Was ist und wie funktioniert eigentlich eduroam?

Text und Kontakt:
Steffen Klemer
steffen.klemer@gwdg.de
0551 39-172361

Dank eduroam funktioniert bei Kunden der GWDG in immer mehr fremden Instituten und Universitäten der Internetzugang via WLAN ohne weiteres Zutun, ganz wie in Göttingen. Während die eduroam-Initiative in diesem Jahr ihren 10. Geburtstag feiert, konnte die GWDG zuletzt wieder einige weitere lokale Institute an dieses weltweite Netzwerk anschließen. Die Technik dahinter basiert auf einer hierarchischen Struktur von Authentifizierungsservern.

Einmal eingerichtet, ermöglicht eduroam den reibungsarmen WLAN-Zugang an über 7.000 Bildungseinrichtungen zwischen Südafrika und Spitzbergen, von Alaska bis Neuseeland. Man schaltet seinen Laptop, sein Smartphone oder seinen eBook-Reader ein und kann sofort lossurfen – und das gewöhnlich sicher in einem verschlüsselten Funknetz. Das klingt zu schön, um wahr zu sein, und funktioniert trotzdem. Im Folgenden soll ein Blick auf die Infrastruktur im Hintergrund geworfen werden, die das ermöglicht.

Ein Internetzugang via WLAN gehört heute gewissermaßen zum Muss für jede Bildungseinrichtung. Und natürlich sollte er leicht einzurichten, sicher und auch für Gäste verfügbar sein. Leider sind diese drei Anforderungen eher diametraler Natur. Verlangt man eine verschlüsselte Verbindung, benötigen die Benutzer Passwörter. Das schließt Gäste aus und erleichtert nicht gerade die Einrichtung. Ein einfaches, bekanntes Passwort für alle schützt die Benutzer wiederum nicht untereinander.

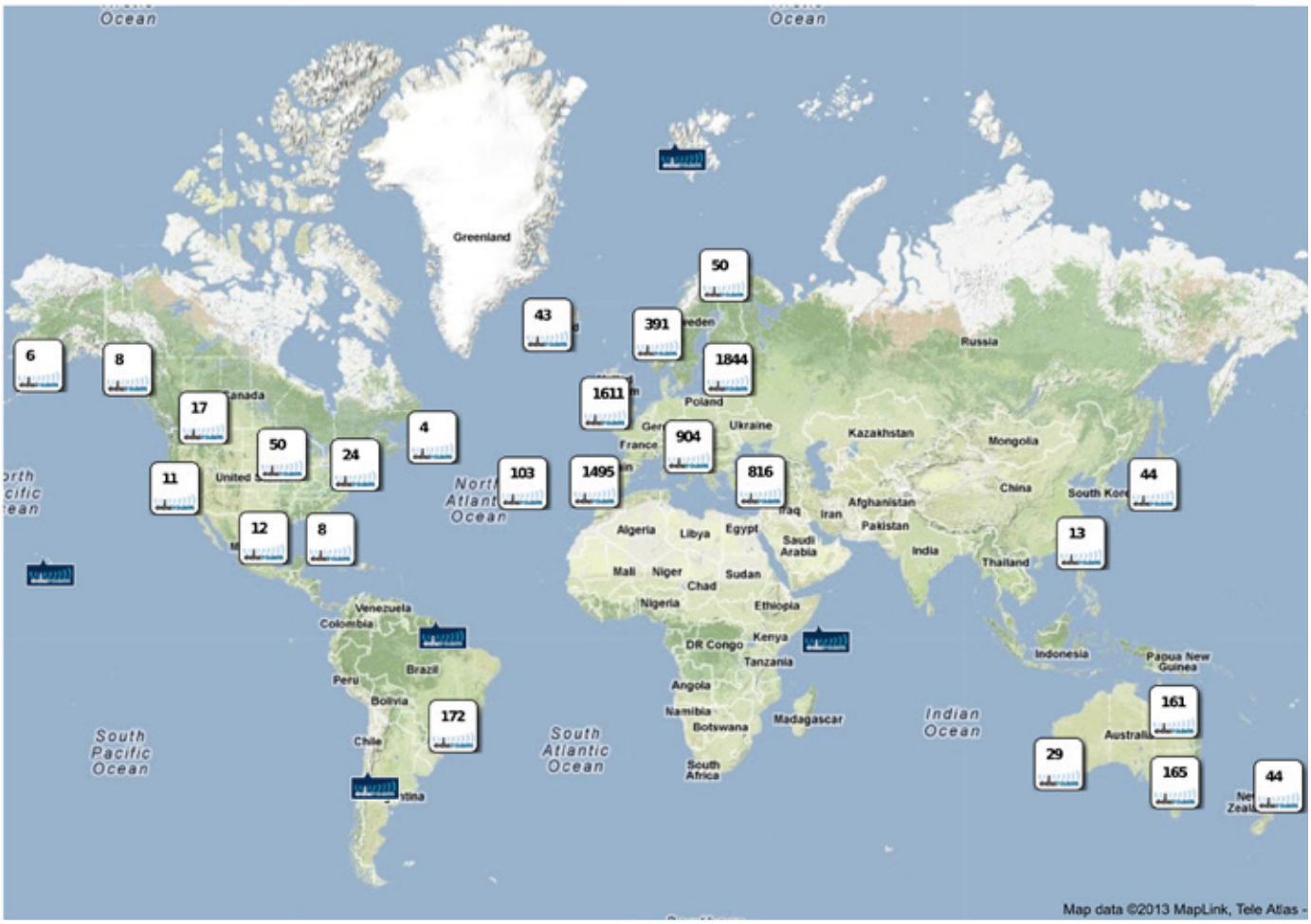
WLAN SICHER, ABER EINFACH

Eine Lösung aus diesem Dilemma suchte 2003 der TERENA-Verein (Trans-European Research and Education Networking Association), ein Zusammenschluss europäischer Netzwerkdienstleister, wie dem DFN-Verein, für die Weiterentwicklung der europäischen Forschungsnetze. Das Ziel des eduroam-Projektes sollte ein Roaming zwischen allen beteiligten Instituten sein. Ein Nutzer loggt sich im fremden WLAN mit seinen bekannten Zugangsdaten (Benutzername und Passwort) ein. Aus Sicherheitsgründen erfolgt dies in einem verschlüsselten Tunnel zwischen dem Nutzer und seiner Heimatorganisation. Die Heimatorganisation überprüft die Authentizität des Benutzers, bestätigt sie, und dem Nutzer wird Einlass in das fremde Netz gewährt. Dieses Vorgehen löst zwei der drei o. g. Probleme um den Preis einer eventuell schwierigeren erstmaligen Einrichtung des WLANs auf Seiten des Nutzers. Das muss jedoch nur einmalig und kann vor allem vor Ort in der Heimatorganisation gegebenenfalls mit Unterstützung des lokalen IT-Service geschehen.

Nach der Demonstration der Machbarkeit mit zunächst fünf europäischen Instituten im Jahr 2003 schloss sich mit Australien bereits 2004 das erste nichteuropäische Land der Initiative an.

1_eduroam-Standorte mit .de-Realm (Karte von eduroam.de)

Heute ist eduroam auf allen Kontinenten, mit Ausnahme der Antarktis, zu finden und vor allem in Europa und dem asiatisch-pazifischen Raum verbreitet. Eine Übersicht über die Standorte in Nordamerika bietet *http://eduroamus.org* und für den Rest der Welt *http://eduroam.org*. Auch die GWDG ist über den DFN-Verein Mitglied der eduroam-Initiative. Mitglieder verpflichten sich mit ihrem Beitritt, gewisse technische und organisatorische Vorschriften einzuhalten. Diese regeln zum Beispiel die Sicherheit, aber auch die Nachverfolgbarkeit missbräuchlicher Nutzung.



2_eduroam-Standorte weltweit (Karte von eduroamus.org/eduroam_international_map)

WEITERER EDUROAM-AUSBAU BEI DER GWDG

Über die GWDG-Infrastruktur konnten zuletzt die Max Planck Digital Library (MPDL) und das Max-Planck-Institut für Sozialrecht und Sozialpolitik in München sowie das Göttinger Wohnheim Kellnerweg an das eduroam angeschlossen werden. In allen drei Fällen konnte es in die bestehende WLAN-Infrastruktur integriert werden. Während es sich bei den beiden Münchener Instituten um kommerzielle Systeme handelt, funktioniert es ebenso mit der selbst entwickelten Lösung der Studierenden auf Basis freier Software. Weiterhin erfreuen sich durch Zusammenarbeit mit der GWDG seit Januar die Mitarbeiter der Universitätsmedizin Göttingen (UMG) eines eduroam-Zugangs. Die Studierenden der Universität Göttingen (inklusive UMG) haben diesen übrigens schon seit 2010, ebenso wie alle weiteren an das Identitätsmanagement der GWDG angeschlossenen Institute.

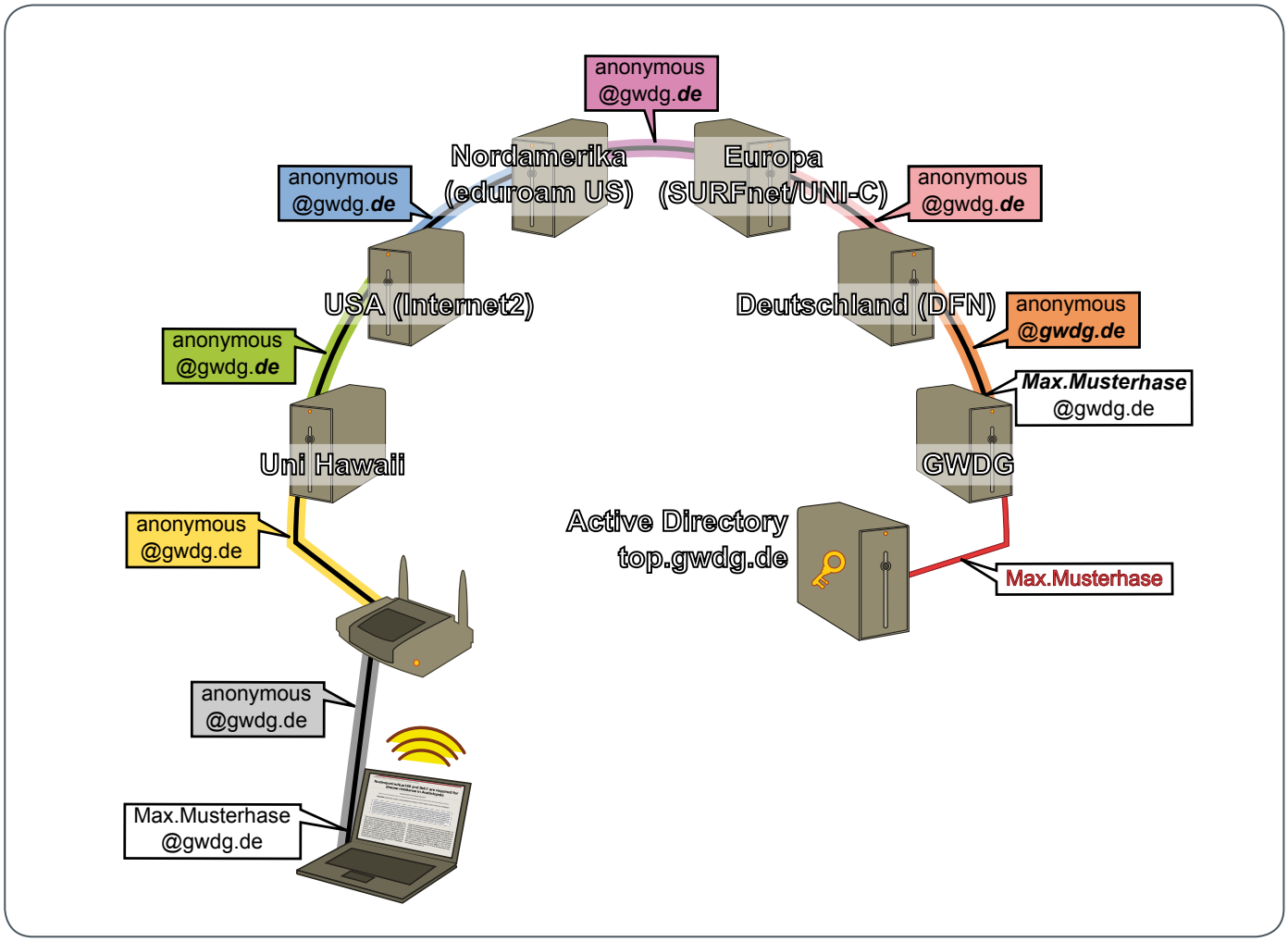
DIE TECHNIK DAHINTER

All dem liegt eine hierarchische Struktur von RADIUS-Authentifizierungsservern zugrunde. Ein Account im eduroam besteht grundsätzlich aus zwei Teilen, dem Username und dem Realm, die durch ein „*@*“ getrennt sind: *user@institut.länderkennung*. Eventuell gibt es unterhalb des Instituts weitere Subdomains wie z. B. im Falle der UMG *max_musterhase@eduroam.med.uni-goettingen.de*. Wichtig ist zu bemerken, dass dieser Login zwar aussieht wie eine E-Mail-Adresse, aber keiner regulären entsprechen muss. Es ist ein rein artifizielles Konstrukt, um Max Musterhase seiner Heimateinrichtung zuordnen zu können.

Aber wie funktioniert das jetzt eigentlich? Ein Client in Göttingen übergibt beim WLAN-Login seinen Login-Wunsch samt eines Accountnamens mittels des Protokolls 802.1x an den Accesspoint. Dieser leitet die Anfrage via RADIUS-Protokoll zum lokalen RADIUS-Server der GWDG weiter (vgl. auch Abb. 3). Er entscheidet

eduroam

Thanks to eduroam wireless access at remotes sites is very easy and secure nowadays. In the last 10 years the eduroam community grew from 5 european member institutes to about 7,000 at the moment. The authentication procedure relies on a hierarchical structure of proxying radius servers whereas the user credentials itself are transferred through a secured end-to-end tunnel from the client to its home organization. GWDG introduced eduroam in 2010 and the number of institutes connected to it via the GWDG infrastructure is growing steadily. Also the number of users in Göttingen nearly doubled in this term to about 6,000 a day. In the peak hours around noon there are nearly 3,500 simultaneous users. GWDG is still improving its eduroam infrastructure for example with new redundant RADIUS servers and a more secure connection to the upstream RADIUS servers in the near future.



3_ Schematischer Ablauf eines eduroam-Logins bei der Universität Hawaii

anhand des Realms, ob er selbst zuständig ist oder die Anfrage ebenfalls weiterleitet. Ist der Realm ein lokaler, beispielsweise gwdg.de oder *uni-goettingen.de*, befragt der Server seine Benutzerdatenbank. Im Falle der GWDG ist dies das Active Directory. Sind Username und Passwort korrekt und darf, um im Beispiel zu bleiben, Max Musterhase eduroam verwenden, sendet der Server sein Okay an den Accesspoint, welcher anschließend die Verbindung für den Benutzer freigibt.

Wichtig bei diesem Verfahren ist, dass das 802.1x- sowie das RADIUS-Protokoll als Tunnel fungieren, durch den der Client auf verschlüsseltem Wege direkt mit dem Authentifizierungsserver spricht. Hierfür existieren unzählige Verfahren, wobei im eduroam zumeist PEAP oder TTLS eingesetzt werden, innerhalb derer auch wieder verschiedene Algorithmen für den eigentlichen Passwortabgleich verwendet werden können. MS Windows bis einschließlich Version 7 spricht nur PEAP. Die GWDG unterstützt beide gängigen Verfahren.

Kennt der RADIUS-Server der GWDG den Realm hingegen nicht, leitet er die Anfrage, wieder via RADIUS-Protokoll, an den zentralen RADIUS-Server des DFN-Vereins weiter. Hier sind alle Realms der *.de*-Domäne hinterlegt. Sollte der Realm einer anderen Länderkennung angehören, leitet der DFN-Verein die Anfrage abermals in der Rolle eines Proxys an den zentralen europäischen Server in Amsterdam weiter. Insgesamt besteht die Hierarchie aus einem zentralen Server pro Kontinent, der wiederum an die einzelnen Länder-Registries weiterleitet und diese dann an die lokalen Institute weiterleiten. Durch die vielen Proxys hindurch spricht der Client weiterhin im gekapselten und verschlüsselten Tunnel innerhalb des RADIUS-Protokolls direkt mit dem Authentifizierungsserver seiner Heimatorganisation. Auch beim Login auf Hawaii sieht nur die GWDG meine Zugangsdaten und ich kann anhand des Serverzertifikats überprüfen, ob wirklich die GWDG am anderen Ende ist.

Abb. 3 zeigt als Beispiel den schematischen Ablauf eines eduroam-Login bei der Universität Hawaii. Die Anfrage wird anhand des Realms *gwdg.de* über den RADIUS-Server der Universität und der Internet2-Community zum Top-Level-Server von Nordamerika weitergeleitet. Von dort führt die Anfrage vom Top-Level-RADIUS des europäischen Raumes über den Server des DFN-Vereins zur GWDG. Hier endet der verschlüsselte Ende-zu-Ende-Tunnel vom Laptop des Clients. Die Logindaten werden gegen das Active Directory der GWDG überprüft und das Ergebnis mittels des RADIUS-Protokolls auf gleichem Wege zurück an den Server der Universität Hawaii gemeldet. Der wahre Username des Clients ist nur innerhalb des Tunnels, also einzig für die GWDG sichtbar.

Das Prozedere mit den Realms hat noch einen weiteren Vorteil. Die Verbindung zum Heimatserver hängt einzig vom Realm ab und nur die Daten im inneren Tunnel werden authentifiziert. Folglich kann in der äußeren Anfrage etwas wie *anonymous@gwdg.de* und nur im inneren Tunnel die wahre Identität *max.musterhase@gwdg.de* angegeben werden – ich bleibe gegenüber der University of Hawaii anonym. Da innerhalb der eduroam-Initiative Regeln

für die Aufbewahrung und den Inhalt der Logfiles bei allen Parteien vorgesehen sind, kann die Heimatorganisation zum Beispiel bei einer Anfrage wegen missbräuchlicher Nutzung Auskunft über die wahre Identität des Nutzers erteilen.

NUTZER BEI DER GWDG

Im Moment nutzen fast 6.000 Kunden der GWDG täglich das eduroam innerhalb Göttingens. Hinzu kommen im Schnitt 80 Nutzer aus fremden Instituten, bei Tagungen zum Teil aber auch deutlich mehr. Die Anzahl von Göttinger Nutzern in fremden Instituten ist im Moment an den meisten Tagen noch einstellig mit vereinzelten Ausschlägen bis zu 100 Nutzern. Sehr bemerkenswert ist der Anstieg der Anzahl lokaler Logins mit Beginn des Wintersemesters im Oktober 2012. Sie stieg vom langjährigen Mittel knapp über 2.000 auf 4.000 und mehr pro Tag. Vermutlich wurde in der Orientierungswoche vermehrt Werbung für eduroam gemacht, da parallel die Verwendung des unverschlüsselten GoeMobile zurückging. Zeitgleich „tummeln“ sich um die Mittagszeit, der Tagesspitze, im Moment fast 3.500 Geräte im Göttinger eduroam.

Auch diese Zahlen zeigen noch einmal, dass eduroam sehr gut angenommen wird und sich der technische Aufwand auf jeden Fall lohnt. Innerhalb der GWDG wird in der näheren Zukunft der bestehende freeradius-Server auf eine leistungsfähigere und performantere Version aufgerüstet und die Struktur redundanter gestaltet. Aufbauend auf einer Erweiterung des RADIUS-Protokolls soll darüber hinaus demnächst auch die äußere Verbindung sicher verschlüsselt zum DFN-Verein erfolgen. Für die Nutzer bleibt es dabei, dass es in den allermeisten Fällen nicht nur in der Theorie, sondern tatsächlich auch in der Praxis überall einfach und sicher funktioniert.