

## **TF-Mobility Meeting Minutes**

**1-2 February 2006, Zagreb - Croatia**

The agenda was bashed and the discussion started with the policy document, which was drafted by the JRA5 group. The reason to discuss this document during the TF-Mobility is to make sure that consensus is reached by all eduroam users (not only JRA5). David, who is main author of the document, reported what was discussed during the JRA5 meeting in Cambridge (January 06) and suggested to discuss the whole policy document.

The following was agreed:

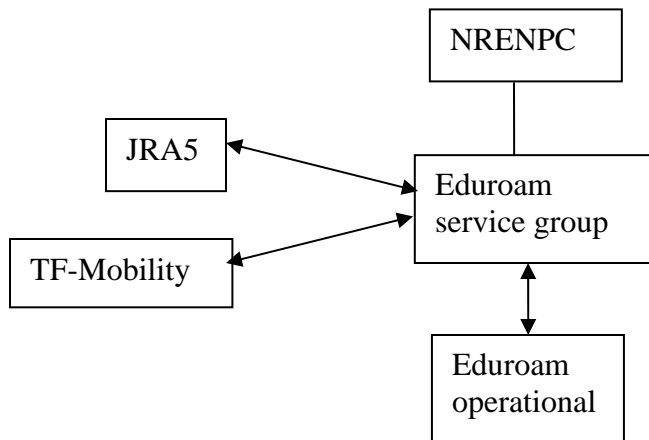
- as general remark: the policy document should be as much as possible technology independent.
- Par 1.1.2 eduroam definition - The definition of eduroam was agreed as: "eduroam provides Internet access for roaming users of research and education networks. The access is based on secure authentication by the home organisation of the user."
- Par 1.1.4 a small change as 'The confederation may peer with other roaming infrastructures'.
- Par 1.1.5 access to eduroam – It was agreed to grant eduroam access to the NRENs constituency.
- Par 1.2.2 eduroam service - One of the issues was whether the NRENPC should appoint the eduroam WG, which will be responsible for the operational development of eduroam. It was agreed that members of eduroam WG be appointed by the eduroam federations.
- Par 1.1.7 - the following phrase was agreed upon concerning the security of the users: 'credential must be preserved and the privacy regulation should be observed'.
- Par 1.2.3 the definition of eduroam operational committee was added

### **Open Policy issues**

Some issues are not addressed in the policy such as:

- how can a member quit the European eduroam confederation?
- policy changes: if changes in the policy occur and some of the members do not agree can these members leave eduroam?
- How are the eduroam members informed about changes in the policy?
- When will the eduroam confederation agreement be in place?
- Mikael Linden pointed out that the policy does not cover liability. Jürgen stated that this is covered by the NRENPC's liabilities.

The relations among the various elements in the eduroam policy, as agreed by the TF-Mobility group are shown in the picture below.



For the explanations of the roles of each of the group, please refer to the updated version of the policy document that will be circulated on the TF-Mobility list by David.

Hansruedi suggested each web site to have the eduroam logo and a link to the eduroam.org and to have this in the policy. This was agreed upon.

**Action:** David to produce a new version of the policy and circulate it for approval

**Action:** David to check with the Danish universities about the possibility to allow secondary schools on board.

**Action:** TERENA to review the last sentence of the eduroam trademark specifications on the eduroam.org.

## New Logo Discussion

The new logo was approved.

**Action:** TERENA to verify the make sure that the new logo is also trademarked.

**Action:** TERENA to update the eduroam web site.

## NRENs Updates

A round table to refer about NRENs activities followed:

**Slovenia:** ARNES has developed and deployed eduroam in a box and so far it has proven to be very successful.

From the statistics it appears that there are 45.000 (eduroam) log entries in a month.

**Switzerland:** SWITCH started a 802.1X trial with some universities. The trial will terminate at the end of March 2006. ETH in Zürich (one of the most important in Switzerland) is interested in joining eduroam, after a redesign they now use an 802.1X infrastructure using Colubris access points and allows for dynamic VLAN assignment.

**Croatia:** CARNet & Srce will have an eduroam.hr website active in a very short time. The majority of dormitories are already eduroam enabled. CARNet has also made an agreement with a commercial provider to allow the academic community to get access. The plan is to connect this with eduroam.

**Sweden:** SUNET is testing eduroam and they plan to join.

**Norway:** UNINETT has joined eduroam and they are performing some tests with one of their universities before starting the deployment. Tests are ongoing to connect eduroam with FEIDE, but there seem to be problems due to the way passwords are stored in FEIDE.

**Czech Republic:** eduroam is running or being prepared in most of the universities in Czech Republic. Research is ongoing on the monitoring area.

**Spain:** A government program started to support installation of new wireless infrastructure in the universities, which will allow for further eduroam deployment.

**Portugal:** In Portugal there are about 150 hotspots, which cover about 75% of the institutions.

**DFN:** The connection of universities to eduroam in Germany is going very slow. At the moment there are 35 institutions connected. There are still some regional networks that use VPN.

**Poland:** Currently only 3 institutions connected.

**Finland:** 200 organisations in the roaming pilot, which is web-based authentication. The plan is to get at least 3 organisation testing 802.1X this year, before starting the deployment.

**Netherlands:** Different roaming activities are ongoing. The first one is to separate the RADIUS infrastructure from eduroam at contract level. The reason for this is that many institutions want to use RADIUS also for different purposes than just eduroam. The other activity is to provide a service that allows users to know where to get eduroam. A big project will start during the year to assess the feasibility of eduroam access beyond the campuses.

**Denmark:** Five institutions have deployed eduroam and in the country eduroam is perceived as a service. A big promotional campaign is under preparation.

**US:** An eduroam test-bed has been set-up. Americans have needs to integrate attributes within eduroam. An interest on using attributes is rising also in Europe and therefore coordination should be encouraged.

## **Deliverables discussion**

Monitoring deliverable: Miro apologised for the delay in this deliverable. Works is ongoing but slower than expected.

eduroam Client: David reported that the tender process that was supposed to take place in UK has been postponed.

Poland and Slovenia provide a customised SecureW2 to help end users configure eduroam.

SSID Deliverable: the deliverable was sent to the list in January 06 and it was approved during the meeting. At the same time it was acknowledged that there is no longer need for the proposed solutions.

## **eduroam-in-a-box (Rok Papez)**

Rok presented the so-called eduroam-in-a-box to support system administrators to configure eduroam. The system (open source), which has a friendly web interface allows for many deployments with the same configuration files.

Rok asked the attendees to test the system and report about the results.

Installing eduroam is not very easy for end-users either, therefore ARNES is working to support end users, expanding eduroam-in-a-box.

## **New technologies tests for eduroam-ng (Klaas Wierenga)**

During the last months new technologies have been tested as an alternative to RADIUS and to allow for a peer-to-peer authentication instead of using the hierarchy of RADIUS servers.

The technologies tested are:

1. RadSec – this has the advantage to use Radius packets format and instead than shared secrets it uses TLS.
2. DNSROAM which combines RadSec with DNS for dynamically locating the peer

The tests, performed between many NRENs, consisted in replacing RADIUS with RadSec/TLS. One scenario was to use a hierarchal model. The use of PKI was solved using different set of certificates according to the peer, which is known in advance. The other option was a meshed top level solution. For some people this solution is an abuse of DNS.

The last test was with a fully mesh solution (DNSROAM), which raised many concerns such as peering belonging to different federations, the use of multiple PKIs, the requirement to open all RADIUS ports (security concerns). For all these reasons, DNSROAM does not seem like the path to follow for now.

Static RADSEC was considered stable enough to be used by majority of testers.

**ACTION:** it was agreed that NRENs that feel like moving to RADSEC should do so. It was also agreed to contact the RADIATOR developers to get better documentation standardize the protocol.

## **PAP-to-EAP-TTLS gateway (Miroslav Milinovic)**

Miro presented the software developed by Srce to convert Radius/PAP packets into radius EAP/TTLS packets. The reason to create a bridge PAP to EAP/TTLS is that the NAS equipment used for the dial-in service in Croatia is not able to support EAP. To secure the users' credentials as soon as possible (after they are provided) a PAP-EAP bridge is used, which makes sure that the users' credential are encrypted before travelling through the RADIUS hierarchy.

It was pointed out that the procedure should not be encouraged, for other purposes (for instance to make web-based redirect secure) as still security issues remain (between the user and the PAP enabled server).

## **Accounting packets**

A discussion took place about the possibility for home institutions to receive the accounting packets of their users wherever they are. The fact that the storage of users' information raises privacy issues is a well known fact, although it a common practice. There was a discussion about obligations from the visited institutions in relation to the log files. The majority agreed that the visited institutions should not send the log file to the user's home institution.

It was agreed to ask Mikael Linden to investigate with the WP29 the privacy regulations with respect to this issue.

Hansruedi will check whether the Swiss law obliges SWITCH to get logs of their users even if they are abroad.

## **Next Meetings**

The next TF-Mobility meeting will take place in Catania on Sunday 14 May, 2006. It was also agreed that the meeting in the fall will take place in October in the week starting on Monday 16.

## **Summary of the actions**

**Action200602-1:** David to produce a new version of the policy and circulate it for approval

**Action200602-2:** David to check with the Danish universities about the possibility to allow secondary schools on board.

**Action200602-3:** TERENA to review the last sentence of the eduroam trademark specifications on the eduroam.org.

**Action200602-3bis:** TERENA to update the eduroam web site.

**Action200602-4:** TERENA to verify the make sure that the new logo is also trademarked.

**Action200602-5:** it was agreed that NRENs that feel like moving to RADSEC should do so. It was also agreed to contact the RADIATOR developers to get better documentation.