#  TECHNICAL REPORT SAMPLE

**TF-Mobility**

**Inter-NREN roaming**

**Final Report**

**James Sankar – UKERNA
Klaas Wierenga - SURFnet**

This report summarises the work of the TERENA Mobility taskforce that has been working on roaming network access solutions from January 2003 to June 2004. The taskforce investigated the requirements and delivery of a unique network access solution that would allow guest users hassle free network access using their own credentials to authenticate at their home institution in order to then if successful be authorised network access. A number of participants from European National Research and Education Networks have collaborated regularly in the TF-Mobility taskforce. Since January 2003, the task force has met five times in face-to-face and videoconference meetings. The taskforce was formally closed in July 2004, but TERENA are still running the mobility@terena.nl mailing list.

The information in this document is supported by TF-Mobility’s website:

**For Further information please contact:**

TERENA Secretariat Tel: +31 20 530 4488

Singel 468 D Fax: +31 20 530 4499

1017 AW Amsterdam E-mail: secretariat@terena.nl

The Netherlands www: http://ww.terena.nl

© TERENA 2004 All rights reserved

Parts of this report may be freely copied, unaltered, provided that the original source is acknowledged, and the copyright preserved.

Production: TERENA Secretariat

Editor:

# Contents

[Contents 3](#_Toc76289792)

[1. Introduction 3](#_Toc76289793)

[2. Acknowledgements 5](#_Toc76289794)

[3. Summary of results 6](#_Toc76289795)

[4. Dedicated website 11](#_Toc76289796)

[5. Glossary 11](#_Toc76289797)

[6. Requirements definition 11](#_Toc76289798)

[7. Inventory of 802.1X network access to roaming requirements 14](#_Toc76289799)

[8. Inventory of VPN based network access to roaming requirements 17](#_Toc76289800)

[9. Inventory of web-based redirection network access to roaming requirements 19](#_Toc76289801)

[10. Roamnode Authentication solution 20](#_Toc76289802)

[11. Preliminary selection for Inter-NREN roaming 24](#_Toc76289803)

[12. Test bed and reference design for inter-NREN roaming 27](#_Toc76289805)

[13. Roaming Policy guidelines 29](#_Toc76289806)

[14. A web repository of tests on Wireless LAN devices 36](#_Toc76289812)

[15. A document outlining the impact of new technology and protocols such as MobileIP on current roaming work. 36](#_Toc76289813)

[16. A summary of national roaming developments 36](#_Toc76289814)

[17. Conclusions 51](#_Toc76289815)

[18. Recommendations for future work 52](#_Toc76289816)

[19. References 58](#_Toc76289817)

#

 **TECHNICAL REPORT SAMPLE**

 TF-Mobility, the taskforce on roaming network access started in March 2002 in Amsterdam as a workshop. Two further meetings in June 2, 2002 in Limerick, Ireland and October 2002 in Amsterdam led to the agreement of a scope of work that was written as a draft taskforce charter with a list of deliverables and associated timescales. A mailing list "mobility@terena.nl" was set up and a website was also created at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The draft charter was submitted to the TERENA Technical Committee on the 16 December 2002 and was approved to formally start in January 2003. Two co-chairs were appointed for the taskforce, Carsten Bormann acted as technical chair, James Sankar acted as process chair.

The aims of the TERENA Mobility taskforce were

* To provide a forum for exchanging experiences and knowledge, and to make the results of the work of the Task Force available to the research networking community and promote the benefits of the technology;
* To identify requirements to address security aspects and regulatory issues as well;
* To define and test an inter-NREN roaming architecture by:
	+ evaluating possible authentication and authorisation techniques in mobile environments (e.g. Web-based, RADIUS+802.1x, VPN) for the research community in Europe;
	+ identifying the most suitable techniques, which will be standards-based, platform independent and use whenever possible infrastructures currently deployed in the NRENs;
	+ describing the elements for a possible inter-NREN WLAN architecture based on these selected technologies;
* To implement and test the proposed architecture amongst the participant NRENs; Quality of Service will also be considered;
* To evaluate mobile equipment and software;
* To evaluate next-generation mobile technology for handovers and roaming (Mobile-IP(v4 and v6)); in this area TF-Mobility will work closely with TF-NGN and the 6NET working group on IPv6 and Mobility.

The objectives of the Task Force were:

* To identify requirements to address security aspect as well as regulatory issues
* To define and test an inter-NREN roaming architecture
* To evaluate mobile equipment and software
* To evaluate next generation mobile technology for handovers and roaming

# 2. Acknowledgements

This report wishes to acknowledge the following people who have contributed to the work of the taskforce, both directly and indirectly.

**TERENA**

Licia Florio, Dick Visser

**TF-Mobility members who wrote the taskforce deliverables (in alphabetical order)**

Carsten Bormann (University of Bremen)

Hansruedi Born (SWITCH)

Tim Chown (University of Southampton)

Paul Dekkers (SURFnet)

Erik Dobbelstijn (SURFnet)

Sami Keski-Kasari (Tampere University of Technology)

Ueli Kienholz (SWITCH)

Jardar Leira (UNINETT)

Niels Pollem (University of Bremen)

Juergen Rauschenbach (DFN)

James Sankar (UKERNA)

David Simonsen (UNI-C)

Roland Staring - (SURFnet)

Klaas Wierenga (SURFnet)

**Thanks are also expressed to any other taskforce members not mentioned that have contributed at TF-Mobility meetings, and on the TF-Mobility mailing list.**

# 3. Summary of results

TF-Mobility has carried out the following activities

**Information site on the TERENA server**

A dedicated web page was established that contained information about the taskforce (charter, scope, mailing list, meetings and deliverables). It was useful for coordinating meetings and disseminating relevant information (agendas, presentations and meeting minutes) to ensure the activities were transparent. A private area was also created so that active taskforce members could review early drafts of the deliverables and provide comments prior to publication of a finalised version.

**Glossary**

A glossary was created as an early deliverable to ensure a common understanding of terms could be agreed amongst the various NREN representatives to ensure that subsequent deliverables were consistent in the use of terms to describe work undertaken. The glossary was initially based on technical terms but it soon was realised that non technical descriptions such as guest user, home institution etc. also needed to be defined to avoid misunderstanding in the production of deliverables. As a result, a second list of non-technical terms was duly written. Both technical and non-technical terms were agreed and merged into the later versions of the glossary deliverable.

**Requirement’s definition**

The taskforce members agreed and documented a requirements definition for inter-NREN roaming based on their experiences of developing and hosting national roaming solutions. A set of major and minor requirements were agreed. These requirements were pragmatic and agreed as achievable within the timeframe of the taskforce.

***The major requirements were***

* The scalability of the proposed solution must be maintained and the administrative overhead must be minimised
* The required security must be maintained for all partners in the process.

***The minor requirements identified were***

* The usability must be good for all needed/used platforms
* Accountability and logging functionality must be provided to track abuse.

It was also stated that where requirements were not possible a reasonable trade-off should be found. This deliverable then explored each requirement in more detail.

**Inventory of web-based redirection network access to roaming requirements**

An inventory was undertaken of a national roaming solution that was based on web-based redirection to a login page to authenticate at FUNET. A description of the roaming solution was undertaken and details about the solution were compared with the major and minor requirements outlined in the requirements definition deliverable to ascertain how closely this national roaming solution met the requirements for inter-NREN roaming.

**Inventory of 802.1X based network access to roaming requirements**

An inventory was undertaken of a national roaming solution that was based on a 802.1X national roaming solution at SURFnet. A description of the roaming solution was undertaken and details about the solution were compared with the major and minor requirements outlined in the requirements definition deliverable to ascertain how closely this national roaming solution met the requirements for inter-NREN roaming.

**Inventory of VPN based network access to roaming requirements**

An inventory was undertaken of a national roaming solution that was based on a VPN national roaming solution at SWITCH and The University of Bremen. A description of the roaming solution was undertaken and details about the solution were compared with the major and minor requirements outlined in the requirements definition deliverable to ascertain how closely this national roaming solution met the requirements for inter-NREN roaming. This deliverable also proposed a scalable VPN solution for inter-NREN roaming called "Controlled Address Space for VPN gateways" and recommended proof of concept tests be undertaken to determine its feasibility.

**Preliminary selection for Inter-NREN roaming**

This deliverable reviewed all three inventories and included a late submission from a fourth roaming solution "Roamnode" developed at the University of Bristol in the UK. A detailed review and comparisons of all the national roaming solutions revealed that there was no single solution that met all the requirements identified by the taskforce, nor was any solution more dominant over others. The deliverable concluded that a solution be developed that could support a variety of national roaming solutions instead. The deliverable then considered in detail the design aspects for

* A RADIUS proxy hierarchy,
* A Controlled Address Space for VPN Gateways hierarchy
* Software enhancements to the Roamnode.

Results of some early development test beds were also included in this deliverable.

**Test bed and reference design for inter-NREN roaming**

This deliverable considered the technical issues and work required at the NREN and organisational site level to create an interoperable environment where guest users from either a web redirection, 802.1X or VPN national roaming infrastructure environments could gain network access at any visited organisations regardless of the roaming solution preferred there.

This deliverable highlighted the following nine scenarios and additional work and .or equipment needed to support other guest users.

 User with | 802.1X | VPN | Web-based |

 Site uses | | |

 -----------------------------------------------------------

 802.1X | Okay | Work reqd | Work reqd |

 VPN | Work reqd | Okay | Work reqd |

 Web-based redirect | Work reqd | Work reqd | Okay |

In addition a separate section detailed ongoing proof of concept tests and scaled trials of the Controlled Address for VPN gateways concept.

**Roaming Policy - draft guidelines**

As all national roaming solutions rely on fostering trust between participating organisations and given the take up in participation in the three tier (European (TERENA) - National - Organisational) RADIUS proxy hierarchy, there was a need to develop a policy and standards so that inter-NREN roaming solutions could scale and be managed easily. This deliverable provided guidelines for Inter-NREN roaming that NRENs needed to agree in order to join the TERENA level RADIUS server.

**A web repository of tests on Wireless LAN devices**

This deliverable was a comprehensive overview of wireless networking (WLAN Standards, the Workings of Wireless, Wireless and the Law, Wireless Security and known wireless problems) and also a detailed repository of wireless product tests and comparisons between different wireless products.

**A document outlining the impact of new technology and protocols such as MobileIP on current roaming work.**

[TO BE ADDED - DELIVERABLE NOT YET WRITTEN]

# 4. Dedicated website

The taskforce has created a public and private website and a mailing list with approximately

15bes.

# 5. Glossary

* Written to ensure a mutual understanding of technical and non-technical terms.
* To be a reference for deliverables and ensure a consistent use of terms.
* Revised on a regular basis to review descriptions and add new items.
* Two separate glossary lists were created and then amalgamated to one, see examples below
* An online version is available at http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/DelB/DelB\_v1-3-5.pdf

# 6. Requirements definition

The requirements definition deliverables was necessary to define the scope of work. It also provided taskforce members with an opportunity to identify and agree on major and minor requirements.

Once the requirements had been defined, the taskforce used them to objectively assess each national roaming solution to determine its suitability as a inter-NREN roaming solution.

This deliverable provided a structure to document each national roaming solution. And highlighted common issues such as security, scalability and policy matters for further consideration.

The requirements identified and agreed were as follows

**Major requirements:**

* The **scalability** of the proposed solution must be maintained.
* The **administrative overhead** must be minimised.
* The required **security** must be maintained for all participating institutions in the process.

**Minor requirements:**

* The **usability** must be good for all needed/used platforms.
* The **functionality** (service access) should be as complete as possible
* The **accountability and logging functionality** must be provided to track abuse.

A number of general and specific vulnerabilities and limitations were also identified as follows.

1. If a visiting or local user’s credentials (username and password) are stolen and another user is granted access using these credentials to authenticate with the victim’s home institution, is the home institution or the “victim” liable for not informing the authorities promptly? Also, can the user who stole the credentials be traced?
2. An authentication method that relies on a chain of RADIUS referrals may suffer additional latency beyond one that is local. It is also subject to failure if any part of the chain is broken (an unavailable server, or a network failure, for example). It is also important to ensure that authentication packets passed between RADIUS serves are not transferred by the default “clear text”. If the network can be trusted, a shared RADIUS secret could be used to improve security. If the network is cannot be trusted, trusted IPSec can be considered.
3. A VPN-based solution where the visiting user establishes a VPN connection to their home institution implies that all VPN traffic is routed from the user’s current location back to their home VPN en route to the real destination. This may cause additional latency and could place a significant bandwidth load on the VPN server, especially if a high volume of high-capacity VPN links is being served...
4. While not all network traffic needs be routed via the user’s home VPN (just traffic destined for the home network may suffice) this may not be possible if the visited site only allows traffic out from its Wireless LAN when it is encapsulated in a tunnel to a “trusted” VPN gateway.
5. Some services are offered to institutions on the basis of observed source IP address. VPN users will have the benefit of appearing to come from their home institution, and thus be able to access such services as if at their home network.
6. VPN users may often be treated as internal to their home network. It is possible that while visiting “untrusted” WLANs that some virus or worm infections may be picked up that may then be relayed to the home network. Home site administrators should bear such risks in mind when setting site security policies.
7. Local authentication schemes should be able to differentiate between locally and remotely authenticating users, such that different levels of access to local resources can be offered based on whether the user is local or a guest.
8. There is an intention to migrate to IPv6 in the future, to take advantage of features including the larger address space. Most NREN’s already have IPv6 deployed natively (dual stack) on their backbone networks. It is expected that most universities will begin connecting natively soon; tunneled IPv6-in-IPv4 access may be used as an interim access measure. Roaming solutions should include IPv6 functionality from the earliest opportunity. .

# 7. Inventory of 802.1X network access to roaming requirements

This section provides a brief summary of the inventory produced by SURFnet on their 802.1X national roaming solution. 802.1X was ratified by IEEE in September 2001[[1]](#footnote-1) and is a layer 2 authentication solution between a mobile device and an access control device. Both wireless and wired networks are supported. 802.1X is used to control the network access at the edge of a network.

In 802.1X, the access control device can also detect the disruption of the connection and close the port if for example a cable is pulled out on a wired link or a wireless node leaves the coverage area of the wireless network. 802.1X authentication information is carried over the Extensible Authentication Protocol (EAP) for wireless or Extensible Authentication Protocol over LAN (EAPOL) for both wired and wireless access. Since there is no layer 3 access method, layer 2 needs to be encapsulated hence the use of EAP on LAN between the client and access control device, switch or authentication server.

This network access technology is different from other AAA schemes because authentication modules can be plugged in to cater for specific needs. If a RADIUS (Remote Access Dial In User Service) server is used, this server should support the Extensible Access Protocol (EAP). EAP can carry a number of authentication protocols, such as Transport Layer Security (EAP-TLS) or Tunnelled Transport Layer Security (EAP-TTLS). Since the ratification of 802.1X, there have been an increasing number of 802.1X client software solutions that have become publicly available. It is reasonable to expect that 802.1X implementations will continue to grow and harden in the next couple of years.

## Level of administrative overhead

Each Wireless LAN must have appropriate 802.1X client software installed; however, many newer operating systems now support 802.1X as standard.

When a new institution requests participation to roaming services, only its realm has to be entered into the National RADIUS Proxy Server, not into the servers of other institutions, because referrals to those institutions are relayed through the National Proxy. Therefore from the institution viewpoint, scalability is achieved without administrative overhead.

## Level of user transparency

The visiting user will initially require 802.1X client software to be installed and/or configured onto the client device. When a visiting user wants to gain network access, the visiting user will be asked to enter their credentials and once authenticated at their home institution, the visiting user can move freely from one wireless network to another, while their mobile device remains connected to the 802.1X enabled networks without additional user or administrative efforts.

If a visiting user tries to connect to a visited institution network, the RADIUS server at that institution will not recognize the visiting user credentials, as the visiting user’s realm is not recognised. When this happens, the RADIUS proxy mechanism ensures that the EAP encapsulated credentials get transported towards the home institution RADIUS server. The visited institution RADIUS server only has to know where to send unknown visiting user credentials and their requests to, in order to be authenticated.

## Security

The IEEE 802.1X standard for port-based authentication is a layer 2 solution between a mobile device and an access control device. In the 802.1X framework, authentication information is carried over EAP; this enables the use of various authentication methods[[2]](#footnote-2) that were mentioned earlier. Access control devices communicate with a RADIUS backend for visiting user verification; this is generally secure and scalable. After authentication, the communication between the mobile device and the access control device is encrypted using dynamic keys.

As long as a strong EAP capable protocol like TLS is used, 802.1X provides a framework that gives a sufficient level of security for the intended purpose, i.e. access control to the home institution network. Tunnelling protocols such as PEAP and TLS and TTLS can be configured to prevent “Man in the Middle” attacks because both the server and the client can validate each other using certificates.

If a security incident occurs, RADIUS can quickly and flexibly block access to a particular user@realm or requests from the particular realm. Once the incident has been resolved, the realm can be unblocked just as easily.

## Scalability

SURFnet has adopted a hierarchical RADIUS backend for user authentication. This solution only works if the mobile device, the access control device and the RADIUS server (in SURFnet’s case) support EAP

# 8. Inventory of VPN based network access to roaming requirements

This section provides a brief summary of the inventory produced by SWITCH on their VPN national roaming solution called SWITCHmobile that interconnects 12 Universities and research institutions.

The University of Bremen has a similar roaming system called Wbone that has been deployed across 5 academic organisations. For clarity the following section summarises SWITCHmobile only.

Visiting users can connect to docking networks. These networks are “open“, i.e. users are not required to input any credentials in order to get basic connectivity. The networks are designed to make it as easy as possible for the users to connect to the network and receive an IP address.

However, at this stage users won't have access to anything interesting yet (like resources on the Internet or at the home organisation). Access is granted exclusively to a list of all the VPN gateways of the participating organisations. This restriction is implemented on access control lists at the docking network. They deny any traffic except from packets that go to one of the listed VPN gateways.

In order to proceed, users have to initiate a VPN tunnel to the VPN gateway of their home campus and get properly authenticated there. Once a VPN session has been established successfully, users can use the Internet (via the VPN gateway at their home organisation) as well as resources at their home campus.

## Level of administrative overhead

The administrative overhead consists of updating the central list of trusted VPN gateways when a gateway is added or its address is changed. Whenever this happens, all the site administrators have to be notified about the change and they must adapt their local ACLs accordingly. The process of notification has been automated and adapting the ACLs might also be automated by the individual organisations.

## Level of user transparency

Users use VPN connections wherever they go, thus the method is transparent wherever they are (assuming the visited site supports VPN access, and does not have NAT or other firewall restrictions – other participating sites in the roaming environment will offer such support).

## Security

VPNs (at least those based on IPsec) are considered highly secure for data in transit. Devices will be considered inside their home network, and thus administrators should be aware of the risks of “infected” devices causing problems when connecting over a VPN.

## Scalability

The solution presented here is suitable for a limited group of organisations (e.g. all universities in Switzerland) but not suitable for a European scale. In order to overcome this limitation, the Controlled Address Space for VPN Gateways (CASG) has been proposed (for details, see the proposed approach section of this document).

# 9. Inventory of web-based redirection network access to roaming requirements

This section provides a brief summary of the inventory produced by FUNET on their web-based redirection national roaming solution.

To gain access outside of the visited institution network, the visiting user must launch their web browser (we assume they have one) which will be automatically redirected to an authentication web page (1), the access control device manages this process by capturing the HTTP connection and redirects the user's web browser to an authentication page (2).

On the authentication page a web form appears where the visiting user must enter their user credentials (e.g. username and password[[3]](#footnote-3)). This can be done over an SSL connection for password security. The access control device will then authenticate the visiting user at the user’s home institution based on their credentials (3) e.g. using RADIUS. If the authentication succeeds (4) the access control device modifies the firewall rules (5) to enable the visiting user to gain access outside of the home institution network. If the authentication fails, an authentication error is returned to the visiting user and the credentials are asked for again. The amount of failed authentication attempts can be limited.

## Level of administrative overhead

Local Access Control Lists may need to be updated so that visiting users are forwarded to an authentication page to enter their credentials. These credentials are then forwarded to a RADIUS proxy server and transferred across a hierarchy of RADIUS proxy servers back to the visiting user’s home institution to authentication with the home institution authentication server. Work may also be required at the national level RADIUS server to redirect credentials via another institution’s RADIUS server or another NREN level RADIUS server.

## Level of user transparency

User transparency will be high, as the user only requires an http-based web browser. These are normally installed in all operating systems as standard. There is no additional client software or configuration required at the user end.

## Security

This solution is less secure because it is based on using MAC-address and IP-address pairs where the attacker must be able to change a network interface card’s MAC address to an authorised MAC address to gain access. Though not impossible, this solution does restrict security breaches to only skilled and/or serious hackers and not typical users.

## Scalability

The Finnish web redirection solution is similar to 802.1X in terms of scalability in that it relies on a hierarchy of RADIUS Proxy servers behind a web proxy handler or the control device to forward authentication requests to a visiting user’s home institution, thus solving any scaling issues. The web redirection authentication solution differs slightly from 802.1X in that it uses an http or (preferably) https web page interface for visiting users to input their credentials that are forwarded to their home institution server rather than at the access control device.

# 10. Roamnode Authentication solution

The Roamnode is an access control device developed at the University of Bristol to provide a low cost solution that fits into the existing network and authentication infrastructure, without complex requirements. The original intention was to only provide secure wired, wireless, and remote access for local users; however, the architecture has developed to allow scalable and seamless roaming between trusting institutions.

The primary design goal of the Roamnode architecture is to de-couple the processes of establishing a physical network connection from the process of establishing a logical network connection. The reason for de-coupling is that each process is the responsibility of a different institution, and each has very different responsibilities. The first process - establishing a physical connection - is the responsibility of the visited institution. The second process - establishing a network connection - is the responsibility of home institution.

The second design goal of the Roamnode architecture is to use very simple interfaces between each component or layer of the protocol stack. This allows a protocol or a mechanism to be easily complemented or replaced with an alternative without disrupting the rest of the system. For example, the Roamnode currently uses the PPTP VPN protocol, but this could be changed to any other VPN protocol that is transported over IP.

The final design goal of the Roamnode architecture is to provide a vertical solution that allows higher layers to interact with lower layers; for example, to deliver location-aware applications, or to allow applications to disconnect users or to query and alter a user's bandwidth allocation.

## Level of administrative overhead

An institution that deploys the Roamnode architecture and peers with the NREN’s national RADIUS proxy server can provide a seamless mobility service, either as a visited institution or as a home institution, without any additional administrative effort.

An overlay network has been created to avoid the need to allocate visitors with public IP addresses prior to establishing their VPN connections to their home institutions (these addresses would need to be public to allow Internet routers to make routing decisions for visiting users' VPN sessions). This is because these public IP addresses would need to be allocated from the visited institutions allocation, which would therefore violate the Roamnode architecture's primary design goal. It also allows institutions with limited or no available public IP address space to participate, without needing to use NAT.

The mobile device can only connect to the visiting user's VPN gateway via the IP-in-IP tunnel that is built between a Localnode and Homenode when the RADIUS ACCESS-ACCEPT packet is returned to the Localnode. This tunnel is built when a visiting user requires connectivity between the Roamnodes, and torn down when the visiting user no longer requires the tunnel. The process is entirely automatic, no management or configuration of the overlay network is required: it is built entirely on-demand.

## Level of user transparency

The username and password need to be entered to authenticate. This is the visiting user’s home institution username and password, and the username must be unique. Roamnode is designed to be entirely transparent to the visiting user as this user is allocated an IP address from their home institutions, so all applications would work as if that user was gaining network access physically at their home institution.

## Security

A visiting user can connect to a visited institution's network only if the visiting user credentials are authenticated by the home institution that is trusted by the RADIUS back-end. This connection provides the minimum connectivity to establish a VPN session with the visiting user's home institution.

The Roamnode architecture has exact knowledge of every visiting user’s name and home institution from the moment that the mobile device connects (this is because the home institution is explicit in the realm). Hence, visiting users are easily traced to their home institution. A central registry of realms and contacts could be maintained on a website to assist in liaising with other institutions. Another option would be to include a RADIUS attribute in the RADIUS transactions that describes a contact address for that institution.

The Localnode only allows the mobile device to send packets to the visiting user's Homenode, and only forward’s packets to the mobile device that have originated from the visiting user's Homenode. This prevents a visiting user from using the service for any other purpose other than connecting to the visiting user's VPN gateway.

Only a cryptographic hash of the visiting user's password is passed to the Localnode, and not the password itself. Therefore, it is not possible to acquire credentials of a visiting user by sniffing the visited institution network, or by a malicious third party masquerading as a trusted authenticator. The Localnode also authenticates itself to the mobile device by passing it a second hash returned from the user's AAA server. The mobile device will not establish the connection to the Localnode unless the hash is correct. Thus trust is established in two directions.

## Scalability

In the Roamnode architecture the visited institution does not need to provide any of its own address space to visiting users. This is because visiting users are simply allocated an RFC1918 address from the Localnode's allocation to allow them to connect to their home institution VPN gateway across the mesh network. The Roamnode can reside behind a properly configured firewall performing NAT, enabling organizations that have a limited number of public IP addresses to participate.

The Roamnode architecture does not require edge hardware that can be quite expensive[[4]](#footnote-4). The Roamnode could be run on a redundant PC for example. A single Roamnode can handle several hundred simultaneous sessions. Roamnodes can also be clustered to create a “virtual” Roamnode, which can handle very many more.

If the volume of connections running through a given VPN becomes a problem, bandwidth limitations could be applied per connection.

# 11. Preliminary selection for Inter-NREN roaming

# This deliverable provided an overview of each national solution and compared each against the defined requirements. The conclusions reached were as follows

The TF-Mobility group confirmed that there was no single national roaming solution that was suitable for inter-NREN roaming. Instead the taskforce agreed on the need to develop infrastructure to ensure interoperability between national solutions could be achieved bearing in mind the need to meet the majority of the requirements identified in earlier deliverables. As an aside, the taskforce decided not consider the following in their work

* **Local - VPN**: VPN users will not be able to access a visited institution’s VPN gateway because although it is technically possible to offer access to all VPN servers, this would not be practical as all participating institutions would have to purchase a VPN server for this single purpose
* **PKI**: It would be good to have PKI when it is ready; currently it is not and would be complex to manage. Given the limited lifetime of TF-Mobility, PKI will not be considered. When PKI is ready, the group agrees it would consider the merits of migrating to such a solution.

This deliverable outlined in technical detail a design for interoperability between 802.1X, web-based redirection and VPN solutions. It highlighted nine scenarios and additional work and or equipment needed to support other guest users.

 User with | 802.1X | VPN | Web-based |

 Site uses | | |

 -----------------------------------------------------------

 802.1X | Okay | Work reqd | Work reqd |

 VPN | Work reqd | Okay | Work reqd |

 Web-based redirect | Work reqd | Work reqd | Okay |

These designs were to be tested with results documented in a preceding deliverable. A phased development and testing programme was recommended and can be seen as follows: -

**Figure 4:** A diagram showing the recommended approach to develop interoperable roaming guest access.

## The group’s main aim is to bring each of the three streams of work as closely together as possible, ideally so that they can interoperate with each other.

TF-Mobility group members have successfully developed a RADIUS backend approach between the UK, Portugal, Croatia, Germany and the Netherlands using 802.1X with EAP/TTLS, and a Radiator RADIUS server[[5]](#footnote-5) at all participating institutions for this demonstration. Finland has also recently confirmed a link to this hierarchy at the TF-Mobility meeting in September 2003. It is envisaged that Deliverable H will test the RADIUS proxy hierarchy and result in an agreed user@realm standard and a defined list of minimum requirements for protocols carried by EAP, and / or considerations of those protocols themselves to form guidelines for NRENs and possibly institutions too.

The RADIUS Proxy hierarchy is currently in place and is growing in terms of NREN participants and institutions. The current status at the time of writing is as follows

The taskforce has also recognised the need for policy guidelines to ensure the RADIUS proxy hierarchy is both manageable and scalable and also to protect and foster trust amongst participating institutions. This work has been completed in a later deliverable.

A proposed solution to solve the VPN scalability problem is to develop a new concept called Controlled Address Space for VPN Gateways. CASG are IP address ranges that each NREN has to obtain for themselves for their VPN gateways. In this way the packet exchanging between the CASG network and the VPN gateway should be secure.

The diagram below describes the proposed architecture for a scalable wireless roaming VPN solution.

Development work in this area was undertaken in parallel to RADIUS interoperability testing.

The Roamnode (PPPoE over Linux) solution is an independent solution that has been developed at Bristol University. The taskforce recommended additional work to the Roamnode software to achieve interoperability with other national roaming solutions and tests thereafter.

# 12. Test bed and reference design for inter-NREN roaming

The original intention for this deliverable was to describe the architecture of the selected inter-NREN roaming solution. However, the “Preliminary selection for inter-NREN roaming” concluded that there will be no single national solution recommended as the European model. This is because no one solution outperforms, each solution has a number of strengths and weaknesses making such choices difficult. In addition there has been a considerable investment made to develop a variety of national solutions and there is a low likelihood that NREN’s will abandon their solutions in favour of a European model.

Therefore the deliverable has instead been focusing on ways to make the three main solutions (802.1X-, Web-redirect-, and VPN-based) interoperate. That is to say, make sure that visiting users that use another solution still can authenticate at the visited institution, even though this solution is not offered to the home institutions users.

The three major approaches have some characteristics that need to be taken into account when creating an interoperable solution. 802.1X based authentication is inherently different from Web based redirection and VPN-based authentication due to different demands on the wireless LAN networks. 802.1X enabled wireless networks require an encrypted channel (with dynamic WEP-keys), whilst the two other mechanisms are based on the concept of open, unencrypted access to the docking network. On the other hand the CASG approach for VPN-based access can not use a RADIUS backend whilst the other two solutions do require this. So the following situation exists:

 Approach | 802.1X | VPN | Web-based |

 Technology | | | |

 ----------------------------------------------------

 encrypted radio | Yes | No | No |

 RADIUS backend | Yes | No | Yes |

The result of these contradicting requirements is that in order to support both types of network authentication two logically separated networks on the radio layer need to be constructed. In the case of an access point it means that the access point must be capable of using multiple SSID’s and can support VLAN assignment, an example can be seen from the following docking network configuration:

Figure 7: Network lay-out with multiple SSID’s and VLAN assignment to support a number of roaming network access solutions.

If the access point is not capable of broadcasting multiple SSID’s it may be necessary to create a layer 1 separated architecture.

In addition to this, an institution that uses 802.1X or Web-based authentication needs to open up their switch for the CASG address-space while an institution that provides VPN-based access needs to set up a RADIUS server that connects to the eduroam RADIUS-hierarchy.

The deliverable describes the test beds that were created at the University of Tampere in Finland (Web-based), SWITCH (VPN-based) and SURFnet (802.1X-based). Each of these institutions have successfully created a setup that allows for guest use for all three approaches, using a different set of hard- and software.

The document describes into detail these three setups and the user experience of visiting users.

Based on the three test beds a reference design has been produced that guides an institution that wants to provide guest access for visiting users in setting up the necessary infrastructure.

The deliverable clearly demonstrates that inter-NREN roaming is indeed possible, time will show in how far these competing and co-existing solutions will continue to exist. However, by building an infrastructure that is able to deal with users using the various access methods provides also for an easy migration for the home institution’s users to one of the other two methods.

# 13. Roaming Policy guidelines

To facilitate the uptake of inter-NREN roaming in a manageable and scalable way and ensure the fostering and protection of trust amongst participants, roaming policy guidelines were needed to cater for roaming users, home and visited institutions, NRENs and the organisation responsible for the TERENA level RADIUS proxy server. This deliverable was created to draft policy guidelines to assist the scaling of the RADIUS proxy hierarchy and other roaming solutions as these emerge. The policy drafted by the group can be seen below as an abridged version:-

# The vision

The vision of the TF-Mobility taskforce is to create a collaborative environment where academic guest users can visit other institutions either nationally or internationally and be offered an automated network access service. The service should be recognizable as an academic roaming service and offer a minimum agreed level of security. Some institutions may make available a range of security options to the guest / roaming user, however it is the responsibility of the guest / roaming user to respect the acceptable use policy of the *visited* institution as well as, of course, to follow the AUP of their *home* institution.

Once authenticated credentials have been sent to the guest /roaming users home institution authentication server and have been successfully processed, the visited institution will “trust” the response from the guest / roaming user’s home authentication server and grant a level of network access based on the visited institutions local site policy. All authentication sessions and network access sessions must be logged for auditing purposes to ensure that any breaches of the local acceptable use policy can be traced and appropriate remedial action can be taken in a timely manner that is acceptable to all participants.

Ideally the guest or roaming user should not have to do anything in addition to what he/she would normally do if physically located at their home institution. It will be necessary for home institutions to educate their own users participating in this service to ensure that they abide by policies contained herein and contact the appropriate person(s) for technical support related matters.

# Roaming Services - General Principles

* The obvious security requirementis that the roaming access must only be available to authorized users, which should include all users authorized for Internet access at the participating NRENs and their institutions.
* All roaming users are required to authenticate at their home institution in order to be granted network access at the visited institution.
* All roaming users are responsible for their own credentials (and transmission thereof) and must abide by the roaming AUP (see section 1.1 hereafter) that has been agreed on behalf of the user by their home institution.
* The visited institution must be able to prove that the network access service has access to the roaming service so that roaming users can recognise and take advantage of it.
* The visited institution must clearly state that the mechanism for the transmission of user credentials is secure. If not secure the visited institution must (if requested) be able to support a user-initiated solution typically from the guest user’s client device so that a securer solution is possible.
* The visited institution has the right to block any roaming user, academic institution or NREN from accessing its local area network access provision.
* The visited institution will determine the authorisation of the network access provision.
* The home institution will be responsible for supporting their guest users including educating users on service support issues and abiding to relevant policies.
* Participants should provide feedback to their institutions on the roaming service and if necessary, escalate any issues to their NREN who in turn on rare occasions may escalate a matter onto Terena to either log or resolve.

# Benefits of roaming services

* There will be a lower administrative burden supporting guest / roaming users.
* Users will ideally be able to gain reasonably secure transparent network access in a less complex and more timely manner without changes required to their client devices and ideally no need for additional user credentials.
* More pervasive transparent and secure guest or roaming access should result in greater opportunities for collaborative research and academic work groups between academic organisations both nationally and internationally.
* The use of authentication servers with logging facilities should provide a better system of traceability than the current solution of manually allocating guest access.
* Some roaming services can also be of local value for local users at the home institutions, i.e. user authentication services.

# Policies

To facilitate the interest shown in roaming services it is important that policies are put in place at appropriate levels to ensure that benefits remain whilst threats and risks are minimized and managed within acceptable levels. The following sections will list policies that relate to different levels of control and responsibility within a hierarchy of trust.

# Roaming Services – Intra-NREN roaming Policy

1. **TERENA level policy (agreements for participation between NRENs and TERENA)**

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. Participating NRENs must abide by this “roaming” service agreement contained herein.
	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.
	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.
	4. NRENs must have the following procedures in place to handle
		1. National authentication server support and maintenance.
		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
		3. Fraudulent use of the roaming service by users or groups of users.
		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.
		5. A mechanism for providing feedback on the roaming service so that guest or roaming users can identify participating institutions and their service offering.
	5. Ideally, NRENs should have a minimum of two authentication servers at different locations on their core network for resilience and redundancy.
	6. The NREN must mandate their participating institutions to notify guest users on the level of security offered for the transmission of user credentials.
	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.
	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.
	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.
	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.
	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.
1. **NREN level policy (agreements for participation between NRENs and their institutions)**

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

* 1. Participating academic institutions must abide by the “roaming” service agreement contained herein.
	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.
	3. Participating academic institutions must provide a secure authentication server that can securely process and forward user credentials as required.
	4. Participating academic institutions should communicate to guest or roaming users on whether and how they offer the roaming service.
	5. Participating academic institutions should inform guest users of the level(s) of security offered for the transmission of user credentials.
	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.
	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.
	8. Participating academic institutions must report any security issues or fraudulent activities to their NREN to manage and resolve accordingly.

14. A web repository of tests on Wireless LAN devices

This deliverable was a comprehensive review of wireless products to be sure that NRENs or institutions who were considering investing in a roaming solution were able to make informed decisions on the choice of equipment in today’s marketplace. Detailed technical information was made available on the UNINETT website as follows

# 5. A document outlining the impact of new technology and protocols such as MobileIP on current roaming work.

16. A summary of national roaming developments

## 16.1 Croatia: Current status in Croatia (CARNet network)

CARNet and University Computing Centre, University of Zagreb (Srce) have set up a national hierarchy of radius servers tied up with LDAP directories. Our goal is to ensure that every institution connected to the CARNet network runs its own radius server and LDAP directory. We see it as a basis for the AAI of A&R community in Croatia.

Our national hierarchy has been started in February 2003, originally as basis for CARNet's dial-in service. Currently (June 30, 2004) we have 197 institutions covered. Out of this number 163 run their own radius and LDAP servers, while 34 are hosted by Srce. Total numbers of registered users is 130647 (June 30, 2004). Our national hierarchy has been connected (via dedicated radius proxy server) to the European Radius Hierarchy (started by TF-Mobility).

Aside of dial-in access our national radius/LDAP hierarchy is also used for:

* wired and wireless (802.1x) access to the CARNet network from student dormitories (currently in operation only in Zagreb (selected dormitories only) and Osijek , the rest is under the construction right now)
* wirelless access at selected venues (e.g. CARNet and Srce building, selected faculties, ).

Our plan is to use the established radius/LDAP hierarchy as the AAI for network access (dial-in, wireless, wired, cable, ...). We have some organisational work in front of us too, esspecially regarding the policies (for users and CARNet member institutions). We plan to stay in the European Radius Hierarchy and look forward to it as a regular service. Current status is illustrated with the next picture.

**Miroslav Milinovic (miro@sre.hr) (30 June 2004)**

## 16.2 Czech Republic: National status of “Eduroam” roaming services

CESNET are currently up and running with national radius servers (radius1.eduroam.cz and radius2.eduroam.cz) which are ready to operate requests from an organisation level radius servers. Our national RADIUS proxy servers are also connected to the Terena (Euro) level radius servers. This means the radius hierarchy is operational but it is still very much in a testing mode. We decided use the FreeRADIUS implementation (because of open source, cost, etc.) but it has not worked as well as had been expected. The operation stability of the FreeRADIUS isn't as good as we had expected. My colleague is testing the RADIATOR at the moment and we'll probably change RADIUS server software in the near future.

CESNET also has allocated the CASG IP address block for VPN gateways. We want to support all three authentication methods; however our priority is still 802.1x.

Discussions about roaming policy are currently in progress. A policy document is being reviewed by our NREN board of directors (representative from universities, academy of science, etc.) and by an independent law company. The end result should be agreement to a national policy document by the end of September. We believe that having the roaming policy and the radius hierarchy in place is absolutely necessary in order to start the pilot project that is scheduled to take place during October.

To date CESNET has received the "promise" of collaboration in this pilot project from five universities (TUL Liberec,CVUT Praha, VSCHT Praha, VSB Ostrava and ZCU Plzen) and we hope that many more institutions will join this project.

Other work activities include the testing some wireless devices (AP, client supplicants), tuning optimal network configuration, and work on the main “eduRoam” information portal for the Czech Republic ([www.eduRoam.cz](file:///C%3A%5CUsers%5CDell%5CDocuments%20and%20Settings%5Cjamess%5CLocal%20Settings%5CTemporary%20Internet%20Files%5COLK21%5Cwww.eduRoam.cz)), the "final product" should be complete very soon.

**Jan Furman (29 June 2004)**

## 16.3 Denmark: National status of Eduroam-project in Denmark

Since Autumn 2003 the Danish NREN, Forksningsnettet, has closely followed the work of the TF-Mobility group. One large and one smaller meeting on roaming have been held with NREN-technical staff and network people at the connected institutions. Generally people are enthusiastic and eager to participate in Eduroam.

Forskningsnettet has in spring this year installed a redundant set of national RADIUS-servers (Radiator) which in turn has been connected to the top level server in Holland as of mid-June 2004. So far only the Danish Technical University is hooked up to the national server but other institutions will join in the coming months.

UNI-C, who runs the NREN, has now become national reseller of the Radiator software to academic institutions.

Denmark has offered to host a secondary top level RADIUS-server to the one in Holland, which is now being implemented. This sort of international redundancy will make sure that international roaming users will not be affected if a large power failure or other such event.

The Danish NREN newsletter announced the Danish participation and new possibilities for students and researchers in mid-June. Also articles will be printed in the campus papers of the larger institutions.

The RADIUS-hierarchy is now also paving the way for the Danish NREN's general offer to use a centralized iPass-service. Each institution can now sign up for the service and will be billed individually (at a lower price pr. minute, negotiated collectively by the NREN). As the authentication requests from iPass are RADIUS-packets these are received by the national roaming-server and redirected to a dedicated authentication iPass-server. Each iPass-user is provided with a unique NREN-ID which is matched to a name, institution etc. and which can hopefully later be used to provide the users with more services.

An administrative web interface has been developed, so that all participating institutions will administer their own users and thereby effectively be in control of their own phone bill. Other services are being considered as 'add on' to the RADIUS-based roaming service, i.e. distribution of IP-phone numbers based on approved authentication, roll based privileges etc.

**David Simonsen (22 June 2004)**

## 16.4 Finland

The original idea was combine authentication databases so that people can go to different universities and get access without trying to find local administrators in order to get a guest account from them. Most of universities were already doing authentication, mostly by web redirection using the RADIUS protocol so the development of a RADIUS proxy hierarchy was a logical choice. Another reason for developing the RADIUS proxy hierarchy was that we are also planning to support 802.1X in near future which also relies on a RADIUS proxy hierarchy.

We have been active participants in the TF-Mobility group and have contributed on many of the deliverables. We have also been the owner and author of Deliverable F: "Inventory of web-based solution for inter-NREN roaming".

The current status in Finland is that we have 20 realms registered with 12 academic and commercial organisations participating. Our pilot will continue to run until June 2005 and we are planning to expand organisational participation to the RADIUS hierarchy by developing a marketing campaign to generate awareness of roaming services to users. In addition we will be investigating RADIUS proxy server monitoring issues and we hope to develop some solutions in this area during this year. Currently we can identify both failed and successful authentication requests but we have no other monitoring information available, for example we cannot monitor an organisation’s RADIUS server availability.

CSC will also create web page for roaming services during this year.

## Sami Keski-Kasari (30 June 2004)16.5

## Germany

Germany has started a pilot project (DFNRoaming) on internet roaming subject on the first of January 2004 chiefly based on results/solutions taken from TERENA TF Mobility and from others sources. A test bed was installed at the DFN premises in Berlin.

At first, the aim was to set up an infrastructure based on IEEE 802.1X port authentication and a top down radius hierarchy was established. Two radius servers (802.1X compatible) were set up at the DFN G-WiN backbone, one for direct use and another one as a backup server. Unfortunately the current status in Germany is that only a few research institutions and universities support 802.1X in their local environments. This problem cropped up mainly due to old access point's technology and insufficient support of the 802.1X supplicants on the user's side what were used on the campus' wireless LAN.

Instead different VPN solutions are used locally. But 802.1X is a promising technology to make WLAN infrastructures more secure, so DFN introduced/offered a so called "Modular 802.1X migration solution (Mod8.X)" that supports a minimum demand web-based authentication immediately and 802.1X based authentication in the future, that means as soon as institutions will be able to set up access points that are capable of 802.1X and that are able to manage more than one “ESSID” for network identification.

Mod8.X can live together with VPN - based authentication and starts with a web-based authentication. Mod8.X comes with a debian Linux box, two LAN Ethernet cards and access points. The debian Linux box has to be configured with 802.1q and VLAN should be enabled. Among other things a firewall script can be easy configured as well. As a web-based solution we recommend tino from the University of Tampere in Finland, tino consists of some perl scripts and a cgi script and is very easy to handle. Naturally some commercial web-based solutions are also possible but we didn't try them.

Because of the Mod8.X modular design, only the access points have to be changed and a second “ESSID” has to be established in the future if you want an upgrade to 802.1X in your WLAN infrastructure. Under DFNRoaming we deploy two “ESSID’s”: "802.1X" and "VPN/WEB". Institutions that want to be part of DFNRoaming are obliged to use these “ESSID’s”, but don't control it.

At the moment we have 15 large institutions registered at the DFN top level radius with approx. 15,000 users. However, this does not mean, that DFNRoaming is operational around these campus networks. There are still a lot of construction areas and we are working on a DFN-wide-map to configure out what is the status of the construction. There is an operational link from DFN top level radius to TERENA top level RADIUS and vice versa. Future plans involve a native 802.1X authentication environment spanning DFN with about 500 research institutions and universities with 1.5 million users (most of them are students).

**Ralf Paffrath, Juergen Rauschenbach (30 June 2004)**

## 16.6 Greece

## 16.7 Netherlands

At the end of 2001 SURFnet, the Dutch NREN, started looking into methods for secure access to wireless LAN's. Early 2002 it was decided to trial 802.1X with the University of Twente and the company Alfa-Ariss. As part of this trial Tom Rixom of Alfa&Ariss developed a freely available supplicant, now known as SecureW2. SURFnet made its RADIUS infrastructure available for use with this technology to provide for guest access.

Based on the success of this trial, the University of Twente decided to mandate 802.1X support in its European tender for a wireless campus. After an expert meeting in April 2002 a number of members of the SURFnet constituency decided to move to 802.1X for (wireless) network access too. In March of that same year SURFnet took the initiative to organize a workshop on network access at TERENA and later a meeting at TNC in Limerick to discuss setting up a taskforce on mobility. In 2003 SURFnet set up a European top level server for TERENA.

The roaming access service is launched under the name Eduroam, the website http://www.eduroam.nl will provide a portal for this service. Currently approximately 50 institutions take part in the RADIUS hierarchy whereas some 15 provide roaming wireless LAN access.

Current and future activities evolve around a number of themes:

**Policy**

Discussion about roaming policies has started. A draft policy has been produced to be included in the contracts with all SURFnets customers.

**Supplicant software**

A contract has been signed with Alfa&Ariss to further develop the SecureW2 software to include pre-built localised versions of the client.

**Tracking and tracing**

A group of universities have jointly developed a first version of a system for tracking and tracing of users in order to track abuse. This software is available at http://www.sourceforge.net/projects/usertracking

**Basic infrastructure**

Although the existing RADIUS-infrastructure that forms the basis of Eduroam performs its tasks satisfactory new developments will constantly monitored to see if any changes are useful or necessary. Emerging technologies like DIAMETER and DNSsec will be evaluated. Furthermore, the use of the existing basic infrastructure to provide other access to services will be investigated.

**Integration with application access**

For (roaming) access to applications SURFnet uses a authentication system for web-based applications called A-Select (<http://www.a-select.org>). This tool allows for the use of various authentication means. SURFnet will investigate the integration of A-Select with the Eduroam service to make the use of various authentication means possible and to deliver a single sign on for both network and application access.

## Klaas Wierenga (1 July 2004)16.8 Norway: National status of “eduroam” in Norway

UNINETT is the NREN for Norway. Among our members are 4 universities and 40 colleges. Other members include miscellaneous research facilities. The daughter company UNINETT ABC aims at providing technological aid and expertise to schools at graduate and high-school and levels.

The future core of the UNINETT authentication system is FEIDE (<http://www.feide.no>) which is a "FEderated ID for Education". FEIDE will provide the user database and PKI. RADIUS servers are used at most organizations and it is one of the goals of FEIDE that they in the future only will function as a proxy for the back-end FEIDE. The FEIDE system will bind the organizations together and enable users to roam across organizations. FEIDE does not facilitate RADIUS by itself and therefore needs local RADIUS servers to handle requests from the various authentication systems. The RADIUS servers can be tied together in a national hierarchy in parallel to the FEIDE network. By connecting this to the European RADIUS hierarchy, it will be able to support roaming for visitors that are participants in "eduroam"

At this stage the various member organizations have employed various wireless security measures ranging from none at all to web portals, VPN and 802.1X. UNINETT is advising its members on the use of 802.1X based security which is supported by FEIDE and also gives the organization a choice of authentication method and encryption in accordance with local security policy.

UNINETT has a FEIDE AA structure in development and 802.1X authentication on wireless networks in place. Several members have signalled their participation and together we have started a nation-wide deployment effort. The top level national RADIUS server is nearly ready for connection to the top level European RADIUS hierarchy so that we can take part in the "eduroam" cooperation.

**Jardar Leira (29 June 2004)**

## 16.9 Portugal: The Portuguese Roaming Project e-U

The Portuguese roaming initiative started within e-U virtual campus project (www.e-u.pt sorry no english version). This project, partially funded by Portuguese government, will implement, among other things, wireless infrastructures on every higher education institution.

FCCN’s role on this project it to study, produce documentation and provide the necessary help on the deployment of these infrastructures, so that they allow roaming for students and teachers in every campus. A pre-requisite to get funds on this project is that all built infrastructure is able to roam users.

To achieve these goals, we start with 8 pilot institutions that tested some hardware and several controlled access solutions like web-based login (nocat and nomadix), VPN access based on certificates and 802.1x. Based on these tests, we adopted 802.1x/EAP as our national roaming solution. Every campus will have at least 2 SSIDs (broadcasted ‘guest-e-U’ and ‘e-U’ that in most places will not be broadcasted). ‘guest-e-U’ is open with no WEP and e-U demands for 802.1x authentication. The first one gives only access to a local Web Server and the second provides access to Internet. So far we have 62 institutions (almost all public and private higher education) in the project in different stages of deployment, 7 with roaming already in place and tested.

In the design of the hotspot we’ve defined some basic principles (in order to make the roaming experience 100% transparent for the end user):

**Preferred EAP’s**: PEAP and TTLS (those are the one’s that we test on the hotspot but the institutions may choose among other ones)

**Broadcasted open SSID**: ‘guest-e-U’ with access to a web server with documentation; software; may not cover all the hotspot

**802.1x SSID**: ‘e-U’ with dynamic WEP key’s (we are avoiding to use WPA/TKIP because of the not so mature drivers and support) with roaming; should cover all the hotspot

**Radio Channel’s:** from 1 to 11 for compatibility with US cards/centrinos – we mention the importance to use non overlapping channels like 1, 6 and 11 but they are free to make their wireless deployment with other channels.

**IP assignment:** the roamers are supposed to get a public IP address to avoid the problems that some software / VPN concentrators have with NAT.

The link for the e-U Project at FCCN is (again english not supported):

http://www.fccn.pt/index.php?module=pagemaster&PAGE\_user\_op=view\_page&PAGE\_id=114&MMN\_position=90:4

This section includes:

Access Point tests results (3Com, Alcatel, Cisco, Enterasys, Gemtek, HP, Nortel, Proxim and SMC);

Vendor cookbooks (Enterasys, Cisco and Alcatel);

Radius server cookbooks (Radiator, FreeRadius and IAS);

Best-practices and other relevant documentation.

## Luis Guido (30 June 2004)16.10 Spain

This section explains the main objectives and the current state of a mobility initiative at a national level in Spain (MovIRIS).

MovIRIS is a national initiative that belongs to the Spanish Research Network. Its main objective is to coordinate Spanish research organizations with the aim of creating a unique mobile environment for their users. To do this, there is a national mobile use policy (currently only in Spanish) that is compatible with European policy. Also, from RedIRIS, we give our organizations the necessary support to ensure their mobile infrastructure is compatible at technical level with the technical solutions supported by the TF-Mobility group.

The main objectives of MovIRIS are as follows:

* 1. To coordinate the starting of a national mobility infrastructure in our community, by being a single point of contact for common problems and solutions.
	2. To develop a national mobility use policy compatible with the European mobility use policy.
	3. To make sure that there is compatibility in the technological level solutions implemented in different national research organizations with those ones supported at European level.
	4. To coordinate information, local to organizations, related with mobile access methods, mobile infrastructure, etc.
	5. To support and promote national initiatives and solutions in the mobility area.

## MovIRIS started two weeks ago, and there are currently 7 organizations involved. Two of them with a quite long experience: one of them uses VPN technology, and the other one has developed a version of NoCat with improved users and roles management.

## Rodrigo Castro (30 June 2004)

## 16.11 Switzerland: SWITCHmobile physical roaming services.

SWITCHmobile is the Swiss physical roaming service for Switzerland. The project was launched in Q4/2001, due to the increasing need to develop a solution that would enable physical roaming between campuses for researchers, professors, students and university staff. The first SWITCHmobile-workshop was held in June 2002, a number of potential solutions were investigated and presented. As a result of this workshop a working group with members from several universities and research institutes was formed and led by SWITCH to investigate whether a technical concept for a national roaming solution was feasible.

The working group agreed on a VPN solution as their preferred solution and published a first version of the technical concept in December 2002. Besides working on the technical concept a test bed with several pilot sites was also created. SWITCHmobile changed it status from trial to operational status in Q2/2003.

When TERENA launched the TF Mobility in Q1 2003 SWITCH participated in an active role one as representatives for the VPN approach. During the lifetime of TF Mobility, SWITCHmobile has mainly focused on the expanding the number of participating sites. Currently, SWITCHmobile has 15 active participating sites (universities and research institutes) with a few additional sites scheduled to join shortly. A map of participating SWITCHmobile sites can be seen below

Aside from the deployment activities, SWITCH is also organising regular working group meetings to facilitate discussions on general issues, problems and solutions. Besides the technical concept the working group has also created a concept for user and communication guidelines to define a common denominator across the SWITCHmobile participating organizations for communicating the SWITCHmobile concept and usage to the users. A small but substantial lab has been built at the SWITCH head office in order to be able to test new technologies and gain experience working towards a possible next-generation SWITCHmobile.

In the near future the stable and deployed VPN solution will still be the favoured solution. Working group meetings will be held three to four times a year, discussing further developments and other concerns. Within our lab we plan to create test beds for emerging technologies: 802.11i, seamless roaming, Mobile IPv6 etc. SWITCH will also participate in the TF Mobility

(v2) and JRA5 of GEANT2 to help and contribute towards a European roaming solution that can cater for our national needs and to expand the reach of roaming services across Europe and internationally.

Further information concerning SWITCHmobile can be found at http://www.switch.ch/mobile

**Hansruedi Born (13 July 2004)**

## UK: National status of Location Independent Networking to facilitate “eduroam” in the UK

In the UK, UKERNA has been closely involved in the work of the TF-Mobility group. In parallel, we have established a JANET Wireless Advisory Group to look into the issues of wireless, mobility and the provision of guest access across the UK. Over the past twelve months, UKERNA and the JANET Wireless Advisory group have been designing and developing the “eduroam” concept based on a RADIUS proxy server hierarchy to support web based redirect, 802.1X and VPN network access methods. An architecture document was produced together with draft policy guidelines necessary to support and encourage participation. The work area has been titled “Location Independent Networking” and has been referred to as “hassle free” guest network access.

There has been significant interest in the development area so far. An example of how the concept has been promoted to the JANET community can be seen on the figure on above.

The Location Independent Networking concept relies on a network of trust to be established between participating JANET organisations that have an authentication server that is configured to allow a guest user to enter and send their credentials onto their home organisation’s authentication server. Once successfully authenticated, the visited organisation will then grant network access to the guest user according to the visited organisation’s local policy.

UKERNA has initiated a development project to trial a two-tier national RADIUS proxy server hierarchy to test whether it can support the Location Independent Networking concept. The University of Bristol has been selected to manage two National RADIUS proxy servers. It has already built the National RADIUS proxy servers and technical support services in anticipation of proof of concept tests that are scheduled to commence in August 2004 with the following five participating organisations :-

* The University of Edinburgh,
* Lancaster University,
* The University of Manchester,
* The University of Southampton,
* The University of Strathclyde,

Once the National RADIUS proxy hierarchy has been successfully tested, the national servers will then be connected to a European level RADIUS proxy server to further test the concept with participating National Research and Education Networks and their organisations.

If the test phase is successful, UKERNA will issue an open Call for Participation to the JANET community in September 2004, with a view to seeking a number of JANET organisations to participate in the national trial service for a period of six months. For the trial service, the National RADIUS proxy service would be hosted at co-locations on the JANET backbone and managed remotely by the University of Bristol.

More details will be made available at http://www.ja.net/development/network\_access/lin.html

**James Sankar (29 June 2004)**

**17. Conclusions**

The aims of the TF-Mobility group have been recognised as relevant and applicable in terms of benefits to academic researchers, staff and students that may have to work in more than one physical location. The work itself has been practical, technical and of sufficient scope and depth to be of use to many NRENs and Universities. The net result has been a significant interest in the mobility area and enthusiasm from the academic communities across Europe and beyond to participate in roaming activities.

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 an easy upgrade path towards 802.1X.

As the group nears the end of its 18 months lifetime, it has been proven that it is possible to create a fully interoperable solution and a cookbook has been written to ensure that the knowledge gained can be shared amongst the NRENs and their institutions.

Interest in participating in these activities has grown significantly with many NRENs developing their own roaming infrastructures to integrate into the interoperable solutions mentioned earlier. As a result, the taskforce has developed a set of policy guidelines to ensure the development service can scale and be manageable and also has the necessary foundations to move current work towards a service model.

Other work has been produced in the development of a product matrix on wireless Access Points and Wireless client cards. In addition a deliverable has been written to consider the impact of Mobile IP / IPv6 on the current roaming infrastructures. The taskforce has completed all of its original deliverables and added some new items along the way; further work has been considered and will be presented in the next section of this report.

# 18. Recommendations for future work

The taskforce consider future work items and whether to request the formation of a new group at meetings in Berlin, Amsterdam and Rhodes. These discussions led to an agreement to continue the work done but also to avoid any overlap from work going undertaken by DANTE in the JRA5 development activity area. A new charter was agreed at the final taskforce meeting in Rhodes in June 2004. The charter details the groups’ recommendations for future work.

### Task Force Mobility (v2)

### Version date: 30.05.04

### Terms of Reference

1. A Task Force is established under the auspices of the TERENA Technical Programme to continue existing TF-Mobility work to develop roaming services for mobile devices using network access technologies already deployed (or planned) in the national research and education networks (NRENs) involved in the task force in close cooperation with the Géant2 joint research activity JRA5 ('Ubiquity (Mobility) and Roaming Access to Services'). In addition, work will be undertaken to review work produced to date and to give consideration for new work areas, namely (1) extending roaming service access beyond NRENs to other networks and (2) develop securer, more flexible and more accountable roaming services by investigating and testing system integration with other Authentication, Authorisation and Accounting solutions. The new group will be known as TF-Mobility (v2).

The focus of this taskforce will be as follows:

1.1 To gather input from the community at large on developing and scaling inter-NREN roaming services to be fed into JRA5.

1.2 To disseminate JRA5 results with respect to inter-NREN roaming services to the community at large.

1.3 To investigate and pilot new technologies for mobility that are (currently) beyond the realm of JRA5.

2. The aims of the Task Force will be:

2.1. ESTABLISH A FORUM:

2.1.1 to provide a forum for exchanging experiences and knowledge;

2.1.2 to make the results of the work of the Task Force and JRA5 available to the research networking community;

2.1.3 to promote the benefits of the technology and assist in the roll out of national roaming infrastructures.

2.2 DEVELOP A TECHNICAL KNOWLEDGE BASE ON ROAMING:

2.2.1 to continue the work of the TF-Mobility group to provide details of Wireless Access Points and Wireless Client performance and interoperability issues and consider other network access devices (e.g. PDAs) and wired network access;

2.2.2 to use the mailing list as a means of keeping up to date on roaming technology developments, new standards, new issues;

2.2.3 to gather information from 2.2.1 and 2.2.2 to produce an approved source of information on the market, products, standards and issues similar to a market/technology appraisal.

2.2.4 to produce PR materials to promote current inter-NREN roaming services available.

2.3. CONTINUE WORK ON THE CURRENT INTER-NREN ROAMING ARCHITECTURES:

2.3.1 to continue testing and scaling the current and emerging inter-NREN roaming architectures (RADIUS hierarchy & CASG);

2.3.2 to review and update the current and emerging national roaming solutions (e.g. Web-based, RADIUS+802.1x, VPN) taking place in NRENs across Europe both in and outside JRA5 and elsewhere;

2.3.3 to revise and update the elements for an inter-NREN WLAN architecture based on current national roaming solutions and emerging roaming developments (2.3.2);

2.3.4 to amend and test (as necessary) on the existing inter-NREN test bed architecture amongst the participant NRENs, consider technical support services and changes to existing policies.

2.3.4 to create a "European weather map" website of roaming information for users, organisations and NRENs that will contain (1) status of RADIUS proxy servers (organisatonal, National, Euro-level), organisational information (network access methods supported, authentication methods supported, local AUP, status of RADIUS server, user feedback)

2.4 CONSIDER THE IMPACT OF FUTURE DEVELOPMENTS ON ROAMING

2.4.1 to identify the determine impact of new and emerging standards such as MobileIP, IPv6 and QoS on roaming;

2.4.2 to consider the impact of QoS and new applications on roaming services;

2.4.3 to investigate and survey the needs of roaming users and participating NRENs and their institutions on future roaming needs;

2.4.4 to undertake a risk analysis of the impact of future developments on roaming.

2.5 SECURITY

2.5.1 to consider security issues affecting roaming

2.5.1.1 to produce a list of security requirements for roaming

2.5.1.2 to consider and investigate possible VLAN vulnerabilities

2.5.1.3 to gather security best practices

3. The Task Force will be open to any individual or representative of an organisation that can offer appropriate expertise, manpower, equipment or services. Participation will be on a voluntary basis.

4. The Co-Chairs of the Task Force will be James Sankar (UKERNA) and Klaas Wierenga (SURFNET) who will be responsible for preparing the agenda of each meeting, and for co-ordinating the work of the Task Force. They will also be responsible for ensuring that all the agreed deliverables are produced.

5. The secretary of the Task Force will be appointed by TERENA. He/she will be responsible for taking the minutes at each meeting, and for making logistical arrangements as necessary.

6. The Task Force will operate with a 2 year mandate, starting 1 July 2004. A report on the progress of the Task Force and the results achieved will be made at the TERENA Networking Conference 2005. The mandate of the Task Force may be renewed by the TERENA Technical Committee (TTC). If the mandate is not renewed, the Task Force will be dissolved. The Task Force may also be dissolved if the TTC considers that it is making insufficient progress or that its activities are no longer useful or relevant, or if the Task Force co-chairs resign and no replacement can be found.

7. The Task Force will meet approximately four times per year (although this may be via telephone or videoconference). Physical meetings will be held at the TERENA Secretariat offices in Amsterdam or at other locations, taking care to reduce overall costs to participants.

8. Reports and other results of the Task Force will be placed on the public domain, with the exception of information that is subject to a commercial Non-Disclosure Agreement.

1. The Task Force will have a mailing list (mobility@terena.nl) for communication between the participants.

### LIST OF DELIVERABLES

|  |  |
| --- | --- |
| **Deliverable Code** | **Description** |
| D1  | In order to provide a knowledge base of information a summary report of discussions about network access, roaming and security issues should be produced every six months. The summary will contain listed issues raised, those resolved and those outstanding and reasons why it is so and will be made available online. |
| D2  | Scale and where necessary upgrade / integrate the current roaming infrastructures to include countries that require participating.  |
| D3  | Create a service support area for the current roaming services that contains the following: D3.1. Current Roaming policies. D3.2. Current best practice D3.3 An online map of participating NRENs and their institutions with details of each institution's campuses that support roaming with details of their network access methods, SSID, Local AUP (ideally each NREN should be responsible for their own area). |
| D4  | Create an online form for roaming users to provide feedback on their experiences of roaming at other institutions so that this information can be automatically passed on to the relevant NREN and then onto the institution. |
| D5  | Produce a document to detail of how to get access to technical support at each NREN for institutions and at TERENA / SURFNET for NRENs. |
| D6  | Produce a forward look document that outlines a way forward to develop roaming over the next 1-2 years, this will include the updated requirements coming from JRA5, lessons learnt from the current development work, a SWOT analysis and a risk analysis based on current and future needs and advances in new technologies, protocols and standards. |
| D7  | Set up an online web area that contains information on security issues that may affect roaming and repository of roaming security best practice. |
| D8  | PR materials to promote roaming services across Europe. |

New deliverables may be added as the Task force sees fit.

# 19. References

## Deliverables produced

Website

http://www.terena.nl/tech/task-forces/tf-mobility/

Glossary

http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/DelB/DelB\_v1-3-5.pdf

Requirements definition

http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/DelC/DelC1-4.pdf

Inventory for a 802.1X national roaming solution

1. [↑](#footnote-ref-1)
2. Username/password, certificates, OTP (One Time Password, f.i. via SMS) or credentials on a mobile operators’ SIM-card. These mechanisms are implemented in the EAP types MD5, TLS, TTLS, MS-CHAPv2, PEAP, Mob@c and EAP-SIM. [↑](#footnote-ref-2)
3. In commercial deployments, “scratch cards” can offer a password valid for a period of time, or a valid password may be sent as an SMS text message to a visitor user. [↑](#footnote-ref-3)
4. This is not exclusively so as HostAP (Linux free AP) supports 802.1X [↑](#footnote-ref-4)
5. [↑](#footnote-ref-5)