

## **TERENA Mobility Meeting,**

TNC, Limerick  
June 2, 2002

Meeting Report by Licia Florio,

### **Participants List:**

Erik Dobbelsteijn	SURFnet
Juergen Rauschenbach	DFN-Verein
Juha Oinonen	CSC/ FUNET
Kaisa Haapala	CSC/FUNET
Klaas Wierenga	SURFnet
Magnus Stromdal	UNINETT
Mauro Campanella	INFN-GARR
Marcin Michalak	ULB
Olav Kvittem	UNINETT
Stanislaw Starzak	POL34, IPSNC
Piotr Sasiedzki	POL34, IPSNC
Ueli Kienholz	SWITCH
Licia Florio	TERENA

Apologised:

Mauro Draoli                      INRC

### **Introduction**

Licia Florio (who chaired the meeting) announced a small change in the agenda. Due to the Aer Lingus strike, Mauro Draoli, who was supposed to make a presentation about an architecture implementation project, which allows integration between Mobile IP protocol and AAA techniques, could not attend the meeting.

Considering this, Marcin Michalak asked to use that time to make a small demo for his presentation. It was agreed.

Licia went through to the actions list agreed during the previous Mobility Workshop in March 2002. The most important action was a preliminary analysis of the technologies to create, eventually, a inter-NRENs roaming. The document was prepared by Klaas Wierenga and was circulated to list before the conference.

Licia reminded, that according to the action lists agreed, UNINETT, SURFnet, SWITCH, POLAND and DFN should provide English documentation (deadline was first week of June) about their mobility activities, in order to define their area of interest. She said that she got information from SURFnet, SWITCH and partially from UNINETT. She said she does not know what the other NRENs are working on, if they are, and what they would be interested in. She asked participants to provide their view, indicating the most important topic according to each NRENs.

The answer is described below:

SURFnet: : 802.11a and b, 802.1x, other authentication and authorisation, mobile-IP

UNINETT: 802.11, mobile-IP

DFN: WLAN projects with several universities, roaming.

SWITCH: mobility, especially roaming

FUNET: WLAN access  
University Libre of Brussels: WLAN, streaming  
POL34: WLANs at universities, authentication and authorisation

## Presentations

Marcin Michalak: 'Internet in your pocket, big networks on small devices'

---

The first part of the presentation provided a general overview about Wireless technologies, such as Bluetooth, GPRS, WLAN, then it was described how wireless technologies can be used on a PDA.

Marcin described briefly Ipv6 tests on a PDA (Compaq iPAQ), as well. Both Windows CE and Linux were used as operating systems.

The second part of the presentation consisted of some demos. Connectivity, streaming audio and video, web browsing, IPv6 tunnelling to Freenet6 have been tested.

Marcin showed how to connect a PDA to a laptop, using a Bluetooth USB adapter to allow the laptop to get an Ipv4 address and using PPP from the laptop to the PDA. A laptop acts as a router and Internet connectivity with a speed up to 721kbps can be achieved.

Comments and questions:

Q. Bluetooth is cheap and easy to use and more and more already included in products. GPRS/GSM equipment is fairly expensive. Infrared needs to have a line of sight. What are measurable parameters to compare various (wireless) technologies?

A. You can measure delay and throughput, but sometimes applications still don't work when measurements seem OK. Experiments are performed to measure streaming QoS performance subjectively.

Q. Why WLAN's are more difficult than wired networks?

A. Wired networks are more predictable and have no radio interference. Wired Ethernet is upper boundary for wireless performance.

Q. Delay on 802.11a is higher because of retransmits. It might be interesting to test Ethernet QoS schemes on wireless Ethernet, which could improve streaming performance. Cisco is proposing a QoS technique for VoIP over WLAN. Is the quality of the applications used on PDAs comparable to those used on laptops?

A. Yes. In general, longer battery life of PDAs is an advantage over laptops in a "mobile" context.

Klaas Wierenga: Proposal for Inter NRENs Wireless Authorization

---

Klaas presented more in details his proposal to test an access mechanism to wireless LAN. The proposal would allow a student or an employee, if properly authenticated and authorised, of one particular institution (which can use the WLAN) to use the WLAN of whatever institution within one of the participating NRENs.

Klaas said that an inventory of the various WLAN infrastructures would be necessary. So far, the policy of DFN, SWITCH, SURFnet and Uninett are known.

He said that, generally, there are three possible solutions to check for authentication and authorisation: VPN, 802.1x and Web-based (pubcookie/shibboleth/PAPI)

VPN: this solution assures a very good security level and it is good for one institution. Normally institutions install clients on their users machines. The drawback is the scalability, extending a VPN amongst many institutions. A good collaboration among institutions would be required.

Web-based: this solution is very user friendly and easy to extend beyond your own institution. The disadvantage is that in this way IP spoofing is possible and Web browser is required. Klaas said that SURFnet want to prevent anonymous abuse.

802.1x Extensible Access Protocol/Tunneled Transport Layer Security: this solution could be used just to transfer the user information to the authentication server, which will transfer the information to the authentication server of the user's domain. This is a generic access technology; all kinds of AAA schemes can be 'plugged in' (username/password, certificates etc). Combination with RADIUS and/or LDAP is possible. The use of 802.1x technology still presents some drawbacks, mainly due to some security concerns and the fact that the standardization is still in progress. Furthermore the clients are only now becoming available. All the participants agreed that no access should be provided before authorisation. 802.1x would guarantee this.

Since it is not clear yet which solution could be the best one, it was proposed to work together on developing the most ideal solution.

Q. Could PAPI (PAPI is a project that uses a WEB-based authentication solution; PAPI uses token and cookies) be used?

A. Klaas answered that PAPI is basically Web-based authentication method with the before mentioned drawbacks.

Q. Some commercial providers use the web- based approach. What are their motives?

A. The providers are focused on providing access and not assuring a high security level. Sometimes they just choose a more easy to implement solution.

## **Discussion**

Mauro Campanella suggested collaborating with other groups that are working on AAA issues, in order to avoid duplication. It was agreed that it is not recommendable to have different authentication and authorisation schemes for miscellaneous applications. Overlap between activities on AAA should be checked, working closer with TF-AACE and TF-LSD.

Klaas said that the mobility activity should be more focused on deploying authorization, in a first moment, and roaming, in more general scenario.

Ueli Kienholz said that SWITCH is looking into a hybrid approach, which would allow each university to choose a VPN-solution for their users (similar to the DFN plan) or use a solution based on session intercept. This approach requires the setup of a separate mobile user network at each University that is routed over an access control device. This device grants access to a number of resources (like VPN-gateways at other universities) without authentication but challenges the user for credentials (e.g. via SSL web page) when another resource is requested. While the VPN solution solves the encryption and spoofing problems it might be hard to deploy to all users devices. Universities not (yet) ready to deploy a VPN solution could use the (easier but less secure) solution based on session intercept.

Juergen Rauschenbach said that DFN are working on VPN-based AAA. He said that at the moment they do not have any infrastructure ready, but only an a project. Juergen proposed to take Mobile IP into consideration.

Olav Kvittem mentioned that UNINETT has been testing the VPN solutions that work on both wireless and wired networks, and on how to scale them up.

IPv6 was mentioned some times as a future mobility scheme on top of a basic authentication scheme.

Since there is a lot to investigate a discussion raised whether a TaskForce should be initiated for this subject. Licia said that a Task Force would be a more formal commitment from people, but in any case every one would work on volunteer bases. Licia said that a charter should be prepared and a list of deliverable to be submitted, as well. She said that if people were really keen to work together a task force would assure a more scheduled work. She asked how many people would be interested in participating in a Task-Force.

**SURFnet, UNINETT, FUNET, DFN, SWITCH** said they would like to participate. They said that since most of the participants are working on the same topic (WLAN access), a Task Force would speed up the information exchange.

The objective of the TF will be to allow a 'mobile' user to get access to his own local resources, from wherever inside the institutions that will be part of the Task Force. The aim of the TF will be to find a method to allow this.

It was agreed that a complete overview of possible methods is really necessary.

Mauro suggested writing down a possible list of deliverables. Licia said that it is not useful to have a long list of deliverables, as people are too busy to work on a lot of topics. She said that it would be better to have a few deliverables, but very focused.

### **Possible Mobility TF-Deliverables**

The following deliverables were discussed. They will be sent in a charter.

Del 0: Requirements (all)

- security levels,
- regulatory issues

Del 1: Inventory of solutions, link to other authentication solutions (all)

- access technologies (performance),
- cross-institutional authentication/authorisation,
- scalability,
- security

Del 2: Preliminary selection

Del 3: Evaluation/Implementation

- interoperability with installed base of authZ/authN mechanisms,
- scalability

Del 4: test

Step 5: test-bed implementation

Product testing (Uninett) and mobility (horizontal/vertical roaming) IPv6 testing will be separate activities.

## **Action and Conclusion**

Due to lack of time it was not agreed who would be the chairman and who would write the charter, so these are two open issues. In particular the selection of a chairman is the first thing to be defined to have a task-force. Below a list of the actions and their deadline is defined:

- Task-force chairman selection: as soon as possible.
- Charter and mission statement: a first draft should be prepared by end of July (duration, deliverables...)
- Next mobility meeting: to be fixed