulen nicht ausreichend, um ortsunabhängig Konnektivität (sogenanntes Roaming) bereitstellen zu können. Die Nutzung eines fremden WLAN wird z.B. explizite administrative Schritte erfordern, die nicht adhoc (sic!) erreichbar sind. Dies ist besonders nachteilig bei benachbarten Hochschulen und Forschungseinrichtungen, zwischen denen Mitarbeiter und Studierende täglich pendeln können sollen, ohne daß (sic!) hierdurch der durchgängige Netzzugang meist zum jeweiligen WLAN erschwert wird, aber auch bei Arbeitstreffen, Konferenzen und Gastaufenthalten störend. Internet-Konnektivität (Netzzugang) (...) ist daher nur durch Zusatzvorkehrungen zu erlangen, die einrichtungsübergreifend organisiert werden müssen. Es bedarf also einer technischen Lösung, die ein weitgehend transparentes Roaming zwischen all jenen Einrichtungen ermöglicht, die ihren Nutzern ohne individuelle vorherige Anmeldung gegenseitig Zugang zum jeweiligen WLAN gestatten wollen.”

Um diese Lösung zu schaffen bzw. aus den bestehenden Lösungen eine allgemein verwendbare Infrastruktur auszuwählen, wurde im Rahmen von TERENA die Task Force »Mobility Group« gegründet, die die Grundlage für »eduroam« schaffen sollte.
Die Task Force behandelte in mehreren »Deliverables« die einzelnen Facetten, die zu

beachten sind:

- Deliverable A war für den Aufbau eines Informationssystems mit relevanten Links für WLAN und Roaming zuständig
- Deliverable B erstellt ein Glossar der technischen und nicht technischen Begriffe im Bereich Mobilität, Roaming, Authentifizierung und Autorisierung, das teilweise in das Kapitel 6 dieser Arbeit eingeflossen ist
- Deliverable C definiert die Anforderungen für eine internationale Roaminglösung
- Deliverable D beschreibt 802.1x-basierte Lösungen,
- Deliverable E Lösungen auf VPN-Basis

und

- Deliverable F widmet sich den webbasierten Varianten

schließlich befasst sich dann Deliverable G mit der vorläufigen Auswahl einer Lösung und Deliverable H mit Testumgebungen und Referenzinstallationen.
In Deliverable I wird eine Policy vorgestellt und schlussendlich wird auch noch ein Abschlussbericht erstellt.
Da die Arbeit dieser TF in Österreich noch immer weitgehend unbekannt zu sein scheint, soll hier eine Zusammenfassung der einzelnen Deliverables einen Überblick erlauben, der auch im Hinblick auf die Errichtung einer Roaming-Infrastruktur in Österreich von Bedeutung sein könnte.

4.1 Deliverable C: Die Anforderungen

Rauschenbach et al. (2003) beschreiben in der Einleitung zu Deliverable C nochmals die Motivation zum Entstehen der Task Force, im Detail schreiben sie:
“This all makes it necessary to implement security measures to avoid abuse by unauthorised users. The measures taken by academic institutions differ significantly, sometimes even between different departments of the same institution. Because of this, there can be incompatibility and scalability issues at the institutional level, let alone at the national level or beyond. These problems have encouraged NRENs to look at developing a more generalised approach to solve these problems and work towards the creation of an architecture for roaming between WLANs, in particular between organisations on a national or European level, to support the travelling scientist/teacher in a nomadic computing scenario.”
Im weiteren definieren sie die Anforderungen, die eine Lösung für eine »Notebook University« erfüllen soll, wobei sie klar zwischen Anforderungen, die erfüllt sein **müssen**, und solchen, die erfüllt sein **sollen**, unterscheiden:

Die möglichen Lösungen **müssen** nach ihnen folgenden Hauptanforderungen genügen:

- Der **Verwaltungsaufwand** muss minimal sein
- Die **Skalierbarkeit** muss sehr gut sein
- Die **Sicherheitsanforderungen** müssen erfüllt werden.

Weiters **soll** folgenden Punkten Aufmerksamkeit geschenkt werden:

- Gute **Benutzbarkeit** für alle verwendeten Plattformen
- **Accounting und Logging:** für den Fall eines Missbrauchs muss eine Rückverfolgung möglich sein

und falls aus irgendeinem Grund eine bestimmte Lösung nicht eingesetzt werden kann, dann ist ein »trade-off« vorzusehen.

4.1.1 Verwaltungsaufwand

Obwohl es – wie die Autoren schreiben – nicht zu den Aufgaben der Task Force gehören kann, etwas zum Ablauf der lokalen Verwaltung zu sagen, ist es aber das erste Ziel überhaupt, den Aufwand je Benutzer zu minimieren, so schreiben die Autoren sogar: “However any extra administrative effort that occurs at the visited institution per roaming occurrence is unacceptable – the chilling effect on inter-NREN roaming would be too great.” (a.a.O., S. 3)

4.1.2 Skalierbarkeit

Sie vertreten weiter die Meinung, dass Roaming-Benutzer – soweit es möglich ist – die existierende Infrastruktur nutzen sollten, dass die Lösung also ohne spezielle Access Control Devices für »eduroam« funktionieren soll. Falls jedoch zusätzliche Systeme notwendig sein sollten, dann muss die Komplexität dieser minimiert werden, außerdem ist auf jeden Fall zu berücksichtigen, dass die Lösung zumindest auch auf europäischer Ebene skalieren muss, was impliziert, dass keine bilateralen Lösungen (mit n^2 Einträgen) in Frage kommen.

4.1.3 Sicherheitsanforderungen

Die offensichtliche Sicherheitsanforderung ist, dass natürlich nur autorisierte Benutzer Zugang zum Roaming erhalten. Diese Benutzer erwarten dann, dass ihre Kommunikation geschützt wird und dass ihre Daten weder manipuliert, noch ihre Sitzung übernommen werden kann.

Auch die besuchte Organisation wird – z.B. im Falle von Missbrauch – durchaus weitere Anforderungen haben, so sollte sie im Idealfall gar nicht tangiert werden, was eigentlich nur durch VPN-Lösungen zugesichert werden kann, zumindest sind aber ihre Sicherheitsanforderungen zu erfüllen.

Auf der anderen Seite steht die Forderung, dass durch die zusätzlich involvierten Elemente im Ablauf des Netzwerkzugriffs Geschwindigkeit und Betriebssicherheit nicht oder nur wenig beeinflusst werden sollen, was wieder durch VPN-Lösungen nicht garantiert werden kann, da hier die Kommunikation zwischen Quelle und Ziel über den VPN-Server im Heimatnetzwerk läuft, was zusätzlichen Verkehr und Umwege verursacht.
Zum Teil werden diese Anforderungen also diametral sein:
Steht Sicherheit im Vordergrund, dann werden Betriebsbeschränkungen wahrscheinlich unvermeidbar sein. Steht einfacher Zugang und Geschwindigkeit im Vordergrund, dann wird bei Problemen wohl auch die Gastorganisation betroffen sein.
Egal welche Technik eingesetzt wird, sie darf nicht verhindern, dass der Besucher selbst Sicherheitstechniken wie IPsec oder generell VPN einsetzen kann, die ihm ein höheres Sicherheitsniveau gewährleisten – NAT und PAT können dabei Probleme verursachen.
Erwähnt wird auch, dass es sinnlos ist, sich über den Schutz des WLANs an sich Gedanken zu machen, da der von IEEE 802.11 verwendete Frequenzbereich auf gar keinen Fall wirksam geschützt werden kann.

4.1.4 Benutzbarkeit

Eine der Hauptforderungen für »eduroam« ist, dass es für den Großteil der derzeitigen Benutzer in WLANs und auch für drahtgebundene Kommunikation der teilnehmenden NRENs funktionieren soll, was bedeutet, dass also eine proprietäre Lösung nicht in Frage kommt, sondern dass die Lösung auf Standards basieren muss.
Wenn möglich, sollte die Lösung auch Geräte wie PDAs und Smartphones unterstützen und den Zugang zu lokalen Ressourcen (wie Druckern etc.) erlauben.

4.1.5 Accounting und Logging

Obwohl die Lösung auf jeden Fall so sicher wie möglich auszufallen hat, sodass ein Missbrauch der Einrichtung schwer gemacht wird, kann ein Missbrauch nicht mit absoluter Sicherheit ausgeschlossen werden. Es ist daher ein möglichst einfach einsetzbares Accounting-System zu installieren, welches es im Fall eines Missbrauchs leicht macht, die notwendigen Daten zu analysieren und den Missbrauch zu verfolgen.
Was ein Missbrauch ist, ist schwer zu definieren, da es hier keine Standards gibt und die einzelnen Universitäten i.d.R. ihre eigenen Betriebs- und Benutzungsordnungen erlassen. Weiters sind auch Unterschiede in nationalen und europäischen Gesetzen bzw. deren Umsetzung zu berücksichtigen.
Den Autoren des Deliverables erscheint es wünschenswert, einen Katalog von zu verfolgenden Vorfällen zu definieren; in allen – nach diesem Katalog – beachtenswerten Fällen sollten jedenfalls auch die CERTs der beteiligten NRENs verständigt werden.

4.2 Deliverable D: IEEE 802.1x

In einem Netz (LAN oder WLAN), das mit IEEE 802.1x arbeitet, muss ein Benutzer zuerst einige Aktionen setzen, bevor er am Netzwerk teilnehmen kann, er muss ...

1. zuerst einmal entweder ein Betriebssystem installieren, das von Haus aus 802.1x unterstützt, oder eine Software nachinstallieren, die das Betriebssystem um diese Funktionalität erweitert.
2. dafür sorgen, dass für ihn ein Account mit den geeigneten Berechtigungen eingerichtet wird, auf den der zuständige RADIUS-Server Zugriff hat
3. sein Endgerät auf DHCP konfigurieren
4. sich mit seinem IEEE 802.1x-Client am Access Control Device anmelden

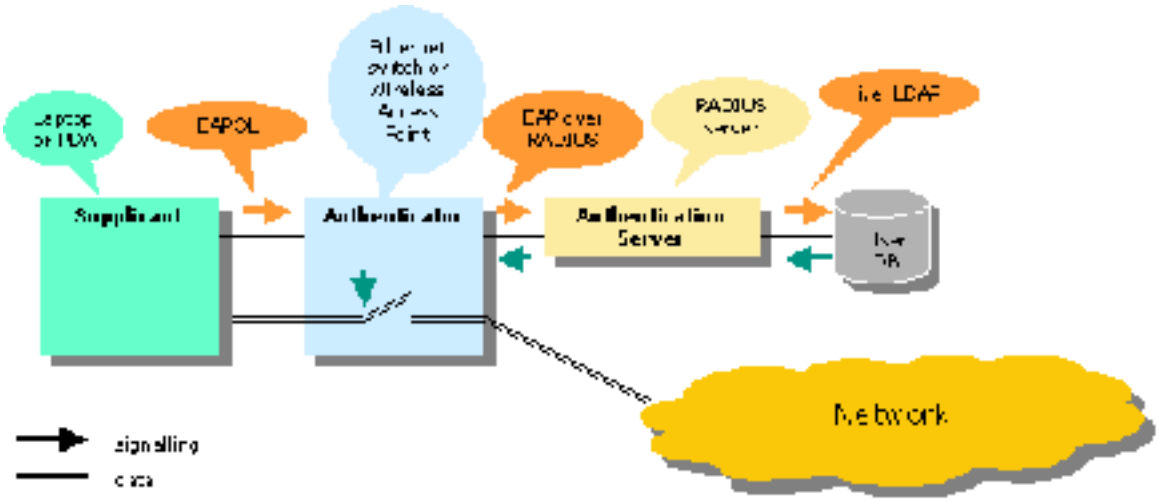

Abbildung 5: Schematischer Ablauf einer EAP-Authentifizierung

Nach erfolgreicher Authentifizierung (mit user@realm) wird dem Client eine IP-Adresse entsprechend den Berechtigungen des Accounts zugeteilt und Ethernet-Connectivity hergestellt.

Falls der lokale RADIUS-Server (»Authentication-Server«), den das Access Control Device kontaktiert, um die Authentifizierung zu verifizieren, aufgrund des übergebenen Realms erkennt, dass er für diesen Benutzer nicht zuständig ist, kontaktiert er den ihm bekannten nationalen RADIUS-Proxy-Server, um ihm die EAP-encapsulated Credentials (also z.B. Benutzername und Passwort) weiterzureichen. Dieser nationale RADIUS-Proxy-Server gibt sie sodann seinerseits entweder einem ihm bekannten zuständigen RADIUS-Server oder dem internationalen RADIUS-Proxy weiter.

Der internationale RADIUS-Proxy übergibt sie gegebenfalls dem zuständigen nationalen Proxy, der sie dann dem RADIUS-Server der Heimatorganisation übermittelt. Einzige Bedingung dabei ist, dass der »Authentication-Server« (also i. A. der RADIUS-Server der

Heimatorganisation) und der »Supplicant« (i. A. der 802.1x-Client am Client des Benutzers) den gleichen EAP-Typ verwenden, das Access Control Device und die RADIUS-Proxy-Server müssen diesen EAP-Typ nicht beherrschen, da sie die Anfragen nur durchreichen, eine aus Sicherheitsüberlegungen interessante Variante wären hier OTPs (One Time Passwords), wobei die Passwörter günstig und praktisch ohne zusätzliche Hardware per SMS versandt werden könnten.
Wichtig ist, dass die Kommunikation zwischen Client (»Supplicant«) und Access Control Device (»Authenticator«) mit dynamischen Keys verschlüsselt werden sollte und dass eine Erweiterung der Hardware nicht notwendig ist, wenn das ACD (also im Falle eines WLANs der Access Point bzw. der Switch im Falle eines LANs) »802.1x enabled« ist[8], eine höhere Verfügbarkeit kann durch redundante Auslegung der Proxy-Server auf jeder Ebene (lokal, national und international) erreicht werden.

4.2.1 Installationen

Bereits 2003 wurden im SURFnet in den Niederlanden WLANs aufgebaut, die 802.1x verwendeten und die auf eine RADIUS-Hierarchie aus *Radiator*-Servern zugreifen konnten. Eine Ausweitung auf öffentliche Hotspots, wie es in der Schweiz inzwischen realisiert ist, ist geplant.

4.2.2 Skalierung

Aufgrund der hierarchischen Baumstruktur (lokal, national, international) ist die Einbindung einer weiteren Organisation, die am Roaming teilnehmen möchte, denkbar einfach:

1. Auf der nächsthöheren Ebene muss der Organisation ein eindeutiger Realm zugeteilt werden
2. Der RADIUS-Server der neuen Organisation muss wissen, für welchen Realm er zuständig ist bzw. welchen RADIUS-Server er kontaktieren muss, wenn er nicht selbst zuständig ist
3. Der RADIUS-Server der übergeordneten Organisation muss wissen, welcher oder welche RADIUS-Server mit dem neuen Realm korrelieren

Andere Organisationen bleiben davon völlig unberührt, das System skaliert somit exzellent in O(1), also sehr viel besser als bilaterale Methoden, deren Aufwand mit der Anzahl der teilnehmenden Organisationen quadratisch steigt und die $O(n^2)$ Einträge benötigen.

4.2.3 Sicherheit

Wie bereits erwähnt wurde, wird durch 802.1x für sich alleine noch kein hoher Sicherheitsstandard gewährleistet[9], erst durch die Verwendung von TLS bzw. TTLS oder PEAP

8 vgl. dazu auch Kapitel 2.4.3
9 vgl. ebenfalls Kapitel 2.4.3

wird die Sicherheit entscheidend erhöht, das muss den Benutzern aber erst klargemacht werden.
Die Kommunikation zwischen den RADIUS-(Proxy)-Servern muss aber auch dann unbedingt (am besten durch IPsec-Tunnels) abgesichert werden, die RADIUS-(Proxy)-Server sollten z.B. durch Firewalls besonders geschützt werden, damit hier keine MITM-Attacke möglich wird.

4.2.4 Benutzbarkeit

TLS braucht Clientzertifikate (bzw. eine PKI) und ist daher zum derzeitigen Zeitpunkt nicht sehr verbreitet, TTLS (oder PEAP) arbeitet – ähnlich wie HTTPS – ohne Clientzertifikate, EAP (und damit natürlich EAP-TTLS oder EAP-PEAP) ist leider z.B. für ältere Betriebssysteme nicht verfügbar oder muss kostenpflichtig nachinstalliert werden.

4.2.5 Accounting und Logging

Es besteht sowohl bei der Gast- als auch bei der Heimatorganisation die Möglichkeit mitzuschreiben, wann sich welcher Benutzer angemeldet hat. Die Gastorganisation hat zusätzlich die Möglichkeit zu protokollieren, wann welche IP-Adresse welchem Benutzer zugeordnet wurde.
Jeder verdächtige Account kann auf jeder beliebigen Ebene der RADIUS-Hierarchie gesperrt werden, das kann für einzelne Useraccounts, aber – aufgrund des Realms – auch für ganze Organisationen durchgeführt werden.

4.3 Deliverable E: VPN

In dieser Arbeit werden von Kienholz (2003) zwei Implementierungen mit VPN-Technologie vorgestellt:

1. die Lösung »SWITCHmobile« der Schweiz
2. eine Lösung namens »Wbone« in Bremen (Deutschland)

und

3. eine Lösung mit Zertifikaten in Portugal

außerdem versucht er einen Weg aufzuzeigen, wie man das auf europäischer Ebene existierende Skalierungsproblem lösen kann, wobei er davon ausgeht, dass es in Europa eigentlich keine Bedenken seitens des Betreibers eines Forschungsnetzes geben sollte, den Mitgliedern eines anderen Forschungsnetzes Connectivity anzubieten, solange die (lokalen) Sicherheitsanforderungen erfüllt sind und kein zusätzlicher administrativer Overhead für den Gastgeber entsteht.

4.3.1 Installationen

Die Schweizer Variante »SWITCHmobile« einer VPN-Zugangslösung wurde in Kapitel 3.1 bereits ausführlich behandelt, hier wird sie nur noch einmal im Überblick präsentiert:
Es wird das Konzept von »docking networks« (Zugangsnetzen) eingeführt, einem i. A. logisch vom Universitätsnetz oder Internet getrennten IP-Netz (LAN oder WLAN), für das gilt:

- DHCP
- gleiche SSID bei allen teilnehmenden APs
- kein Zwang zu WEP oder anderen Protokollen auf Schicht 2 im OSI-Modell
- keine lokale Authentifizierung notwendig

Über Access Control Lists (ACLs) wird, wenn so gewünscht ist, gewährleistet, dass aus diesem Netz nur die VPN-Gateways der an Roaming teilnehmenden Organisationen erreicht werden können.

Die zweite vorgestellte Lösung »Wbone« in Deutschland verwendet (sogenannte) private Adressen nach RFC 1918 für das Zugangsnetz. Wieder sind nur die VPN-Gateways der Partnerorganisationen erreichbar, die sich aber ebenfalls im gleichen privaten Netz befinden müssen, wodurch dann aber keine Liste der VPN-Konzentratoren notwendig ist.
Diese Partnerorganisationen müssen die privaten Adressen allerdings routen, damit eine Verbindung hergestellt werden kann; die Verwendung der privaten Adressen muss somit auch koordiniert werden, daher wird die Verwendung von routbaren IP-Adressen (wie im Schweizer Modell) diskutiert.

Als dritte Lösung wird kurz auch auf eine Lösung der Technical University of Lisbon eingegangen, in der aber ein lokales VPN-Gateway kontaktiert wird – diese Lösung entspricht daher logisch eher dem Ansatz IEEE 802.1x, nur dass eben kein 802.1x-Client, sondern ein VPN-Client notwendig ist und dass statt mit User Credentials mit Zertifikaten gearbeitet wird, die man sich über einen zentralen Server per HTTPS generieren kann.

4.3.2 Skalierung

Die beiden ersten vorgestellten Implementierungen funktionieren gut auf lokaler und teilweise auch auf nationaler Ebene, eine Ausweitung auf europäische oder internationale Ebene dürfte aber schwer möglich sein: im einen Fall müsste die Vergabe der privaten IP-Adressen koordiniert werden und diese Adressbereiche müssten dann sogar geroutet werden, im anderen Fall wären u.U. sehr lange Listen von VPN-Gateways zu pflegen und in allen ACLs der teilnehmenden Organisationen up-to-date zu halten.

Mit jedem neuen Teilnehmer hätten alle anderen Teilnehmer dessen VPN-Gateways in ihre ACLs aufzunehmen. Das ist zwar bis zu einem gewissen Grad automatisierbar, die Listen würden aber mit jedem Teilnehmer länger.
Aus diesem Grund wurde überlegt, ob es eine andere Möglichkeit gibt, mit VPN eine auf europäischer Ebene skalierende Lösung zu bauen – die Antwort lautet: CASG!

4.3.3 Controlled Address Space to Gateways: CASG

Die Idee dabei ist, dass es nicht nur bei jeder teilnehmenden Organisation ein lokales, frei zugängliches »docking Network« gibt, sondern auch ein »relay network« des NREN:
Jedes europäische Forschungsnetz reserviert einen Adressbereich (am besten aus dem globalen Adressraum des NREN, sonst muss NAT eingesetzt werden) für den CASG (alternativ wäre es auch möglich, dass TERENA einen großen Bereich für alle VPN-Gateways im europäischen Wissenschaftsnetz reserviert).
In diesem Bereich, der je nach Größe des nationalen Forschungsnetzes (classless) zwischen 128 und 4096 Adressen umfassen würde, können nun die Forschungseinrichtungen ihre VPN-Gateways installieren, indem dem VPN-Gateway eine virtuelle IP-Adresse aus dem nationalen CASG zugewiesen wird.
Für eine bereits teilnehmende Organisation ändert sich nur dann etwas, wenn ein neues Land (und damit ein neues NREN) an »eduroam« teilnehmen will. Kommt dagegen nur eine neue Organisation innerhalb eines bereits teilnehmenden Landes dazu, dann muss nur dem VPN-Gateway dieser neuen Organisation eine IP aus dem CASG seines NRENs zugewiesen werden, die neue Organisation hat ihrerseits nur die CASGs der an »eduroam« teilnehmenden NRENs in ihrer ACL freizuschalten, andere Organisationen sind nicht betroffen, die Liste der CASGs, die einzupflegen ist, ist nur so lang wie die Anzahl der teilnehmenden NRENs (maximal also ca. 30).

4.3.4 Nationales CASG

Sobald ein IP-Paket in das Netz eines NRENs übertragen wird, hat dieses spezielle NREN volle Kontrolle darüber, was es mit diesem Paket macht, es können somit unterschiedliche Routing-Technologien zum Einsatz kommen, um das IP-Paket an diejenige physikalische Adresse zu übermitteln, die mit der virtuellen Adresse des zuständigen VPN-Gateways assoziiert ist.

VLAN

Eine mögliche Variante wäre, dass das NREN ein VLAN einrichtet, in dem sich dann alle VPN-Gateways befinden. In diesem VLAN könnten dann wieder einzelne Bereiche den einzelnen Forschungseinrichtungen zugeteilt werden, die dann dort – ohne dass das NREN bemüht werden müsste – ihre VPN-Gateways installieren könnten.

VPN Forwarding

Eine andere Möglichkeit wäre es, ein physikalisches Relay-Netzwerk aus Komponenten aufzubauen, die ein VPN-Forwarding zum zuständigen VPN-Gateway durchführen.

Solche Komponenten könnten z.B. mit NAT (source und destination) und auch mit PPTP arbeiten.

Wo NAT nicht möglich ist, muss diese Komponente einen Tunnel (SSL, TLS, IPsec, etc.) zum Netzwerk des assoziierten VPN-Gateway aufbauen. Das Gateway muss dann auch auf die virtuelle Adresse hören, das Gateway selbst könnte z.B. mittels CARP redundant ausgelegt sein.

4.3.5 Sicherheitsanforderungen

VPN bietet heute die größtmögliche Sicherheit, um beliebige Daten über das öffentliche Internet zu transportieren. Falls dabei keine PKI, in der sich Client und Server gegenseitig authentisieren, zum Einsatz kommen kann, gibt es eine einzige mögliche Schwachstelle: es bleibt dem Benutzer überlassen zu verifizieren, ob er tatsächlich mit dem richtigen VPN-Gateway kommuniziert. Wenn das erreicht werden kann, dann werden danach sowohl die Authentifizierung als auch der gesamte folgende Datenverkehr verschlüsselt, ohne dass der Benutzer noch spezielle Sicherheitsmaßnahmen setzen muss.

4.3.6 Benutzbarkeit

Wenn prinzipiell die Möglichkeit besteht, das VPN-Gateway der Heimatorganisation zu erreichen (egal ob über CASG, ein gemeinsames »docking network« oder bilaterale Abkommen), dann funktioniert die Lösung ausgesprochen gut, da ja immer nur der VPN-Client mit dem zugehörigen VPN-Gateway spricht, d.h. dass in einem Zugangsnetz parallel durchaus auch unterschiedliche VPN-Technologien (z.B. PPTP und IPsec) zum Einsatz kommen können.

Ein Problem könnte sein, dass bei der ersten Variante (also CASG) selbst das lokale VPN-Gateway an der Heimatorganisation (und das wird i. A. den meisten Verkehr im WLAN betreffen) – wenn man keine zweite Adresse definiert, die die Benutzer dann z.B. über ein zweites Profil einstellen können – nur über den Umweg der virtuellen CASG-Adresse erreicht wird; das könnte aber durch spezielle Routingmechanismen der lokalen Organisation verhindert werden, wodurch der Verkehrsfluss (wenn notwendig) optimiert würde.

Auch bei der zweiten Variante (VPN-Forwarding) würde der (logisch) lokale Verkehr über die erwähnten Forwarding-Komponenten geführt werden, das könnte aber dadurch verhindert werden, dass den lokalen Benutzern aus Performancegründen empfohlen wird, die »echte« IP-Adresse des VPN-Gateways zu nutzen, was aber den Nachteil hat, dass

der Benutzer 2 unterschiedliche Profile verwenden muss: eines (lokal) an der Heimatorganisation und das andere, wenn er eine Gastorganisation besucht.
Die Verwendung von VPN-Technologien auf modernen Notebooks stellt im WLAN kein Limit für die erreichbare Übertragungsgeschwindigkeit dar – diese ist sicher durch die generell niedrige Bandbreite im WLAN vorgegeben.

4.3.7 Accounting und Logging

Da der Zugang zum »docking network« völlig frei ist, dieses Netz aber entweder durch die Verwendung privater IPs bzw. von ACLs und Firewalls vom Netz der Gastorganisation und vom Internet völlig getrennt ist, die nach außen sichtbare IP aber von der Heimatorganisation vergeben wird, ist die Gastorganisation mit den Gästen überhaupt nicht befasst, was einen großen Vorteil gegenüber den anderen Lösungen darstellt: der gesamte AAA-Prozess läuft nur an der Heimatorganisation ab, das einzige, das der Gastorganisation passieren kann, ist, dass entweder ihre APs z.B. mit einer DoS-Attacke lahm gelegt werden, was aber sowieso nicht verhindert werden kann, oder dass es zu einem Missbrauch der Bandbreite der Organisation kommt, was aber durch die geringe vorhandene Maximalbandbreite im WLAN eher unwahrscheinlich erscheint.
Ob die Gastorganisation z.B. die MAC-Adressen, die im Netz verwendet wurden, mitprotokollieren will oder nicht und ob das überhaupt sinnvoll erscheint, ist dabei eine Entscheidung der Gastorganisation; eine eindeutige Zuordnung zu einem Benutzer (»Tracking«) kann damit nicht erreicht werden.

4.4 Deliverable F: Web Redirect (Webbasierter Zugang)

Der Aufbau einer webbasierten Lösung ist denkbar einfach: so ist es nicht notwendig, irgendwelche spezielle Hardware zu kaufen oder besondere Clients zu installieren:
Der Benutzer erhält im Zugangsnetz per DHCP eine IP, startet danach einfach seinen Webbrowser und versucht irgendeine Seite zu öffnen. Das Access Control Device erkennt, dass der zugehörige Rechner noch nicht authentisiert ist und leitet die Anfrage auf eine Seite mit einem Webformular um, wobei dieser Teil der Kommunikation per HTTPS abgewickelt werden sollte. Dort werden die Benutzerdaten abgefragt.
Aufgrund des Realms wird – wie bei der dot1x-Variante – in der RADIUS-Hierarchie nach dem zuständigen AAA-Server gesucht und – falls eine positive Antwort zurückkommt – das ACD informiert, dass es Verkehr von diesem Rechner durchleiten soll. Das Abmelden kann entweder vom Benutzer (wieder über ein Webformular) initiiert werden und zusätzlich z.B. auch durch ein ARP- oder ICMP-Timeout geschehen.

4.4.1 Installationen

Eine derartige Lösung ist z.B. in Finnland im Einsatz, viele andere Teilnehmer verwenden es als »Fall-back«-Lösung, da kein spezieller Client und i. A. keine spezielle Hardware erforderlich ist.

4.4.2 Skalierung

Da im Prinzip die gleiche RADIUS-Infrastruktur verwendet werden kann, die für 802.1x ausführlich besprochen wurde[10], gelten die gleichen Ergebnisse wie dort:
das System skaliert exzellent in O(1).

4.4.3 Sicherheit

Auch wenn man davon ausgeht, dass die Kommunikation mit dem Webformular, in dem man seine User Credentials eingibt, per HTTPS erfolgt und der Server, auf dem dieses Webformular läuft, speziell abgesichert ist und der Verkehr zwischen den RADIUS-Servern in sicheren Tunnels abläuft, ist diese Variante leider doch mit einer ganzen Reihe von Unsicherheiten ausgestattet:

- Da das Zertifikat des Webservers im Gastnetz dem Besucher i. A. nicht bekannt ist, könnte die Umleitung auf ein »gefaktes« Webformular sowohl durch einen rogue Access Point als auch durch einen anderen WLAN-Client, der sich als Access Point ausgibt, erfolgen, was nur durch den Aufbau einer TERENA-weiten PKI vermieden werden könnte. Erste Grundlagen dafür werden gerade geschaffen, Erfahrungen mit abgelaufenen HTTPS-Zertifikaten zeigen aber, dass das Bewusstsein der Benutzer hier noch nicht sehr ausgeprägt ist.
- Die Authentifizierung könnte (wie auch in der dot1x-Variante) an mehreren Stellen der RADIUS-Hierarchie mit einer MITM-Attacke abgefangen werden, hier allerdings noch einfacher, da kein Tunnel zum zuständigen AAA-Server aufgebaut wird, sondern die Credentials auf den RADIUS-Proxy-Servern im Klartext vorliegen.
- Da User Credentials i. A. nur beim Start des Browsers abgefragt werden und danach der Rechner (bzw. dessen MAC-Adresse) am NAD freigeschaltet wird, ist es relativ leicht eine Sitzung zu übernehmen (»Session Hijacking«), indem man z.B. eine »disassociate message« an einen authentisierten Client schickt und mit seiner MAC-Adresse weiterarbeitet.

4.4.4 Benutzbarkeit

Aufgrund des einfachen Aufbaus und der Verwendung eines Webbrowsers als Client ist diese Lösung sehr einfach zu verwenden, vom Benutzer werden keine speziellen Kennt-

10 siehe Kapitel 4.2 und 4.2.2

nisse oder Fähigkeiten gefordert, auch der Aufbau der Infrastruktur (ACD) ist i. A. sehr einfach: viele Switches unterstützen eine derartige Funktion. Ansonsten gibt es noch die Möglichkeit diese Funktionalität z.B. unter Linux mit Apache, PHP und Perl zu bauen bzw. fertige (freie oder kommerzielle) Lösungen einzusetzen.

4.4.5 Accounting und Logging

Auch hier gelten im Prinzip die gleichen Bemerkungen wie bei 802.1x[11].

4.5 Deliverable G: Vorläufige Auswahl

Wie Sankar & Chown (2003) schreiben, hat die TERENA Task Force »Mobility Group« die unterschiedlichen Lösungen, die in den Teilnehmerländern inzwischen zum Einsatz kamen, untersucht und dabei auch versucht herauszufinden, wie groß der Aufwand ist, aus den (zumeist) lokalen Lösungen eine Lösung zu bauen, die auch auf europäischer Ebene funktioniert[12].

Im Deliverable G wird dann nicht eine einzelne Variante als europäische Lösung ausgewählt, es wird vielmehr untersucht, welche Probleme auftreten können, wenn man die einzelnen Varianten zu einer europäischen Lösung ausbauen möchte. Dabei ist es noch einmal sehr wichtig festzuhalten, dass die verschiedenen Organisationen in den einzelnen Forschungsnetzen sehr unterschiedliche Anforderungen an die Zugangskontrolle und die Sicherheitsmaßnahmen stellen. Trotzdem wäre eine Infrastruktur, die den »nomadischen User« in seiner Arbeit unterstützt, ohne dass lokale Verwaltungsarbeit notwendig ist, ein großer Vorteil für die akademische Gemeinschaft.

Der Unterschied zwischen drahtgebundenem und drahtlosem Zugang ist dabei nicht von Bedeutung: obwohl eine Lösung also auch im drahtgebundenen Netz einsetzbar sein sollte, fokussierte sich die Arbeitsgruppe auf den drahtlosen Bereich, wo auch besondere zusätzliche, die Sicherheit betreffende Anforderungen dazu kommen.

Noch einmal werden die Haupt- (Skalierbarkeit, Verwaltungsaufwand, Sicherheit) und die Nebenziele (Benutzbarkeit, Funktionsfähigkeit und Accounting) definiert und die Hauptschwachstellen zusammengefasst:

1. Wer verständigt wen, wenn User Credentials gestohlen werden?
   Kann man diesen Diebstahl verfolgen?
2. Die Zugangsmethoden, die eine RADIUS-Hierarchie verwenden, müssen mit mehr Verzögerung (»Latency«) rechnen, als bei einer lokalen Lösung. Wie kann der Benutzer bei Problemen erfahren, wo das Problem in dieser Kette auftritt?
   Es ist sicherzustellen, dass die User Credentials zwischen den einzelnen RADIUS-

11 Kapitel 4.2.5
12 vgl. dazu die Abschnitte »Skalierung« in den vorigen Kapiteln

Proxy-Servern auf keinen Fall im Klartext übermittelt werden, daher sollten – unabhängig von der gewählten Authentifizierungsmethode – die Daten zwischen den RADIUS-Servern am besten in verschlüsselten Tunneln übertragen werden.

3. VPN-Lösungen, in denen der Verkehr immer über das VPN-Gateway des Heimatnetzes läuft, müssen ebenfalls mit mehr Latenzzeit rechnen, außerdem ist zu überprüfen, ob die VPN-Gateways auch mit hohen Datenraten wirklich fertig werden.
4. Auch wenn es eigentlich nicht notwendig wäre den gesamten Verkehr ins Heimatnetz zu routen: wenn eine lokale Lösung nur VPN-Tunnels zulässt, dann muss der gesamte Verkehr diesen Weg nehmen.
5. Im Falle von Services, die z.B. aus Lizenzgründen nur auf Basis der IP freigegeben werden, haben die Benutzer von VPN-Lösungen den Vorteil, immer mit einer IP aus dem Heimatnetz aufzutreten.
6. Aus Sicherheitsgründen sollten die Sicherheitsbeauftragten des Heimatnetzes aber immer bedenken, dass Benutzer, die sich mit VPN einwählen, sich u.U. in einem unsicheren Netz befinden und somit vom Intranet zu trennen sind.
7. Zugangskontrollmethoden, die lokalen Zugang geben, sollten (z.B. ebenfalls aus Lizenzgründen) die Möglichkeit haben zu unterscheiden, ob sich nun ein Benutzer der eigenen Organisation oder ein Gast authentisiert hat.
8. Auch wenn IPv6 nach wie vor nicht sehr weit verbreitet ist, sollte dieser Aspekt nicht unberücksichtigt bleiben.

Folgende Lösungen werden auf ihre Tauglichkeit für eine Roaming-Infrastruktur auf europäischer Ebene untersucht:

1. IEEE 802.1x
2. VPN
3. Webbased
4. Roamnode

weitere Methoden, wie z.B.:

- clientless VPN
  Ein SSL-Tunnel mittels HTTPS und ASP, also Applikationen, die sich in Webseiten einbinden lassen und über den Browser aufgerufen werden können
- Federating Software mit Single Sign On wie Shibboleth (vgl. Lienhardt, 2005 und Linden & Viitanen, 2005)
- MobileIP im IPv6-Umfeld

werden hauptsächlich deswegen nicht betrachtet, weil kein Mitglied der Arbeitsgruppe mit einer dieser Lösungen arbeitet.

4.5.1 IEEE 802.1x

Die Voraussetzungen, Vor- und Nachteile wurden bereits in vorigen Kapiteln besprochen, daher soll hier nur mehr auf die Möglichkeit der Zusammenarbeit mit anderen Lösungen und mögliche Beschränkungen eingegangen werden:

Da 802.1x auf Layer 2 arbeitet und nach erfolgter Authentifizierung IP-Connectivity erlaubt, gibt es keine Probleme mit IP-Applikationen, so ist es z.B. möglich, eine VPN-Verbindung nach einer 802.1x-Authentifizierung zu initiieren. Es ist auch möglich Gästen, die keine gültige dot1x-Authentifizierung durchführen können, ein Gast- oder Quarantäne-LAN zuzuweisen, aus dem sie dann z.B. eine VPN-Verbindung aufbauen oder eine webbasierte Authentifizierung durchführen können oder zumindest Zugang zu gewissen lokalen Ressourcen erhalten.

Eine Frage, die oft zu berücksichtigen ist: Welchen Einfluss hat NAT?

NAT (als Layer-3-Protokoll) hat keine Wechselwirkung mit dot1x (Layer 2), trotzdem sollte NAT (wenn möglich) nicht eingesetzt werden, weil es durchaus andere Probleme auf höheren Schichten des OSI-Modells verursachen kann.

4.5.2 VPN

Auch die Voraussetzungen, Vor- und Nachteile für VPN wurden bereits im Detail besprochen.

Für eine europaweite Verwendung muss unbedingt entweder ein internationaler CASG oder ein Verbund aus nationalen CASGs aufgebaut werden – dieser fehlt im Gegensatz zur RADIUS-Hierarchie noch. Da im Gegensatz zur dot1x-Variante im Verbund aus nationalen CASGs beim Hinzukommen eines neuen Landes alle bisherigen Teilnehmer ihre lokalen ACLs updaten müssen, muss auch ein Verfahren zur Benachrichtigung entwickelt werden, nationale Ansätze dafür gibt es bereits.

An einer Organisation, die primär VPN als Lösung anbietet, ist webbasierter Zugang technisch auch möglich, wenn nur Seiten aufgerufen werden, die ebenfalls im CASG definiert sind (z.B. Webmail-Server etc.) und die dann nicht umgeleitet werden; es erscheint also sinnvoll im CASG auf jeden Fall auch clientless VPN-Server (also HTTPS-Server), z.B. für Webmail etc. anzubieten. Beim Aufruf einer Seite, die außerhalb des CASGs liegt, wird entweder eine Seite angezeigt, die darauf hinweist, dass das ohne VPN-Client nicht möglich ist, oder es wird die webbasierte Authentifizierung durchgeführt, wenn man das als »Fall-back« definiert hat.

Mit dot1x verträgt sich die VPN-Lösung aber nicht, da 802.1x ja den Netzzugang als solchen beschränken soll, für die VPN-Lösung aber bereits eine IP-Verbindung bestehen muss. Für 802.1x ist es daher notwendig, entweder eigene APs oder zumindest eine andere SSID zu verwenden, die mit einem anderen VLAN, das 802.1x erlaubt, assoziiert ist.

Einige wireless ACDs erlauben weiters die Definition eines »walled garden«, also freien Zugriff zu bestimmten eingeschränkten Ressourcen für anonyme Benutzer.
Ob NAT einen Einfluss auf diese Lösung hat, hängt davon ab, wie sie umgesetzt wird. Die Variante von SWITCH wird davon nicht beeinflusst; wenn aber das »docking network« geNATet wird, dann funktionieren nur VPN-Lösungen, die NAT beherrschen (z.B. von *Cisco*).

4.5.3 Web Redirect

Um aus der webbasierten Zugangslösung eine international verwendbare Variante zu machen, ist ebenfalls der Aufbau einer RADIUS-Hierarchie notwendig. Falls eine solche bereits für 802.1x aufgebaut ist, dann kann diese auch für die webbasierte Methode Verwendung finden; es gelten dann die gleichen Skalierungswerte, wie für dot1x, allerdings ist die Methode aufgrund mehrerer Sicherheitslücken auch bei Verwendung von HTTPS bei weitem nicht so sicher; diese Schwächen wurden zur Zeit der Entstehung dieses Deliverables noch verharmlost, weil der »Normaluser« (ohne Spezialkenntnisse) diese Schwächen damals noch nicht so einfach ausnutzen konnte. Inzwischen sind aber Angriffstools fix und fertig im Netz zu finden, die keinerlei Experten-Knowhow erfordern.
NAT hat keinen Einfluss auf diese Lösung, aber wieder gilt: wenn möglich, kein NAT verwenden, da Applikationen auf höheren OSI-Schichten damit Probleme haben können.
Weiters hat diese Lösung keinerlei Einfluss auf die Datenrate, da sie ja nur zur Authentifizierung verwendet wird – die mögliche Bandbreite wird im WLAN durch die 802.11-Variante und generell durch den Uplink des Access Control Devices limitiert.

4.5.4 Roamnode

Die University of Bristol hat eine weitere Methode entwickelt, die in den vorhergegangenen Deliverables noch nicht berücksichtigt wurde, sie soll daher an dieser Stelle im Detail vorgestellt werden (vgl. dazu auch Howlett, 2002 und Howlett & Skelton, 2003):
Bereits 2001 wurde eine Idee entwickelt, die drahtlosen und drahtgebundenen Zugang am Campus und VPN-Verbindungen von außerhalb erlauben sollte. Das Ziel dabei war, den Zugang zu einem physikalischen Netzwerk von dem zu einem logischen Netz auch deshalb zu trennen, weil das i. A. in der Verantwortung unterschiedlicher Organisationen liegt: für das physikalische Netz ist der Gastgeber zuständig, für die logische Verbindung sollte aber das Heimatnetz verantwortlich sein.
Als zweites Designziel wurden möglichst einfache Schnittstellen zwischen den Schichten im OSI-Protokollstack ins Auge gefasst, um u.U. Protokolle einfach durch andere ersetzen zu können. Derzeit wird daher als VPN-Protokoll PPTP eingesetzt, das könnte aber mit relativ wenig Aufwand durch andere VPN-Protokolle, die ebenfalls über IP trans-

portiert werden, ersetzt werden.
Und als drittes und letztes Ziel wurde definiert, dass es eine vertikale Lösung sein sollte, die es erlaubt, auch Protokolle auf niedrigem OSI-Layer ansprechen zu können.
Die gefundene Lösung ist im Prinzip eine Kombination aus lokaler und remote Authentifizierung:
Der Client startet aus einem privaten Netz (RFC 1918) lokal eine PPPoE-Verbindung zum »Localnode« (also dem Roamnode beim Gastgeber) und authentisiert sich dort in der Art »user@realm« und einem sicheren Hash des Passworts (nicht mit dem Passwort selbst!), der Localnode reicht das per RADIUS an einen RADIUS-Proxy-Server weiter, der aufgrund des Realms entscheidet, an welchen RADIUS-(Proxy-)Server er es – falls er nicht selbst zuständig sein sollte – weiterreicht (dieser Teil stimmt also weitgehend mit den Varianten 802.1x bzw. webbasierter Zugang überein!).
Wenn der AAA-Server des »Homenode« den Benutzer authentisiert, dann werden zwischen Homenode und Localnode IP-in-IP-Tunnel inklusive Routinginformationen aufgebaut, der Localnode modifiziert seine ACLs so, dass Kommunikation zwischen Client und Homenode ermöglicht wird. Schlussendlich startet der Client (wenn sich der Localnode auch bei ihm authentifiziert hat) automatisch und transparent für den Benutzer eine VPN-Verbindung zu seinem VPN-Gateway. Diese Methode verbindet also die Vorteile der sehr gut skalierenden RADIUS-Hierarchie mit der Anforderung, nach außen nur eine IP aus dem Heimatnetz zu verwenden. Außerdem ermöglicht diese Variante die (interne) Verwendung von privaten IP-Adressen, ohne dass nach außen geNATet werden muss.
Ein weiterer Vorteil dieser Lösung ist, dass keine spezielle (u.U. sehr teure) Hardware benötigt wird; der Roamnode kann z.B. auf einem (redundant ausgelegten) Standard-PC installiert werden, der dann hunderte gleichzeitige VPN-Verbindungen terminieren kann.
Voraussetzung für Roamnode ist ein PPPoE-Client, was für PCs und Notebooks kein Problem darstellt, sehr wohl aber für PDAs und ähnliche Devices. Die Benutzbarkeit wird als sehr gut angegeben, 95% der Benutzer können nur aufgrund der zur Verfügung gestellten Dokumentation, also ohne persönliche Hilfe, eine Verbindung aufbauen.
Die Lösung benötigt kein NAT, es kann aber (Einschränkungen s.o.) eingesetzt werden.

4.5.5 Gegenüberstellung

Noch am 19. Dezember 2003 schreiben Sankar und Chown (Sankar & Chown, 2003, S. 28): “The original aim of this deliverable was to agree on one national roaming solution and design a scalable and interoperable architecture based on that recommendation across Europe. From investigations and discussions so far, it is clear that there is no single solution that meets all the requirements, or can address the vulnerabilities and limitations identified. It is also impractical to expect NREN s to abandon their existing

national solutions in favour of another approach, but they might be willing to modify existing deployments to support interoperability. (...) Ideally, the longerterm aim remains to move towards a single solution, but this is unlikely to be practical for some time."

Sie fassen dann die Lösungen aus Sicht der benötigten Clients und der notwendigen Access Control Devices bzw. aus Sicht von RADIUS, CASG und Zertifikaten zusammen:

National Solution	**Client**	**Access Control Device**
802.1X	802.1X capable Access control devices	Access control device
VPN	Needs VPN capability	One access control device between docking network and CASG (which does not do any AAA itself, just limits access to the CASG)
VPN & PKI (IPSec)	Needs VPN capability to find the most useful local VPN gateway.	VPN gateway in the visited institution as the access control device
Web-based	Web browser with TLS/SSL capability	Access control device between the docking network and the Internet, but often not (never?) in the AP
„Roamnode"	A client capable of supporting PPPoE	RADIUS or VPN Gateway at the home institution HomeNode?)

Zugriff auf das Gastnetzwerk

National Solution	**RADIUS**	**Security Certificates**	**CASG**
802.1X	YES	NO YES with EAP-TLS?	NO
VPN	NO	NO	YES
VPN & PKI (IPSec)	NO	YES	NO
Web-based	YES	NO	NO
„Roamnode"	YES	NO	YES

Zugriff (zur Authentifizierung) auf das Heimnetz

Obwohl Roamnode nach Meinung des Autors dieser Arbeit die gestellten Anforderungen in Bezug auf Sicherheit, Benutzbarkeit und Zuständigkeit sehr gut erfüllen würde, wird diese Lösung (wie auch Shibboleth) von der Task Force nicht weiter verfolgt, weil sie eine der anderen Forderungen, nämlich, dass der Einsatz von vorhandenem Equipment möglich sein soll bzw. dass eine vorhandene Lösung integriert werden kann, nicht voll erfüllt.

Noch einmal untersuchen daher die Autoren das Zusammenspiel der nur 3 Hauptvarianten (802.1x, VPN und webbasierter Zugang) aufgrund folgender Matrix (S. 32):

User@ Site	802.1X	VPN	Web
802.1X	(1)	(2)	(3)
VPN	(4)	(5)	(6)
Web	(7)	(8)	(9)

Kombinationen zwischen Gast- und Heimatnetzwerk

Will das Gastnetzwerk seinen Besuchern alle 3 Möglichkeiten anbieten, dann muss das Zugangsnetz 802.1x und zumindest auch VPN anbieten, es sind dann wenigstens zwei SSIDs (»802.1x« und »VPN«) vorzusehen.
Mit Hilfe von CASG kann auch einem Web-Benutzer ohne Authentifizierung Zugriff auf ausgewählte Web-Server eingeräumt werden (»Clientless VPN«). Erst bei Nutzung anderer Dienste ist die bereits mehrfach beschriebene Authentifizierung notwendig.
Die Autoren geben in ihrer Arbeit Beispielkonfigurationen für die VLANs, SSIDs etc. an, die im Detail hier nicht angeführt werden, weiters wird jede der 9 möglichen Kombinationen aus Benutzersicht zusammengefasst, es ergeben sich folgende Szenarien, wenn das Gastnetz alle 3 Varianten anbietet:

1. 802.1x-Benutzer in einem fremden Netz – Fälle (1), (4) und (7)
   - das Endgerät muss mit dem Zugangsnetz (SSID »802.1x«) verbunden werden
   - der Benutzer muss sich im 802.1x-Netz anmelden
   - er erhält per DHCP eine IP-Adresse und Internetzugang
2. VPN-Benutzer in einem fremden Netz – Fälle (2), (5) und (8)
   - das Endgerät ist mit dem Zugangsnetzwerk (SSID »VPN«) zu verbinden
   - das Endgerät bekommt per DHCP eine IP-Adresse zugewiesen
   - der Benutzer startet einen VPN-Client und wählt sich in seinem Heimatnetz ein
3. Web-Benutzer in einem fremden Netz – Fälle (3), (6) und (9)
   - das Endgerät ist mit dem Zugangsnetzwerk (SSID »VPN«) zu verbinden
   - das Endgerät bekommt per DHCP eine IP-Adresse zugewiesen
   - der Benutzer startet einen Webbrowser und ruft eine beliebige Seite auf
   - es erfolgt ein Redirect auf eine Anmeldeseite (HTTPS)
   - der Benutzer gibt seine Zugangsdaten ein
   - er erhält (zeitlich beschränkten) Internetzugang

Explizit nicht betrachtet werden Möglichkeiten, Gästen Zugang zum eigenen VPN-Gateway zu geben, oder auch Fälle, die eine PKI voraussetzen, da eine solche praktisch noch nirgends (vollständig) implementiert ist, PPPoE (»Roamnode«) ist aber noch Teil der vorgeschlagenen weiteren Vorgehensweise:

- Die Skalierungs- und Zusammenarbeitsprobleme lösen
- Tests für skalierbare VPN-Lösung durchführen, CASG aufbauen
- RADIUS-Hierarchie aufbauen
- Software für PPPoE-Lösungen vorantreiben

und die Ergebnisse dann in einem Endbericht zusammen zu fassen.

Für die RADIUS-Hierarchie wird sodann eine dreistufige Variante vorgeschlagen, in der ein (redundant ausgelegter) Top-level-RADIUS-Proxy-Server (TRPS) mit den RADIUS-Servern der NRENs (NRPS) verbunden ist, die dann ihrerseits mit den RADIUS-Servern der teilnehmenden Organisationen (ORPS) verbunden sind:

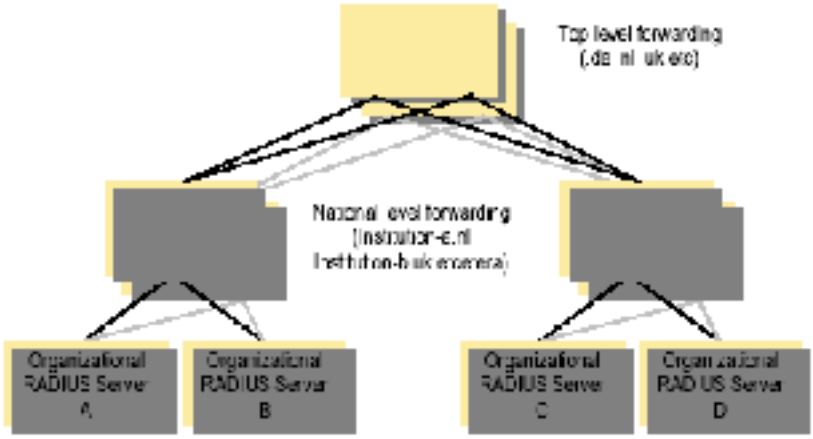

Abbildung 6: RADIUS-Hierarchie

Aus Verfügbarkeitsgründen wird empfohlen, dass zumindest der Top-Level-Server und die Server der NRENs in Wirklichkeit aus mindestens 2 unabhängig voneinander arbeitenden Servern bestehen und dass es ermöglicht werden soll, dass zwei Organisationen innerhalb eines NRENs auch direkte Pfade zwischen ihren RADIUS-Servern (ORPS) schalten können, ohne den Umweg über den nationalen RADIUS-Proxy (NRPS) gehen zu müssen.

Im für VPN vorgeschlagenen CASG wird jetzt die Lösung eines europaweiten Adressbereichs nicht mehr behandelt, stattdessen wird vorgeschlagen, dass jedes NREN einen eigenen CASG aufbaut, wobei es dem jeweiligen NREN überlassen ist, welche Methode es verwendet[13]. Aufgrund der Erfahrungen der Universität Bremen (»Wbone«) und der Tatsache, dass im europäischen Raum ca. 640 Millionen Einwohner leben, wird geschätzt, dass in etwa 16.000 öffentliche IP-Adressen gebraucht werden, eine Abschätzung, wie sich das in Zukunft entwickeln wird, ist nicht möglich.

Zum Thema »Roamnode« (PPPoE) wird festgestellt, dass unklar ist, wie viel Arbeit notwendig ist, damit diese Methode mit den anderen zusammenarbeiten kann, außerdem ist noch Arbeit bei der Architektur des Systems notwendig und die Tests für folgende sieben Szenarien fehlen noch:

1. Roamnode-Benutzer in einem fremden Roamnode-Netz
2. Roamnode-Benutzer in einem Netz mit einer der 3 Standard-Zugangsmethoden
3. Ein Benutzer einer der 3 Standard-Zugangsmethoden in einem Roamnode-Netz

Aus den Ergebnissen dieser Tests muss dann der Abschlussbericht resultieren.

13 vgl. dazu Kapitel 4.3.4

4.6 Deliverable H: Testumgebungen und Referenzdesign

Zu Beginn der Arbeit (Wierenga, 2004) wird nochmals auf Deliverable G verwiesen, in dem *keine* einzelne Methode vorgeschlagen wurde, weil keine der Varianten eindeutig hervorsticht: jede Zugangslösung hat ihre Stärken und ihre Schwächen, der Aufwand der Entwicklung der einzelnen Lösungen macht es außerdem unwahrscheinlich, dass nationale Entwicklungen zu Gunsten eines einzigen europäischen Modells verworfen werden.

Deliverable H befasst sich daher hauptsächlich mit den Möglichkeiten des Zusammenspiels der 3 Hauptvarianten (802.1x, VPN und webbasierter Zugang) und stellt Beispielslösungen vor. Wieder wird auf die grundsätzlichen technischen Unterschiede der 3 Lösungen, auf die hier bereits in Kapitel 4.5.5 ausführlich eingegangen wurde, hingewiesen.
Es wird aber auch explizit angemerkt, dass viele Access Points der ersten Generation es *nicht* unterstützen, zwei oder mehrere SSIDs gleichzeitig zu broadcasten; in diesem Fall ist es notwendig, die Trennung der VLANs auf OSI-Ebene 1 vorzunehmen, also tatsächlich je zwei APs zu installieren: einen für 802.1x und einen für die anderen Lösungen.
Für dot1x und den webbasierten Zugang wird wieder auf die RADIUS-Hierarchie verwiesen, für den VPN-Zugang schreibt Wierenga (2004, S. 7): “It is assumed that guest users get restricted network access with their VPN-client to their home institution s VPN-server as long as it uses an IP-address from the CASG. For the remainder of this document it is assumed that the CASG is in place.”

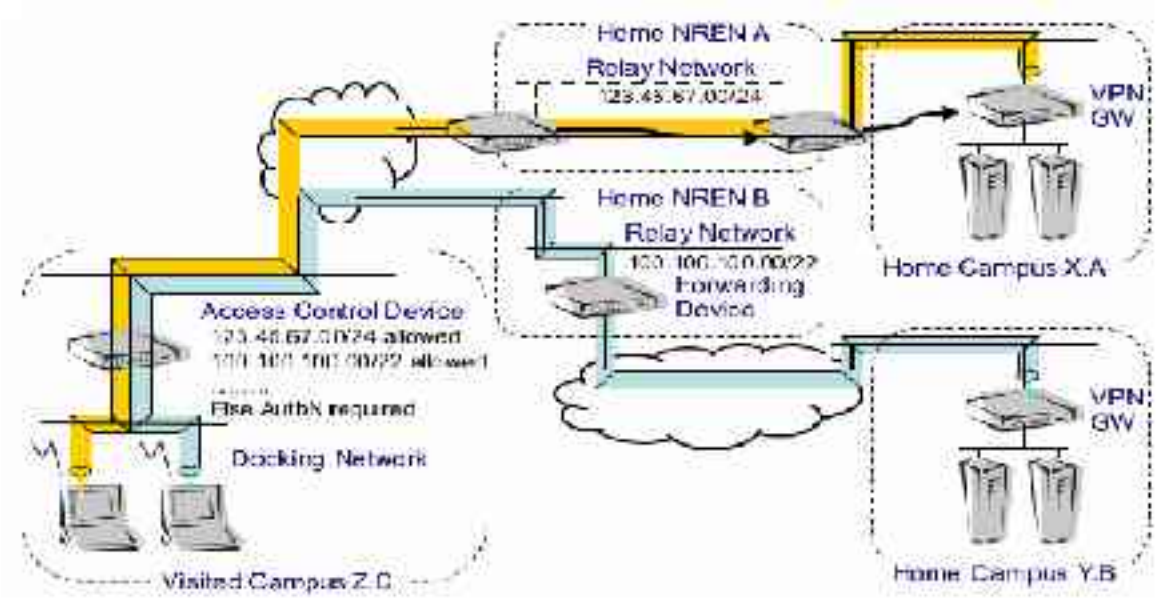

Abbildung 7: CASG

Als Testumgebungen für die 3 Varianten wurden folgende Organisationen bestimmt:

- SURFnet (802.1x)
- Technical University of Tampere (webbasierter Zugang)
- SWITCH (VPN-Lösung)

Die SSIDs dieser Insellösungen wurden noch nicht synchronisiert, so heißt z.B. die SSID für den VPN-Zugang im SURFnet »eduroam-guest«, bei SWITCH dagegen »web-vpn«.

4.6.1 SURFnet

Um zur SURFnet-Standardmethode 802.1x, die mit EAP-TLS sehr sicher ist, auch webbasierten Zugang und VPN anbieten zu können, wurde als »Captive Portal« das finnische GPL-Programm *Tino* implementiert und ein eigenes WLAN installiert, das nicht auf IEEE 802.1x beruht.

Im Zugangsnetz wurden Access Points eingesetzt, die mehrere SSIDs unterstützen, die auf verschiedene VLANs abgebildet werden. Wie nun Benutzer anderer Zugangsarten im SURFnet Zugang erhalten, wurde bereits in Kapitel 4.5.5 genau beschrieben, auf das Problem CASG wird nicht näher eingegangen (s.o.: “it is assumed that the CASG is in place”).

4.6.2 SWITCH

Auch in der Schweiz wurde ein »Captive Portal« implementiert, hier eine kommerzielle Lösung von *Bluesocket*, und ein zweites WLAN für 802.1x installiert, wobei für die VPN-Lösung bereits ein CASG existiert.

4.6.3 Technical University of Tampere (TUT)

Die bevorzugte Methode an der Technischen Universität Tampere ist der webbasierte Zugang mit Hilfe des bereits erwähnten Programmes *Tino*, das unter der GPL läuft. Für Benutzer einer der anderen Methoden wurde ein eigenes Netz, das 802.1x unterstützt, installiert und die Access-Listen der Layer-3-Switches so modifiziert, dass VPN-Konzentratoren im Bereich eines CASGs aus dem VLAN der Web-Benutzer erreicht werden können.

4.6.4 Referenzdesign

Im weiteren Verlauf der Arbeit wird dann detailliert auf das Design des Netzes auf OSI-Layer 2 und 3 eingegangen und auch die RADIUS-Hierarchie beschrieben.

Wierenga schreibt zum Thema PKI hier (a.a.O., S. 17) im Gegensatz zu allen bisherigen Arbeiten: “In most cases there is already a PKI in place, so it can be assumed that this is not a problem” und zum Thema Sicherheit innerhalb der RADIUS-Hierarchie sagt er an gleicher Stelle: “It is of course recommended to create a secret that can not be easily

guessed since otherwise the RADIUS-message can be decrypted. This is not a big problem with EAP-authentication using 802.1X since the credentials are also transmitted over a SSL-encrypted tunnel between the client and the final authentication server".
Wie Hofherr (2005, S. 94) empfiehlt auch er – falls EAP-TLS wegen fehlender PKI nicht in Frage kommt – die Verwendung von EAP-PEAP oder EAP-TTLS.
In der Zusammenfassung (a.a.O., S. 33) kann man in Übereinstimmung mit dem bisher Gesagten lesen: "It has been acknowledged by the taskforce that currently there exists no single roaming solution that satisfies all the requirements that the various NRENs have", etwas überraschend geht es dann aber mit folgendem Satz weiter: "Recent developments however show that consensus is building towards a single, RADIUS-based, European roaming infrastructure based on 802.1X" und er ergänzt, dass es mit den, den Deliverables G und H zugrunde liegenden Untersuchungen, geglückt sein sollte zu zeigen, dass es für die gängigsten Zugangslösungen im Umfeld von TERENA eine sanfte Migration in Richtung 802.1x geben kann, während gleichzeitig eine »Abwärtskompatibilität« für bestehende dot1x-Infrastrukturen möglich ist.
Er schließt mit den Worten "Time will show if and how fast this co-existence will seize to exist".

4.7 Deliverable I: Roaming Policy Document

Florio et al. versuchen in Deliverable I Richtlinien zu erstellen, die ein allgemein akzeptierbares, skalierbares und transparentes Gastnetz (also eine Roaminginfrastruktur) möglich machen sollen.
Sie versuchen dabei in keiner Weise direkt auf irgendein nationales oder europäisches Recht Bezug zu nehmen oder unterschiedliche Gesetzesauslegungen (z.B. im Bereich Urheberrecht, Datenschutz und Vorratsdatenhaltung) zu vereinheitlichen, es geht vielmehr darum eine Art von »Web of Trust« zwischen den akademischen Einrichtungen und den NRENs aufzubauen.
Ziel der Arbeitsgruppe ist es dabei auch, dass der Dienst als ein akademisches Roaming-Service mit nur minimalen Ansprüchen bzgl. (Daten-)Sicherheit verstanden wird. Es liegt weiter in der Verantwortung des nomadischen Benutzers, sowohl die ihm zumindest vorerst unbekannte lokale Acceptable Use Policy, als auch die Betriebs- und Benutzungsordnung des Heimatnetzes zu befolgen.
Idealerweise sollte er im Gastnetz genau mit den Einstellungen einen Netzzugang erhalten, mit denen er sich auch in seinem Heimatnetz einwählt, ohne, dass er irgendetwas zusätzlich tun oder installieren muss. Es liegt dann an der Heimatorganisation ihren Angehörigen Informationen oder Schulungen zukommen zu lassen, wie sie diese Infra-

struktur nutzen können und wen sie im Falle eines Problems kontaktieren sollen.
Die grundsätzlichen organisatorischen Punkte für eine Roaming-Infrastruktur werden folgendermaßen zusammengefasst:

- Der Zugang darf nur autorisierten Personen möglich sein, das sind Personen, die auch bei einem NREN oder einer teilnehmenden Organisation berechtigt sind, das Internet zu nutzen
- Alle Roaming-Benutzer müssen sich bei ihrer Heimatorganisation authentisieren, damit sie an der Gastorganisation Internetzugang erhalten
- Die Benutzer sind für Ihre Zugangsdaten und deren Übermittlung selbst verantwortlich und müssen die AUP, die die Heimatorganisation mit dem NREN abgeschlossen hat, befolgen
- Der Gastgeber muss die Möglichkeit haben zu überprüfen, ob das Roamingservice vom Zugangsnetz aus erreicht werden kann
- Die gastgebende Organisation muss dem Besucher klar darlegen, dass die Übertragung der Benutzerdaten sicher ist; falls die Übertragung nicht sicher ist, dann muss der Benutzer die Möglichkeit erhalten, von seinem Device aus eine sicherere Verbindung herzustellen
- Die besuchte Organisation hat das Recht jeden beliebigen Benutzer, jede beliebige Organisation oder sogar jeden beliebigen NREN zu sperren.
- Der Gastgeber entscheidet darüber, wie und welche Verbindung erlaubt wird
- Die Heimatorganisation ist dafür verantwortlich ihre Benutzer zu unterstützen und zu schulen

Wie der Benutzer, der i. A. keinerlei Einblick z.B. in die RADIUS-Hierarchie hat, allerdings die Verantwortung für die Übertragung seiner Zugangsdaten übernehmen soll, wird nicht beantwortet, genauso wenig wie die Frage, wie die gastgebende Organisation z.B. durch Testaccounts verifizieren soll, ob eine Anmeldung technisch überhaupt möglich ist. Der Punkt “(...) muss der Benutzer die Möglichkeit erhalten, von seinem Device aus eine sicherere Verbindung herzustellen” kann nach Meinung des Autors nur bedeuten, dass (solange keine flächendeckende PKI implementiert ist) VPN auf jeden Fall auch anzubieten ist!
Aus dem Recht, jederzeit ganze NRENs zu sperren, ergibt sich wieder das Problem der Transparenz: einem neuen Besucher dieses NRENs muss erst irgendwie klargemacht werden, dass er jetzt leider nicht an »eduroam« teilnehmen kann.
Im Anschluss an die wohlbekannten Vorteile einer Roaming-Infrastruktur werden zwei Richtlinien für die Abkommen zwischen den NRENs und TERENA bzw. zwischen den

Forschungseinrichtungen und dem zuständigen NREN vorgestellt[14].

4.8 Final Report

Die TERENA Task Force »Mobility Group« traf sich zum ersten Mal schon im März 2002 im Rahmen eines Workshops in Amsterdam. Die Mitglieder der TF-Mobility trafen sich im Zeitraum Jänner 2003 bis Juni 2004 insgesamt fünfmal entweder real oder in Videokonferenzen und beendeten die TF formell im Juli 2004.

Die bereits erwähnte Mailingliste mobility@terena.nl blieb aber auch danach aktiv und ist es bis heute geblieben; auch die Website bleibt – als Teil der TERENA-Homepage – weiter online und wird weiter gewartet.

Als Ergebnis der Arbeit der TF wurden mehrere Deliverables veröffentlicht[15], in denen unter anderem die Kriterien (gegliedert nach Muss- und Soll- bzw. nach Haupt- und Nebenanforderungen) definiert wurden. Weiters wurde erhoben, welche Lösungsansätze in Europa hauptsächlich verbreitet sind (webbasierter Zugang, VPN und IEEE 802.1x). Diese unterschiedlichen Varianten wurden in Hinblick auf die Erfüllung der Kriterien und auf die Möglichkeit der Koexistenz evaluiert.

In einer Vorauswahl[16] wurde auch noch die sehr interessante Lösung »Roamnode« in die Betrachtungen mit einbezogen und es wurde festgestellt, dass – wenn man die geeignete Infrastruktur in Form einer RADIUS-Hierarchie für dot1x und webbasierten Zugang und CASG für VPN bzw. durch Weiterentwicklung von »Roamnode« schafft – keinem der Ansätze eine eindeutige Präferenz auszusprechen ist, da keine einzelne Lösung in allen Punkten Vorteile gegenüber allen anderen Varianten hat.

So fassen Sankar und Wierenga (2004) die 9 Kombinationen der gängigsten Zugangslösungen auf Seite 8 wie folgt zusammen:

User with Site uses	802.1X	VPN	Web-based
802.1X	Okay	Work reqd	Work reqd
VPN	Work reqd	Okay	Work reqd
Web-based redirect	Work reqd	Work reqd	Okay

Es zeigt sich klar, dass – wenn man bestehende Lösungen einbauen will – in allen Fällen zusätzliche Arbeit notwendig ist.

Im Zuge der Untersuchungen wurde auch deutlich, dass es Bedarf an definierten Über-

14 siehe Anhang 8.3
15 vgl. Kapitel 4.1 - 4.7
16 siehe Kapitel 4.5

einkommen zwischen den einzelnen Ebenen der RADIUS-Proxy-Hierarchie gibt, für die in Deliverable I (Kapitel 4.7) Vorschläge erarbeitet wurden.
Noch einmal werden Stärken und Schwächen der einzelnen Lösungen vorgestellt, auch auf »Roamnode« wird nochmals eingegangen, zusätzlich wird auf die Auswirkungen von IPv6 eingegangen, auch wenn derzeit noch kein großer Druck besteht, auf IPv6 umzustellen, da im akademischen Bereich in Europa im Moment noch genug IPv4-Adressen vorhanden sind; trotzdem sollte nach Meinung der Autoren darauf geachtet werden, dass eine Lösung auch IPv6 unterstützt, was durch aktuelle kommerzielle webbasierte Lösungen nicht gegeben ist.
Während auch IPv6-VPN-Lösungen gerade erst entwickelt werden, sollte es mit 802.1x keinerlei Probleme haben, da dot1x ja auf OSI-Ebene 2 arbeitet und die RADIUS-Hierarchie entweder in einem Dual-Stack-Modus des lokalen RADIUS-Servers, der dann die anderen RADIUS-Server per IPv4 kontaktiert, oder einer generellen IPv6-RADIUS-Hierarchie genauso gut unter IPv6 betrieben werden kann.
Innerhalb der IPv6-Protokollfamilie etabliert sich auch ein neues Protokoll: Mobile IPv6, eine IPv6-Variante, in der die mobilen Devices – ähnlich wie bei der VPN-Lösung – fixe IP-Adressen aus dem Heimatnetz beziehen, sodass das Gerät immer unter der gleichen IP-Adresse erreichbar ist (was ein großer Vorteil für Applikationen wie z.B. VoIP oder auch VoWLAN ist). Da das Endgerät – im Gegensatz zur VPN-Variante – auch die tatsächliche IP-Adresse (die aus dem Gastnetz) übermittelt, können lange Umwege vermieden werden, weil die Pakete nicht unbedingt immer den Umweg über das Heimatnetz nehmen müssen.
Zuletzt werden noch nationale Entwicklungen der einzelnen NRENs präsentiert:

4.8.1 CARNet (Kroatien)

Jede Organisation im CARNet, dem NREN Kroatiens, soll sowohl einen RADIUS-Server als auch einen LDAP-Server betreiben, was ursprünglich als Infrastruktur für Einwählzugänge (»dial-in«) gedacht war.
Diese Infrastruktur besteht bereits seit Februar 2003 und schon im Juni 2004 nehmen an die 200 Organisationen teil, von denen über 80% eigene RADIUS- und LDAP-Server in Betrieb haben.
Diese Infrastruktur bietet sich natürlich auch für Roaming (WLAN und drahtgebunden) an und wird daher zusammen mit IEEE 802.1x eingesetzt, um z.B. Zugänge in Studierendenheimen zu ermöglichen.

4.8.2 CESNET (Tschechische Republik)

Bereits 2004 waren zwei nationale RADIUS-Proxy-Server mit den zentralen TERENA-

RADIUS-Servern verbunden und leiteten die Anfragen der tschechischen Organisationen bei Bedarf dorthin weiter.
Als RADIUS-Server wurde aus Kostengründen die freie Lösung FreeRADIUS gewählt, CESNET versucht alle 3 Hauptzugangslösungen national zu unterstützen und hat daher auch einen CASG implementiert, priorisiert jedoch IEEE 802.1x.
Die aktuelle Liste der teilnehmenden Organisationen findet man auf www.eduroam.cz

4.8.3 Forskningsnettet (Dänemark)

Auch die Dänen haben bereits Mitte 2004 redundante RADIUS-Server (*Radiator*) mit dem Proxy-Server von TERENA in den Niederlanden verbunden und so den Grundstein zur Teilnahme an eduroam gelegt. Außerdem wurde in Dänemark ein zweiter Top-Level-RADIUS-Server installiert. Die RADIUS-Infrastruktur wird gleichzeitig auch in Kooperation mit *iPass*, dem größten kommerziellen Zugangsprovider der Welt, verwendet.

4.8.4 Funet bzw. CSC (Finnland)

In Finnland wurde und wird von vielen Universitäten ein webbasiertes Modell der Zugangskontrolle eingesetzt, wobei im Hintergrund RADIUS eingesetzt wird, daher war es logisch, dass man ebenfalls auf die RADIUS-Hierarchie gesetzt hat, außerdem ist geplant in Zukunft 802.1x ebenfalls einzusetzen.
Ein Problem, das in Finnland identifiziert wurde, ist, dass es schwer oder überhaupt nicht möglich ist zu überprüfen, ob der RADIUS-Server einer anderen Organisation überhaupt erreicht werden kann, einzige – einigermaßen skalierende – Lösung könnte sein, dass die NRPS mit Testaccounts regelmäßig die ORPS kontaktieren und das Ergebnis z.B. auf einer gemeinsamen TERENA-Website zugänglich machen.

4.8.5 DFN (Deutschland)

Obwohl auch in Deutschland schon früh zwei NRPS installiert wurden, werden z.T. aufgrund veralteter Access Points zumindest zum Zeitpunkt des Erscheinens des Final Reports im Juni 2004 lokal hauptsächlich VPN- und keine dot1x-Lösungen eingesetzt[17].
Es wurde daher eine ready-to-go-Lösung entwickelt, die eine sanfte Migration zulassen sollte: »Modular 802.1X migration solution – Mod8.X«.

4.8.6 GRNET (Griechenland)

Wie einige andere Länder verband auch Griechenland seine NRPS mit den europäischen Top-Level-RADIUS-Servern im Sommer 2004. RADIUS-Server wurden bereits für viele Dienste (wie z.B. Dialup, VPN, VoIP, WiFi, ...) eingesetzt, die damit alle prinzipiell am Roaming teilnehmen könnten. Genauer betrachtet wurden dann

17 vgl. dazu auch Kapitel 3.2

- Wireless Access
- L2TP-VPNs
- Layer-3-VPNs auf MPLS-Basis
- VoIP

Eingesetzt werden z.B. an der National Technical University of Athens (NTUA) alle drei Hauptvarianten:

Abbildung 8: Zugangsinformation an der NTUA

4.8.7 SURFnet (Niederlande)

Schon Ende 2001 begann man im SURFnet nach sicheren Methoden des Zugangs zu WLAN-Netzen zu suchen und installierte daher bereits Anfang 2002 eine Testumgebung mit 802.1x, wobei auch ein eigener freier 802.1x-Client (*SecureW2*) entwickelt wurde und die RADIUS-Infrastruktur auch für Gäste geöffnet wurde. Nach dem positiven Verlauf des Tests schlossen sich im April 2002 weitere Institutionen an und im März wurde ein Workshop für TERENA abgehalten, was letztendlich zur Gründung der Task Force »Mobility-Group« führte.

2003 installierte SURFnet dann den ersten Top-Level-RADIUS-Proxy-Server für Europa. SURFnet ist in diesem Umfeld nach wie vor stark engagiert und arbeitet aktuell an folgenden Problemstellungen mit:

- Roaming Policy[18]
- Client-Entwicklung
- Usertracking (Abuse)

18 vgl. Kapitel 4.7

- Basisinfrastruktur (Gibt es neue Technologien?)
- Zugang zu Applikationen (*A-Select*)

4.8.8 UNINETT (Norwegen)

In Norwegen gibt es eine zentrale PKI: FEderated ID for Education (»FEIDE«).
FEIDE selbst unterstützt kein RADIUS, die lokalen ORPS sollen daher als Proxy dienen und auf FEIDE zugreifen; diese RADIUS-Server können aber auch parallel zum FEIDE-System miteinander verbunden werden und so die Grundlage für »eduroam« bilden.
Obwohl auch in Norwegen alle drei der Hauptvarianten eingesetzt werden, wird aufgrund dieser teilweise bereits vorhandenen Infrastruktur national auf 802.1x gesetzt.

4.8.9 FCCN (Portugal)

Das Roaming-Projekt in Portugal ging aus dem virtuellen Campus-Projekt »e-U« hervor, in dem u.a. eine WLAN-Infrastruktur für den gesamten Bereich der höheren Bildung aufgebaut werden sollte, in der Roaming sowohl für Lehrende als auch für Studierende möglich gemacht werden sollte, was eine Bedingung für eine finanzielle Unterstützung durch die Regierung war.
Aus einer Testphase mit 8 Organisationen und allen drei Standardlösungen (webbasierter Zugang mit *NoCat* bzw. *Nomadix*, VPN und dot1x) wurde 802.1x mit EAP (wobei PEAP und TTLS empfohlen werden) als nationale Roaming-Lösung ausgewählt, wobei Gäste aber nur Zugang zu lokalen Webservern, nicht zum Internet erhalten.

4.8.10 RedIRIS (Spanien)

In Spanien wurde vom NREN im Juni 2004 eine Initiative namens »MovIRIS« gestartet, die folgende Ziele verfolgen sollte:

1. Koordination der Bestrebungen eine Infrastruktur für Mobilität aufzubauen
2. Entwicklung einer nationalen AUP innerhalb der TERENA-AUP
3. Sicherstellung der Kompatibilität der nationalen Lösung mit »eduroam«
4. Koordinierung der Informationen zum Thema Wireless Roaming
5. Unterstützung und Förderung nationaler Initiativen

4.8.11 SWITCH (Schweiz)

Die Lösung »SWITCHmobile« wurde bereits detailliert in Kapitel 3.1 behandelt.

4.8.12 UKERNA (Großbritannien und Nordirland)

Im Vereinigten Königreich wurde eine eigene WLAN-Arbeitsgruppe im JANET (Joint Academic Network) gegründet, die sowohl die drei üblichen Hauptvarianten als auch die »Roamnode«-Lösung der University of Bristol näher betrachtet.

Entwickelt wurde dann eine »LIN Service« (Location Independent Networking) genannte, auf IEEE 802.1x und RADIUS basierte Lösung, deren technische Details man bei Howlett (2005) findet und die sich über die RADIUS-Hierarchie nahtlos in die »eduroam«-Umgebung einfügt.

In den abschließenden Zeilen schreiben Sankar & Wierenga (a.a.O., S. 53):

“The group has identified a key set of roaming requirements and has assessed these against a variety of roaming infrastructure deployments within NRENs. Their first conclusion reached was that no single solution meets all the key requirements listed. As a result an interoperable solution was recommended and substantial work was undertaken to design, build and test RADIUS proxy hierarchy and Controlled Address Space for VPN Gateway concepts. This integration approach also provided institutions with a realistic and easier upgrade path towards 802.1X.”

Sie ergänzen im letzten Kapitel »Recommendations for future work« (a.a.O., S. 54):

“The Task Force considered future work items (...) but also to avoid any overlap from work going undertaken by DANTE in the Joint Research Activity Ubiquity (Mobility) and Roaming Access to Services (JRA5) in the Geant2 project”.

4.8.13 Außereuropäische Länder

Wie man der Karte auf Seite 56 entnehmen kann, nehmen inzwischen auch Länder teil, die nicht in Europa liegen, weitere NRENs aus Übersee haben Kooperationsinteresse bekundet.

4.9 Zusammenfassung

Aus Sicht der Zugangsanbieter ergibt sich nach Maschtera (2005) damit folgendes Bild:

Dockingnetzwerk:

- 802.1x-Benutzer können am Zugangsnetz erst nach erfolgreicher Authentifizierung auf OSI-Ebene 2 teilnehmen. Danach erfolgt automatisch die Freigabe des Internetzugangs
- VPN- und Web-Benutzer können am Dockingnetzwerk ohne Authentifizierung teilnehmen. Die Authentifizierung für den Internetzugang erfolgt erst auf OSI-Ebene 3
- Aufgrund dieser technischen Unterschiede beim Andocken sind (zumindest) zwei VLANs und damit assoziierte SSIDs erforderlich

Authentifizierung:

- 802.1x- und Web-Benutzer werden über einen Authentifizierungsserver des Gastnetzwerks bzw. eine RADIUS-Hierarchie authentifiziert

- VPN-Benutzer werden vom Authentifizierungsserver des Heimatnetzwerks über das VPN-Gateway authentifiziert

Internetzugang:

- 802.1x- und Web-Benutzer haben den Internetzugang über das Gastnetzwerk
- VPN-Benutzer haben den Internetzugang (die IP-Adresse) über das Heimatnetzwerk

Benutzer	Docking	Authentifizierung	Internetzugang
802.1x	mit Auth.	RADIUS Hierarchie	Gastnetzwerk
VPN	ohne Auth.	Heimatnetzwerk	Heimatnetzwerk
Web	ohne Auth.	RADIUS Hierarchie	Gastnetzwerk

Hauptmerkmale der Verfahren

Aufgrund der Übereinstimmungen sowohl in Bezug auf die RADIUS-Hierarchie als auch in Bezug auf die IP-Zuteilung bei 802.1x und dem webbasierten Verfahren und der einfachen Handhabung könnte ein Gast, der sonst 802.1x verwendet, eine Verbindung auch ohne weiteres über einen Browser herstellen. Es ist aber nicht möglich, beide Verfahren über ein gemeinsames Zugangsnetz abzuwickeln.

Falls aus Sicherheitsgünden empfohlen, können die Gäste nach Freigabe des Internetzugangs auch jederzeit VPN-Verbindungen zu ihren VPN-Gateways herstellen. Bei entsprechender Konfiguration wird nur der Verkehr zu ausgewählten Netzwerken über die VPN-Verbindung geleitet, der übrige Internetverkehr wird über das Gastnetzwerk abgewickelt, was auch Zugriff auf lokale Ressourcen ermöglicht. Maschtera ist daher der Meinung, dass das VPN-Verfahren nur dann einen Sinn hat, wenn

1. bei Inbetriebnahme des Endgerätes automatisch eine VPN-Verbindung aufgebaut wird und dem Benutzer die Mühe erspart werden soll, im Gastnetzwerk ein anderes Verfahren anzuwenden,
2. Missbrauch ausschließlich mit dem Heimatnetzwerk in Verbindung gebracht werden soll. Das Gastnetzwerk darf dann allerdings **nur** das VPN-Verfahren anbieten.

Die Bereitstellung eines VPN-Zugangs erfordert aber lediglich, den Gästen den Zugang zu ihren VPN-Gateways freizugeben und ist unabhängig davon, ob das Gastnetzwerk dieses Service ihren eigenen Benutzern auch lokal vorschreibt bzw. den eigenen mobilen (externen) Benutzern anbietet.

Die Schweiz, eigentlich lange Zeit ein Verfechter der VPN-Lösung (die intern auch nach wie vor in SWITCHmobile eingesetzt wird), setzt im Bereich »eduroam« nun ebenfalls auf dot1x.

Born (2005b) schreibt dazu (S. 25): “(...) akademische Benutzer möchten flexibel und un-

kompliziert an den verschiedensten Orten Internetzugang erhalten: zu Hause, unterwegs und selbstverständlich auch auf dem Campus. Die Schweiz hat sich mit der Unterzeichnung der Bologna-Deklaration anno 1999 dazu verpflichtet, die Mobilität der Studierenden auf nationalem und internationalem Niveau nachhaltig zu verbessern.
Nebst nationalen Roamingbestrebungen (wie beispielsweise SWITCHmobile in der Schweiz) haben die oben erwähnten Umstände die Forschungsnetzwerke in ganz Europa dazu bewegt, auch auf internationalem Niveau aktiv zu werden" und zur Auswahl einer bevorzugten Methode ergänzt er (a.a.O.): "Web-Authentifizierung skaliert, ist aber leider unsicher (MITM-Attacken); VPN-Authentifizierung ist zwar sicher, skaliert jedoch nicht im Grosseinsatz (sic!); 802.1X skaliert und ist sicher, jedoch eine junge, noch nicht sehr verbreitete Technologie. Aus den zur Verfügung stehenden Technologien und deren Charakteristiken wurde 802.1X als Basis für Eduroam auserwählt."
Als weitere Gründe, die neben der Skalierbarkeit für dot1x sprechen, nennt er WPA und 802.11i, die (zukünftigen) Sicherheitsstandards im WLAN-Umfeld, in denen 802.1x eine entscheidende Rolle spielt. Er erwähnt aber auch, dass die Übermittlung der Benutzerdaten über die RADIUS-Hierarchie ein gewisses Problem im Bereich des Datenschutzes darstellt, was die verwendbaren Methoden auf zwei Kategorien einschränkt, in denen die Daten verschlüsselt zum Heimatserver übertragen werden:
Public Key (z.B. EAP-TLS mit PKI) und Tunneled Authentication (z.B. EAP-TTLS oder EAP-PEAP) wobei aufgrund des großen Aufwands EAP-TLS ausscheidet, wenn eine PKI nicht schon für andere Anwendungen vorhanden ist.
Er schreibt weiter (S. 26): "Auch SWITCH ist seit kurzem teil (sic!) von Eduroam. Im Q3/05 wurde zu Trial-Zwecken die RADIUS-Hierarchie von Eduroam um einen schweizerischen Country-RADIUS-Server ergänzt, welcher von SWITCH betreut wird. Somit steht Mitgliedern der SWITCH Community nichts im Wege, bei gegebenem Interesse eine Verbindung zu Eduroam zu etablieren."

In Österreich gibt Bauer (2005) Ende November 2005 bekannt, dass ACOnet mit zwei RADIUS-Proxy-Servern offizieller Teilnehmer an »eduroam« ist, was bedeutet, dass Universitäten und Forschungseinrichtungen im ACOnet, die 802.1x und/oder webbasierte Zugangskontrolle anbieten, nach Abschluss einer Teilnahmevereinbarung und wenn sie die Teilnahmebedingungen[19] erfüllen sofort an »eduroam« teilnehmen können.
Es erscheint dem Autor dieser Arbeit aber auch sinnvoll, wenn ACOnet am »eduroam«-Nachfolgeprojekt »GN2 JRA5: Roaming and Authorisation« aktiv teilnehmen würde.
Infos zu den Aktivitäten in Österreich finden sich auf www.ACO.net/eduroam.

19 vgl. Kapitel 5.4

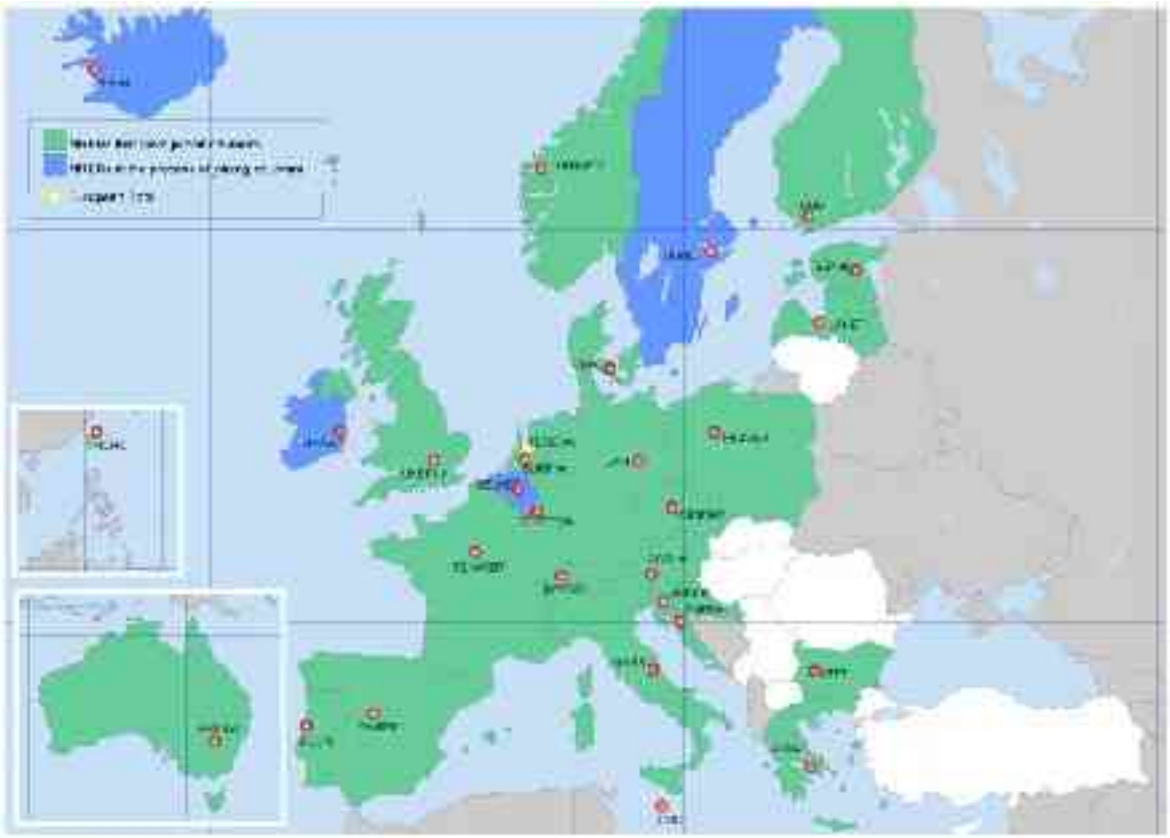

Abbildung 9: Karte der teilnehmenden Länder (Stand 10.3.2006)

Länder, die bereits an »eduroam« teilnehmen

Länder, die gerade dabei sind, sich an »eduroam« anzuschließen

Mitglieder von TERENA, die (derzeit noch) nicht an »eduroam« teilnehmen

5 Conclusio

Im Bologna-Papier »Der Europäische Hochschulraum« schreiben die Europäischen Bildungsminister (1999):
“Wir bekräftigen unsere Unterstützung (...), um (...) die folgenden Ziele, die wir für die Errichtung des europäischen Hochschulraumes und für die Förderung der europäischen Hochschulen weltweit für vorrangig halten, zu erreichen: (...) Förderung der Mobilität durch Überwindung der Hindernisse, die der Freizügigkeit in der Praxis im Wege stehen”.
Ein Weg diese angesprochene Mobilität zu erhöhen, ist der Aufbau einer europaweiten Infrastruktur, die es den Angehörigen der Forschungs- und Bildungseinrichtungen Europas ermöglicht, ohne großen Aufwand an einer Gastinstitution Zugang zu den gewohnten Ressourcen zu erlangen.
Zielgruppe für diese Arbeit sind in erster Linie die Sicherheitsbeauftragten und die Leiter der ZIDs der Universitäten und Forschungsorganisationen im ACOnet, die darüber zu entscheiden haben, ob eine Institution an dieser Infrastruktur teilnehmen will, und wenn ja, auf welche Weise und zu welchen Bedingungen.
Die NOCs der beitrittswilligen ACOnet-Teilnehmer werden die vorgestellten Technologien wahrscheinlich zum größten Teil kennen bzw. müssen die Entscheidung umsetzen; dafür ist dann eine tiefer gehende Befassung mit der Implementierung der gewählten Methode notwendig.

5.1 Die vorhandenen Lösungen

Die Bestandsaufnahme der TERENA-Arbeitsgruppe »Mobility Group« zeigte drei wesentliche Ansätze für Zugangsverfahren:

5.1.1 IEEE 802.1x

802.1x ist eine Authentifizierung an der äußeren Grenze (»edge«) des Netzes auf OSI-Layer 2[20], zusätzlich kommt EAP/EAPoL zum Einsatz, das verschiedene Authentifizierungsmethoden unterstützt.
Auch wenn hier die Entwicklung und Integration schnell fortschreitet, ist aber aus gegenwärtiger Sicht davon auszugehen, dass es auf absehbare Zeit etablierte Campusnetze bzw. WLAN-Installationen geben wird, die 802.1x nicht oder nicht durchgängig unterstützen; die Gründe hiefür liegen in erster Linie darin, dass nicht für alle Betriebssysteme Clients (gratis) verfügbar sind.
Um an einem europaweiten Roaming teilnehmen zu können, muss eine Organisation nur

20 vgl. Kapitel 2.4.3

mit ihrem NREN Kontakt aufnehmen, die Teilnahmevereinbarung unterzeichnen, den lokalen RADIUS-Server (am besten per IPsec-Tunnel) mit dem RADIUS-Proxy des NREN verbinden, den RADIUS-Server entsprechend konfigurieren, eine Website mit Informationen für die Benutzer installieren und die eigenen Benutzer z.B. in der Verwendung des Realms in Gastnetzen entsprechend schulen.
Bei entsprechender EAP-Methode und wenn auch die beteiligten RADIUS-Server entsprechend abgesichert sind, ist dot1x zwar sicher genug, es bleibt aber das Problem der eigentlich unbekannten Gäste im eigenen Netz: es ist eher eine sicherheitspolitische, als eine netzwerktechnische Entscheidung, ob man das will oder nicht.
Aktuelle Tendenzen in der »eduroam«-Community (Mobility-Mailingliste) gehen allerdings in die Richtung, dass ein Teilnehmer den Gästen alle 3 Hauptvarianten oder zumindest 802.1x anbieten **muss**[21].

5.1.2 VPN

Frühe Campus-WLANs, die auf Sicherheit Wert gelegt haben und die keine proprietäre Lösung einsetzen wollten, mussten eine VPN-basierte Lösung implementieren. Dabei wird das WLAN-Zugangsnetz (»docking network«) als VLAN vom restlichen Campusnetz entweder durch Verwendung sogenannter privater IP-Adressen oder durch Firewalls bzw. ACLs getrennt; der Client erreicht andere Netze erst nach dem erfolgreichen Aufbau eines VPN-Tunnels zu einem bekannten VPN-Gateway.
VPNs sind in der Regel übersichtlich und vergleichsweise einfach aufzusetzen, da es sich um homogene Lösungen frei verfügbarer und/oder kommerziell vertriebener Produkte handelt, die in gleicher Weise im Heimat- wie (wenn erlaubt) auch im Gastnetz eingesetzt werden können. Wenn der Besucher Zugang zum VPN-Gateway seiner Heimatorganisation erhält, dann ist er nicht von einer eventuellen VPN-Lösung im besuchten Netz abhängig: die Clients der Endnutzer müssen nur auf die eigenen Gateways abgestimmt sein und brauchen im Roaming-Fall nicht gewechselt oder umkonfiguriert zu werden, was dann auch für Applikationen gilt, die u.U. eine IP aus einem bestimmten Bereich erwarten, z.B. SMTP.
Als Lösung für Roaming wurde die Idee des »Controlled Address Space for Gateways« (CASG) entwickelt. CASG soll es ermöglichen, aus einem besuchten Zugangsnetz heraus transparent auf die Gateways der anderen Institutionen und damit auch auf jene auf dem eigenen Campus zuzugreifen, ohne die Gateways einzeln in die Zugangslisten aufnehmen zu müssen, indem je NREN ein bestimmter IP-Adressraum für die VPN-Gateways definiert wird. So ist in den ACLs maximal ein IP-Adressbereich je NREN einzutragen und diese Liste muss nur geändert werden, wenn ein neuer NREN dazukommt.

21 siehe auch Kapitel 5.4

5.1.3 Webbasierte Variante

Diese Methode ist sowohl in der Anwendung als auch in der Implementierung sehr einfach: Der Aufwand für den Betreiber ist minimal und der Benutzer braucht gar keinen speziellen Client sondern nur einen Web-Browser. Aus diesem Grund ist diese Lösung auch bei öffentlichen Hotspots üblich.
Für Roaming gelten die gleichen Bedingungen wie für 802.1x, allerdings gibt es eine ganze Reihe von zusätzlichen Schwachstellen, die teilweise relativ einfach ausgenutzt werden können, daher sollte diese Methode – wenn überhaupt – nur als »Fall-back« Verwendung finden. Wenn Sicherheit wirklich ernst genommen wird, dann wird man auf diese Variante wohl eher verzichten (müssen).

5.2 Kompatibilität der Lösungen

Roaming zwischen Einrichtungen, die jeweils das gleiche Verfahren anwenden, ist klar ersichtlich einfacher als gemischte Kombinationen.
In einer homogenen 802.1x-Kombination sollte die Authentifizierung problemlos funktionieren, wenn der zuständige RADIUS-Server im Verbund und somit auch entfernt erreichbar ist. Das gilt analog auch für Einrichtungen, die den webbasierten Zugang nutzen. Damit ist auch eine Kombination möglich: Die 802.1x- und die webbasierte Lösungen können für die Überprüfung der Zugangsdaten jeweils auf eine gemeinsame RADIUS-Hierarchie zurückgreifen, können aber nicht das gleiche Zugangsnetz verwenden, wenn die Accountdaten unter dot1x nicht im Klartext übertragen werden sollen. RADIUS-Server mit der dieser Funktionalität gibt es sowohl als kommerzielles Produkt (z.B. *Radiator*) als auch als Freeware (z.B. *FreeRadius* oder *OpenRADIUS*).
Lokale RADIUS-Server sind für DSL- oder Modemzugänge zumeist ohnehin vorhanden und können ohne viel Aufwand auch für das internationale Roaming genutzt werden.
VPN und 802.1x vertragen sich nicht, es muss daher eine physikalische oder zumindest logische Trennung (im WLAN z.B. mit unterschiedlichen SSIDs) der Zugangsnetze vorgenommen werden, dabei sollte die SSID für die 802.1x-Verbindung nicht versteckt werden, da aktuelle Windows-Clients damit Probleme bekommen könnten.
VPN und die webbasierte Lösung verwenden zwar unterschiedliche Wege der Authentifizierung, können aber ein gemeinsames Zugangsnetz nutzen, allerdings sollte – aus den bereits erwähnten Sicherheitsüberlegungen – die webbasierte Variante (nach Meinung des Autors) nicht eingesetzt werden!

5.3 Die Entscheidung

Im Wissenschaftsbereich sind verschiedene Zugangslösungen für mobile Endgeräte im Einsatz. Die einfachste und kostengünstige, leider aber auch recht unsichere Variante ist das webbasierte Verfahren. Weiters sind gegenwärtig vor allem in schon länger bestehenden WLANs mit VPN-basierten Verfahren am häufigsten anzutreffend. Diese gewährleisten ein sehr hohes Sicherheitsniveau und sind (nach Installation und Konfiguration des notwendigen Clients) relativ einfach anzuwenden, haben aber gewisse Skalierungsprobleme, die jedoch mit Verwendung von CASGs deutlich gemildert werden können.
IEEE 802.1x skaliert mit einer europaweiten RADIUS-Infrastruktur sehr gut und wird von der Wirtschaft derzeit als das Mittel der Wahl gesehen, wodurch auch laufend weitere Clients entwickelt werden, sodass man davon ausgehen kann, dass in Zukunft jedes moderne Betriebssystem 802.1x und entsprechende EAP-Varianten automatisch unterstützen wird.
Da der Aufbau einer RADIUS-(Proxy-)Hierarchie deutlich einfacher ist, als die Installation eines CASG und auch besser skaliert, hat sich die Task Force »Mobility Group« für die Variante IEEE 802.1x als primär anzustrebende Lösung für »eduroam« ausgesprochen.
In der »Joint Research Activity 5: Roaming and Authorisation« von GÉANT2 wurde ein Nachfolgeprojekt gestartet, das die Aufgaben der TERENA TF »Mobility Group« und der »AACE (Authentication and Authorisation Collaboration for Europe)« verbindet.

5.4 Teilnahmebedingungen

5.4.1 Organisation von »eduroam«

Aktuell wurde von Simonsen (2006) ein Dokument für die Richtlinien zur Teilnahme an »eduroam« in Europa vorgestellt, in dem er zuerst 3 Ebenen des »eduroam«-Verbundes definiert:

1. Ein Gremium der NRENs als »Policy Management Authority« (PMA): NRENPC
2. Eine Arbeitsgruppe aller teilnehmenden NRENs (Eduroam service group)
3. Einen operativen Ausschuss von 3-4 Personen, berufen von der Arbeitsgruppe

Die bisherige TF-mobility soll dabei die Arbeitsgruppe in ihrer Arbeit unterstützen.

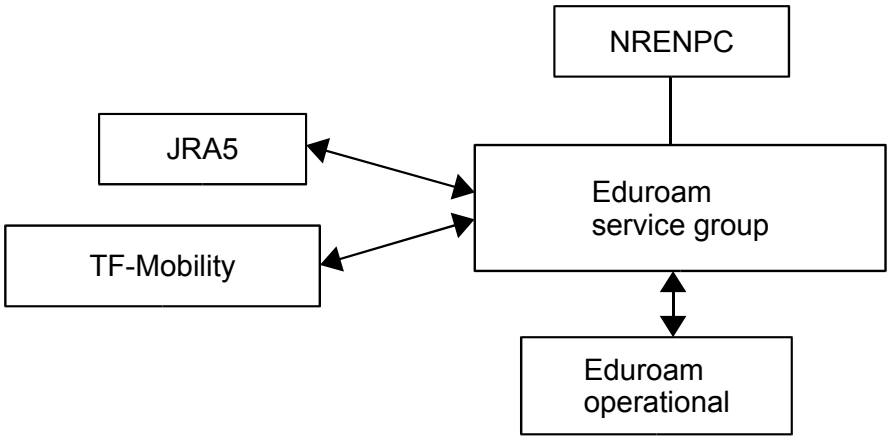

Abbildung 10: eduroam-Organisationsstruktur

Für die Teilnahme an »eduroam« sind dann nach seinem Vorschlag vier Bedingungen zu erbringen:

- Erfüllung der Sicherheitserfordernisse
- Einverständnis mit den SLAs
- Anerkennung von NRENPC als PMA für »eduroam«
- Anerkennung der »incident handling procedures« (s.u.)

die er dann noch detaillierter ausführt:

User Credentials müssen nach seinem Vorschlag end-to-end verschlüsselt werden, sodass nur der Benutzer selbst bzw. seine Heimatorganisation Zugriff auf die Daten haben.

Mitglieder des Verbundes (also die NRENs) und der Verbände (die Institutionen eines NREN), die teilnehmen wollen, müssen sich verpflichten, die Server so sicher wie möglich aufzusetzen und dem »eduroam«-Verbund zu vertrauen.

Die Mitglieder des Verbundes (also die NRENs) fordern von ihren Mitgliedern die Einhaltung der Richtlinien, diese verlangen es von den Benutzern.

Die teilnehmenden NRENs sind verpflichtet, eine mehrsprachige Webseite einzurichten und zu betreiben, auf der Informationen über die teilnehmenden Institutionen und zur Nutzung anzuführen sind. Wenn möglich soll dafür die Adresse www.eduroam.TLD[22] verwendet werden.

5.4.2 Incident Handling

Im Falle von Missbrauch oder einer Verletzung der Teilnahmebedingungen sollen bestimmte Prozeduren »zeitgerecht« durchgeführt werden – nach Meinung des Autors die größte Schwachstelle in diesem Konzept, da das sehr weit gefasst ist und die Erfahrung innerhalb ACOnets zeigt, dass schon in Österreich sehr unterschiedlich (sowohl in der Art als auch in der Geschwindigkeit) reagiert wird. Es werden außerdem keine Reaktionen

22 also z.B. www.eduroam.at

definiert, wie auf einen Verstoß gegen die lokale BBO reagiert werden soll bzw. darf.
Je nach Art der Verletzung der Richtlinien werden 4 Prozeduren vorgeschlagen:

- Nachricht an den Policy-Bereich im operativen Ausschuss
- Entscheidung über eine temporäre Sperre (Arbeitsgruppe/NRENPC)
- Entscheidung über Ausschluss (NRENPC)
- Bestätigung des Ausschlusses (NRENPC)

d.h., dass es für akute Vorfälle keine garantierten Antwortzeiten gibt (auch wenn auf Ebene der NRENs Kontaktdaten vorzusehen sind), was nur zu Unsicherheiten sowohl für den Gastgeber als auf für den Gast führen kann, weil es immer wieder zu undefinierten Zuständen kommen kann.

5.5 Österreich

Wie erwähnt, hat ACOnet mit der Installation von zwei nationalen RADIUS-Proxy-Servern die Grundlage zur Teilnahme an »eduroam« und damit auch einer nationalen Lösung auf Basis 802.1x inzwischen geschaffen[23].
Eine nationale Infrastruktur für VPN (CASG) steht in Österreich aber noch aus, obwohl – wie in den letzten Kapiteln behandelt – ja viele Gründe dafür sprechen.

5.5.1 Kriterien für die Auswahl der möglichen Zugangsverfahren

Tabellarisch werden hier nochmals alle Vor- und Nachteile der drei Hauptvarianten gegenübergestellt:

1. Webbasierte Zugangslösung

Vorteile	Nachteile
• kein spezieller Client notwendig • einfach aufzusetzen • intuitiv verwendbar • kann RADIUS-Hierarchie verwenden (gute Skalierung)	• unsicher: - MITM durch rogue Access Points - MITM durch kompromittierte Webpage - MITM durch kompromittierte RADIUS-Server - Session Hijacking über MAC-Spoofing • IP aus dem Bereich des Gastnetzes - AUP des Gastgebers unbekannt - Gast dem Gastgeber unbekannt - Abuse betrifft den Gastgeber • Logging (Gastgeber) aufwändig • Accounting sehr schwierig • Sperrung schwierig, da nur auf Account- und nicht auf Benutzerebene möglich

23 vgl. Seite 55

2. 802.1x

Vorteile	Nachteile
• Clients für viele OS verfügbar • wird von allen namhaften Herstellen unterstützt • damit Quasi-Standard für Netzzugang • kann RADIUS-Hierarchie verwenden (gute Skalierung)	• Ohne Client (oder Alternativen) kein Netzzugang • relativ unsicher: - MITM durch rogue Access Points - MITM durch kompromittierte RADIUS-Server - Session Hijacking • Sicherheit von EAP-Methode abhängig • IP aus dem Bereich des Gastnetzes - AUP des Gastgebers unbekannt - Gast dem Gastgeber unbekannt - Abuse betrifft den Gastgeber • Logging beim Gastgeber schwierig • Accounting sehr schwierig • Sperrung schwierig, da nur auf Account- und nicht auf Benutzerebene möglich

3. VPN

Vorteile	Nachteile
• ausgereifte Lösungen, Standard • Clients für viele Betriebssysteme • IP aus der eigenen Organisation - Intranet-Zugang - AUP der Heimatorganisation - Abuse betrifft Heimatorganisation - Logging/Accounting an Heimatorganisation	• Ohne Client (ohne Alternativen) kein Netzzugang • keine lokalen Services der Gastorganisation • Daten nehmen u.U. lange Umwege • ohne CASG keine internationale Skalierung

Es ist dann wohl Sache der Leiter der ZIDs zu entscheiden, zu welchen Bedingungen die einzelne Universität oder Forschungseinrichtung entweder an einer nationalen Lösung in Österreich oder an »eduroam« teilnimmt oder nicht – diese Entscheidung wird sich nach obigen Tabellen wahrscheinlich an zwei Fragen ausrichten:

1. Will die Einrichtung Gäste in ihrem Netz, die die Einrichtung nicht kennt und von denen die Einrichtung – wenn man realistisch bleibt – annehmen muss, dass ihnen die BBO der Einrichtung nicht bekannt ist?
   Wenn nein, dann bleibt als Lösung für das Zugangsnetz nur VPN
2. Will die Einrichtung, dass die User Credentials ihrer eigenen Angehörigen einen u. U. unsicheren Weg nehmen und möglicherweise kompromittiert werden?
   Wenn nein, dann bleibt (ohne PKI) als Lösung für den remote Access nur VPN

Oder anders ausgedrückt: wenn eine Teilnahme an »eduroam« in Zukunft nur dann möglich sein sollte, wenn man alle drei Varianten (oder zumindest 802.1x) anbietet, so muss man als Gastgeber folgende Punkte akzeptieren:

1. Gäste bekommen (wenn sie nicht VPN verwenden) eine IP aus dem Gastnetz, damit landen auch Abuse-Meldungen primär beim Gastgeber
2. Sitzungen von Gästen, die webbasierten Zugang verwenden, können relativ leicht von anderen Benutzern des Zugangsnetzes übernommen werden, Beschwerden landen wieder beim Gastgeber, der dem nur schwer nachgehen kann

Ist einer dieser Punkte nicht akzeptabel, so scheidet »eduroam« im Sinne einer Komplettlösung bzw. mit 802.1x als einziger Lösung aus und man muss eine nationale oder auch internationale Kooperation für VPN-Lösungen, also einen CASG, anstreben.
Als Heimatorganisation muss man sich darüber im Klaren sein, dass die User Credentials der eigenen Benutzer in Gastnetzen bei Verwendung von webbasierten Lösungen nicht bzw. bei 802.1x nur bedingt sicher sind, da an mehreren Stellen MITM-Attacken gestartet werden können. Auch hier ist es dann eine Frage der subjektiven Sicherheitseinstufung, ob man andere Lösungen als VPN anbieten möchte oder nicht.

5.5.2 Empfehlung für die TU Graz

Um nun zum Abschluss der Arbeit wieder zum Ausgangspunkt zurück zu kehren:
Wie soll die TU Graz an dieser Infrastruktur teilnehmen?

Aufgrund oben angeführter Überlegungen lautet die Empfehlung des Autors:
Gästen an der TU Graz sollen 2 Arten von Zugängen geboten werden:

1. Web-Surfen auf Seiten in einem definierten DNS- oder IP-Bereich über den HTTP-Proxy der TU Graz (also eine Art CASG für Webserver, für Universitäten in Österreich an der TU Graz bereits realisiert), inkludiert somit auch »clientless VPN«
2. Zugriff per VPN auf definierte VPN-Gateways (CASG oder lokale Liste)

Den Angehörigen der TU Graz wird aufgrund unseres Prinzip der »Single Credentials« empfohlen, an Gastorganisationen ebenfalls nur VPN zu verwenden, solange es keine Lösung mit OTP in TUGonline gibt.
Eine Teilnahme an »eduroam« mit verpflichtendem 802.1x muss abgelehnt werden, weil der Aufwand, der bei uns aufgrund unserer BBO für Accounting und Logging sowie die Verfolgung von Missbrauch entsteht, zu groß ist.
An einer Lösung mit VPN besteht aber großes Interesse. Sollte ACOnet kein CASG zur Verfügung stellen (s.u.), so erklärt sich der ZID der TU Graz bereit, eine Liste der VPN-Gateways für Österreich zu pflegen.

5.5.3 Empfehlung für ACOnet

Der Autor kann anderen ACOnet-Teilnehmern keine Empfehlung für oder gegen die Teilnahme an »eduroam« geben, das liegt wie schon erwähnt in der Verantwortung der jeweiligen ZIDs.
Bei Teilnahme an »eduroam« muss aber ACOnet als NREN und jeder Teilnehmer alles anbieten, was in der jeweils gültigen Version der »eduroam«-Policy vorgeschrieben ist, ACOnet kann aber natürlich bei aktiver Teilnahme an »eduroam« bzw. dem Nachfolgeprojekt auch Einfluss auf diese Policy nehmen.

Unabhängig von einer Teilnahme an »eduroam« ist aber aufgrund der Ergebnisse der Umfrage[24] im ACOnet (zusätzlich) eine Lösung anzustreben, die auch für diejenige Teilnehmer akzeptierbar ist, die Gästen keine IP aus ihrem Bereich zur Verfügung stellen wollen oder aus unterschiedlichen Gründen weiter auf VPN setzen.
Wenn es ein CASG für ACOnet gibt, dann ist es relativ einfach, dieses bei Bedarf mit den vorhandenen CASGs anderer NRENs zu verbinden und beispielsweise für den DACH-Bereich für VPN eine Roaming-Infrastruktur als Ergänzung zur RADIUS-Hierarchie aufzubauen. Dadurch würden dann auch Forschungseinrichtungen, die auf VPN setzen, am Roaming (zumindest begrenzt) teilnehmen können.
Dass auch international immer noch an der Entwicklung von CASGs Interesse besteht, kann man der noch immer aktiven Mailingliste mobility@terena.nl bzw. dem webbasierten Archiv der Liste auf http://www.terena.nl/mail-archives/mobility/ entnehmen.

Ob eine CASG-Infrastruktur (wie in den früheren Besprechungen geplant) umgesetzt wird oder nicht, liegt an den zentralen Stellen im ACOnet oder anders ausgedrückt: am ZID der Universität Wien.
Für eine rein österreichische Lösung würde aber schon eine Liste der VPN-Konzentratoren, die (halb-)automatisch in die ACLs übernommen werden könnte, durchaus ausreichen – diese Entscheidung sollte die Technische Betriebs- und Planungsgruppe für ACOnet (TBPG) im Zuge ihrer nächsten Sitzung im Juni 2006 treffen.

Abschließend empfiehlt daher der Autor den Verantwortlichen im ACOnet zusätzlich zur RADIUS-Infrastruktur auch einen CASG anzubieten und nochmals über die Möglichkeit eines ACOnet-weiten Docking-Netzes in der Verantwortung von ACOnet nachzudenken.

24 vgl. Kapitel 2.3

6 Glossar

AAA

oder »Triple A«: Authentication, Authorization, Accounting
(also Authentisierung, Autorisierung und Abrechnung: Wer? Was? Wie viel?)

ACD

Access Control Device;
Ein Gerät, das die Zugangskontrolle durchführt

ACL

Access Control List;
Zugriffsliste; Einfache Form einer Firewall

ACOnet

Austrian Academic Computer Network;
Österreichs Datennetz für Wissenschaft, Forschung und Lehre; NREN

AES

Advanced Encryption Standard;
Symmetrisches Verschlüsselungsverfahren;
In den USA als Standard zugelassen, für IEEE 802.11i vorgesehen

Airsnort

Freies Tool, um WLAN-Traffic zu entschlüsseln

AP

Access Point;
Hardware, die i. A. als Hub zwischen drahtloser und drahtgebundener Kommunikation dient

A-Select

Das »A-Select Authentication System« ist ein innovatives ASP-Konzept, das von SURFnet entwickelt wurde

ASP

Hier im Sinne von Application Service Provider gebraucht;
Ermöglicht authentisierten Zugang zu Diensten über einen Webbrowser;
im Falle von HTTPS spricht man dann auch von »clientless VPN«

AUP

Acceptable Use Policy;
BBO

BBO

Betriebs- und Benutzungsordnung;
AUP

Captive Portal

fängt HTTP-Requests ab und leitet auf andere Seiten um (Web-Redirect)

CARNet

NREN von Kroatien, vgl. ACOnet;

CARP

Common Address Redundancy Protocol;
Ermöglicht, dass sich mehrere Geräte eine MAC- und eine IP-Adresse teilen

CASG

Controlled Address Space for Gateways;
Liste von Netzwerkadressen vertrauenswürdiger VPN-Konzentratoren

CERT

Computer Emergency Response Team;
Organisation, die z.B. auf AUP-Vorfälle und Malware reagiert

CHAP

Challenge Handshake Authentication Protocol;
Ein Authenitifizierungsprotokoll aus der PPP-Familie, das das Passwort – im Gegensatz zu PAP – nicht im Klartext überträgt

DACH

Kurzbezeichnung für Deutschland, Österreich und Schweiz

Deliverable

Ausdruck im Projektmanagement; physikalisches Produkt einer Projektarbeit, i. A. eine Zusammenfassung der Ergebnisse

DFN

Deutsches Forschungsnetz;
Ähnliche Aufgaben wie ACOnet in Österreich

DHCP

Dynamic Host Configuration Protocol;
Ein Protokoll, das Netzwerkkomponenten u.a. ihre IP-Adresse automatisch zuweist

docking network

Zugangsnetz:
Das Netzwerk, in dem (WLAN-fähige) Geräte physikalischen Zugang erhalten

DoS

Denial of Service;
Angriffsszenario, in dem ein Dienst (Service) ausgeschaltet werden soll, indem entweder der Dienst selbst direkt angegriffen wird oder aber dadurch, dass der Server, auf dem der Dienst läuft, unerreichbar gemacht werden soll

dot1x

IEEE 802.1x

EAP

Extensible Authentication Protocol; RFC 2284;
Ein PPP-Authentifizierungsprotokoll, das es erlaubt, beliebige andere Authentisierungsprotokolle einzubinden, die dann erst nach der Link Control Phase aufgerufen werden

EAPoL

In OSI-Layer 2 verpackte EAP-Pakete

EAP over RADIUS

In RADIUS verpackte EAP-Pakete

eduroam

Education Roaming;
Infrastruktur für inter-institutionales Roaming

Ethernet

Vernetzungstechnologie für lokale Netze

Federating Software

ASP (Application Service Provider)

FEIDE

FEderated ID for Education;
Zentrale PKI Norwegens

Firewall

Ein Set von Netzwerkkomponenten (Hard- und/oder Software), das die Ressourcen eines (privaten) Netzwerks vor Angriffen aus anderen Netzwerken schützt

GÉANT

Europäisches Gigabit-Netzwerk der NRENs

GPL

GNU Public License;
Lizenzmodell der Free Software Foundation für freie Software

Greenspot

Eine Clearing- oder Verrechnungsstelle für Roaming zwischen verschiedenen WISPs

GSM

Global System for Mobile Communications;
Funknetz-Standard im Bereich von 450 bis 1900 MHz

GUI

Graphical User Interface;
Grafische Benutzeroberfläche (z.B. Windows) bzw. Programme, die auf einer solchen Oberfläche aufsetzen

Heimatorganisation, Heimorganisation, Home Institution

Die Organisation, an der der Benutzer registriert ist und an der der Benutzer normalerweise arbeitet

Hotspot

Öffentlicher Wireless AP (z.B. in Hotels und Restaurants oder auf Flug- und Bahnhöfen)

Identity Provider

Die Organisation, die die Accountdaten des Benutzers verifizieren kann, i. A. also seine Home Institution

IEEE

Institute of Electrical and Electronics Engineers (»I Triple E«);
Berufsverband von Ingenieuren aus den Bereichen Elektrotechnik und Informatik. Bildet Gremien für die Standardisierung von Technologien

IEEE 802

IEEE-Projekt, gestartet im Februar 1980 (daher der Name), das Standards im LAN auf OSI-Schicht 1 und 2 definiert

IEEE 802.1x

IEEE-Standard zur Authentifizierung in Rechnernetzen am Netzwerkzugang. Jedem physischen Anschluss werden 2 logische Anschlüsse (Ports) zugeordnet: ein freier Port und ein kontrollierter Port, der nur nach einer Authentisierung (am freien Port) erreichbar ist

IEEE 802.11

IEEE-Standard zur Nutzung drahtloser Netzwerkkommunikation;
definiert den physikalischen und den MAC-Layer.
WEP ist Bestandteil dieses Standards

802.11a	54 Mbps im 5 GHz-Band
802.11b	11 Mbps im 2,4 GHz-Band
802.11g	54 Mbps im 2,4 GHz-Band
802.11h	erweitertes 802.11a
802.11i	Authentifizierung und Verschlüsselung für a/b/g/h: 802.1x, WPA, AES

IETF

Internet Engineering Task Force;
Entwickelt Internetstandards (hauptsächlich im Bereich TCP/IP)

IKE

Internet Key Exchange;
Protokoll zur automatischen Schlüsselverwaltung in IPsec

IKT

Informations- und Kommunikationstechnologie;

IP

Internet Protocol;
Das dem Internet (mit TCP) zu Grunde liegende Protokoll;
Die derzeit aktuelle Version 4 wird in absehbarer Zeit von Version 6 (IPv6) abgelöst werden

IPA

Internet Privatstiftung Austria;
Gemeinnützige Stiftung der ISPA

IPsec

Protokoll, das die Sicherheitsschwächen von IP lösen soll

ISO

International Organization for Standardization;
internationale Vereinigung der Standardisierungsgremien

ISP

Internet Service Provider;
Zugangsprovider

ISPA

Internet Service Provider Austria;
Verband der österreichischen Internet-Anbieter

L2TP

Layer 2 Tunneling Protocol;
Verschlüsselungsprotokoll der IETF (RFC 2661)

LAN

Local Area Network;
räumlich begrenztes Computernetzwerk

LDAP

Lightweight Directory Access Protocol;
Netzwerkprotokoll, das die Abfrage und die Modifikation von Informationen eines Verzeichnisdienstes (*Directory*) erlaubt

LEAP

Lightweight EAP; Cisco-Wireless EAP

MAC-Adresse

Media Access Control address;
ursprünglich als eindeutige Kennung der Netzwerkkarte (NIC) gedacht

Malware

Schadensprogramme;
Das »Böse« im Internet: Viren, Würmer, Trojaner, ..

Mbps

Megabit per Second; Mbit/s; Mb/s;
Daten(übertragungs)rate

MIC

Message Integrity Check;
»Michael«-Algorithmus

MIPv6

Mobile IPv6;

MITM

Man-In-The-Middle;
Angriffsszenario, in dem versucht wird, sich in die Kommunikation zwischen zwei Partnern unbemerkt einzuschleichen, um Daten abzufangen oder abzuändern

MPLS

Multiprotocol Label Switching;
Protokoll unterhalb des IP-Layers; kapselt Layer-2 und -3 Protokolle

NAD, NAS

Network Access Device (bzw. Server);
ACD zum (lokalen) Netzwerk

NAT

Network Address Translation;
(Gewünschte) Änderung einer IP-Adresse, z.B. um private auf öffentliche IP-Adressen abzubilden

NIC

Network Interface Card;
Die Netzwerkkarte; das Verbindungselement zwischen Netzwerkkomponente (z.B. PC, Switch, ...) und Netzwerk

NOC

Network Operations Center;
Netzwerkabteilung einer Einrichtung

NREN

National Research and Education Network;
Nationale Forschungsnetze – z.B. ACOnet in Österreich

NRENPC

NREN Policy Committee;
Die PMA für eduroam in Europa

NRPS

National RADIUS Proxy Server;
Proxy-Server auf Ebene eines NREN

O(1), O(n), O(n²)

Ordnung; beschreibt den Aufwand, der (in den Beispielen) entweder konstant, linear oder quadratisch mit der Anzahl der beteiligten Organisationen wächst

OpenVPN

Freie softwarebasierte VPN-Variante, die es für (nahezu) alle gängigen Betriebssysteme gibt

ORPS

Organisational RADIUS Proxy Server;
RADIUS-Server einer an eduroam teilnehmenden Organisation

OSI-Modell

Open Systems Interconnection Reference Modell;
7-Schichten-Modell für die Datenkommunikation;
TCP/IP fasst mehrere dieser 7 Schichten zusammen, wodurch es real dann nur 4 Schichten gibt

OTP

One Time Password;
Passwörter, die nur in einem bestimmten Zeitfenster einmal gültig sind

PAP

Password Authentication Protocol;
Protokoll aus der PPP-Familie, das auf einer klartextlichen Übertragung von Benutzername/Passwort basiert

PAT

Port Address Translation;
Eine spezielle Form von NAT, in der nicht nur die IP-Adressen, sondern auch Portnummern umgeschrieben werden

PEAP

Protected EAP;
Erweiterung von EAP durch die IETF;
Quasi-Standard durch *Microsoft* und *Cisco*;
TLS-Tunnel ohne Authentifizierung des Clients (ähnlich wie HTTPS)

PKI

Public Key Infrastructure;
System zur Generierung, Prüfung und Verwaltung digitaler Zertifikate

PMA

Policy Management Authority;
Legt die Richtlinien und Bedingungen für die Teilnahme an einem Projekt fest

Port

Anschlussbuchse an Netzwerkkomponenten

Portnummer

Adresskomponente, um z.B. in TCP Datenpakete den richtigen Diensten (Protokollen) zuzuordnen

PPP

Point-to-Point Protocol;
Protokoll zum Verbindungsaufbau (hauptsächlich für Wählleitungen)

PPPoE

PPP over Ethernet;
Aufbau einer Punkt-zu-Punkt-Verbindung über Ethernet (also »lokal«);
benötigt keine initiale IP-Adresse, arbeitet auf OSI-Layer 2

PPTP

Point To Point Tunneling Protocol;
benötigt eine IP-Adresse, arbeitet auf OSI-Layer 3

Protokoll

Exakte Vereinbarung, wie Daten zwischen Computern bzw. Prozessen ausgetauscht werden

Proxy-Server

Bearbeitet Anfragen nicht selbst, sondern leitet sie stellvertretend (z.B. aufgrund eines Realms) an andere Server weiter

PSK

Pre-shared Key;
unsichere Methode von WEP; arbeitet mit einem vordefinierten Schlüssel

RADIUS

Remote Authentication Dial In User Service;
Ein AAA-Dienst mit zugehörigem Protokoll.
Spielt z.B. mit LDAP-Servern zusammen; wird in vielen RFCs behandelt

RAS

Remote Access Server;
ACD zum Netzwerk i. A. über Wählleitungen

Realm

(Eindeutige) Kennzeichnung der Zugehörigkeit zu einem Bereich;
wird i. A. hinter einem »@« an den Benutzernamen gehängt;
der Benutzername schaut dann u.U. aus wie eine E-Mail-Adresse:
user.realm@domain oder user@realm.domain RFC 4282

Relay-Network

CASG

RFC

Requests for Comments der IETF;
Definieren (durch ihre Akzeptanz) quasi Internetstandards

Roaming

WLAN Roaming

ist die Möglichkeit, sich mit einem WLAN-fähigen Gerät von einem AP zum anderen zu bewegen, ohne dass die Verbindung abreißt (besser: *Handover*)

Wireless Roaming

ist die Möglichkeit, mit den eigenen Benutzerdaten an einer fremden Ein-

richtung Zugang zu Ressourcen im Netzwerk zu erlangen

Rouge Access Point

Ein unbekannter AP, der nur vorgibt, zur Infrastruktur zu gehören

Shibboleth

Shibboleth ist ein standardisiertes Verfahren zur verteilten Authentifizierung und Autorisierung für Webanwendungen und Webservices mit SSO

Single Credentials

ähnlich wie bei SSO gibt es für viele Dienste die gleichen User Credentials

SLA

Service Level Agreement;
Vereinbarungen zum Thema Verfügbarkeit bzw. Reaktionszeit

SOHO

Small Office, Home Office;
Klein- und Mittelunternehmen (KMU), Heim-Benutzer

Spam

Unerwünschte (Massen-)E-Mails

SSID

Service Set Identifier;
(unverschlüsselte) Kennung eines Funknetzwerkes

SSL

Secure Sockets Layer;
Verschlüsselungsprotokoll für Datenübertragungen im Internet

SSO

Single Sign On;
Zugriff auf unterschiedliche Dienste mit nur einmaliger Authentifizierung

SURFnet

Forschungsnetz der Niederlande;
NREN wie ACOnet, DFN und SWITCH

SWITCH

Schweizer Forschungsnetz;
NREN wie ACOnet, etc.

TCP

Transmission Control Protocol;
Protokoll, das den Datenaustausch z.B. im Internet definiert

TERENA

Trans-European Research and Education Networking Association;
Vereinigung europäischer NRENs zur Entwicklung und Verbesserung der IKT-Infrastruktur in Forschung und Lehre

TKIP

Temporal Key Integrity Protocol;
eine (sicherere) hardwarekompatible Erweiterung von WEP.
Bestandteil von WPA

TLD

Top Level Domain;
Endung von Internetadressen.
Unterscheidung nach »country-code« (ccTLD, z.B. at, de), »generic« (gTLD, z.B. com) bzw. »sponsored« (sTLD, z.B. jobs)

TLS

Transport Layer Security;
Standardisierte Weiterentwicklung von SSL

TRPS

Top level RADIUS Proxy Server;
Übergeordneter RADIUS-Proxy-Server von TERENA

TTLS

Tunneled TLS;
Ähnlich wie PEAP eine Erweiterung von EAP-TLS

User Credentials

Berechtigungsnachweis; i. A. Benutzername und Passwort

Visited Institution

Die Organisation, die der Benutzer »besucht« und die ihm physikalischen Netzzugang (*visited Network*) gewährt

VLAN

Virtual LAN;
Über geeignete Netzwerkkomponenten können virtuell getrennte Netze betrieben werden, die dann logisch getrennt sind

VoIP

Voice over IP;
IP-Telefonie; Sprache über das Datennetz

VoWLAN

Voice over WLAN;
Sprachdaten über das WLAN

VPN

Virtual Private Network;
Ein Computernetz, das zum Transport privater Daten ein öffentliches Netz (zum Beispiel das Internet) nutzt, in dem die Daten dann wie in einem LAN (aber zumeist verschlüsselt) übertragen werden

VPN-Konzentrator, VPN-Server, VPN-Gateway

Server für VPN; terminiert VPN-Verbindungen (Gegenstück: VPN-Client)

Web based login

Authentifizierungsmethode, in der nur ein Browser gestartet werden muss. Der Aufruf einer beliebigen Seite wird auf ein Anmeldungsformular auf einem Server umgeleitet, der dann bei erfolgreicher Authentifizierung die ACLs entsprechend modifiziert; Captive Portal

WEP

Wired Equivalent Privacy;
Veralteter Standard-Verschlüsselungsalgorithmus für WLANs.

Wi-Fi Alliance

Organisation aus vielen im Bereich WLAN angesiedelter Unternehmen, die es sich zur Aufgabe gemacht hat, Produkte unterschiedlicher Hersteller auf der Basis IEEE 802.11 zu zertifizieren und damit die Interoperabilität verschiedener WLAN-Geräte zu gewährleisten.

WISP

Wireless ISP;
Hotspot-Betreiber

WLAN

Wireless LAN;
Lokales Funknetz auf Basis IEEE 802.11

WPA

Wi-Fi Protected Access;
Soll die schwache WEP-Verschlüsselung ersetzen;
verwendet TKIP, EAP und IEEE 802.1x;
verlangt im Enterprise-Mode zwingend RADIUS

WPA2

entspricht im Enterprise-Mode weitgehend IEEE 802.11i

ZID

Zentraler Informatikdienst;
Dienstleistungseinrichtung im Bereich IKT an Universitäten

7 Bibliographie

Al-Atassi, T. (2004). UNIL's Wireless Local Area Network and SWITCHmobile. SWITCH-journal, Juni, 35-37.

Bauer, K. (bauer@cc.univie.ac.at). (28.10.2005). [eduroam] EDUroam membership. E-Mail an die eduroam-Mailingliste im ACOnet (eduroam@noc.aco.net)

Bormann, C., Paffrath, R., Pollem, N. & Rauschenbach, J. (2003). WLAN-Roaming im Europäischen Wissenschaftsbereich. DFN Mitteilungen, 63, 12-15.

Born, H. (2005a). Meilenstein der e-Academia: Studenten surfen an öffentlichen Hotspots gratis. SWITCHjournal, November, 22-24.

Born, H. (2005b). Eduroam. SWITCHjournal, November, 25-26.

Dobbelsteijn, E. (2003). Deliverable D. Inventory of 802.1X-based solutions for inter-NRENs roaming, Version 1.2 (online) http://www.terena.nl/activities/tf-mobility/deliverables/delD/DelD_v1.2f.pdf (28.1.2006)

Europäische Bildungsminister (1999). Der Europäische Hochschulraum. Gemeinsame Erklärung der Europäischen Bildungsminister, Bologna.

Florio, L., Sankar, J., Simonsen, D. & Wierenga, K. (2004). Deliverable I. TF-Mobility roaming policy document. Version 1.2 (online) http://www.terena.nl/activities/tf-mobility/deliverables/delI/Roaming_policy_document_v.1.2.pdf (28.1.2006)

Hofherr, M. (2005). WLAN-Sicherheit. Professionelle Absicherung von 802.11-Netzen. Hannover: Heise Zeitschriften Verlag GmbH & Co KG

Howlett, J. (2002). The University of Bristol's Nomadic Network (online). http://www.ukerna.ac.uk/services/events/archive/2002/network-access/nomadic-network.pdf (4.2.2006)

Howlett, J. (2005). UKERNA LIN Service Technical Specification. Version 0.87 (online). http://www.terena.nl/mail-archives/mobility/pdfr41cg7ooOS.pdf (4.2.2006)

Howlett, J. & Skelton, N. (2003). The Nomadic Network. Providing Secure, Scalable and Manageable Roaming, Remote and Wireless Data Services (online). http://www.terena.nl/activities/tf-mobility/TNC03/Josh.ppt (4.2.2006)

IEEE-SA (2006). Get IEEE 802® - IEEE 802.11 LAN/MAN Wireless LANS (online). http://standards.ieee.org/getieee802/802.11.html (28.1.2006)

Kahler, U. (2001). DFN@home. Direkter Draht zur Uni. DFN Mitteilungen, 56, 4-5.

Kamrat, I., Peter, R. O. & Krapf, W. (2002). Ausschreibungsunterlagen Wireless LAN an der TU Graz (online). http://www.zid.tugraz.at/ki/netz/extern/wlan/ausschreibung.html (14.1.2006)

Keski-Kasari, S. & Harri Huhtanen, H. (2003). Deliverable F. Inventory of web-based solution for inter-NREN roaming, Version 1.1 (online) http://www.terena.nl/activities/tf-mobility/deliverables/delF/DelF-f.pdf (28.1.2006)

Kienholz, U. (2002). SWITCHmobile – Connecting Mobile Users. SWITCHjournal, 2, 4-6.

Kienholz, U. (2003). Deliverable E. Inventory of VPN-based Solutions for Inter-NREN Roaming, Revision 4.4 (online) http://www.terena.nl/activities/tf-mobility/deliverables/delE/DeliEv4.4-np.pdf (28.1.2006)

Koller, S. (2004). Das WLAN abg. net.guide, 01, 15-17.

Krutak, G. (2003). Ist Sicherheit im WLAN machbar? net.guide, 03, 20-22.

Lienhardt, J. (2005). Verteilte Authentifizierung, Autorisierung und Rechteverwaltung (AAR). Aufbau einer AAR-Infrastruktur unter Verwendung von Shibboleth. DFN Mitteilungen, 69, 26-27.

Linden, M. & Viitanen, V. (2005). Roaming Network Access Using Shibboleth (online). http://www.terena.nl/publications//tnc2004-proceedings/papers/linden.pdf (4.2.2006)

Maschtera, W. (wilfried.maschtera@zid.uni-linz.ac.at) (26.6.2002). Re: wlan and roaming. E-Mail an Peter, R. O. (Reinfried.Peter@TUGRAZ.AT)

Maschtera, W. (wilfried.maschtera@maschtera.at) (28.8.2005). Re: [eduroam] Diplomarbeit. E-Mail an Peter, R. O. (Reinfried.O.Peter@TUGraz.at)

Nestvogel, J. & Hoelzner, K. (2002). Schneller Wechsel. DFN Mitteilungen, 58, 6.

Paffrath, R. (2002). Sicheres Roaming. DFN Mitteilungen, 60, 12-14.

Paffrath, R. (2004). DFNRoaming goes Plug'n'Play. DFN Mitteilungen, 66, 10-11.

Paffrath, R. (2005). DFNRoaming praktisch sicher. DFN Mitteilungen, 69, 24-25.

Pattloch, J. & Paffrath, R. (2003). DFNRoaming – Unterwegs ins Wissenschaftsnetz. DFN Mitteilungen, 63, 4-5.

Peter, G. (2003). Roaming für das Deutsche Forschungsnetz. DFN Mitteilungen, 63, 3.

Rauschenbach, J., Bormann, C. & Pollem, N. (2003). Deliverable C. Requirements definitions for inter-NREN roaming, Version 1.4 (online). http://www.terena.nl/activities/tf-mobility/deliverables/delC/DelC1-4.pdf (28.1.2006)

Sankar, J. & Chown, T. (2003). Deliverable G. Preliminary selection for inter-NREN roaming, Version 1.0 (online) http://www.terena.nl/activities/tf-mobility/deliverables/delG/DelG-final.pdf (28.1.2006)

Sankar, J. & Wierenga, K. (2004). Inter-NREN roaming. Final Report (online) http://www.terena.nl/activities/tf-mobility/deliverables/TF-MobilityfinalReport.pdf (28.1.2006)

Sikora, A (2002). Sicherheit im WLAN. TecCHANNEL.de (online). http://www.tecchannel.de/netzwerk/sicherheit/401879/ (14.1.2006)

Singh, S (2000). Geheime Botschaften – Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. München, Wien: Carl Hanser Verlag SBN 3-446-19873-3

Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J. & Lear, E. (1996). Address Allocation for Private Internets (online). http://www.ietf.org/rfc/rfc1918.txt (14.1.2006)

Schmidt, M. (Markus.Schmidt@one.at). (21.12.2005). WLAN Kooperation. E-Mail an Peter, R. O. (Reinfried.O.PETER@TUGraz.at)

Simonsen, D. (2006). European eduroam confederation policy (online). http://www.terena.nl/mail-archives/mobility/pdfOa8Tsrqmwz.pdf (30.1.2006)

Telekom & IT Report (2003). WLAN-Roaming. 5, 9.

Ullmann, K. (2001). Netze für mobile Nutzer. DFN Mitteilungen, 57, 6.

Vrtala, A. (2005). Security: Risikomanagement, Angriffsmethoden, Schutz. Skriptum zur Vorlesung an der Donau-Universität Krems, 53.

Wein, R. (2003). Greenspot. Ispa-news, 2, 13-14.

Wierenga, K. (2004). Deliverable H. Testbed and reference design for inter-NREN roaming, Version 1.0 (online) http://www.terena.nl/activities/tf-mobility/deliverables/delH/DelHv1.0.pdf (28.1.2006)

Wissenschaftsnetz in Zahlen (2005), DFN Mitteilungen, 68, 8-9.

8 Anhang

8.1 Umfrage unter den ACOnet-Teilnehmern

Folgendes Datenblatt liegt den Ergebnissen im Kapitel 2.3 zu Grunde:

1. Organisation:	
2. Kontakt:	Name: E-Mail:
3. Teilnahmewunsch:	○ ja ○ nein
4. WLAN vorhanden:	○ ja ○ nein ○ geplant ○ nicht geplant
5. RADIUS vorhanden:	○ ja ○ nein
6. RADIUS-Server:	Server-Typ: unterstützt □ EAP □ EAP-MD5 □ EAP-SIM □ EAP-TTLS □ EAP-PEAP □ LEAP andere Features:
7. Zugang ins WLAN:	□ frei □ MAC □ WEP □ 802.1x □ Web Redirect □ VPN andere Zugriffsbeschränkungen:
8. SSIDs:	○ verborgen ○ nicht verborgen unterschiedliche SSIDs: ○ ja ○ nein Falls ja, Zweck:
9. Vom WLAN ins Netz:	□ frei □ userabhängig □ NAT □ VPN andere Netz-Zugangsbeschränkungen
10. Securitypolicy:	erlaubt unbekannte Personen im eigenen Netz: ○ ja ○ nein ○ spezielles VLAN andere Policies:
11. Ergänzungen:	

8.2 Access Point- und VLAN-Konfiguration

Wie bereits an mehreren Stellen in dieser Arbeit erwähnt, muss man – wenn man alle drei der Hauptvarianten anbieten will – mehrere (logische) Zugangsnetze anbieten:
Dies kann entweder dadurch geschehen, dass man (falls die Access Points nicht mehr als eine SSID zulassen bzw. keine VLAN-Fähigkeit besitzen) wirklich zwei physikalisch getrennte WLANs mit eigenen Access Points aufbaut, oder indem man (über SSIDs) logisch getrennte VLANs im WLAN einsetzt.
In der weiteren Folge wird hier nur der Fall von mehreren SSIDs auf Access Points behandelt, der Fall mit getrennten WLANs ergibt sich analog.

8.2.1 Übersicht

Aufgrund der unterschiedlichen Charakteristiken (Layer 2 bzw. Layer 3) müssen zumindest 2 VLANs (mit assoziierten SSIDs) angeboten werden:

- ein VLAN für 802.1x
- ein VLAN, mit dem sich die VPN-Clients und die clientlosen Benutzer verbinden

Diese beiden VLANs werden über einen 802.1q-Trunk zu einem Layer-3-Switch geführt, der dann entscheidet, was mit den Paketen zu geschehen hat:
Im Falle von 802.1x muss (über die RADIUS-Hierarchie) bestimmt werden, ob der Client Netzzugang (eine IP-Adresse) erhält oder nicht.
Im anderen VLAN wird per DHCP schon vorab eine IP vergeben, im Falle von VPN (und CASG) erlaubt der Switch Kommunikation nur mit den definierten VPN-Konzentratoren, für webbasierten Zugang leitet der Switch den ersten HTTP-Request auf eine interne (HTTPS gesicherte) Webpage um, die dann eine Authentifizierung (über die RADIUS-Hierarchie) durchführt und am Switch entsprechende ACLs installiert.

8.2.2 Konfigurationsbeispiel

SSID	VLAN-ID	Zweck	Parameter
	108	VLAN für Access Points, RADIUS server	
web-vpn	163	VPN und webbasierter Zugang	offen, kein WEP, DHCP
802.1X	117	802.1x	802.1X, WEP, DHCP

Die VLAN-IDs sind dabei jene, wie sie bei SURFnet eingesetzt werden (diese sind aber frei wählbar), die Bezeichnungen der SSIDs sind derzeit von NREN zu NREN noch verschieden, hier wäre eine Vereinheitlichung wünschenswert, Simonsen (2006) schlägt für 802.1x als SSID »eduroam« vor.

Da bei 802.1x die Zuteilung des VLANs bzw. der IP-Adresse ja erst nach erfolgreicher Authentifizierung erfolgt, ist eine weitere Unterteilung dieses Bereichs z.B. in Gäste und Angehörige der eigenen Organisation (oder auch noch granularer) denkbar:

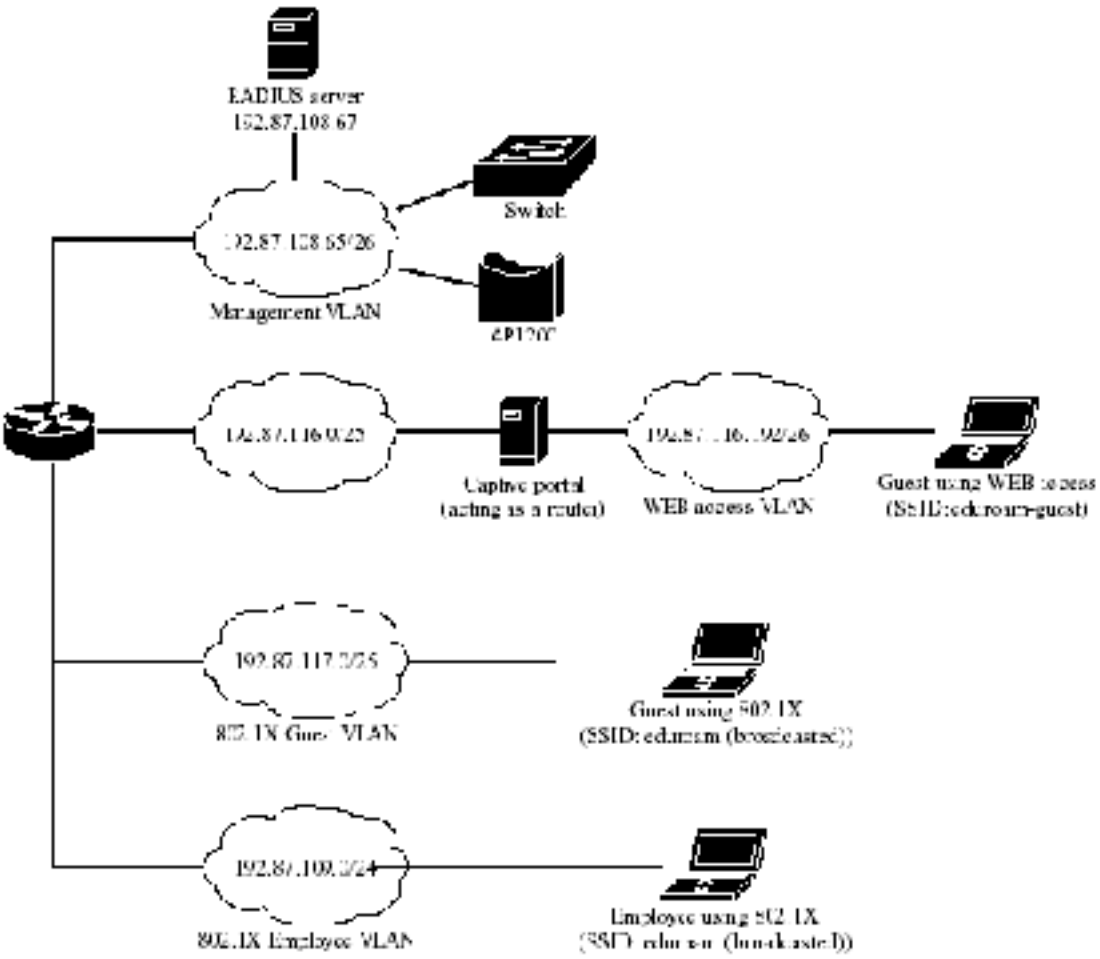

Abbildung 11: Netz-Design auf OSI-Ebene 3

Dieses Design auf OSI-Ebene 3 – WEB-access (Sic!) bezeichnet hier den webbasierten Zugang – basiert dabei auf folgendem Konzept auf Ebene 2:

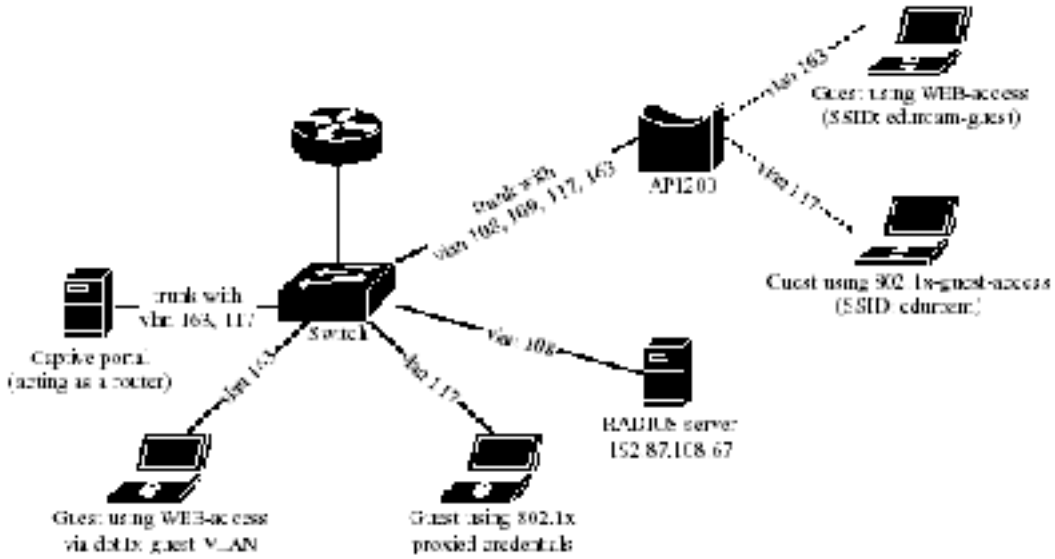

Abbildung 12: Netz-Design auf OSI-Ebene 2

8.3 eduroam-Vereinbarungen (Deliverable I)

1. TERENA level policy

TERENA will adopt this document as the TERENA roaming policy. All participating NRENs connecting to or wishing to connect to the TERENA authentication servers (European top level RADIUS servers) to participate in inter-NREN roaming must abide by the following as a minimum

1.1. Participating NRENs must abide by this roaming service agreement contained herein.

1.2. NRENs are responsible for ensuring that their national authentication servers can provide a secure means of transferring user credentials to and from other proxy authentication servers as required.

1.3. NRENs must have signed agreements in place with their academic institutions to participate in the supply and receipt of national and inter-NREN roaming services.

1.4. NRENs must have the following procedures in place to handle

1.4.1. National authentication server support and maintenance.

1.4.2. Security issues. It is advisable that the NRENs keep their CERT groups informed of development work and have channels in place to work together on issues that affect both parties

1.4.3. Fraudulent use of the roaming service by users or groups of users.

1.4.4. A monitoring facility to show the status of the national authentication servers so that home institutions can use this information as part of any guest user fault reporting activity.

1.4.5. A mechanism for providing feedback on the roaming service so that guest or roaming users can identify participating institutions and their service offering.

1.5. Ideally, NRENs should have a minimum of two authentication servers at different locations on their core network for resilience and redundancy.

1.6. The NREN must mandate their participating institutions to notify guest users on the level of security offered for the transmission of user credentials.

1.7. The NREN must mandate their participating institutions to educate their users in the roaming service and ensure that any technical support issues are handled at the home institution only. If the home institution determines the fault lies at the visited institution, only then should the issue be raised with the visited organisation technical support team.

1.8. The NREN must mandate their participating institutions to log authentication

sessions and network access sessions so that they can trace a user for both security and capacity planning purposes.

1.9. The NREN must mandate their participating institutions to report any security issues or fraudulent activities to their NREN and manage and resolve such matters accordingly and report these to TERENA.

1.10. NRENs are not expected to provide privacy against casual snoopers; it is therefore the responsibility of the home institution and the guest user to have appropriate end-to-end privacy solutions in place to secure communications.

1.11. NRENs should have written guidelines for participating institutions to assist them in drafting local site and user policies to ensure compliance with the roaming service agreements with their NREN.

2. NREN level policy

A national policy framework must be in place so that all participating institutions have signed acceptance to that agree to the following as a minimum

2.1. Participating academic institutions must abide by the roaming service agreement contained herein.

2.2. Participating academic institutions are responsible for educating their users to respect the local AUP of the visited institution that their users that have been granted network access to and are obliged to help resolve any issues that relate to their users.

2.3. Participating academic institutions must provide a secure authentication server that can securely process and forward user credentials as required.

2.4. Participating academic institutions should communicate to guest or roaming users on whether and how they offer the roaming service.

2.5. Participating academic institutions should inform guest users of the level(s) of security offered for the transmission of user credentials.

2.6. Participating academic institutions must educate their users in the roaming service and ensure that any technical support issues are handled at the home organisation only. If the home organisation determines the fault lies at the visited institution, only then should the issue be raised with the visited organisation technical support team.

2.7. Participating academic institutions must log authentication sessions and network access session and be able to trace a user for both security and capacity planning purposes.

2.8. Participating academic institutions must report any security issues or fraudulent activities to their NREN to manage and resolve accordingly.

8.4 Abbildungsquellenverzeichnis

Abbildung 1	http://www.wirelessdevnet.com/articles/80211security_2/
Abbildung 2	*Getronics*, Informationsveranstaltung über 802.1x, 26.1.2006
Abbildung 3	http://www.switch.ch/mobile/howitworks.html
Abbildung 4	http://www.switch.ch/mobile/locations.html
Abbildung 5	http://aaa.surfnet.nl/info/eduroam/wlan.jsp
Abbildung 6	Sankar & Chown (2003)
Abbildung 7	Wierenga (2004)
Abbildung 8	Sankar & Chown (2003)
Abbildung 9	http://www.eduroam.org/map/eduroam-current.jpg
Abbildung 10	http://www.terena.nl/activities/tf-mobility/meetings/11/minuteszag06.pdf
Abbildung 11	Wierenga (2004)
Abbildung 12	Wierenga (2004)

8.5 Linkliste

ACOnet	http://www.aco.net/
Bluesocket	http://www.bluesocket.com/
DFN	http://www.dfn.de/
eduroam	http://www.eduroam.org/
GÉANT	http://www.geant.net/
Greenspot	http://www.greenspot.de/
IEEE	http://www.ieee.org/
IEEE 802.11	http://standards.ieee.org/getieee802/802.11.html
IETF	http://www.ietf.org/
IPA	http://www.nic.at/ipa/
iPass	http://www.ipass.com/
ISPA	http://www.ispa.at/
RFC	http://www.rfc-archive.org/
SWITCH	http://www.switch.ch/
TERENA	http://www.terena.nl/
Tino	http://www.cc.puv.fi/~teu/tino/
Wbone	http://www.wbone.org/
Wi-Fi Alliance	http://www.wifi.org/