

TF-Mobility meeting

8 July 2008

Umeå, Sweden

1. Welcome

Klaas Wierenga, as chair of TF-Mobility, welcomed the participants.

Klaas reminded that the TF-Mobility mandate will officially expire in September 2008. Therefore during the meeting a decision should be taken on whether continue or not the work of TF-Mobility and in case suggestions for a possible new charter should be put forward.

2. Activities update

A summary of the status of the various TF-Mobility activities followed, mainly aimed at understanding what has each task has achieved during the two-year mandate.

2.1. RadSec updates - Stefan Winter

Stefan gave an update on RADIUS developments within IETF.

Stefan announced that the re-chartering of radext working group took place, which means that both RADIUS over TCP and TLS authentication of RADIUS peers will now be in scope for the radext working group.

Stefan also reported that the work on FreeRADIUS, funded via GN2, has started and that TCP transport has been implemented.

A discussion on loop detection (when using RadSec both on the client and server-side) took place. Stefan explained that the problem is due to the fact that with RadSec it is not possible to discover the IP address from which the request is initiated. Stefan proposed two possible solutions to this problem, which were discussed. Paul Dekkers said that most of the configurations on the client-side are dynamic and therefore it is difficult to keep track of the connections, therefore a possible solution would be the use of static client configurations and to agree on the set of IPs used.

As result of the discussion it was agreed to check the subjects in the certificates used by the servers.

The case of mixed environments (RADIUS-RadSec) was discussed. In principle this should be avoided whenever possible, however the migration from RADIUS to RadSec might lead to mix environments.

Stefan presented the idea of eduroam@home, which translates into putting RadSec on an AP to take it to an arbitrary place, like for example at home, a conference and similar. Victoriano Giralt reported that he tried it and it worked smoothly.

Tomasz started a discussion whether all eduroam networks should be seen as "trusted" locations, with a strong connection and commitment into academia. The result of the discussion was that even if users get on the Internet via eduroam, users are just "somewhere on the internet" and therefore it should not be assumed that

their traffic is in any way privileged. Stefan also reminded that eduroam service has never been advertised differently, even if some people might have interpreted it in a different way.

Tomasz then said he might reconsider using the SSID eduroam as the "native" campus connection because his users might be unable to establish the level of trust they can put into the eduroam network.

2.2 Liaison with other international activities: TNC and NAC - Mark O'Leary / Klaas

Klaas gave a quick overview about TNC scope. Since recently TNC work has been brought into IETF, which will make TNC work more open.

Mark gave an update on the developments on the OpenSEA client, which is progressing and available for testing online (see <http://open1x.sourceforge.net/>). However the full list of features requested by JANET is not available yet.

2.3. Updates on eduroam developments world-wide – Klaas

Klaas reported on eduroam developments in Canada. eduroam initiative in Canada is carried out by Canadian universities rather than CANARIE (the body that provides connectivity to the universities). These universities are cooperating to eventually provide federation support and infrastructures.

The Canadian eduroam website (available since recently) provides lots of information:

<https://wiki.bc.net/atl-conf/display/CANEDUROAM/Canada+eduroam>

Jose Manuel reported on eduroam developments in Peru and El Salvador.

3. eduroam Service Activity updates - Miroslav Milinovic

Miroslav gave an update about the GN2 eduroam Service Activity (SA5) meeting held in Berlin in June, during the GN2 technical workshop.

Miroslav reported that 33 NROs/NRENs have signed the eduroam policy. Some NRENs have asked for some extra time to comply the policy. This is the case of JANET(UK), which should sign the policy by the end of 2008.

Miro reported that the Russian NREN has contacted him to join eduroam (Miro is currently following up on that) and that Andorra will join eduroam as an independent country.

The eduroam website (launched in March 2008) will get some new sections, namely training and monitoring sections and an improved version of the eduroam cookbook. The private area (which will be a wiki) for the website should be ready in the fall.

With regards to the cookbook, Miroslav pointed out that the cookbook could be expanded to also include a "how to section" on eduroam configuration with Novell and AD as well as other less common RADIUS version. Attendees were invited to provide feedback on this.

Miroslav showed maps depicting eduroam presence in each country and asked people to send him comments. The maps are generated using the values stored in the eduroam database.

Lastly a new version of the eduroam policy should also be produced when the new eduroam service activity will start (Spring 2009).

4. Fast roaming work - Tomasz Wolniewicz

Tomasz experimented with fast handover for voice over IP over wireless networks. Ideally when users move from one AP to the other, there should not be a loss of packets (or in any case it should be minimum). The practical results showed instead that the time needed to re-authenticate users to the new AP is still quite high and in the case of eduroam it can take up to several seconds.

5. National Updates

University of Tohoku - Hideaki Sone presented the authentication process used for eduroam in Japan. This implementation uses VPN, which is set up in a transparent way for the client. The client authenticates with the AP at the visited institution; the AP is connected to a VPN gateway, which connects to the VPN server at the home institution.

The solution presented raised concerns on how to prevent session hijacking and on how the VPN tunnel is established.

Hideaki agreed to circulate his paper to the mobility list for further comments.

RESTENA – Stefan reported on the pilot to use the public administration (municipality of city of Luxembourg) as an eduroam service provider. Stefan said not to particularly like the intermediate page users see before being allowed on the Internet. This page promotes the public administration as an eduroam hotspot.

JANET – Mark reported on the discussion ongoing with the mobile operators in UK to allow eduroam enabled users to also roam on commercial networks.

FUNET – Mikael Linden reported that there are still lots of institutions that are using captive portals. FUNET are trying to move them away but the process is quite slow.

CARNet – Miroslav reported on the pervasiveness of eduroam in Croatia. He said that there are 31 SP and more than 200 IdP in Croatia. Lots of work is now being invested into the monitoring infrastructure. There are also some initiatives to provide eduroam in public places, like museums and libraries, but nothing concrete has happened so far.

CESNET – Milan Sova reported that there are about 60 institutions connected to eduroam. CESNET have started tests with RadSec. In the long term RadSec should replace IPSec, currently in use.

RedIRIS – Jose Manuel reported that TTS (Trouble Ticketing System) is now in place.

PIONIER – Tomasz reported that the main activity in Poland is focused on finalising the eduroam national policy in order to comply with the national legislation.

SURFnet – Paul reported that SURFnet are developing a tool (applet) to configure the wired/wireless eduroam supplicant. The tool works for both SecureW2 and Mac OS X built-in supplicants.

Some objections about this tool were raised by some of the attendees, as the usage of the tool implies that users would have to trust the applet and enter their credential into the applet to configure their machines. Although Paul disagreed with these

remarks (when users insert their credential into the applet they are using their home institution intranet), he said that the issue could be solved by first authenticating users via their federation, so the applet would become one of the services offered by the federation.

6. Future of TF-Mobility and discussion on the new charter

Klaas asked whether the group felt that TF-Mobility should continue or end in September 2008.

The general consensus was that TF-Mobility is a well-know established forum in Europe (and beyond) and therefore it should continue. Participants felt that the added value of TF-Mobility is to allow anybody to present some ideas or test in an informal way and gather comments from a wide community of experts.

Klaas then presented his proposal on how to continue the work of TF-Mobility.

He said that both TF-Mobility and TF-EMC2 focus on middleware even if with some differences; a way forward (also discussed with Diego Lopez, chair of TF-EMC2) would be to re-focus both task forces following the protocol stack. In this new perspective all network-oriented middleware tasks should fall into TF-Mobility, whereas application-oriented middleware tasks should be dealt within TF-EMC2.

There was consensus on the proposal.

Possible topics for the next TF-Mobility charter were presented.

6.1 Location awareness – Mark

Mark presented his proposal for the work on Location awareness technologies, which span beyond wireless technologies.

There could be room for some work on policies and regulations, especially considering that locating a person would have to comply with privacy regulations.

He suggested that the new TF-Mobility charter could include work on the creation of a general framework, which would collect information from users different devices (GPS, RADIUS logs and others). The information could then be used to provide the users with specific information related to the place they are visiting.

It was agreed to add this topic into the charter.

6.2 DNSSEC - Milan

Milan said although DNSsec up taking is growing, there are currently still some obstacles coming from the commercial CAs. Milan said that DNSsec work could be divided into two groups:

- Rollout: this case would involve technologies as well as polices. As in most of the cases NRENs do not operate DNSsec directly, it would be difficult for NRENs to influence this area. Stig Venas suggested concentrating in the creation of an API to securely verify DNS.
- Users deployments: Milan said that this aspect would be quite interesting, as most of the applications are not DNSSEC aware. However, being this aspect more focused on application it might have to be discussed within EMC2.

6.3 UMTS and possible interaction with mobile operators - Stefan

Stefan proposed his idea to better explore UMTS. Both UMTS and GPRS are ubiquitous technologies, but still expensive for users. The EU is working to regulate

the data roaming cost, which should bring the costs down. Stefan proposed that NRENs become data (roaming) provider or at least that the issues involved in becoming roaming provider be explored.

Klaas pointed out that the business model should be looked at.

Stefan proposes some options one of which could involve TERENA becoming APN or a virtual operator.

It was agreed to add this topic into the charter and produce at least recommendations. Paul also suggested looking at WiMax.

7. Conclusions

There was an open discussion on how to continue TF-Mobility work. It was agreed that Klaas would collect the input received and would prepare, together with Licia, a skeleton for the new TF-Mobility charter. Ideally the new charter should be ready for approval in September 2008.

8. Next Meeting

Next TF-Mobility meeting will take place on 2 December 2008 in Utrecht (the Netherlands).

List of Attendees

Name	Affiliation
Kolbjørn Barmen	UNINETT
Paul Dekkers	SURFnet
Licia Florio	TERENA
Victoriano Giralt	University of Malaga
Maja Gorecka-Wolniewicz	PIONIER
Roland Hedberg	Umeå University
Thomas Lenggenhager	SWITCH
Mikael Linden	CSC, the Finnish IT Center for Science
Jose-Manuel Macias	RedIRIS
Miroslav Milinovic	Srce
Anders Nilsson	Umeå univ / SUNET
Mark O'Leary	JANET(UK)
Hideaki Sone	Tohoku University
Milan Sova	CESNET
Stig Venaas	UNINETT
Torbjörn Wiberg	Umeå Universitet/SWAMI
Klaas Wierenga	Cisco Systems
Stefan Winter	RESTENA
Tomasz Wolniewicz	PIONIER