



TF-Mobility and Network Middleware Meeting

Tuesday, December 2

Utrecht

Licia Florio

Table of Contents

1. Welcome and Apologies	1
2. TF-Mobility and Network middleware work items	2
2.1 Standardisation process – Leif Johansson	2
2.2 Support for development next generation eduroam – Stefan Winter	2
2.3 Location awareness – Mark O’Leary	2
2.4 DNSSEC – Milan Sova	3
2.5 Integration with other mobile operators – Stefan Winter	3
2.6 Metering and monitoring – Miroslav Milinović	4
2.7 Sensor and mesh networks – Kurt Bauman	4
3. SIP and AAI integration - Davor Jovanovic	4
4. OpenSEA – Josh Howlett.....	5
5. IETF report – Stefan Winter.....	5
6. Mobile broadband at campuses - Glenn Wearen	6
7. Eduroam SA updates – Miroslav Milinovic	6
8. InfoCard and eduroam Enrique	6
9. National Updates	7
10. A.O.B.	7
n. Date of Next Meeting, AOB and Close	7

1. Welcome and Apologies

Klaas Wierenga, who chairs the task force, welcomed the attendees to the meeting and introduced the new TF-Mobility terms of reference, available on-line at:

<http://www.terena.org/activities/tf-mobility/docs/TFMobility-tof-08-10.pdf>

The agenda was hashed and approved with the addition of a new topic, concerning the new name of TF-Mobility.

According to the new terms of reference, agreed by the group and approved by the TERENA Technical Committee in September 2008, the remit of the task force has been changed to reflect the outcome of the redefinition of focus of the two middleware-oriented taskforces, known as TF-EMC2 and TF-Mobility. Consequently, TF-Mobility will focus on roaming and networking middleware and it will be called TF- Mobility and Network Middleware.

Because of the length of the new name, the TERENA Technical Committee (TTC) suggested the

use of an acronym, such as TF-MNM. Klaas asked the group whether the task force should be generally referred to as TF-MNM or as TF-Mobility, as it has been known for years.

The discussion that followed suggested the both acronym might be appropriate, depending on whether the group feels important to stress the redefinition of scope for the task force or to maintain continuity with the past. Because no agreement could be found, it was proposed to discuss this topic further on the mailing list.

For all official documentation the full name should be used.

2. TF-Mobility and Network middleware work items

Work item leaders presented some proposals for possible work to be carried out in their work items. Because most of the presentations were at very high level and mostly aimed to gather inputs, it was agreed that all work item leaders would send a more detailed plan on the work to be undertaken within their activities. Proposals should be circulated over the list by March.

Action: By first week of March, work item leaders to circulate a plan about their items.

2.1 Standardisation process – Leif Johansson

As Leif could not make the meeting, Klaas explained the aim of this work item.

One of the aims of the task force is to promote the usage of standardised technologies in the field of mobility. To achieve this, the group will liaise with other relevant projects as well as international bodies, such as IETF, to exchange results and ideas.

Concerning this matter, Stefan Winter added that participation to the IEEE is possible for non-members as well. Therefore he asked whether IEEE would be relevant for this group and in the affirmative case whether there would be volunteers to follow IEEE.

2.2 Support for development next generation eduroam – Stefan Winter

Stefan explained that this work item would cover very much RadSec developments. Although RadSec is covered within GN2 and GN3 (starting from the spring 2009), it is felt important to get inputs from a wider community than GN2/GN3.

Other potential topics to be addressed within this work item include chargeable user identity and the interaction between eduroam and InfoCard.

2.3 Location awareness – Mark O'Leary

Mobile devices use network technologies that can provide user location and context information. Location data can be used by mobile applications to provide personalised content reactive to dynamic environments.

Mark proposed that he would prepare a questionnaire to collect information on what NRENs are doing in this area. JANET(UK) for instance is preparing a report on their activities in this area.

Mark also added that this work item could also cover the standardisation part, looking at possible standards that might be relevant. Mark said that all aspects of location awareness should be considered, including user's privacy

Action: Mark to circulate a questionnaire to the mobility list to gather information on existing activities on location awareness.

2.4 DNSSEC – Milan Sova

DNSSEC deployment is rather slow and only a few countries use DNSSEC for their country code top-level domain. Because the deployment of DNSSEC at root levels has some political implications, Milan suggested this group not to be involved into this issue.

Milan proposed instead to investigate how applications can become DNSSEC-aware and how to store some data (for instance certificates) into DNSsec and use them for the application. Previously Stig Venas had also suggested creating an API to securely verify DNS.

Milan was asked what happens when a top-level domain is not signed. The answer was that DNSSEC is in this respect similar to any other PKI, therefore the top-level domain needs to be signed or at least self-signed.

Milan said that if DNSSEC were available for all eduroam participants, RadSec would make use of DNSsec, rather than using a dedicated RadSec PKI.

Klaas asked whether it would be possible to self-sign a domain and test with that.

A discussion followed. The conclusion was that this work item could:

- start collecting information about the deployment of DNSSEC in the countries represented in the task-force
- prepare what is necessary to self-signing eduroam.org and test that with RadSec.

Action: Milan to circulate information on the procedures needed to sign eduroam.org

2.5 Integration with other mobile operators – Stefan Winter

The aim of this work item is to investigate ways to collaborate with commercial providers that have hot-spots to support eduroam roaming users. If these agreements were in place in more countries, the eduroam community could have a wider access area.

Kurt reported that SWITCH talked with commercial mobile providers and that they were very interested in eduroam. Diego said that he spoke with some Spanish mobile providers and they would be interested in doing some trial with eduroam.

Stefan, however, pointed out that most of mobile operators make use of captive portals that are not compatible with the eduroam policy (web-based access to eduroam is not allowed for security reasons). Mark reported that JANET signed an agreement with a mobile operator that uses indeed a captive portal; users do not use eduroam credentials for this.

Miro asked if wired world is also included or if this work item should be confined to wireless only. Everybody agreed the work item should be also included wired eduroam networks.

It was agreed that this work item could collect all the national initiatives where agreements have been made between eduroam national operators and commercial operators. The list could be hosted on the work item page on the TF-Mobility pages.

Action: Stefan to send a request to the list to collect information.

2.6 Metering and monitoring – Miroslav Milinović

Miro presented his ideas about the work to undertake in this work item. The monitoring and metering tools should be concentrated on three aspects: users, infrastructures and services. Standardisation of logs is still unsolved, so this work item could also start some work on this direction.

Miro proposed to monitor all applications that make use of RADIUS (for instance SIP), which also include eduRoam. Chargeable user identity¹ could be handled via this.

2.7 Sensor and mesh networks – Kurt Bauman

Kurt presented the plan for this work item. The vision is to extend the fibre infrastructure with mesh and sensor networks. Kurt proposed to investigate on:

- the need for sensor networks; maybe use-cases could be defined;
- the technologies to use (WiMAX, UMTS etc);
- the security of the sensor nets;
- the monitoring and measuring tools.

Mark reported that Lancaster University, in UK, is working on a project using sensors. Diego said he would contact some people in Spain that are working on this. Somebody reported that Portugal might be doing some research on sensor-net, so it would be good contacting Lino Santos.

Action: Diego and Mark to report whether their national contact would be interested in joining this work item.

3. SIP and AAI integration - Davor Jovanovic

Davor presented the solution implemented by SRCE, in which access to SIP systems is granted to users via the Croatian federation. In the specific case of the project presented, a special client was developed.

Milan pointed out that most clients would not be able to support the process presented. Furthermore users have different devices that want to connect from and therefore a dedicated client for each of the possible user devices should be implemented.

Ken suggested looking at the IETF especially in what concerns SIP authentication issues. Standardisation of SIP clients is quite tricky due to the large variety of clients, with different authentication methods.

Diego pointed that the presentation brought up a more general issue, namely how to deal with non-web applications that are not federated.

¹ See TF-Mobility minutes: <http://www.terena.org/activities/tf-mobility/meetings/16/tf-mobilityv1.0.pdf>

4. **OpenSEA – Josh Howlett**

OpenSEA alliance works to develop an open source 802.1X supplicant. Josh reported on the development. The client has been ported into Vista and seems to work; there are some issues with the usage of the clients under Linux, which are being addressed.

5. **IETF report – Stefan Winter**

Stefan reported on the various meeting he attended during the IETF in November. The first part of the report was about RadSec and more specifically about radext working group.

Stefan also reported on the internationalisation issues that will affect eduroam. The problem occurs in international roaming due to the fact that eduroam interprets the realm for routing requests. Sticking to ASCII characters for realm names as up until now would keep the problem out of eduroam.

Some group within the IETF committed to write a document describing how bad AAA proxies are. Stefan attended a meeting with these people and proposed to broaden the scope of the document to also include why proxies might be necessary, see for instance in eduroam.

Stefan also reported on EAP method updates, which will allow:

- To tie together inner and out EAP method; this should enable the supplicant to talk to the IdP in a secure way;
- To enable EAP peer communication.

A draft that states the requirements for tunnelling protocols is under discussion; this would mean that if a new tunnelling protocol is created it should follow those requirements.

a) NEA (Network Endpoint Assessment) - The standardisation processes seems to come along.

However, Stefan pointed out that endpoint assessment tools are able to query users' registries accessing in this way to all kind of private information. Users, in most of the cases, are not aware of which information NEA clients request, which seems to be against regulations.

One option would be ask for user consent.

On this respect, Josh said that the possibility to access to users' registries is related to the TPM chip in modern mainboards; it is a vendor-specific thing what to ask in an assessment.

NEA working group is deciding on how to standardise on the attributes that applications need.

Currently NEA is not looking at remote posture issues, neither at virtual machines.

b) Diameter WG – In the past, TF-Mobility had considered using Diameter for eduroam. It turned out that one the Diameter features (the dynamic discovery) is broken. The specific IETF WG agreed to change Diameter discovery to follow RadSec behaviour.

c) Diameter TLS negotiation – Stefan flagged a new issue about Diameter: the initial diameter negotiations are either unsecured or rely on external security. The (external) IPSec operation mode is (arguably) secure, whereas the TLS one is not.

d) CAPWAP WG – Stefan reported on IETF wg called capwap (Control And Provisioning of Wireless Access Points). Capwap aims to provide interoperability among WLAN backend architectures. If this were to be deployed the problem of overlapping WLAN in eduroam is one of the issues that could be addressed in a non-vendor-specific way.

There is 802.1x revision and Stefan is looking at this. The revision will take care of providing better support for wired networks and it would improve the error reporting to the client.

Stig Venaas work on authenticated DHCP will become part of a dhcp working group.

6. Mobile broadband at campuses - Glenn Wearen

Glenn presented the wireless strategy implemented by HEAnet. A consultant company was hired to investigate on campus needs. The strategic findings showed overwhelming agreement among campuses concerning their wishes, but there was no request on a particular technology.

The first phase of roll-out started, which start in 2008 and will end in 2010, will deliver a national high quality and affordable wireless service. The second phase (from 2010 until 2013) will address the designing of a on and off-campus WiMAX solution.

A tender was open to provide national coverage. Four providers answered to the tender. The service was launched in Sep 2008.

7. Eduroam SA updates – Miroslav Milinovic

Miro gave an update on eduroam SA. The European confederated eduroam service is funded via GN2 project and will continue to be funded in GN3 as well.

Miro gave an overview on what has been achieved and presented some of plans for the eduroam work within GN3.

8. InfoCard and eduroam – Enrique de la Hoz

Enrique presented the principles of InfoCards.

InfoCards is an xml document that contains information about users (users decide which information to put in the infoCard). An IdP based on the infoCard presented by the user generates a signed token containing the related attributes. The token is presented to the SP to get access to a resource. Because the token is technology agnostic, both OpenID and SAML1.1 can be used.

Enrique presented a proposal to combine InfoCard with eduroam.

The authentication would be normal eduroam authN as in PEAP-TLS, but the RADIUS response could contain an InfoCard.

Somebody pointed the same approach could be followed using Kerberos instead than InfoCard. Diego said that Kerberos is not widely spread, whereas InfoCard is.

A discussion followed about the added value of the integration of eduroam and InfoCard for users, as result of which it was said that the approached proposed would replace the WAYF. In the case in which the InfoCard could also contain information about the user's location, then the proposed solution could help Mark's work item.

To avoid double authentication of the users (once for eduroam and once to access their IdP), Stefan asked whether it would be possible to send the actual token, rather than the artefact. Enrique explained that in many cases users do not have their own computers, but use public computers at the university. In this case users are able to get their InfoCard only after they have logged in to eduroam (the InfoCard would be sent via the RADIUS).

9. Highlights about National Updates

- eduroam SP will be available in Luxembourg city downtown.
- DFN is using a new map for eduroam: www.eduroam.de
- UK is launching a service to support people with limited mobility to allow them to access courses etc.

10. A.O.B.

Stefan reported that WPA-TKIP is broken.

TKIP was meant to work with older hardware; it has features to be backward compatible. In fact it has been broken because of these features. However it is worth noting that damages that can be done with the published attacks on TKIP are rather limited for the moment. However institutions operating eduroam should be take into account this problem and migrate to different encryption methods.

Mark said that the UK mobile advisory board is preparing a document describing the type of attack and how to prevent it. Mark will share the document with the group.

Action: Mark to send the document to the mobility list.

n. Date of Next Meeting, AOB and Close

The next TF-Mobility meeting will be on 7 May in UK. JANET will host it.

Action List

Reference	Who	Action	Status
02122008-01	Work item leaders	By the first week of March, work item leaders to circulate a more detailed plan about their items.	
02122008-02	Mark O'Leary	To circulate a questionnaire to the mobility list to gather information on existing activities on location awareness.	
02122008-03	Milan Sova	To circulate the information on the procedures needed to sign eduroam.org	
02122008-04	Stefan Winter	To send a request to the list to collect information about national initiatives where agreements have been made between eduroam national operators and commercial operators.	
02122008-05	Diego Lopez and Mark O'Leary	To report whether their national contact would be interested in joining the sensornet work item.	
02122008-06	Mark O'Leary	To send the document about TKIP attack prepared by the JANET advisory board to the mobility list.	

List of Participants

First Name	Last Name	Affiliation
Wenche	Backman	CSC/Funet
Kurt	Baumann	SWITCH
Enrique	de la Hoz de la Hoz	University of Alcala
Paul	Dekkers	SURFnet
Licia	Florio	TERENA
Michael	Helm	ESnet
Davor	Jovanovic	Srce
Kenneth	Klingenstein	Internet2
Diego	Lopez	RedIRIS
José-Manuel	Macías	RedIRIS
Danijel	Matek	Srce
Miroslav	Milinic	Srce
Anders	Nilsson	Umeå university SUNET
Mark	O'Leary	JANET(UK)

Viviani	Paz	AusCERT
Dubravko	Penezic	Srce
Jaime	Pérez	RedIRIS
Juergen	Rauschenbach	DFN-Verein
Milan	Sova	CESNET
Glenn	Wearen	HEAnet Ltd
Torbjörn	Wiberg	Umeå universitet/SWAMI
Klaas	Wierenga	Cisco Systems
Stefan	Winter	RESTENA