CMST 11(2) 169-173 (2005) DOI:10.12921/cmst.2005.11.02.169-173

COMPUTATIONAL METHODS IN SCIENCE AND TECHNOLOGY **11(2)**, 169-173 (2005)

Eduroam: past, present and future

Klaas Wierenga[1] **and Licia Florio**[2]

[1]*SURFnet bv, Postbus 19035, 3501 DA Utrecht, The Netherlands*
e-mail: Klaas.Wierenga@SURFnet.nl

[2]*TERENA Secretariat, Singel 468 D, 1017 AW Amsterdam, The Netherlands*
e-mail: florio@terena.nl

Abstract: The number of mobile devices within academia has increased significantly over the last couple of years and users expect to be able to get connectivity everywhere, at home, on the road and at educational institutions. At the same time however, the security of wireless LANs becomes more and more of a concern In 2003, the TERENA Task Force on Mobility [1] was created to look at WLAN security issues and to formulate requirements to design an international roaming solution that would provide National Research and Educational Networks' (NRENs') users with secure Internet access at academic campuses across Europe. The solution proposed was tested and proved to be very successful with more and more institutions joining it. This infrastructure is called *eduroam*, which stands for Education Roaming. Within the 6th framework project GÉANT2 [2], the aim is to expand the existing infrastructure into a pan-European full service for Roaming and Authentication/Authorisation.

Key words: Eduroam, RADIUS, Wires Equivalent Privacy

1. INTRODUCTION

The number of mobile devices within academia has increased significantly over the last couple of years. The majority of laptops sold nowadays have wireless LAN capabilities built-in and users expect to be able to get connectivity everywhere, at home, on the road and at educational institutions. At the same time however, a number of tools (such as Kismet [3] and Airsnort [4]) show that the security of wireless LANs based on Wireless Equivalent Privacy (WEP) is not effective at all.

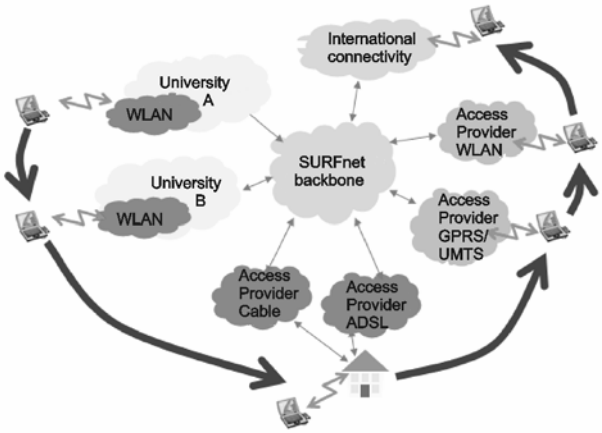

Fig. 1. Roaming users

As users are becoming mobile they are expressing the desire to have their familiar environment, services and privileges available whenever they move from one site to another. The number of researchers and students "roaming" between different NREN domains is increasing and so is their demand for these services.

The roaming needs of users have led to a number of national and international initiatives to provide network roaming for their constituencies. Within the TERENA task force on Mobility, requirements were formulated to develop an international roaming solution that would provide NREN users with secure Internet access at academic campuses (WLAN and wired) across Europe with the following characteristics:

- Minimal administrative overhead (per roaming user)
- Good usability
- Maintaining required security for all partners
- Scalable.

TERENA's Mobility task force identified three possible approaches in current use:

- Web-based authentication with RADIUS backend (Finland),
- VPN-based authentication (Germany and Switzerland),
- 802.1 X-based authentication with RADIUS backend (The Netherlands).

Each solution was evaluated and characterised as follows:

- Web: Scalable, Unsafe, Already Deployed
- VPN: Not Scalable, Safe, Already Deployed
- 802.1X: Scalable, Safe, New.

Based on these characteristics and on the fact that upcoming security standards like WPA and 802.11i all build on 802.1X, TF-Mobility has concluded that 802.1X authentication with a RADIUS hierarchy-based backend is the method

of choice, even though not every institution is able to support it currently because of legacy equipment [5].

2. THE CREATION OF *eduroam*

One of the goals of the Mobility task force was to design an inter-NREN roaming infrastructure; having selected 802.1X as the authentication method, it was agreed to set-up a test-bed based on 802.1X and RADIUS servers.

Fig. 2. *eduroam* logo

This test-bed has evolved into a pan-European pilot called eduroam (Education Roaming) [6]. The *eduroam* service builds on a hierarchical system of RADIUS servers. TERENA deploys a (distributed) European top-level RADIUS server to which all European NREN's that participate connect with their national RADIUS server. Every institution that wants to participate in eduroam connects its institutional RADIUS server to the national server of their NREN.

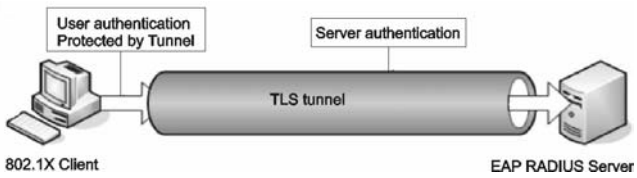

Fig. 4. Tunnelled authentication (© Alfa&Ariss)

Figure 3 shows the typical operation based on 802.1X for guest user at an eduroam-participant site in the Netherlands. The user, belonging to the institution called Institution B, provides his credentials; the RADIUS server of Institution A discovers that it is not responsible for the institution_b.nl realm and proxies it to the national RADIUS proxy server (that in turn might proxy it to the European server in case the user is coming from another country). This national server forwards the credentials to the home-institution of the user where they are verified. The 'acknowledge' of a successful authentication travels back over the proxy-hierarchy to the visited institution and the user is granted access. Because the user credentials travel via a number of intermediate servers, not under control by the home-institution of the user, it is important that the credentials are protected for privacy reasons. This requirement limits the types of authentication methods that can be used. Basically there are two categories of useful authentication methods, those that use credentials in the form of some public key mechanism with certificates (EAP-TLS, EAP-SIM) or those that use the so-called tunnelled authentication (EAP-TTLS, PEAP). Authentication using both server and end-user certificates requires the roll-out of a public key infrastructure (PKI certificates which has proven difficult in most NREN's. Most institutions therefore use a tunnelled authentication method that only requires server-certificates. These server certificates are used to set up a secure tunnel between authentication server and mobile device, through which the user credentials are securely transported.

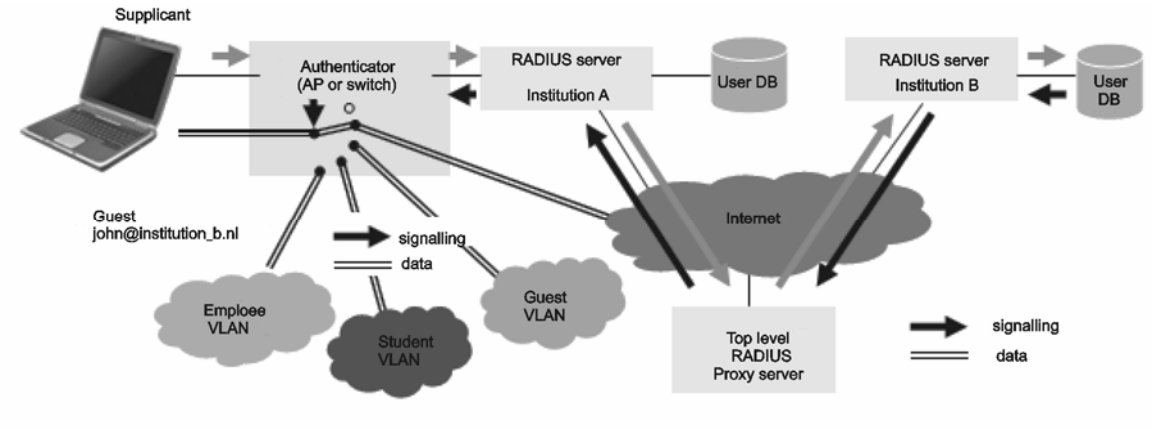

Fig. 3. *eduroam* basic set-up (© SURFnet)

3. CURRENT SITUATION

At the time of writing (June 2005) more than 350 institutions in 19 countries participate in eduroam.

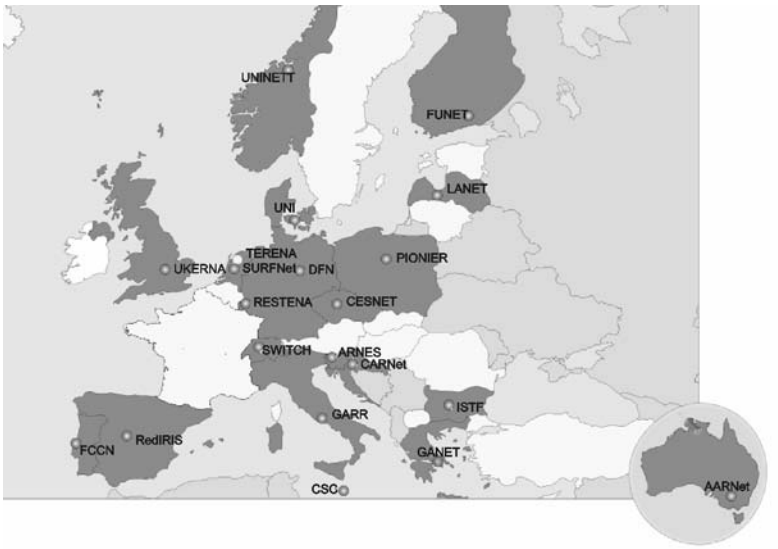

Fig. 5. Current *eduroam* participants (© TERENA)

Most countries that participate in eduroam are setting up a web page showing which institutes are participating in *eduroam*. In the United States of America the Internet2 working group FWNA [7] has started an initiative to create a RADIUS hierarchy for higher education and to become *eduroam* participants. Also in the Australian-Pacific region an *eduroam* initiative has started [8] and also a first pilot connection with the US has been established. To co-ordinate global efforts, an *eduroam* global working group [9] has been formed.

4. FUTURE DEVELOPMENTS

The current set-up of *eduroam* works remarkably well, in fact its design based on authentication at the home-institution and authorisation at the visited institution has proven to be so powerful that within the GÉANT2 project, a full pan-European authentication and authorisation infrastructure service will use the current architecture to build upon. This activity will take place in Joint Research Activity 5: Roaming and Authorisation. The aim is not only to build an infrastructure for network roaming but also for access to applications and to provide single sign-on across applications and networks. The activities in JRA5 will focus on improving the current infrastructure in a number of areas in order to turn the pilot infrastructure into a full European roaming service. Specific areas of attention are:

• Technology

The trust establishment between the RADIUS entities in eduroam is accomplished using a static shared secret for each peer, where authentication requests are passed on from one entity to the other until the request reaches the authenticating server. This approach has a number of disadvantages: the trust is static and has to be preconfigured, all authentication traffic flows through the whole hierarchy even though it is only of interest to the end-systems and having a chain of intermediate systems introduces single points of failure.

In order to overcome these limitations, three alternative solutions are investigated, PKI, Diameter and DNSsec. The common denominator for all three solutions is that they decouple the (hierarchical) trust establishment with the actual transport of credentials and the fact that they aim at interoperability with the existing *eduroam* architecture providing a gradual evolution path.

• Policy

Eduroam has grown to its current level by making it as easy as possible to join. It can be regarded as a very loosely-knit trust-fabric. Now that *eduroam* is evolving into a true production service, the need has arisen to address policy issues in a more formal way. To achieve this, policies will be developed to address the responsibilities and liabilities of the various parties involved (users, institutions, NREN's) as well as a set of guidelines and requirements for participation.

• Usability

The grand vision of allowing users to get online everywhere without further configuration or administrative effort has become somewhat hampered by the fact that through the grassroots approach that was taken *eduroam* has come in many flavours. Different NREN's and institutions have chosen different approaches with respect to standardisation on SSID's, wireless encryption standard ('vanilla' 802.1X, WPA, WPA2/802.11i etc.). This results in the user having to reconfigure his mobile device, even though the same credentials can be used. In order to overcome this, harmonisation will take place to reduce the degrees of freedom in implementation. Special attention will also be given to communicate the locations with *eduroam* access, by means of maps showing *eduroam* enabled hotspots, correct settings, etc.

• Management & monitoring

A monitoring framework will be put into place to monitor the infrastructure on a structural as well as an ad-hoc basis.

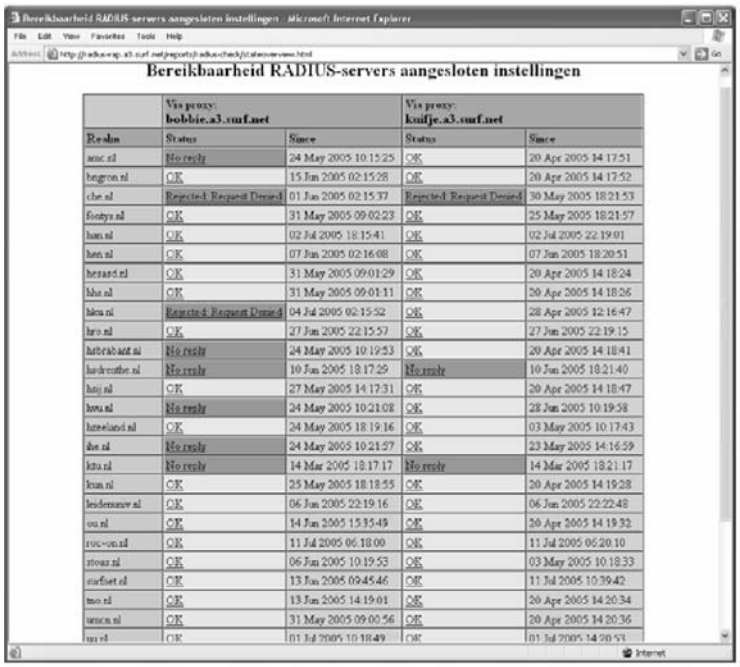

Fig. 6. RADIUS monitoring

Together with monitoring of use and abuse, this will allow for the creation of a stable infrastructure.

• Integration with AAI

A last important point for consideration is integration with the Authentication and Authorisation Infrastructure (AAI) that is being built in the GÉANT2 project. A federation will be built to allow NREN's and institutions throughout Europe (and beyond) to share resources. In order not to duplicate efforts, or even worse, create two separate infrastructures with overlapping functionality special attention will be given to integration with this AAI. Ultimately, it is foreseen that *eduroam* network access will be one of the resources shared among the members of this federation.

3. CONCLUSION

Eduroam has proven itself as a scalable, secure and successful pilot service. This is proven by the fact that more and more countries and institutions participate, also beyond Europe, thus making it more and more beneficial for the participants.

Foreseen improvements of the infrastructure concentrate on the 'backplane' of the service, while keeping intact the institutional set-up. This combined with the fact that new security standards like WPA and 802.11i are built upon the 802.1X framework, ensuring that an investment in *eduroam* participation is justified. It is TERENA's and GÉANT2's intention to expand the *eduroam* service to encompass as much of the academic community as possible. It should be noted that since the system requires a national-level RADIUS server, this implies that the NREN in these countries need to be involved.

Acknowledgements

This paper is based on deliverables written by participants of the TERENA TF-Mobility and the GÉANT2 roaming and authorisation activity as well as on numerous discussions with members of these and other related bodies. The authors would like to express their gratitude to the participants of these groups for their highly valued feedback.

References

[1] TERENA Task Force on Mobility, http://www.terena.nl/tech/task-forces/tf-mobility
[2] GÉANT2 project, http://www.geant2.net/
[3] Kismet, http://www.kismetwireless.net/
[4] Airsnort, http://airsnort.shmoo.com/)
[5] Final report of TF-Mobility, http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/TF-MobilityfinalReport.pdf
[6] eduroam, http://www.eduroam.org
[7] FWNA, http://security.internet2.edu/fwna/
[8] eduroam Australia, http://www.eduroam.edu.au/
[9] eduroam global working group, http://www.eduroam.edu.au/gwg-eduroam/

KLAAS WIERENGA is manager of Middleware Services at SURFnet. He is co-chair of the TERENA taskforce on Mobility (TF-Mobility) and active member of the TERENA Task Force on Middleware (TF-EMC2) and the Internet2 working group on network authentication (SALSA NetAuth). Klaas also leads the roaming task within the "Roaming and Authorisation" activity of the EU-funded project Géant2.

LICIA FLORIO works as a Project Development Officer for TERENA and her work focuses mainly on the coordination and support for middleware and roaming activities within the European Research and Education Networks in Europe. She is the coordinator for the TERENA Task Force on Mobility (TF-Mobility) and for the TERENA Task Force on Middleware (TF-EMC2). Licia also follows middleware development in the area of Grid technology.