

## **TF-Mobility Meeting**

**Marseilles, 06 Feb 2008**

### **Welcome and Introduction**

Klaas welcomed the participants and bashed the agenda.

### **Round table**

On the sake of time it was agreed the participants to provide a very short update on their current activities during the round table introduction.

**Restena** – Stefan reported that has connected their university to eduroam and they are now in the process to connect a couple of schools;

**CRU** - eduroam is in production and it seems to work;

**SRCE** – wired eduroam is provided in all dormitories in Croatia.;

**RedIRIS** – they are migrating to FreeRADIUS;

**SWITCH** – the deployment of eduroam is still quit slow;

**PIONIER** – there are currently 15 universities connected;

**FUNET** – they are working on a sort of eduroam in a box, wirmare based;

**SURFNet** – currently the monitoring has high priority;

**CESNET** – Milan presented his proposal to migrate to EAP-TLS;

### **Liaison TF-Mobility/JRA5/SA5**

Klaas pointed out the importance to report JRA5 and SA5 results to TF-Mobility. Although there is quite a significant overlap between the active participants in TF-Mobility and JRA5/SA5, TF-Mobility mailing list gathers a wider audience including some university eduroam operators as well as expert outside Europe. Both Juergen and Miro agreed that this is an important communication channel and they will make sure to involve TF-Mobility list in the technical discussion in the very early stage.

### **SensorNet for monitoring – Dubravko Penezic**

Dubravko presented the architecture of the document that he sent to the list. The aim of the system is to gather information to verify that eduroam works properly, such the strength of the signal, the authN method used and whether the authN works, the status of the access point and so on.

There were some comments on the architecture, mainly about the added value of using a sensor-net for managing a wireless infrastructure. There was also a discussion about the type of hardware to use and the type of sensors.

**Action:** Dubravko to update the document in order to provide use-cases and to include the comments.

## **Using eduroam infrastructure for other Applications – Jose Manuel Macia Luna**

During the last meeting Jose-Manuel agreed to test how what applications and devices to use for the purpose. He investigated and his suggestion would be to only use VoIP and video-streaming.

The aim would be to provide indications for the right type of network for the specific applications.

Klaas pointed out that this is an area that spans a bit outside the classic mobility focus, but it might be worth looking at for the future especially now that wireless and mobile devices are more reliable.

**Action:** Jose Manuel would be worth to prepare a document to highlight how eduroam network (or a wireless network) can support video applications.

## **eduroam SA5 Updates – Miroslav Milinovic**

Miro provided an update on the SA activity after the meeting in Rome. The eduroam service has been launched in September 2007. The new website is under preparation; the work also includes eduroam user database and the monitoring tools.

Miro reported that eduroam policy and service definition has been approved and the signing process has begun

**Action:** Miro to circulate the eduroam database proposal to get comments.

## **TCG and TNC - Jonas Gyllenhammar (Juniper)**

Jonas explained the difference between TNC and TCG.

TCG (Trusted Computing Group) working group was formed in 2003 to deal with the problem of reducing end-points attacks.

TCG solution for the problem was to create a network access control policy and architecture. The architecture, also known as TNC (Trust Network Connect) is based on a set of non-proprietary specifications, to enable the application and enforcement of security requirements for endpoints connecting to a network.

TNC has been designed to help network administrators to enforce security requirements for endpoints connecting to the corporate network.

TNC architecture is supported by many vendors including Microsoft, Juniper, Nortel, IBM etc.

Jonas acknowledged that TCG is aware of the problems for roaming users and they are trying to address them.

A discussion followed to understand the differences between TCG and NEA (Network Endpoint Assessment) the working group operating within the IETF. NEA aims to define procedures to assess the posture of endpoint devices against the network organization's posture policy.

Jonas said that TCG and NEA are lately communicating in a positive way and there are hopes for a closer collaboration between these two groups.

Some of the attendees asked whether there are TNC use cases available.

Jonas said that there are use-cases for TNC used at the universities, but

currently they are only applied to the employees, as it is quite difficult to control students, who access with different devices from different locations. For more information please see also:

<https://www.trustedcomputinggroup.org/groups/network/>

### **Chargeable User Identity - Tomasz Wolniewicz**

Tomasz presented the problem that they are observing within their universities, namely that users would set a static link to their universities AP from their home. This becomes particularly inconvenient when a user belonging to university A sets a static link to the network of university B. During the TF-mobility list discussion Jochem van Dieten had pointed out RFC 4372 allows using an identifier that relates to a specific user and they are testing this procedure in Poland. The feeling of the group was that providing a unique user identifier would become a necessity in the eduroam service of the future. It was pointed that on the TF-Mobility list or during the next TF-Mobility list a discussion should take place to agree on which attribute to use. Milan suggested using targetedID.

**Action:** Tomasz to report about the results of the tests using RFC 4372.

### **Deploying EAP-TLS based authN – Milan**

Milan proposed a solution to get rid off of the RADIUS hierarchy and use client certificates (EAP-TLS). The reason for implementing TLS is that some devices and system support TLS better than TTLS.

The presentation triggered lot of discussion, as this would imply the set-up of a mechanism to exchange and download the various root CAs used to generate the certificates.

Milan presented the way EAP-TLS is being implemented by CESNET to allow user to log-in with their national federation credentials to request a client cert for eduroam. The validity of the cert is decided by the CA.

**Action:** Milan to report about EAP-TLS implementation.

### **DAMe report - One year since the project started - Sascha Neinert**

Sasha presented the latest developments for DAMe.

The XSupplicant has been changed in order to support an AuthZ token, in order to use eduroam infrastructure to transport also authR attributes. The second phase of DAME is now focusing on SSO, mainly combining eduroam and edugain.

The SAML used for web-based access comes from the network part.

### **RadSec updates – Stefan Winter**

Stefan is doing lots of work to push RadSec within IETF, which includes working on a IETF draft and on recharting an IETF WG to address these issues.

Stefan said that RadSec is already being used, for instance both the ETLR servers are both RadSec enabled and in Luxembourg only RadSec is used. Stefan expects some good results from the coming IETF in March and will report on the progresses.

**Action:** Stefan to report about RadSec developments.

## **Next Meeting**

The next meeting will take place on July 8 in Umeå (Sweden).

## **List of Actions**

**Action:** Dubravko to update the document in order to provide use-cases and to include the comments.

**Action:** Tomasz to report about the results of the tests using RFC 4372.

**Action:** Milan to report about EAP-TLS implementation.

**Action:** Miro to circulate the eduroam database proposal to get comments.

**Action:** Stefan to report about RadSec developments.