

## **Forth TF- Mobility meeting**

### **Minutes**

**Date:** 30th January 2004

**Venue:** TERENA, Amsterdam

#### ***Attendees***

Hansruedi Born (HB)	SWITCH
Tim Chown (TC) (streaming)	University of Southampton/UKERNA
Licia Florio (LC)	TERENA
Carles Fragoso (CF)	CESCA
Jan Furman (JF)	CESNET
Luis Guido (LG)	FCCN
Sami Keski-Kasari (SK)	TUT
Antonia Kujundzic (AK) (videoconference)	CARNet
Jardar Leira (JL)	UNINETT AS
Diego Lopez (DL) (videoconference)	RedIRIS (via videoconference)
Ralf Paffrath (RP)	DFN-Verein
Spiros Papageorgiou (SP)	GRNET
Rok Papež (RP)	ARNES
Niels Pollem (NP)	Universitaet Bremen, TZI
Jürgen Rauschenbach (JR)	DFN-Verein
James Sankar (JS) (videoconference)	UKERNA
Lino Santos (LS)	FCCN
David Simonsen (DS)	UNI-C
Klaas Wierenga (KW)	SURFnet

#### ***Introduction***

Due to the weather condition JS could not get to Amsterdam and was therefore connected via videoconference. CB was also unable to attend and sent his apologies in advance so KW was appointed as chairman for this meeting.

DL and AK were also connected via videoconference.

#### ***Deliverable G***

Although the deliverable G was discussed exhaustively during the previous meeting in Berlin and since then a lot of work has been done there were some concerns about

security, especially about the use and protection of resources when using the Controlled Address Space for VPN Gateways (CASG) method.

It was asked whether the CASG approach should use a secret list of addresses. The answer was that there is no need for this as the VPN concentrator should be secure enough to deal with possible attacks.

As the deliverable G is in a final stage it was agreed to approve the deliverable G (it is now on-line on the TF-Mobility Web page) and to add a security paragraph to the deliverable I to take into consideration these issues.

ACTION1: KW to add a security paragraph to the deliverable I.

### ***Deliverable H***

KW introduced the deliverable H presenting an “interworking scenario”. He said that in his view this deliverable should be really practical with configuration examples as well.

To have the three solutions (802.1x, VPN, Web-based redirect) in place as described in the “interworking scenario” the access points should broadcast two SSID one to support 802.1x and another one to support VPN.

In Holland this could be achievable as most of the access points in use are Cisco, and are capable of broadcasting two SSIDs. The deliverable should consider a solution for institutions with access point that are non 802.1Q capable.

Some security issues were discussed. The Web approach does not provide encryption for the users credentials when traversing through RADIUS servers across the RADIUS hierarchy.

It was advised therefore to let the home institution to decide on their policies for their own users’ security. It was also agreed that there was a need to define a trust relationship matrix between institutions and to add this to the deliverable.

ACTION2: the trust relationship between institutions should be documented in Deliverable H. Contributions from everybody.

HB presented the results of some small scale trials of the CASG model. His proposed model has the docking network separated by the NREN network as well as the access control device. The range of addresses allocated depends on the number of VPN gateways in use.

HB described two approaches that he has considered: dedicated routing and VPN forwarding. Dedicated Routing is a proven concept but one in some cases it will not work as follows

**Case 1:** Some NREN's might dispose a network architecture which makes the routing of the subnets to the specific academic organization impossible.

**Case 2:** Supposing VPN gateways have already been deployed and active, some do not support the addition of a secondary virtual IP address on an interface to accommodate the current IP address and the NREN IP address range for the CASG.

To overcome these limitations in dedicated routing, HB has considered VPN forwarding as a solution, which is based on a forwarding network containing forwarding devices, maintained by the NREN. The range of addresses allocated for the forwarding network depends on the number of VPN gateways.

IPsec (one possible but common used VPN protocol) can work in two different ways (transport mode or tunnel mode), so HB described the difference. Within '**transport mode**' only the payload information is encrypted. IP header data is left original, but some information is included to the encrypted IPsec header (additionally added).

Transport mode is used for host-to-host VPN and any change in the IP header data will be flagged as a violation.

In the '**tunnel mode**' the whole original data packet is encrypted (header and payload), encapsulated and an independent new IP header is added. Since the new IP header is totally independent of the encryption algorithm, changes within the header will not be flagged with a violation.

While the VPN forwarding approach (proof of concept) only works with the IPsec 'tunnel mode', 'tunnel mode' and 'transport mode' can be used within the dedicated routing approach.

The new deadline for reporting results from larger scale CASG trials must be included within deliverable H before the end of April.

ACTION3: DFN, Bremen and SWISS will test the international CASG and refer about the results for deliverable H.

ACTION4: HB to start the discussion for the setup of CASG on the mailing list.

ACTION5: HB to add in the deliverable H the case in which a user tries to start a security attack before being the CASG authentication is done.

### ***Deliverable I***

According to KW deliverable I should contain the recommendations for people who want to implement one of the three solutions.

Deliverable I will also contain a policy draft to cover the aspect of intra-NREN roaming.

LF explained that although there have been many discussions about who is responsible for roaming/nomadic/guest users when they roam; there is not any document that describes the policy assumptions on which the work of the group is based upon.

LF said that the document should be positioned at a high level that lists some guiding principles and stressed that it should not consider detailed legislations at national levels or the harmonisation of such laws.

KW explained SURFnet's statement that both the home and the visited institution are responsible in the roaming process. The home institution is responsible to identify the

users, but the visited institution should take all the relative precautions to support guests users as securely as is practically possible and ensure that their own network is also as secure.

If a security incident occurs before the user has been authenticated then the local institution is responsible. James sent a high level policy statement that had been drafted for UKERNA's national trial service that is currently being developed. It was agreed that both of these documents would be used as a starting point to produce a policy document that should be clear and concise.

ACTION6: LF to write a policy draft document by Feb 13 and forward to James Sankar & David Simonsen for feedback and comments.

The new deadline for this deliverable is end of April.

### ***Deliverable J***

JL has put on-line (<http://www.uninett.no/wlan/>) information about WLAN Networks, such as standards, products, security issues and he has tested products as well. JL asked for a feedback about the site, especially on the section related the product testing.

JL added a link "Feature lookup and compare products" in the section called "Product testing", whose purpose will be:

- having a place where NRENs and others can find technical information about wireless products, primarily Access Points for indoor infrastructure.
- enabling the "selected few" (TERENA/NRENs etc.) to add/edit on this database of information
- enabling anyone to add comments on individual products. (DB/PHP vs. Wiki)

It was agreed that the list of products should be restricted to those deemed relevant and important to the TF-Mobility scope. It was also agreed that everybody should provide feedback and contribution to this deliverable whilst Jardar will concentrate mainly on gathering data on access points.

ACTION7: Everybody will provide feedback about the fields of information that should be added/removed in the WLAN product database from the suggested prototype by end of February.

ACTION8: The database content will be finalised and then it will be moved to the TERENA website.

### ***Deliverable K***

ACTION9: JL asked for contributions from everybody.

### ***Deliverable L***

Tim agreed in Berlin to lead deliverable L. Tim was contacted during the meeting and it was agreed that this deliverable will only contain information about MobileIPv6  
The deadline for this deliverable is end of April.

ACTION10: TC to produce a draft version for this deliverable by the end of April

## ***GEANT2***

JR presented JRA5 within Geant 2, which will build on top of TF-mobility.

The future of the task force was discussed, also in relation to Geant2.

LF and DL explained that TF-AACE is a bit different in terms of practical results from TF-Mobility therefore join the two groups was not considered a good idea.

It was agreed to end the current TF-Mobility group in June 2004 with all deliverables completed. A new group will then be proposed to Terena based on the same format, membership and frequency of meetings but with a revised charter that would be in line with the work of Geant2 objectives and would therefore focus on roaming but with consideration of the integration of AAI infrastructures. It was also proposed that should the TF-AACE taskforce continue, there would be scope for an additional activity whereby both groups would hold one joint event per year (which will be attended by JRA5 members as well) to discuss overlapping issues and present their work. It was also proposed that each group should have a member from the other group actively involved to ensure good communications are in place between both groups.

ACTION11: The next charter of TF-Mobility will be prepared during TNC 2004, in Rhodes and will be circulated to all TF-Mobility members for comment.

## ***Presentation of TF-Mobility in Rhodes***

The possibility of presenting a live demo was discussed. At the moment there is no guarantee that the local organisation can provide a RADIUS link. Another issue is the wireless LAN structure. To have a demonstration at least a WEP key should be provided and at the moment it is not clear. It was agreed to check on the spot and in case to have a demo in a BoF, which could be arranged at the last moment.

It was also that TF-Mobility will meet separately in Rhodes not together TF-AACE.

ACTION12: KW to investigate the possibility for a BoF, JS to assist in raising this idea with Shirley Wood (Terena Conferences Director).

## ***Other Business***

### **SSID**

During the meeting in Berlin, it was proposed to have a unique SSID, the same in all Europe, but there was no further discussion about this.

KW said that in the Netherlands EduRoam is being used. TF-Mobility could use the same one. It was agreed to propose EDUROM as SSID (not to enforce it). As far as the security issues concerning to make available to everybody the SSID name, it was said that security should not rely on the SSID.

## **Final Report**

JS asked information about the final report. LF said that it is not mandatory but because of the progresses made by the group and because of the fact that there will be a new TF-Mobility, it would make sense to have a final report. This should be prepared at the end of the task force, for instance over the summer.

ACTION13: JS+ KW to write it

ACTION14: LF to circulate a template for this.

## ***Summary of the Actions***

<b>Action</b>	<b>Deadline</b>	<b>Description</b>
<a href="#"><u>ACTION1</u></a>	30-04-04	KW to add a security paragraph to deliverable I. Contribution from all
<a href="#"><u>ACTION2</u></a>	30-04-04	Define the trust relationship between institutions in deliverable H
<a href="#"><u>ACTION3</u></a>	15-04-04	DFN, Bremen and SWISS will test the international CASG and refer about the results for deliverable H.
<a href="#"><u>ACTION4</u></a>	asap	Start the discussion for the CASG setup on the mailing list.
<a href="#"><u>ACTION5</u></a>	15-04-04	HB to add into deliverable H the case in which a user tries to start a security attack before being the CASG authentication is done
<a href="#"><u>ACTION6</u></a>	13-02-04	LF to write a policy draft document by Feb 13 and forward to JS & DS for feedback and comments.
<a href="#"><u>ACTION7</u></a>	20-02-04	Everybody to provide feedback about fields of information that should be added/removed from the prototype that JL presented
<a href="#"><u>ACTION8</u></a>	29-02-04	JL and LF to move the content of the database to TERENA.
<a href="#"><u>ACTION9</u></a>	30-04-04	JL asked for contributions from everybody for deliverable K
<a href="#"><u>ACTION10</u></a>	30-04-04	TC to produce a draft version of deliverable L
<a href="#"><u>ACTION11</u></a>	10-06-04	To prepare a charter for the next TF-Mobility
<a href="#"><u>ACTION12</u></a>	ongoing	KW to investigate the possibility for a BoF.
<a href="#"><u>ACTION13</u></a>	30-06-04	JS+ KW to write the final report
<a href="#"><u>ACTION14</u></a>	31-05-04	LF to circulate a template for the final report before TNC