

**23rd TF-Mobility and Network Middleware Meeting - Wednesday, 16 February 2011**

Lyon, France. The meeting was hosted by the University of Lyon and CRU.

Table of Contents

1. Welcome and Apologies.....	1
2. Approval of Agenda, Minutes of Last Meeting and Update of Action List.....	1
3. Work items updates - All Work items (WI) leaders	2
3.1 Standardisation process.....	2
3.2 Support for the development of the next generation eduroam.....	3
- EAP Channel Binding	3
3.3 Support for eduroam world-wide & 3.7 Metering and monitoring	3
3.4 Location awareness.....	4
3.5 Future DNS.....	4
3.6 Enabling Ubiquitous Mobility.....	5
- 3G/4G handoff investigation	5
3.8 Sensor and mesh networking	5
5. Work items updates - All Work items (WI) leaders (Part II)	6
5.1 Scalable 2-factor authentication.....	6
5.2 Integration of network middleware with identity federations	6
5.3 Liaison with GN3 & other initiatives	6
5.4 New mobile technologies	6
6. Mobility & Network Middleware Activities	6
6.1 eduroam Cookbook	6
6.2 eduroam initiative in the United States of America	7
6.3 EAP-TLS in eduroam using TCS Personal Certs.....	7
7. National and Community Updates	7
8. Date of Next Meeting	8
9. AOB and Close	8
10. Summary of Actions.....	8

1. Welcome and Apologies

Klaas Wierenga welcomed everyone to the meeting. Attendance and Apologies were recorded on the event registration page: http://www.terena.org/events/details.php?event_id=1918

2. Approval of Agenda, Minutes of Last Meeting and Update of Action List

The agenda was modified as the day progressed with the final version available online: <http://www.terena.org/activities/tf-mobility/meetings/23/>

The minutes of the last meeting held on the 23rd of September 2010 were approved without corrections and are available at:

<http://www.terena.org/activities/tf-mobility/meetings/22/minutes.pdf>

Summary of Actions

Reference	Who	Action	Status
20100923-01	Paul Victoriano	Document the issue of mixing 802.11a/b/g/n and post to the mailing list.	<i>Stefan has posted the question with some community follow-up</i>
20100923-02	Lalla	Report on why the Italian Anti-Terrorism/User Identification Laws aren't compatible with eduroam use	<i>Claudio Allochio clarified with his ministry and that eduroam is the only approved mechanism. (Law had an expiry date of Dec 2007, and extended repeatedly)</i>
20100923-03	Leif Roland	Lead the preparatory work on a 2-factor this work item.	<i>Became a work item for the current incarnation of TF-MNM.</i>
20100923-04	Brook	Create a mailing list for '2factor' WI	<i>Done.</i>
20100923-05	All	Send updated text for Work Items by end of October to TF Chair.	<i>Done.</i>
20100923-06	Brook	Transfer Josh Howlett's presentation to the next TF-MNM agenda.	<i>Done. Update to be presented by Rhys Smith.</i>

20100923-02: Lalla reported that Article 7 of the Anti-Terrorism Law (regarding user identification on wifi networks) was suppressed by decree. It is expected that a new law will be passed to replace this and explicitly mention federated mechanisms of authentication as being acceptable.

3. Work items updates - All Work items (WI) leaders

3.1 Standardisation process

Stefan presented on work on the standardisation process (see <http://www.terena.org/activities/tf-mobility/meetings/23/tf-mobility-lyon-standardisation.pdf> or <http://www.terena.org/activities/tf-mobility/meetings/23/tf-mobility-lyon-standardisation.odp>).

He covered three (3) areas:

- RADIUS/TCP
- RADIUS/TLS
- 802.1X-2010

RADIUS/TCP has been published at <http://tools.ietf.org/search/draft-ietf-radext-tcp-transport-09> and the author (Alan DeKok) is in attendance. RADIUS/TLS is still discussing the issue of multiple ports for Authentication, Accounting and Dynamic Authorisation Changes vs a single port (TCP/2083) with a revised version of the document <http://tools.ietf.org/html/draft-ietf->

[radext-radsec-07](#) due prior to the cut-off period for IETF 80 (Prague). 802.1X-2010 will allow network identification on the wired so there can be multiple networks announced and discovered by clients. There was some confusion over which vendors has support for this in their switches.

[**ACTION**] Klaas to identify what series of equipment is capable of these features.

3.2 Support for the development of the next generation eduroam

Stefan Winter presented on eduroam "nextgen" (see <http://www.terena.org/activities/tf-mobility/meetings/23/tf-mobility-lyon-nextgen.pdf> or <http://www.terena.org/activities/tf-mobility/meetings/23/tf-mobility-lyon-nextgen.odp>) which covered the topics:

- GN3 Deliverables
- Use of RADIUS/TLS
- eduroam Trust Profile for Certificate Authorities
- GN3 Year 3 work

Of note is the work of eduPKI which has defined a trust profile for eduroam RADSEC see: <https://www.edupki.org/documents/trust-profile-related-documents/> The profile was tested and at the end of 2010 it was accepted by the eduroam community. Currently only the eduPKI CA supports this profile. The use of TCS to issue eduroam certificates was discussed and two issues were highlighted:

- how would eduroam RADIUS servers trust the TCS CA rather than the parents roots of this CA;
- as the RA procedures to issue eduroam certificates are slightly different from those used in TCS some modifications would be required.

Milan clarified how TLS certificate validation utilises the certificate chain. Leif said that is the only way to ensure that commercial CAs can be used for eduroam is to test the chain validation. It was clear that until further testing to confirm/deny the issues raised that only the eduPKI CA is to be used and not certificate authorities that have multiple children from their root.

[**ACTION**] Leif and Milan to explore certificate chain validation to verify the applicability of the use of TCS certificates for dynamic RADSEC.

- EAP Channel Binding

Alan DeKok presented on EAP Channel Bindings (see: <http://www.terena.org/activities/tf-mobility/meetings/23/Channel%20Bindings.ppt>) which ensures that information reported by intermediate equipment accurately reflects network usage. Currently accounting traffic can be unreliable, which limits its value in abuse reporting cases.

Klaas gave the example of credit card purchases supplying a user with a paper receipt that can be checked against bank records for verification. Channel Binding offers the same utility by ensuring that the client and intermediate equipment agree with the information sent to a RADIUS authorisation server.

3.3 Support for eduroam world-wide & 3.7 Metering and monitoring

Miroslav Milinović combined his presentations on eduroam world wide and the metering and monitoring work (see: <http://www.terena.org/activities/tf-mobility/meetings/23/eduroam2008->

[2010.pdf](#)).

He reported on the Global eduroam Governance Committee (GeGC) which has been formulating a compliance statement and joining process for eduroam deployments beyond the GN3 Confederation. He made particular reference to emerging efforts in Kenya and South Africa. José-Manuel reported that El Salvador and Peru are willing to host proxy servers for Latin America and have been in discussion with RedIRIS which was a result of a RedIRIS hosted meeting in Madrid with participants from RedCLARA.

Brook reported that Noemi from RNP had recently made contact following discussions with Stefan at TNC2010 and reported that there will soon be peering trials between Brazil and The Netherlands and wanted assistance in co-ordinating these efforts.

3.4 Location awareness

Mark O'Leary talked about the projects that he is co-ordinating with the help of student projects at the University of Southampton and the JANET 802.1x special interest group. The projects want accurate mapping information but the precision and quality of the data within the GN3 monitoring database is only at the resolution of a campus. For a site with thousands of access points they are often all located at the one point.

Mark has a student working on an iPhone app for a 1 year project. The 802.1x special interest group is looking at an Android application. These applications will look at crowd sourcing geolocation data of eduroam access points with an upstream approval process by administrators as a method of more accurate data collection.

Mark has previously announced a location aware survey and said it was "coming soon" but this time it really is coming soon and will be announced on the TF-MNM mailing list mobility@terena.org in the coming weeks.

[**ACTION**] Mark to announce the location aware survey to the TF-MNM mailing list.

3.5 Future DNS

Roland presented a DNSSEC update (see <http://www.terena.org/activities/tf-mobility/meetings/23/Presentation%20DNSSEC%20TF%20MNM%2020110216.pdf>) which revealed that while DNSSEC validations had been rising at the previous meeting they are largely static at the moment. There were some announcements that [.ac.uk](#) [.lu](#) and [.li](#) have been signed. Some domains haven't pushed their keys to the root but work will work toward that in the coming weeks.

Roland reported there is a bug in BIND (9.6) that was visible when [.nl](#) and [.fr](#) was signed and particularly the signing of [.net](#) made this issue very noticeable. Last weekend [.fr](#) disappeared off the DNSSEC signed internet.

SURFnet have published a white paper on applications of cryptography: <http://bit.ly/sn-crypto>

Roland called for participation in the creating of a validating resolvers data-mining tool. Mark O'Leary and Stefan Winter indicated interest in this area as domains had been signed in their countries. Roland indicated that signed domains, even if child domains aren't signed, are useful

points for data capture as the [.ac.uk](#) will receive queries for its keys from validating resolvers. Another new topic of research is into client behaviour. Initial effort has been signing domains and validation but not work into the affect on stub resolvers.

[**ACTION**] Roland to make a call on the mailing list regarding the measuring of validating resolvers and stub client investigation activities.

3.6 Enabling Ubiquitous Mobility

Paul Dekkers presented on a call to arms on areas supporting ubiquitous mobility (see: <http://www.terena.org/activities/tf-mobility/meetings/23/eam-feb11-01.ppt>).

Some NRENs are considering becoming MVNOs (Mobile Virtual Network Operator) so it may be possible for them to have roaming agreements with each other, in the case in which the MVNOs could really be able to manage the authN, the accounting and the billing.

Klaas asked whether academic MVNOs could offer data roaming services between countries without the tariff charges that traditional roaming incurs. This was taken as an area for further exploration by NRENs active in this area.

JANET is the first NREN that has plans to become an MVNO, although they are not considering handling billing themselves. They have a tender underway and expect to have an announcement in Q2 2011. Mark stated that ideally JANET would be investigating LTE (3GPP Long Term Evolution) services this year - but the existing deployments aren't at a stage where it can be seriously considered.

Brook referred the group to the O2/Telefónica announcement that they are offering free public WiFi not only for their own customers but all WiFi users indicating that offloading all 3G users on to WiFi is beneficial (see: <http://news.o2.co.uk/Home-Page-Body-Announcement/O2-redefines-Wi-Fi-landscape-with-launch-of-O2-Wifi-2e9.aspx>). Paul and Mark agreed that the 3G and WiFi business units of mobile operators were separate and needed to generate their own revenue which appears to be more important than supporting other business units.

Paul reaffirmed the advantage within Research & Education that if the "eduroam" SSID is available then automatic offloading from 3G to WiFi will occur quickly and automatically and there is limited demand for not R&E users on R&E campuses. Mark stated that there needs to be a benefit to the institution deploying eduroam rather than just a benefit to the 3G operator in their offloading as there are many JANET customers with sites that are heavily frequented by tourists and need to align the benefit of offering the service to their organisation and not the tourist attraction.

- 3G/4G handoff investigation

Leif presented on the work of a consultant with a background in 3G/LTE (see: <http://www.terena.org/activities/tf-mobility/meetings/23/sunet-3g-handover-lyon.pdf>). This report focused on business approaches with mobile operators and how that can benefit the R&E community and how they can participate.

3.8 Sensor and mesh networking

Kurt presented on the A⁴-Mesh-Project (see: <http://www.terena.org/activities/tf->

mobility/meetings/23/sunet-3g-handover-lyon.pdf). The project is building Authentication, Authorization, Accounting and Auditing in Wireless Mesh Networks. The addition of auditing is to detect and remedy erroneous nodes in the system. The project website can be found at <http://a4-mesh.unibe.ch/>

5. Work items updates - All Work items (WI) leaders (Part II)

5.1 Scalable 2-factor authentication

Joost van Dijk presented the different community efforts for 2-factor auth (see <http://www.terena.org/activities/tf-mobility/meetings/23/2factorauthN-tf-mnm-feb15-2011.pdf>)

The talk focused on 2-factor authentication, community efforts in this space, a comparison of 2-factor technologies and the current work within SURFnet to support 2-factor authN using iPhone. The SURFauth application will initially be made available for iPhone (arriving in the App Store by May) and Android systems. There are plans to investigate the support for other devices.

Joost called on the community to announce their work on 2-factor authentication and to acquire use cases and ideas in this space. Those interested should join <http://www.terena.org/maillinglists.php?list=2factor@terena.org>.

5.2 Integration of network middleware with identity federations

It was agreed at in the interest of time to refer to the presentation and updates given during the TF-EMC2 meeting.

5.3 Liaison with GN3 & other initiatives

Licia mentioned that the GN3 project has proposed a feasibility study that covers some of the topics that have been presented by Leif and Paul. The study if approved should be conducted during this year leading to a procurement process.

Klaas raised concerns with starting such a large activity/procurement without knowing exactly what to do. There should be more research in the deployment of these services at a smaller scale to inform this work.

The JRA3 roaming task has investigated the possibility of NREN networks carrying 3G operators' traffic in return providing university students and staff access to 3G networks outside of campuses. This is reported in a deliverable that will soon be published. (http://www.geant.net/Research/Multidomain_User_Application_Research/Pages/home.aspx)

5.4 New mobile technologies

Klaas mentioned some interested in 802.11u, which becomes particularly relevant in light of the discussion regarding 3G operators (discussed earlier). Currently there are no open implementations of 802.11u known to the participants.

6. Mobility & Network Middleware Activities

6.1 eduroam Cookbook

Stefan was unable to present and called on the group to provide feedback on his presentation (see: <http://www.terena.org/activities/tf-mobility/meetings/23/tf-mobility-lyon-cookbook.pdf>)

6.2 eduroam initiative in the United States of America

Philippe Hanset joined the group via videoconference link to provide an update of the work within the USA and his work on deploying eduroam.

Of note is the use of CILogon project <http://www.cilogon.org/> to offer EAP-TLS eduroam services to the 300 participant organisations within the InCommon identity federation. The downside is that these organisations aren't becoming eduroam hotspots but the benefit in being able to show user demand and concentrations of activity will make wider demand for eduroam visible.

Brought up the issue of dynamic DNS lookup; it was pointed out that the DNS answer can only be trusted if there is a secure connection, for which RADIUS over TLS would be required.

6.3 EAP-TLS in eduroam using TCS Personal Certs

José-Manuel Macías presented on RedIRIS' testing TCS client certs (see: <http://www.terena.org/activities/tf-mobility/meetings/23/TF-MnM-Lyon.pdf>)

José-Manuel presented how EAP-TLS works for both FreeRADIUS and Radiator and that TCS certs used include a user's identifier in the unstructured name field of the certificate. The main use-case is to support EAP-TLS as it's one of the default EAP-types supported by Microsoft Windows. This also indirectly promotes the use of the SIR federation and has been in production since February.

Tomasz noted that in Poland they are also supporting EAP-TLS using different certificates, with almost no info about the users. Tomasz expressed concerned in the using these certs for privacy reasons and information disclosure.

Paul drew people's attention to his presentation at the 21st TF-MNM meeting <http://www.terena.org/activities/tf-mobility/meetings/21/eap-fast-02.ppt> that indicated serious fragmentation issues with EAP-TLS. RedIRIS have not noticed this as a problem.

7. National and Community Updates

- Finland** they will join FTicks. Investigated becoming MVNO, but a final decision is still pending. JANET's procurements document could help.
- Sweden** FTicks is a high priority at the moment for roll out.
- France** [RENATER Activities Update](#): Main priority is to make roaming easier for end-users and they plan to take some strong measures such as institutions that are not fully eduroam compliant will not be displayed on the eduroam map. They will also introduce a "metre" to classify institutions.
- Poland** No major news, but more institutions have joined and it seems like the ministry of education is aware of eduroam.
- The Netherlands** Less problems with eduroam reported by the users since SURFnet rationalised EAP-types. SURFnet also offered pre-configured eduroam APs for institutions and events; this seems to work very well.
- Spain** Work done to offer monitoring tools (see Jaime's presentation at TF-EMC2). Documentation on Nokia and BlackBerry devices are available, more to come.

8. Date of Next Meeting

The next TF-MNM meeting will be held virtually via videoconference and has been scheduled for the end of June. It was agreed that the 25th meeting is to be held in the week starting on Nov 7th, venue and exact dates to be confirmed.

9. AOB and Close

The meeting closed at 17:30. (Minutes published 24 February 2011)

10. Summary of Actions

Reference	Who	Action	Status
20110216-01	Klaas	Identify what series of equipment is capable of 802.1X-2010.	
20110216-02	Leif Milan	Explore certificate chain validation to verify the applicability of the use of TCS certificates for dynamic RADSEC.	
20110216-03	Mark	Announce the location aware survey to the TF-MNM mailing list.	
20110216-04	Roland	Make a call on the MNM and DNSSEC mailing lists regarding the measuring of validating resolvers and stub client investigation activities.	

Document History

Date	Comment	Status
16 Feb 2011	Initial text collaboratively written in Google Docs.	Internal
24 Feb 2011	Initial version published for comment.	Published
25 Feb 2011	Minor corrections after feedback from community including: <ul style="list-style-type: none">• SURFnet list as a country.• France update link included in agenda but not minutes.	Published