

2nd TF-Mobility Meeting

Date: 18 May 2003

Venue: Zagreb, Croatia

Attendees	Organisation name
Carsten Bormann	Universitaet Bremen, TZI
Andrea Baldi	ESA
João Castro	UMIC / FCCN
Piero Castoldi	CNIT
Jan Gruntorad	CESNET
Licia Florio	TERENA
Kaisa Haapala	CSC/Funet
Karri Huhtnamem	TUT
Avgust Jauk	ARNES
Baiba Kaskina	TERENA
Sami Keski-Kisari	TUT
Ueli Kienholz	SWITCH
Jose Montenegro	University of Malaga
Dubravko Penezic	SRCE
Juergen Rauschenbach	DFN-Verein
James Sankar	UKERNA
Matti Sarinea	TUT
Lino Santos	FCCN
Stig Venaas	UNINETT
Sime Visic	FOI (HR)
Klaas Wierenga	SURFnet
Zelio Saric	SPAN (HR)

Apologies

Pollem, Niels - Universitaet Bremen TZI

Agenda

1. Welcome and Agenda
2. Current Deliverable Update.
 - A quick update on the progress of the current deliverables (B,C,D, E,F only) and how to finalise the deliverables.
 - Agree the deliverables to move to the public area
3. Definition and presentation of a non-technical glossary.
 - If possible agreement on general terms.
4. Deliverable G: Possible approach
 - Agree preliminary selection for inter-NREN roaming.
 - Compare authentication solutions (consider using a table to summarise each solution's features to aid in comparison).
 - Describe inter-operability issues between each solution.
 - Agree a solution
 - Review & agree deliverable G milestones.
5. Any other business
6. Next meeting

1. Introduction

James and Carsten introduced themselves to the participants and agreed the agenda. They both expressed their satisfaction at the deliverables produced to date and the quality of discussion on the mobility list.

A review of deliverables B, C, D, E and F was undertaken, followed by three short presentations describing the three possible roaming solutions identified (deliverables D, E and F), together with details of how each would interoperate and be made scalable for a European roaming solution.

2. Current Deliverable Update

Deliverable B: Creation of glossary of terms for: mobility/roaming/authentication and authorisation technologies

Owner: Licia Florio

Licia reported on deliverable B and thanked the mobility group for the comments received. Licia has amended the list of terms and this deliverable is ready to be moved to the public area. The list of terms will expand as necessary during the lifetime of the task force. The current version of the deliverable contains all the technical terms used so far.

Deliverable C: Requirements definitions for inter-NREN roaming
Owner: Juergen Rauschenbach

Juergen gave a brief update on the progress of Deliverable C and reported that the deliverable, had been circulated and discussed on the mailing list before the meeting. Klaas mentioned that the list of requirements should be reorganized so that one can see which items are of priority / importance such as scalability and security for example. As a result this deliverable needs a final revision, and a further round of comments before it can be moved to the public area.

Action: Juergen will update deliverable C with comments received from the mobility group and will modify the non-technical terms to ensure consistency with the non-technical glossary. The final version will be moved to the public area by June 6 2003.

Deliverable D: Cross-domain 802.1X solution
Owner: Erik Dobbelsteijn

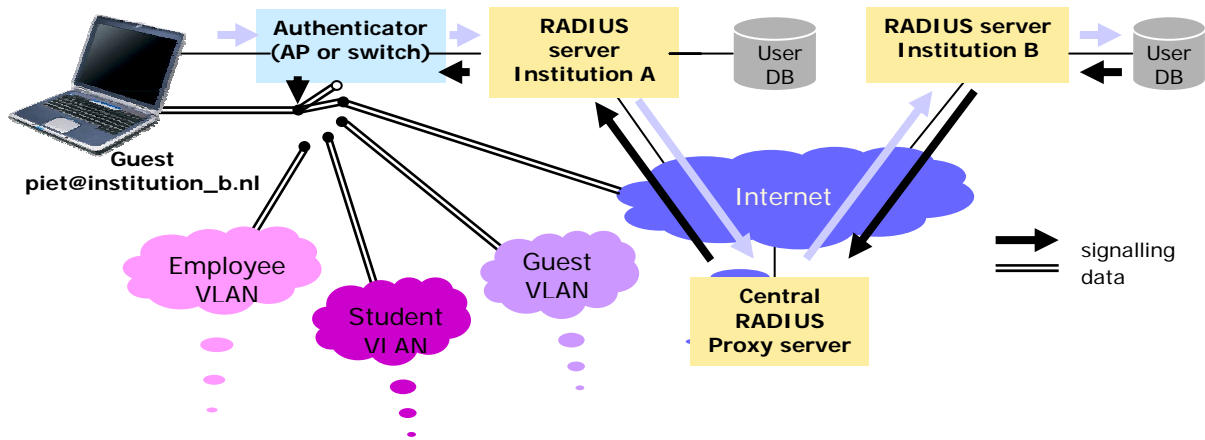
Klaas (on behalf of Erik) gave a summary of deliverable D. Klaas stated that the IEEE 802.1X standard was a layer 2 solution between a client and either a wireless access point (wireless network) or a switch (VLAN) as 802.1X can be used to control the access to a network at the "edge" of the network. 802.1X authentication information is carried over the Extensible Authentication Protocol (EAP) that enables the use of various authentication methods that each institution can choose. SURFnet has adopted a hierarchical RADIUS backend for guest access. This solution only works if the client, the access point and the RADIUS server (in SURFnet's case) support EAP. Interoperability with the other solutions and security issues were also mentioned.

Two scenarios for 802.1x for the user perspective were also presented;

- a. A user from institution A wants to get authenticated in his own institution (A). In this case the RADIUS server at institution A authenticates the user.
- b. A user from institution B wants to get authenticated at institutions A. In this case the RADIUS server at institution A doesn't recognise the user's credential, which are forwarded to the Central RADIUS server and from here to the RADIUS sever at institution B, where the authentication takes place. The response is sent back to the access point.

Klaas mentioned that there were two models for RADIUS to RADIUS authentication, either each RADIUS at the NREN level trusts another NREN RADIUS server at the same level, or TERENA hosts a RADIUS server at a higher tier that all NREN level RADIUS servers point to. It was agreed that the latter approach would be more manageable and scalable and ensure all NRENs have a single point of contact for such RADIUS issues.

The diagram describes the RADIUS architecture to be used for the 802.1x architecture.



Action: Klaas to update and circulate the latest version of deliverable D for final comments. The final version will be moved to the public area by June 6 2003.

Action: Klaas to consider the issue of NAT with Deliverable D

Action: Klaas to provide information about SURFnet RADIUS server set-up.

Deliverable E: VPN solution

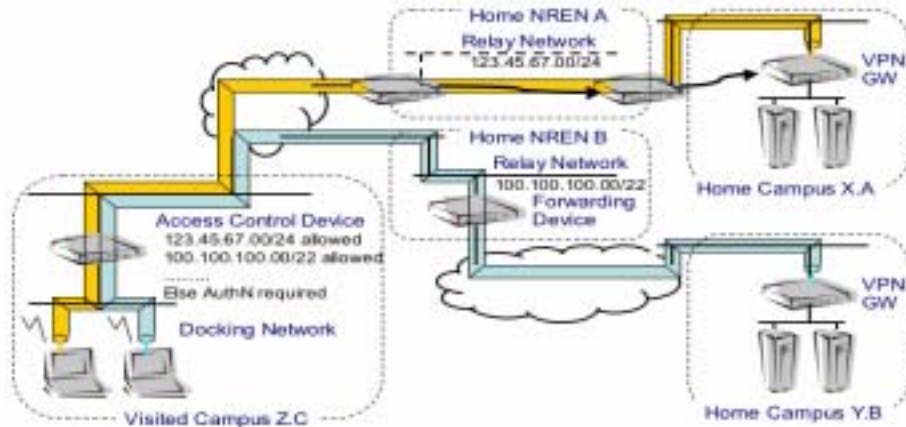
Owner: Ueli Kienholz

Ueli began by describing the VPN solution to the group. He said that the VPN approach does not require visiting users to authenticate locally. Instead, docking networks allow a visiting user to just connect and establish a VPN tunnel to the VPN gateway (layer 3) back at the visitor's home institution. The access control devices at the docking networks (e.g.routers with ACLs) grant access to these VPN gateways.

In Germany, the allocation of private address space has resolved the access control problem. Extending this solution to the European scale would require the coordination of address space between NRENs, and/or requesting address space from RIPE.

In Switzerland the access control problem has been solved by each SWITCHmobile organisation keeping a list of all VPN gateways of the other SWITCHmobile organisations. This means that the docking networks could connect only to the addresses specified in these lists. The list is hosted on a Website where the network administrators of the universities can enter and change their entries as well as download the complete list. Extending the SWITCHmobile approach would require access control lists with several thousand entries being implemented and kept up to date at thousands of access control devices throughout Europe.

A proposed solution to solve the scalability problem has been proposed defining “Relay Networks”, which are network spaces, one for each NREN, that get a range of addresses from their own NREN address space. In this way the packet exchanging between the relay network and the VPN gateway should be secure. The diagram below describes the proposed architecture for a scalable wireless roaming VPN solution.



Action: Ueli will update deliverable E with comments received from the mobility group and will modify the non-technical terms to ensure consistency with the non-technical glossary. The final version will be moved to the public area by June 6 2003.

Action: Niels Pollem to research the RFC on AAA server.

Action: Ueli to consider the issue of NAT with Deliverable E

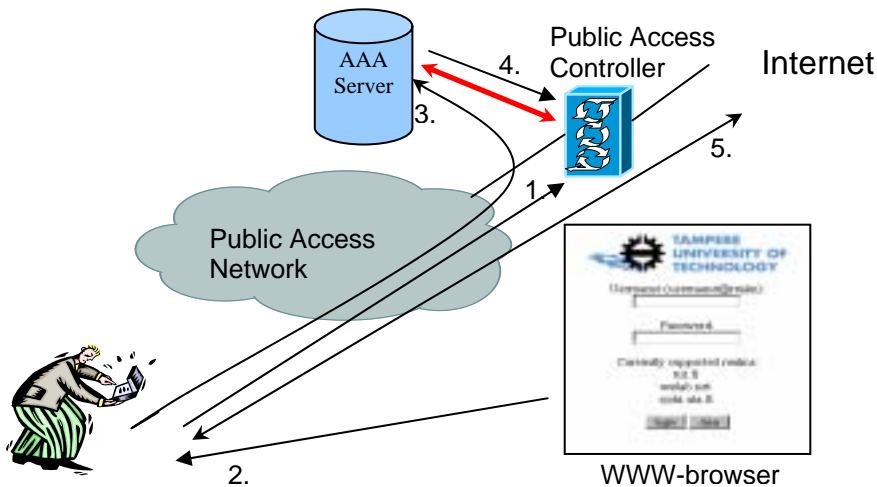
Deliverable F: Web based solution

Owner: Sami Keski-Kasari

Sami presented his solution of a web based wireless authentication solution to the group. At the edge of the network, an access control device, commonly referred as access controller acts as router or bridge to control network access, redirects unauthenticated users to a web page to request user credentials. Once credentials have been given and authentication and authorisation (typically from a AAA server, in Finland, RADIUS is used as the backend server) have been accepted, the authenticated user is allocated an IP-address via DHCP (the IP address is assigned from that "visited" network at the beginning of the session). The user can then access the Internet.

This set-up provides accountability support also. Let assume the case that a user gets authenticated at his home RADIUS and then a local IP address is assigned to him. A malicious attack can be detected. The access controller can send RADIUS accounting messages telling who is signed in, what his IP address is and how much traffic he has transferred. Also duration of session can be checked. It works like in 802.1X case. Messages can be stored to every RADIUS server that belongs to the path (RADIUS roaming case) so administrators of visited university can directly see users that are logged in the network and if they are doing something nasty drop them out.

The diagram below describes the architecture for the wireless roaming web-based solution.



Action: Sami will update deliverable F with comments received from the mobility group and will modify the non-technical terms to ensure consistency with the non-technical glossary. The final version will be moved to the public area by June 6 2003.

Action: Sami to consider the issue of NAT with Deliverable F

3. Definition and presentation of a non-technical glossary

It was agreed that a list of non-technical terms be used to ensure consistency of non-technical descriptions for all the taskforce deliverables. Carsten facilitated a brainstorming session to agree terms the group will use.

Action: James, Klaas, Licia and Carsten to produce a first draft for discussed on the mobility mailing list. (Ideally this should be finalised by Monday 2nd June so that drafts can be updated in time for the deadline of June 6th 2003).

4. Deliverable G: Possible approach

Owner: James Sankar

The original plan for Deliverable G was to agree on one of the three roaming solutions and design a scalable architecture for wireless roaming across Europe. Many NRENS have spent considerable sums of money and time on each roaming approach and no one approach is considerably better than the others. As a result, deliverable G will be the drafting of an approach to scale a solution that can cater for all three solutions, with the longer-term aim of moving to a single solution.

802.1x & web-based solutions

The discussion then identified similarities in the approaches of deliverables D and the F, thus concluding that interoperability between these two solutions was quite easy.

VPN solution

Carsten described the German scenario, to have an idea of how many addresses they would need. If we assume that there are 640 M people and that in Bremen they have 600 K user and they would need 60 addresses space to make VPN working, then at EU level they would need 16K addresses space. The numbers do not consider public hot spot. NL and FI do not have a VPN concentrators, so for them would be hard participating. It was agreed that as beginning each NRENs would allocate their own space to create 'rely networks'.

Klaas has proposed that SURFnet would build and configure a top tier RADIUS server that NREN level RADIUS servers could direct NREN visitor users to, to authenticate at their home institution. This server would be housed at SURFnet but could be moved to Terena (so long as there are resilient links to this server). The following countries NREN have expressed interest in this activity:

- Croatia, Portugal, Finland, NL, UK, Germany (but they would like to verify what they would need exactly).

Action: Klaas to supply details of this development activity and dates of when the RADIUS is scheduled to be ready for service.

Action: Klaas to produce information to the mobility group on what local requirements are necessary to enable NREN RADIUS servers to communicate with the TERENA level RADIUS.

Action: Erik/Klaas, Ueli and Sami to

1. List a set of parameters that each solution requires for a scalable European solution (including items that NRENs must agree on to make it work).
2. Identify how each solution will interoperate with the other solution (step-by-step); 802.1x to VPN, 802.1x to Web-based, VPN to 802.1x, VPN to web-based, Web based to 802.1x, Web based to VPN.
3. Deliverable owners to produce the answers to points 1 & 2 by May 28th 2003 to enable the first draft of deliverable to be produced.

Action: James to produce the first draft of deliverable G by 30th June 2003.

5. Other business

Portugal (FCCN) has just started getting involved in TF-Mobility. FCCN has been testing two different solutions: the first is the one based on 802.1x/EAP+RADIUS. They have tested the mobility part (proxying requests) with success, at a national level, between 8 different Portuguese universities. FCCN has also been involved in the different solutions

tested by Portuguese universities. One of them is the one implemented by IST, which uses certificates + IPsec.

They are currently involved in testing if these two solutions can converge at a national level.

Action: FCCN to supply details of their PKI solution to the mobility group.

6 Next Meeting

The TF-Mobility will be held on either the 22nd of September, probably in Berlin.

Summary of Actions

Action no	Owner	Action	Deadline
18.05.03 -1	LF	To move del B to the public area	Done
18.05.03 -2	ED/KW	<ol style="list-style-type: none"> 1. List a set of parameters that each solution requires for a scalable European solution (including items that NRENS must agree on to make it work). 2. Identify how each solution will interoperate with the other solution (step-by-step); 802.1x to VPN, 802.1x to Web-based, VPN to 802.1x, VPN to web-based, Web based to 802.1x, Web based to VPN. 3. RADIUS set-up 	28.05.03
18.05.03 -3	CB-LF-JS	Finalise the non-technical glossary	2-6-03
18.05.03 -4	JR	To update deliverable C with comments received from the mobility group and will modify the non-technical terms to ensure consistency with the non-technical glossary. The final version will be moved to the public area.	6-6-03
18.05.03 -5	ED/KW	To update deliverable D with comments received from the mobility group and will modify the non-technical terms to ensure consistency with the non-technical glossary. The final version will be moved to the public area.	6-6-03
18.05.03 -6	ED/KW	To consider the issue of NAT with Deliverable D	6-6-03

18.05.03 -7	UK	To update deliverable E with comments received from the mobility group and will modify the non-technical terms to ensure consistency with the non-technical glossary. The final version will be moved to the public area.	6-6-03
18.05.03 -8	UK	To consider the issue of NAT with Deliverable E	6-6-03
18.05.03 -9	NP	Niels Pollem to research the RFC on AAA server.	No date agreed
18.05.03 -10	SKK	To update deliverable F with comments received from the mobility group and will modify the non-technical terms to ensure consistency with the non-technical glossary. The final version will be moved to the public area.	6-6-03
18.05.03 -11	SKK	To consider the issue of NAT with Deliverable F	6-6-03
18.05.03 -12	KW	To supply details of the top level RADIUS development activity and dates of when this scheduled to be operational.	No date agreed
18.05.03 -13	KW	To produce information to the mobility list on what necessary local requirements are to enable NREN RADIUS servers to communicate with the TERENA level RADIUS.	No date agreed
18.05.03 -14	JS	To prepare a first version of Del G. Inputs for the deliverable by 15-06-03	30-6-03
18.05.03 -15	FCCN	FCCN to supply details of their PKI solution to the mobility group	Done

CB= Carsten Bormann
 NP_ Niels Pollem
 ED = Erik Dobbelsteijn
 KW= Klaas Wierenga
 LF = Licia Florio
 JS= James Sankar
 JR= Juergen Rauschenbach
 SKK= Sami Keski-Kasari
 UK= Ueli Kienholz
 FCCN = Portugese NREN