

## **Third TF- Mobility meeting**

### **Minutes**

**Date:** 22<sup>nd</sup> September 2003

**Venue:** Fokus Institute, Berlin

#### *Attendees*

<i>Kolbjørn Barmen</i>	UNINETT
<i>Carsten Bormann</i>	Universitaet Bremen, TZI
<i>Rodrigo Castro</i>	RedIRIS
<i>Tim Chown</i>	University of Southampton
<i>Licia Florio</i>	TERENA
<i>Ksenija Furman Jug</i>	ARNES
<i>Christian Grimm</i>	University of Hanover, RRZN
<i>Sami Keski-Kasari</i>	Tampere University of Technology, TUT
<i>Ueli Kienholz</i>	SWITCH
<i>Antonia Kujundzic</i>	CARNet
<i>Dubravko Penezic</i>	SRCE
<i>Niels Pollem</i>	Universitaet Bremen, TZI
<i>Vladimir Rabljenovic</i>	SRCE
<i>Juergen Rauschenbach</i>	DFN-Verein
<i>James Sankar</i>	UKERNA
<i>Milan Sova</i>	CESNET
<i>Peter Weik</i>	FOKUS Fraunhofer
<i>Klaas Wierenga</i>	SURFnet

#### **UMTS Test-bed at Fokus**

Fokus presented their work in developing platforms that support WLAN, GPRS, Bluetooth, satellite, UMTS, SMS etc. to run applications and value added services. The testbed has a WLAN / UMTS component that supports a variety of technologies that are vendor and technology independent and open to third parties. Fokus are also working with international partners in academia and commerce to expand the testbed worldwide. They are working with vendors, end user, application developers and content providers.

Fokus are interested in working with NRENs, however some financial investment would be necessary. Further details about the test bed are available at

<http://www.fokus.franhofer.de/3gb>

The presentation slides are available on the TF-Mobility web page (<http://www.terena.nl/tech/task-forces/tf-mobility/>)

## **Deliverable G – JS**

James Sankar reviewed deliverable G, going through the different solutions.

### **802.1X**

The 802.1x summary was broadly accepted. 802.1x had become a standard in June 2001. It was remarked that in this solution the intermediate RADIUS servers are only used to transport EAP messages, which contain the user credentials. The EAP messages are encrypted with TTLS, TLS and PEAP (without the end-user noticing this) and therefore they cannot be modified by the intermediate RADIUS.

Klaas said that in Holland they want to enforce 1X, but to facilitate users coming from other countries they would like to set-up a VPN gateway or a Web base access.

### **VPN**

The VPN summary was incorrect and requires a rewrite.

**Action** - Ueli Kienholz agreed to volunteer to write this section again.

It is important to note that the Swiss approach does not rely on RADIUS.

The VPN + PKI summary was no different in its concept to VPN and though added as a variant in the deliverable would not be pursued in Deliverable H due to the group's resource and time constraints. Ueli Kienholz explained that in a first moment this solution on XP appeared really easy due to the fact that it's based on temporary certificate, so neither revocation for the certificates and nor request for the users are necessary. It was also agreed that though technically feasible, the group would not consider PKI within the focus of the group, as its main aim was to support mobility only. Though important, it was agreed that security was too important but should not dominate the importance of the main aim.

### **Web-based Redirection Server**

The web-based redirection authentication summary was reviewed and broadly accepted.

This approach uses the same back end as 802.1X, but has some security issues.

### **PPPoE**

PPPoE was discussed and it was agreed that this was an independent solution that the group would recommend software enhancements to in order to interoperate with the other roaming solutions mentioned earlier.

It requires a proprietary solution to provide an IP tunnel, but it uses a RADIUS backend.

**Action** - Josh Howlett emailed the group to confirm that he was happy to work on software enhancements to make the “Roamnode” interoperate with other mobility solutions.

The group agreed that ideally the two proposed parallel streams of work (RADIUS proxy hierarchy and Controlled Address Space for VPN Gateways) should be integrated or at the least, brought as closely together as possible.

Interoperability between each type of mobility user and mobility network requires documentation in deliverable G with assistance from Klaas (802.1x), Ueli (VPN) and Sami (web-based redirection) by

1. Precise Pros and Cons of each solution.
2. Writing step-by-step how one user can gain network access to a visited network
3. Detailing the additional work needed at the visited and home institution to enable interoperability to work.
4. Write guidelines for system administrators to be able to support different types of mobility users.

It was also agreed that a separate section that deals specifically with security & trust issues for each solution should be added, including how to deal with security incidents, who to manage trust and identify responsibilities.

The group also recommended that a 1-side A4 document detailing participation guidelines be written by the leaders of the two mobility solutions (RADIUS proxy hierarchy and Controlled Address Space for VPN Gateways) to ensure the solutions remain manageable. (Action on KW and UK/CB) This document will be part of deliverable G.

### **Mobility Users Cases Matrix**

<b>User-type</b> \ <b>User@</b>	<b>802.1x network</b>	<b>VPN network</b>	<b>Web-based redirect network</b>
<b>802.1x user</b>	KW	KW	KW
<b>VPN user</b>	UK	UK	UK
<b>Web-based redirect user</b>	SK	SK	SK

The group agreed that more documentation is needed to detail the two mobility solutions (RADIUS proxy hierarchy and Controlled Address Space for VPN Gateways) to be clear about exactly how the systems will work, how these will be supported and if possible how these will interoperate. A detailed understanding of how each proposal will be design and built would also be needed, however some of this work would overlay with deliverable H.

The group agreed not to concern themselves with the following:-

1. Local - VPN: VPN users will not be able to access a visited institutions 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.
2. 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 like to migrate to such a solution.

James and Tim agreed to reduce the summary section and focus (with the help of TF-Mobility members) on the drafting the interoperability issues and justifying the scope and approach for the further mobility work.

Carsten Bormann explained more in detail the meaning of **CASG** (Control Address Spaces for Gateway). The addresses space allocation will be provided by several NRENs. These addresses space will be known to everybody. The advantage of this solution is that it reduces the dimension of the access list, breaking it down to the dimension of the docking network.

The users could connect directly to the docking network, without using anything else. Klaas proposed to use RADIUS to verify the VPN concentrators. This solution appeared doable and it will be investigated more.

Klaas also proposed to use Web based access for both VPN and .1X users. The users should introduce their credentials that will be verified against a RADIUS server. According to Ueli this could be doable.

**Action:** Ueli will investigate more and will refer to the group.

The group acknowledged that the draft had a considerable amount of work to be written and agreed and as a result the draft was rescheduled to in its final version by **mid November 2003**. The date is subject to the level of contribution received from all the TF-Mobility members.

There were a lot of specific technical discussions on WLAN, AAA, security, operating systems and trust issues during this session. These discussions varied in complexity but were too specific and random to be minuted.

### **Deliverable H – KW**

This deliverable will describe the test-bed architecture. Though the content of this deliverable strongly depends on Deliverable G, it was agreed to start working on Deliverable H, even if Deliverable G is not in its finale state.

Some guidelines for the preparation of the deliverable were provided and reported below:

1. Action - Interoperability matrix – document how to make this happen at both ends (**KW, UK, SK**) (Have this in place by mid - November 2003)
2. Document a “trust model” / AUP – make this explicit/
3. Accounting and billing – write some points that would be useful for each solution.

4. A naming scheme was agreed for the European RADIUS server. Counting on the fact the schema [user@realm](#) is almost a standard for those using RADIUS, it was decided to use:  
[user@realm.countrycode](#) for the European RADIUS.  
Croatia who is already connected to the European RADIUS server uses at the moment a different schema, but they agreed to migrate to [user@realm.countrycode](#)  
A small document will also be prepared to provide the guidelines for countries which intend to join the European RADIUS.
5. Agree a naming scheme for SSID. A proposed SSID name was SURFnet. Some recommendations will provide to broadcast a SSID or redirect to a webpage with SSID information and user guidelines.
6. Ueli and others agreed that at the least, the CASG approach should have a fallback mechanism in place to access the RADIUS proxy hierarchy.
7. Another solution mentioned was to have a web-based redirection web page that contained user guidelines for the various mobility solutions to assist users.

**Action** – Ueli has volunteered to undertake VPN tests with the RADIUS Proxy hierarchy.

**Action** – Dubravko will change their RADIUS schema.

### **Deliverable J - JL**

The initial scope of the deliverable was to test all the WLAN product is too ambitious and is not focused on UNINETT WLAN equipment (Cisco, Small office, home office). Extra tests will be performed but only on Cisco products.

There is a web page [www.uninett.no/wlan](http://www.uninett.no/wlan) and comments are welcome. So far Jardar has received no feedback or comments.

**Action** – TF Mobility members to provide feedback on the product testing web page.

## **Deliverable K - JL**

Jardar wants to collect testing results and put these into a database. Most of the information have been translated and inserted onto a database, but at the moment it doesn't work. Contributions are welcome.

**Action** - Licia to make a link on the TF-Mobility web page to the product database.

**Action** – TF-Mobility members to review the database and provide feedback on what information should be contained.

## **Deliverable L - TC**

Tim believed we should look at IPv6 and Mobile IP implications for each method (web-based, VPN, 802.1x) and assess whether the infrastructure can be IP independent. The other question was whether we use IPv6 whilst roaming today? It is possible but this relies on dual stack (IPv4/v6) technology.

Tim will continue to provide news on current IPv6 / MobileIP developments.

Question raised - Can client devices access everything via IPv6 if authentication failed (e.g. Web redirect page)?

A: it needs a routable address and possibly a “care of” address.

**Action** – Tim to produce a document skeleton: useful to sort the above 3-4 threads into a roadmap.

## **Any other business**

### Futures

Klaas discussed the future options for the group, namely set a new taskforce, extend the taskforce (could have an impact on Geant2) and also what areas to work on.

Klaas has recommended the following to Geant;

- Extending work beyond WLAN to other network access areas
- Integration to access to applications and network (e.g. single sign on)
- Content Adaptation for Mobile devices
- New technologies (e.g. IPv6, Mobile IPv6)

No firm conclusions on the future of the group were agreed; however most of the members did not want the work to end in June 2004.

### Promotion and awareness of TF-Mobility taskforce

Klaas wanted to continue to promote awareness of the positive work being produced by the group. A suggestion was to organise a Terena workshop on WLAN and security, this was received as fine in principle, but members were unsure of a suitable date.

February was proposed as a suitable month.

Another topic area was for national workshops where administrators are trained in how to extend access to international users by offering some special support infrastructure for other mobility solutions.  
 Another alternative was for TF-Mobility members to attend and speak at national and international events about the work of the group.

**Action** - Licia to create a section on the TF-Mobility web page for TF-Mobility members to provide information and links to events where they have spoken about TF-Mobility.

**Action** – All members to email Licia with details of conferences that they have presented on the work of the TF-Mobility group.

**Summary**

Work is progressing on the technical details for deliverables G and H.

The agreed actions are as follows:

<b>ACTION</b>	<b>Responsibility</b>
1. To assist in technical rewriting of deliverable G	<b>KW, UK, SK- 30 Oct</b>
2. To rewrite and submit a further draft of deliverable G	<b>JS, TC 15- Nov</b>
3. To write a 1-side A4 document to add to Del H detailing participation guidelines for the RADIUS proxy hierarchy to ensure the solution can be extended and yet remain manageable.	<b>KW 15 Nov</b>
4. Dubravko to change their RADIUS schema	
5. To write a 1-side A4 document detailing participation guidelines for the Controlled Address Space for VPN Gateways, to ensure the solution can be extended and yet remain manageable.	<b>UK,CB 30 Oct</b>
6. Proposed work to be documented / agreed on how & what software enhancements are needed to make the “Roamnode” interoperate with other mobility solutions	<b>JH + All 30 Oct</b>
7. To begin Deliverable H immediately.	<b>KW</b>
8. To produce an interoperability matrix and document how to make this happen at both ends	<b>KW, UK, SK 30 October</b>
9. To document a “trust model” / AUP.	<b>KW</b>
10. Ueli has volunteered to undertake VPN tests with the RADIUS Proxy hierarchy.	<b>UK</b>
11. TF-Mobility members to provide feedback on the product testing web page to Jardar.	<b>All</b>
12. Create a link from the TF-Mobility web page to the product database.	<b>LF</b>
13. TF-Mobility members to review the database and provide feedback on what information should be	<b>All</b>

contained.	
14. Produce a draft structure for Deliverable L.	<b>TC</b>
15. Create a section on the TF-Mobility web page for TF-Mobility members to provide information and links to events where they have spoken about TF-Mobility.	<b>LF (done)</b>
16. Email Licia with details of conferences TF-Mobility work has been and will be presented.	<b>All</b>
17. Produce a draft structure for Deliverable L.	<b>TC</b>

### **Next meeting**

The next meeting will take place on January 23<sup>rd</sup> 2004 at the Terena offices in Amsterdam.

### *Key*

*CB= Carsten Bormann*

*JL = Jarda Leira*

*JS = James Sankar*

*KW = Klaas Wierenga*

*LF= Licia Florio*

*SK = Sami Keski-Kasari*

*TC= Tim Chown*

*UK= Ueli Kienholz*