07.01.08

Deliverable DS5.1.1: eduroam Service Definition and Implementation Plan

Deliverable DS5.1.1

Contractual Date:	31/10/07
Actual Date:	07/01/08
Contract Number:	511082
Instrument type:	Integrated Infrastructure Initiative (I3)
Activity:	SA5
Work Item:	1
Nature of Deliverable:	R (Report)
Dissemination Level	PU (Public)
Lead Partner	CARNet
Document Code	GN2-07-327v2

Authors: Miroslav Milinović (CARNet/Srce), Juergen Rauschenbach (DFN), Stefan Winter (RESTENA), Licia Florio (TERENA), David Simonsen (UNI-C), Josh Howlett (UKERNA), SA5 and JRA5 group

Abstract

This document describes the eduroam service. It contains a general overview of the service (including its aims, its elements, and security), a description of the service's service elements, users, operation, and service organization as well as a description of the operational requirements required of confederation members. This document should be read in conjunction with the policy document signed by all eduroam confederation members (GN2-07-328)

Table of Contents

Table of Figures

0 Executive Summary

eduroam is a secure international roaming service for members of the European eduroam confederation (a confederation of autonomous roaming services). The European eduroam confederation is based on a set of defined organisational and technical requirements that each member of the confederation must agree to (by signing the eduroam policy (GN2-07-328) and follow.

As part of GEANT2, the European eduroam service is managed by the National Research and Educational Network Policy Committee (NREN PC), which in turn delegates the supervision of the European eduroam service to the SA5 group. In turn, SA5's eduroam Operational Team (OT) carries out the day-to-day operations of eduroam, and runs the eduroam confederation service.

This document describes the eduroam service. It contains:

- A general overview of the service, including its aims, its elements, and security.
- A descriptive breakdown of the service into Service Elements, Users, and Operation.
- A breakdown of the eduroam service organisation.
- A description of the operational requirements required of confederation members.

Note that further details of the service can be found in Deliverable DJ5.1.4 "Inter-NREN Roaming Architecture: Description and Development Items", and Deliverable DJ5.1.5,2: "Inter-NREN Roaming Infrastructure and Service Support Cookbook - Second Edition".

Finally the resources needed for running the European eduroam service are described in Appendix D "Resources".

1 Introduction

eduroam (EDUcation ROAMing) allows users from participating academic institutions secure internet access at any eduroam-enabled institution. The architecture that enables this is based on a number of technologies and agreements, which together provide the eduroam user experience: “open your laptop and be online”.

The basic principle underpinning the security of eduroam is that the authentication of a user is carried out at their home institution using their specific authentication method. The authorisation required to allow access to local network resources is carried out by the visited network.

To provide this facility, the European eduroam service is a confederated service, built hierarchically. At the top level sits the confederation level service, and this primarily provides the confederation infrastructure required to grant network access to all participating members of the eduroam service at any time. This confederation service is built upon the national roaming services, operated by the national roaming operators (NROs) (in most cases NRENs). National roaming services make use of other entities, for example campuses and regional facilities.

A hierarchical system of RADIUS servers is used to transport the authentication request of a user from the visited institution to their home institution, and the authentication response back. Typically, every institution deploys a RADIUS server, which in turn is connected to a local user database. This RADIUS server is connected to a central national RADIUS server, which in turn is connected to a European (or global) RADIUS server.

Because users have usernames in the format “user@realm” (where realm is the institution’s DNS domain name, often of the form institution.tld, where tld is the country code top-level domain), the RADIUS servers can use this information to route the request through the hierarchy until the home institution is reached. Usage of realms in generic top-level-domains (for example terena.org) requires a different handling and MUST be requested via SA5.

Access points or switches use the IEEE 802.1X standard that encompasses the use of the Extensible Authentication Protocol (EAP). Using the appropriate EAP-method, either a secure tunnel is established from the user’s computer to their home institution through which the actual authentication information (username/password etc.) is carried (EAP-TTLS or PEAP), or mutual authentication by public X.509 certificates is used (EAP-TLS). The three authentication methods mentioned before establish a secure TLS tunnel from the end-user device to its home authentication server and are not subject to eavesdropping by intermediate parties.

Currently, RADIUS transports the user's name in an attribute User-Name, which is visible in cleartext. This is masked by using an anonymous user name in this field, but the final vision of eduroam is that no attributes will be transmitted in cleartext.

The confederated eduroam service encompasses all the elements necessary to support the European service. Aside of the confederation infrastructure itself, these elements include:

- Establishing trust between the member federations.
- Monitoring and diagnostic facilities.
- Central data repository providing information about the eduroam service.
- Confederation level user support (i.e. support for member federations).

These elements are described in more detail later in the sections that follow.

2 Service Elements

This section describes the infrastructure elements of the European eduroam service. This includes the technology infrastructure and supporting elements (for example, monitoring and diagnostic facilities, central data repository, eduroam web site and the trouble ticketing system).

2.1 Technology Infrastructure

The confederation infrastructure relies on a distributed set of AAA servers. The current configuration uses RADIUS as the AAA protocol, and is implemented as a hierarchy of RADIUS servers. The RADIUS hierarchy for a national eduroam federation consists of several RADIUS servers located at the various institutions, which are directly or indirectly connected to the top-level national RADIUS proxy server. See Figure 2.1.

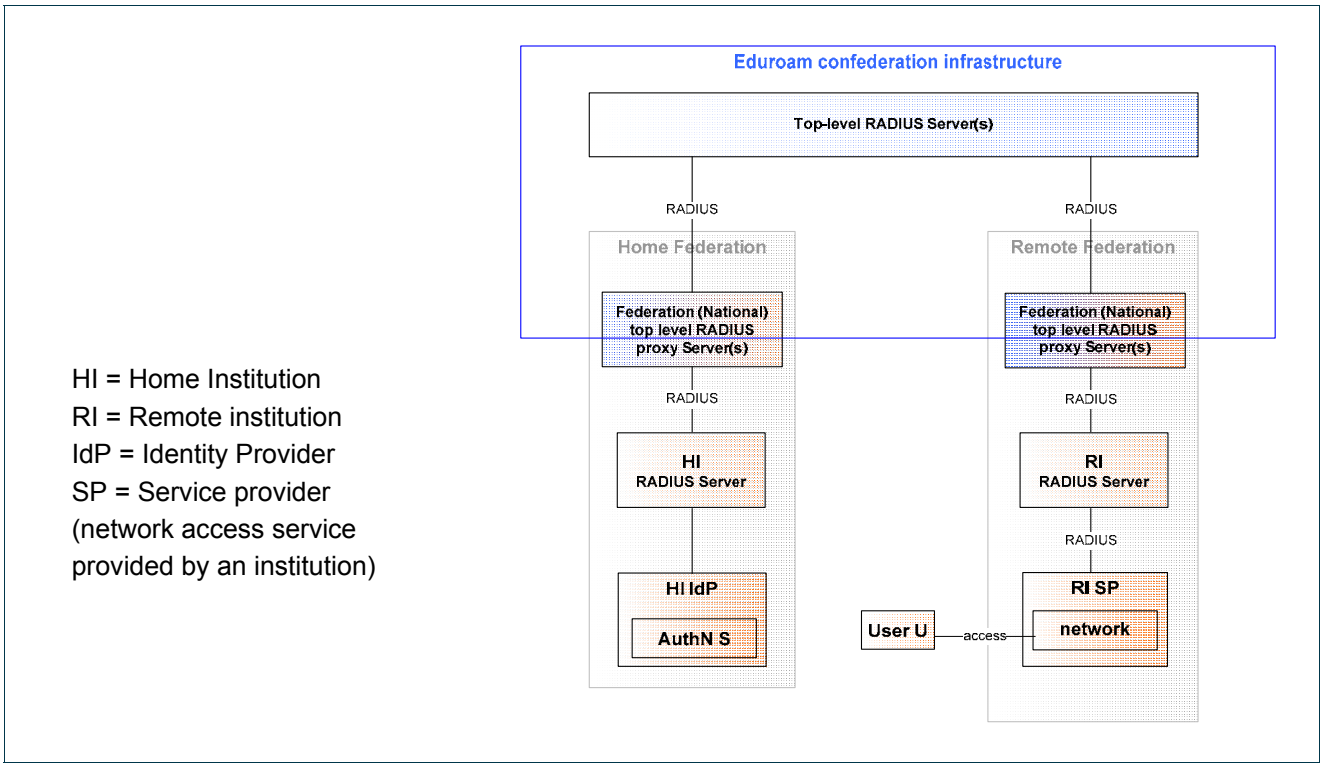

Figure 2.1: Current eduroam confederation structure

The eduroam top-level RADIUS servers interconnect the participating national eduroam federations. They provide the means to find the correct national top-level RADIUS server of a given users' federation, and to transport all information in a secure way. eduroam top-level RADIUS servers are maintained by the OT.

Note: The eduroam service is based on the results of the study reported in DJ5.1.4. These results demonstrate that the 802.1X-based solution provides the most scalable, secure and future-proof solution. Other AAA protocols than RADIUS may be used in the infrastructure at a later stage of deployment.

The elements are described in more detail below:

2.1.1 Top-level RADIUS Server (TLRS)

Currently the confederation top-level RADIUS Servers for the European confederation are located in the Netherlands and Denmark. Each server has a list of connected country domains (.nl, .dk, .hr, .de etc.) serving the appropriate NRENs. They accept requests for federation domains for which they are authoritative, and subsequently forward them to the associated RADIUS server for that federation (and transport the result of the authentication request back). Requests for federation domains they are not responsible for are forwarded to the proper federation TLRS.

As well as European NRENs, there are eduroam participants in other parts of the world (.au, .jp, .cn etc). These realms are also handled by the TLRS in Europe, though these NRENs are not members of the European confederation.

2.1.2 Federation level RADIUS Server (FLRS)

A federation RADIUS server has a list of connected institutional servers and the associated realm. It receives requests from the confederation servers and institutions it is connected to, and forwards them to the proper institution (or in case of a request for a confederation destination, to a confederation server).

2.1.3 Home and Remote Institutional RADIUS

The Institutional RADIUS server is responsible for authenticating its own users (at home or remotely when visiting another institution) by checking the credentials against a local identity management system. It is also responsible for forwarding requests from visiting users to the respective federation RADIUS server. Upon proper authentication of a user the local institutional RADIUS server may assign a VLAN to the user.

Note that the institutional RADIUS server is the most complex of all. Whereas the other RADIUS servers merely proxy requests, the institutional server also needs to handle the requests, and therefore needs to be able to terminate EAP requests and perform identity management system lookups.

The Identity Management System contains information on end users (for example, usernames and passwords). They must be kept up-to-date by the institution responsible.

2.1.4 network access elements

eduroam is not dependant on access technologies. Users of eduroam can access the service either by wireless (the main focus of eduroam) or wired connection.

However, the active network equipment required for each method is different: for a wireless infrastructure, access points are needed, while for a wired infrastructure switches are required

In both cases specific supplicant software is required on the user's machine.

The elements mentioned above are described below.

2.1.4.1 *Supplicants*

A supplicant is software that uses the 802.1X protocol to send authentication request information, using EAP. Supplicant software is often built into the Operating System, but can also be a separate program.

In order to use the eduroam service and access the network, users must configure the supplicant software on their machine. This configuration is valid all over the eduroam confederation. See Deliverable DJ5.1.5,2: "Inter-NREN Roaming Infrastructure and Service Support Cookbook - Second Edition" for information on supplicants and their configuration.

2.1.4.2 *Access Points*

Access Points are required for wireless access only.

Access Points need to be 802.1X capable. They must be able to forward access requests coming from a supplicant to the institutional RADIUS server, to give network access upon proper authentication, and to possibly assign users to specific VLANs based on information received from the RADIUS server. Furthermore Access Points exchange keying material (initialisation vectors, public and session keys, and so on) with client systems to prevent session hijacking. See 2 "Service Elements".

2.1.4.3 *Switches*

Switches are used for wired access only.

Wired infrastructures can be configured to provision 802.1X (and therefore eduroam). This means that eduroam users can access the network through wired technology, but to do this the switches that are used to connect end users' computers need to be 802.1X capable and enabled on the ports that are to be used for eduroam access.

These switches need to be able to forward access requests coming from a supplicant to the institutional RADIUS server, to grant network access upon proper authentication and to possibly assign users to specific VLANs based on information received from the RADIUS server.

2.2 Supporting infrastructure

2.2.1 Monitoring and diagnostics

The basic purpose of the eduroam monitoring is to test the proxy forwarding functionality of the top level (national federation) eduroam confederation proxy server and report the results of the test, both as a "weather" map and as graphs showing the response time behaviour.

The tests (authentication requests) are generated by a client outside of the monitored top level domain. This client is maintained by the Operational Team (OT). The responses are generated by an IdP RADIUS server. This IdP server can be located at the same site as the monitoring client, or at the site of the top level proxy under monitoring.

The monitoring structure can be seen in Figure 2.2:

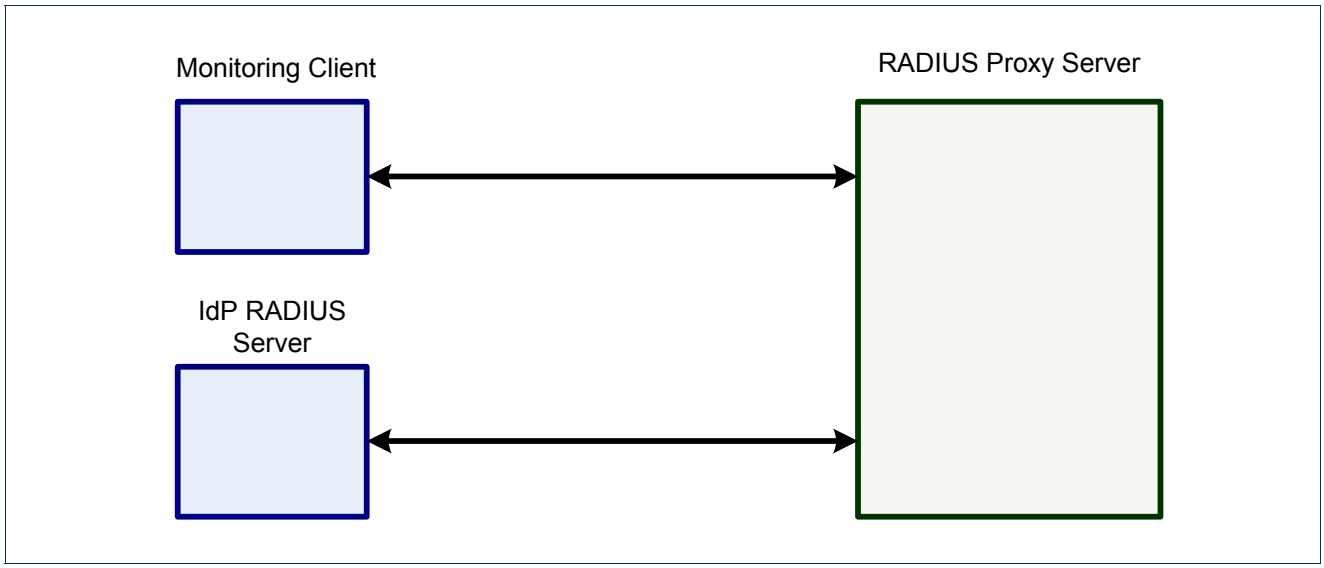

Figure 2.2: eduroam Monitoring

Monitoring components are:

- Monitoring client: This is a RADIUS client capable of sending various types of RADIUS request (for example PAP and EAP).
- RADIUS Proxy Server: This is a monitored server.

- IdP RADIUS Server: This is the server that issues the response, thus acting as loop-back server. Its function is to close the tunnel and create standard and specified responses. This function might be realised on the monitored server (RADIUS proxy server).

Further development of the monitoring facilities will be oriented towards testing real-user experience in real use case scenarios, and towards providing diagnostic tools.

2.2.2 eduroam Web site

The eduroam web site will be available at http://www.eduroam.org. It will be run and maintained by the OT in conjunction with the GÉANT2 PR team.

The site is still under development, and its final content will depend upon the requirements of users. The current premise is that the home page will be the central information point for eduroam users. Below that, the site will also have private areas to support the operational side of eduroam. One example is the provision of a dedicated area of the website to be used to gather information from member NROs (for example contact information, service coverage, usage statistics, and number of eligible and active users).

The eduroam web site will also offer usage statistics and monitoring information on the eduroam infrastructure.

NRO representatives will be granted an account on the eduroam private area in order to upload the information they are requested to provide.

The OT will support new eduroam members accessing the eduroam website, especially for accessing protected areas.

2.2.3 eduroam database

The information stored in the eduroam database will be collected with the help from NROs and includes:

- NRO representatives and respective contacts.
- Local-institutions (both SP and IdP) official contacts.
- Information about eduroam hot spots (SP location, technical info).
- Monitoring information.
- Information about the usage of the service.

There will be limited access to the database through the eduroam Web site.

2.2.4 Trouble ticketing system (TTS)

The OT will install and maintain a TTS in order to document its work, and to allow NROs (as well as local institution administrators) to report any irregularities in the eduroam service.

2.2.5 Mailing lists

Two mailing lists will be provided:

- SA5 group list.
- eduroam Operational Team (OT) list.

Both lists will be used for day-to-day communication as well as official broadcasts.

3 Users

This section describes the identified user categories and the way the eduroam service elements are mapped to these categories. A summary of this mapping is provided in section 3.3.

3.1 End Users

End users are the individuals who use eduroam technology to access the network, whether at their home institution or whilst visiting other sites. Broadly speaking there are two types of end-users: the technology aware and the technology unaware. The former ("power users") will understand documentation on eduroam and will understand how to configure their laptop to use eduroam. The latter ("consumers") require more assistance. Currently, in terms of the service portfolio, no distinction is made between these two categories and they are addressed for now in the same way. The table in section 3.3 shows that end users have access to the eduroam web-site, database for accessing general information and access to basic monitoring tools. It is recognised that over time a more refined distinction between the end-user categories should be made with consequent refinement of the service portfolio mapping.

3.2 Administrative personnel

Administrative Personnel refers are those users who are running parts of the eduroam infrastructure that are not handled directly by the OT; namely, the federation-layer and the institution-layer.

This subdivides this user group into: federation-level personnel and institution-level personnel.

3.2.1 Federation-level personnel

- Staff for server operation: This user group would probably contain a small number of staff per participating federation. Since the eduroam prototype has already been running for a significant amount of time, it is expected that this group already has a high skill level regarding operating a RADIUS server.
- Staff for trouble ticketing and handling user support: The eduroam trouble-ticketing system will have a federated structure. This means that at the federation level, there will be staff handling trouble tickets themselves, escalating tickets to the operational team, or delegating them to the affected institutions in

their constituency. Since the eduroam prototype did not include trouble ticket management, it would be useful to provide supporting material on how to work with the TTS.

3.2.2 Institution-level personnel

- Staff for service operation: Service operation on an institutional level differs significantly from that of operating a federation server. The staff within institutions need to configure, monitor and troubleshoot equipment that performs authentication with an identity management system. Given that identity management systems are quite diverse, it is impossible for SA5 to provide exhaustive documentation on how to configure each and every backend system.
- Staff for trouble ticketing and handling user support: This group represents local staff that handles day-by-day user support. They should be supported by the respective NRO. SA5 will provide basic materials in order to help NROs, and provide consistent and uniform service to the end users.

3.3 eduroam User Summary

The table below cross-references user groups with the eduroam service elements that they would be expected to use:

Service elements	User group		
	End user	Inst. Level personnel	Federation-level personnel
Basic monitoring facilities	Yes	Yes	Yes
Full monitoring and diagnostics facilities	No	Yes (limited to the information regarding the respective inst.)	Yes
Public access to the eduroam web site	Yes	Yes	Yes
Access to the internal eduroam website	No	Yes (limited to the information regarding the respective inst.)	Yes
Public access to the eduroam database	Yes	Yes	Yes
Access to the all information in the eduroam database	No	Yes ((limited to the information regarding the respective inst.)	Yes
TTS	No	Yes	Yes
SA5/OT Mailing lists	No	No	Yes
Support form OT	No	No	Yes

Table 3.1: Service Elements

4 Service Organisation

As part of the GÉANT2 Project, the European eduroam service is managed by the National Research and Educational Network Policy Committee (NREN PC), which in turn delegates the supervision of the European eduroam service to the SA5 group.

The SA5 group consists of representatives of all federations connected to the eduroam confederation. Official members of the SA5 group are the representatives of those roaming federations that are GN2 project partners and have signed the eduroam policy. SA5 may also accept unofficial members, which are representatives of other roaming federations that liaise with the European eduroam service.

Day-to-day operations are carried out by the eduroam Operational Team (OT). It consists of SA5 members (as of December 2007 the members are Srce, Surfnet, UNI-C, and TERENA), and is approved by the SA5 group and the NREN PC. The SA5 leader manages and oversees the work of the OT.

The eduroam service model is illustrated in Figure 4.1:

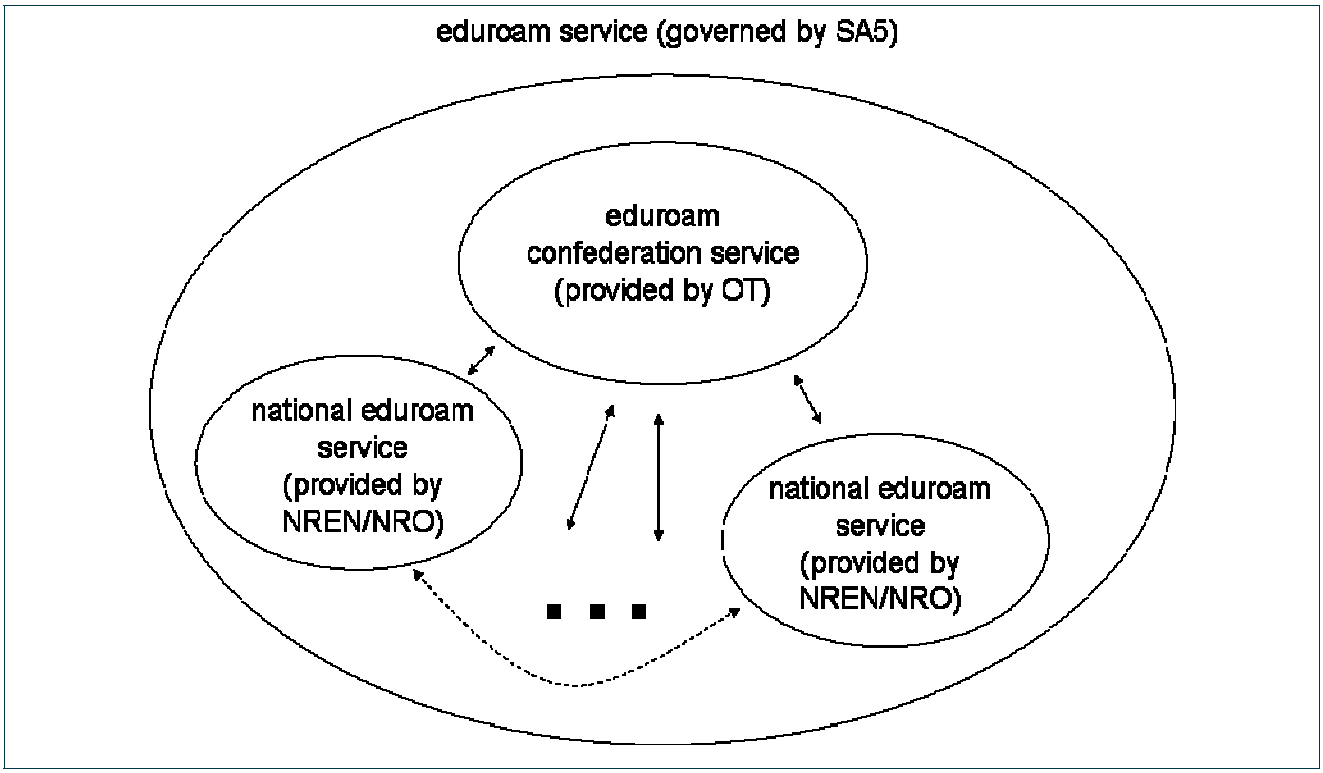

Figure 4.1: eduroam service model

4.1 Roles and responsibilities

The overall roles and responsibilities of the NREN Policy Committee, the GÉANT2 Executive Committee and DANTE as the Coordinator of the GÉANT2/GN2 project are defined in the Consortium Agreement (GN2-06-221/GEA-00-073v4) and the Rules of Procedure/Special Resolution establishing the Exec (GEA-04-062v13, article 3.3). The Executive Committee acts within the powers delegated to it by the NREN Policy Committee.

In addition to the above references, this section describes the specific roles and responsibilities of the:

- NREN-PC.
- eduroam confederation members (NROs).
- SA5 group.
- OT.

4.1.1 GÉANT2 Executive Committee

The Policy Committee delegates management of the GÉANT2 Project to the GÉANT2 Executive Committee. This is described in Article 3.3 of the Rules of Procedure/Special Resolution establishing the Exec (GEA-04-062v13).

4.1.2 DANTE

DANTE acts as overall project coordinator of GÉANT2. DANTE has overall responsibility for relationships with third parties and for liaison between the Parties of the Project.

4.1.3 NREN PC

The NRENPC has established a GÉANT2 project management that gives a management role for the GN2 project as a whole to the GÉANT2 Executive and DANTE. The SA5 role is, in general terms, embedded in this structure.

NREN PC coordinates the cooperation of the European NRENs in the GÉANT2 project and approves the budget plans. The NREN PC appoints the supervision of the European eduroam service to SA5 group.

NREN PC will approve basic SA5 items (for example, SA5 leader), the OT and eduroam policy proposed by the SA5 group. NREN PC also handles the disputes that cannot be resolved by the SA5 group.

4.1.4 eduroam confederation members (NROs)

NROs should appoint at least one representative to the SA5 group.

The tasks of eduroam confederation members are:

- Participation in the work of SA5.
- Assure the adherence to the eduroam policy (GN2-07-328 “eduroam policy - for signing”).
- Provisioning of necessary support and information to the OT.
- Provisioning of the support to the respective roaming users.

4.1.5 SA5 group

The SA5 group manages the eduroam service (note that research items stay in JRA5). It is the responsibility of SA5 to manage the work of the OT and provide it with necessary input.

The tasks of the SA5 group are:

- Supervision of the operational team.
- Formulating recommendations on monitoring and diagnostic tools and supporting scripts that should be used in providing service
- Further policy development (in coordination with JRA5/TF Mobility).
- Integration of further research results from JRA5/TF Mobility.
- Formulating recommendations on application of trust means.

- Dissemination work (providing material for web pages, enhancement of the confederation visibility, including the provision of promotional material) in coordination with NA2.
- Evaluation of usage related data and publishing of corresponding graphs and statistics.
- Improvement of eduroam service definition and procedures.
- Participation in organisation of training events for the operational personnel (wherein SA5 provides the content and NA8 assists in organisational matters).
- Providing support for the confederation members (provision of federation web presentation in English and with appropriate access information, exchange of technical knowledge, motivating events etc).
- Liaison on technical matters with other non-GÉANT2 or non-European roaming (con-)federations.

4.1.6 OT

The OT handles day-to-day operations. It is responsible for the smooth operation of the confederation service.

The tasks of OT are:

- Operating the eduroam confederation infrastructure.
- Monitoring the eduroam confederation.
- Handling fault resolution procedures.
- Providing support for new member federations.
- Coordination of trust means.
- Gathering of statistics on usage and error reports.
- Development of diagnostic tools and scripts support.
- Incident handling according to the defined and agreed procedures.
- Maintenance of the central repository (data base) providing information about the eduroam service.
- Maintenance of the eduroam service web pages and trouble ticketing system.

4.1.7 Service level agreement

The OT is responsible for running the confederation service. Therefore, the OT maintains:

- The confederation infrastructure (explained in section 2.1).
- Monitoring and diagnostic facilities.
- eduroam data base.
- eduroam web site.
- Confederation trouble ticketing system.

The goal for the availability of these services is in the range of 98.9%.

The availability of each of the services listed above will be measured as the ratio between the accomplished and theoretically possible uptime of the respective servers. Proper monitoring tools will be used for that purpose and the results will be kept by the OT.

OT must keep all applicable service logs for a minimum period of six months.

5 Service Operation

This section defines operational procedures for the eduroam service.

The OT and SA5 will use the following tools for communication:

- Mailing lists (provided by DANTE).
- Trouble ticketing system (TTS).
- Internal region of the eduroam web site.
- Face to face meetings and video conferences.

5.1 User Support Processes

The processes for delivering user support are described in this section. However, please note that end user support to the end users is delivered by the local institutions' personnel.

eduroam is a comparatively new development and a new service. Therefore, we have limited experience of what problems eduroam users may experience as they move around supporting institutions, using network resources in different ways. For that reason, it is impossible to present a definitive description of all user support scenarios that may be encountered.

However, the following sections describe possible support scenarios based on current knowledge and experience. As experience grows, these scenarios and solutions will be expanded.

The eduroam service organisation model assumes that the home institution and respective NRO will provide the user with the information and knowledge to use the eduroam service. It is up to the home institution to provide the necessary user support to the roaming user.

Furthermore the NROs and their member institutions are encouraged to provide user support to the visiting users regarding the use of eduroam service.

The OT primarily provides the support to NROs, but also disseminates information and tools that can be used by the local institutions' administrators and end users.

5.1.1 Support for End Users

End users may roam inside their home federation or across its boundaries. If an end user roams inside their home federation, local user support rules are applied.

If a user roams across the boundaries of their home federation, they should contact their home institution's personnel in order to get necessary assistance or report an incident.

In case more information is needed or some action in the visited federation has to be performed, the visited federation personnel are contacted by the user's home institution's personnel.

If needed, respective federation-level personnel are contacted along with the OT. Still, end users should contact only the institution-level personnel.

NROs and their member institutions are encouraged to provide direct user support to the visiting users.

5.1.2 Administrative personnel

- Federation-level personnel:
  - Escalate problems to the OT whenever the problem includes the confederation service or tackles the basic eduroam technology used
  - Contact other involved federation directly, but must also inform the OT.
- Institution-level personnel:
  - Escalate problems to the federation-level personnel whenever they need assistance.
  - Contact the OT whenever the problem includes the confederation service, but must also inform federation-level personnel.

5.1.3 Problem escalation scenarios

Given the current experience with the eduroam environment, we foresee the following scenarios for user support. These scenarios will be further developed as we gain more operational experience. As experience grows, the support service will adapt to match the new requirements.

5.1.3.1 *Problem escalation involving user and institution-level personnel*

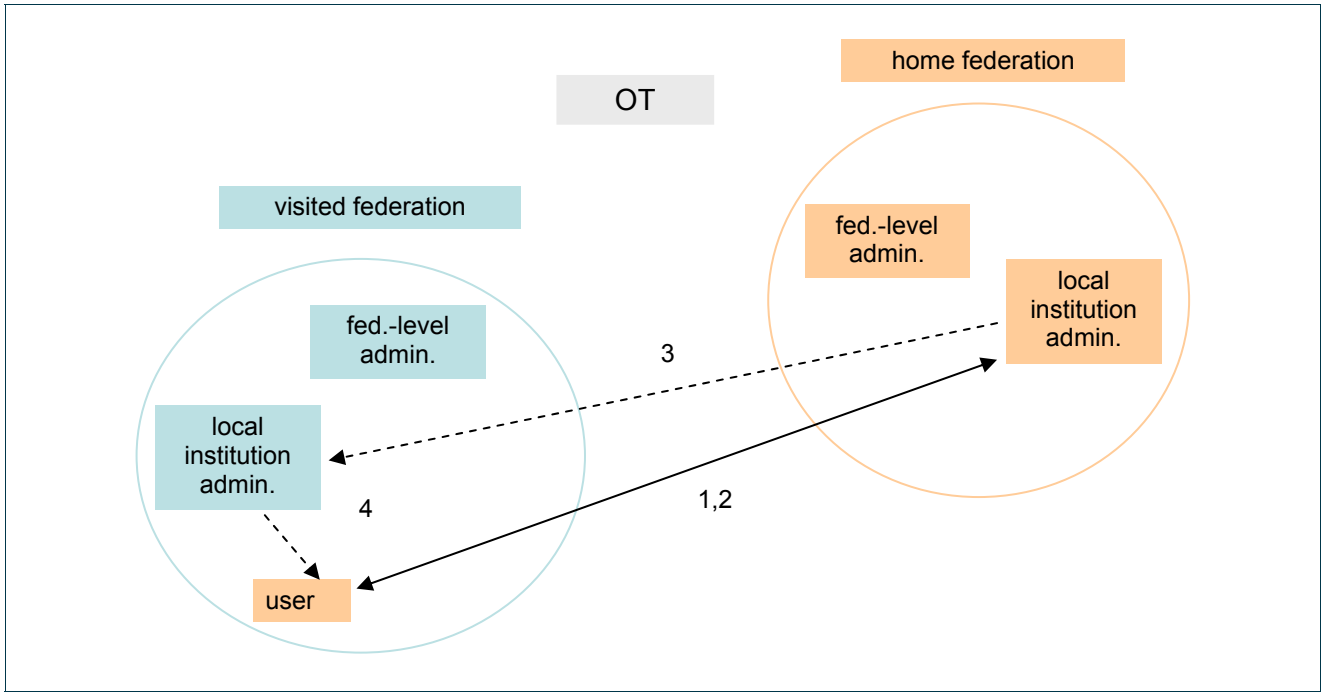

Figure 5.1: Problem escalation scenario, user and institution personnel

In this scenario, a user has a problem accessing the network while using eduroam service outside their home federation. The steps the user might follow are:

1. User calls their home institution and asks for help from local administrative personnel.
2. Local administrative personnel at the user's home institution will check the validity of the user's credentials and help in setting up the end user's machine. They should also check if their system receives proper authentication requests from the visited site via the respective part of the eduroam infrastructure. If they discover problems with the user's credentials or with the setup of his machine, they should provide necessary help to the end user.
3. If local administrative personnel at the user's home institution discover problems receiving a proper authentication request from the visited site, they should contact local administrative personnel at the visited institution to fix the problem. Local administrative personnel at the visited institution should provide all necessary information.
4. If needed, local administrative personnel at the visited institution should inform the visiting user how to fix the problem.

5.1.3.2 *Problem escalation involving user, institution and federal-level personnel*

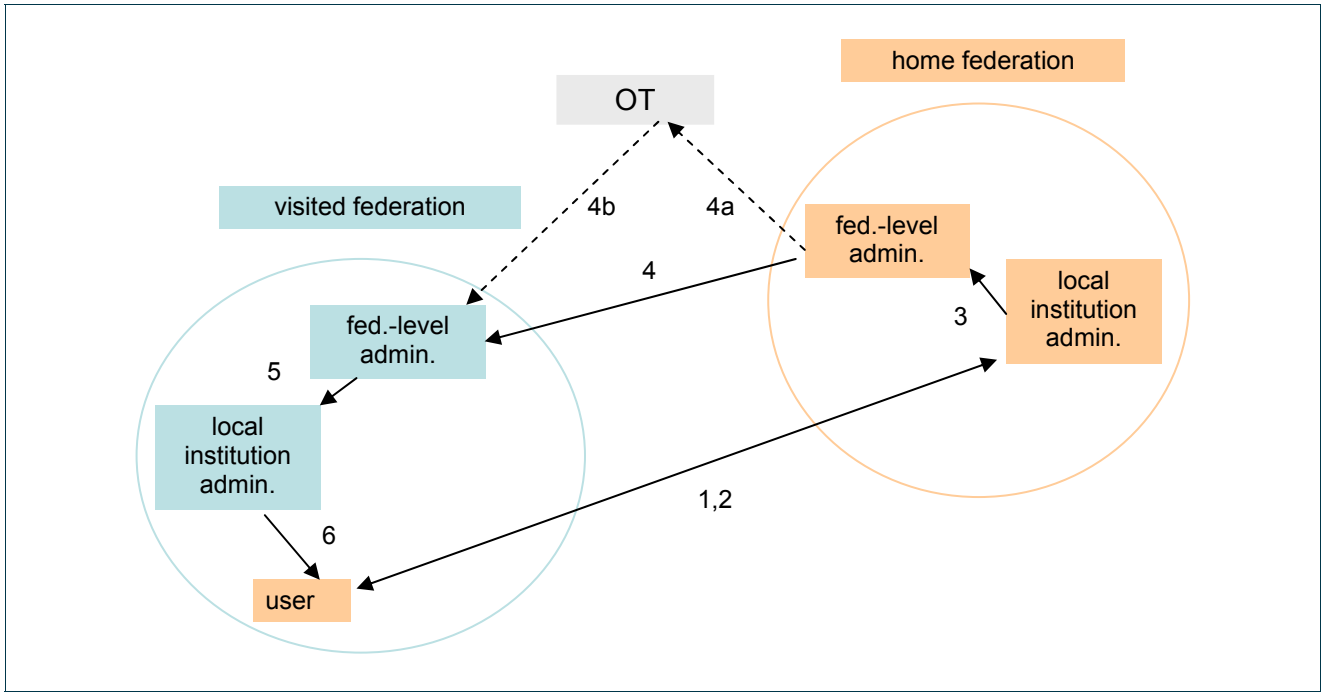

Figure 5.2: Problem escalation scenario, user, institution and federal-level personnel

In this scenario, the user has a problem accessing the network while using the eduroam service outside of their home federation, but the problem needs to be escalated to federal-level:

1. The user must call their home institution and ask for help from local administrative personnel.
2. Local administrative personnel at the user's home institution will check the validity of the user's credentials and help in setting up the end user's machine. They should also check if their system receives a proper authentication request from the visited site via the respective part of the eduroam infrastructure. If they discover problems with the user's credentials or with the setup of the user's machine, they should provide necessary help to the end user.
3. If local administrative personnel at the user's home institution discover the problem is in receiving authentication requests from the visited site and they can not resolve the problem by contacting local administrative personnel at the visited institution, they should contact administrative personnel of their federation.
4. End user's federation administrative personnel should carry out further checks, and if need be contact the visited federation administrative personnel. Visited federation administrative personnel should provide necessary information in order to resolve the problem. If needed (steps 4a and 4b in Figure 5.2) OT is involved in resolving problem. OT will then make sure that the proper authentication requests can be sent from one federation to the other using the confederation infrastructure.
5. Visited federation administrative personnel should contact the visited institution's administrative personnel in order to resolve the problem and check if the proper authentication requests are sent as required.
6. Local administrative personnel at visited institution should inform the visiting user that the problem has been fixed.

5.2 Maintenance procedures

5.2.1 Scheduled maintenance

Scheduled maintenance of top level RADIUS servers (TLRs), as well as the other servers and services, is under the control of the OT, and must be announced seven (7) days in advance through the SA5 mailing list. Scheduled maintenance should be scheduled in the period: Tuesday to Thursday 6:00 – 8:00 CET. A ticket on the TTS should be opened by the respective OT member and closed with a short comment on the performed action.

Scheduled maintenance of top level RADIUS servers (TLRs) must be planned so it does not break the service.

Scheduled maintenance work performed by the NRO inside the respective federation should be announced two (2) days in advance through the SA5 mailing list. A ticket on TTS should be opened by the respective NRO representative and closed with a short comment on performed action.

5.2.2 Unscheduled maintenance

Unscheduled maintenance consists of maintenance work that cannot be planned in advance, usually performed to avoid security incident or service malfunction.

Unscheduled maintenance of top level RADIUS servers (TLRs), as well as the other servers and services under control of the OT, must be announced as early as possible (the preferred period is 24 working hours in advance) through the SA5 mailing list. A ticket on TTS should be opened by the respective OT member and closed with a short comment on the performed action.

Unscheduled maintenance work performed by the NRO inside the respective federation should be announced as early as possible (the preferred period is 24 working hours in advance) through the SA5 mailing list. A ticket on the TTS should be opened by the respective NRO representative and closed with a short comment on the performed action.

5.3 Security incidents

Ideally the generic security incidents handling procedure valid for GÉANT2 project has to be followed. As that procedure is not operational yet we hereby define a simple procedure that will be used in the meantime.

Whenever necessary and appropriate, incidents should be handled by the respective CERT(s). In addition to that, some further actions (explained below) must be taken:

In case of a security incident caused by an end user, the affected institution must inform its NRO. The NRO will then inform the end user's home federation through their respective NRO official contact in SA5.

NROs should regularly report to the OT about the number and type of these incidents. No further details, especially information that could violate and end user's privacy, should be communicated to the OT.

In the case of any security incidents that affect the eduroam confederation infrastructure, the OT should start resolving the incident not later than two (2) working hours after the incident has been discovered or reported by an eduroam user or member. Basic information about the incident must be sent to the SA5 list. NROs affected with the incident must help in resolving the problem. A ticket at TTS should be opened. The ticket should be closed with a short comment when the incident is resolved.

In case of cross-confederation incidents, the OT must be involved in the resolution process.

5.4 Policy violation

In the case of a severe policy violation by a federation, the OT will react in the following way, including an escalation to SA5 if appropriate (which might result in further escalation to the NREN PC), depending on the level of violation:

- Issue a notice on the SA5 list of the policy breach and initiate an evaluation process not later than two (2) working hours after the violation has been discovered or reported by an eduroam user or a member.
- Propose a temporary quarantine period (the length of the period as well as the exact measures are case by case dependent)
- Propose (through SA5) to the NREN PC a disqualification of the federation from the confederation.
- Act upon the NREN PC decision and announce membership termination with grievance process.

All incidents that affect the eduroam confederation service, as well as all severe cases of policy violation, shall be presented as a part of regular OT service reports.

5.5 Malfunction

Malfunction of the top level RADIUS servers (TLRs) as well as the other servers and services under control of the OT must be reported to the SA5 mailing list. The OT should start resolving the problem not later than two (2) working hours after the malfunction has been discovered or reported by an eduroam user or a member. A ticket on the TTS should be opened by the respective OT member and closed with a short comment on the performed action.

Malfunction in a member federation should be announced through the SA5 mailing list. A ticket on the TTS should be opened by the respective NRO representative and closed with a short comment on the performed action.

5.5.1 RADIUS Attribute monitoring

The existence of VLAN assignment attributes in authentication responses is almost always a sign of a misconfiguration on the sending (identity provider) side. It can be the source of hard to trace problems at the service provider side and ultimately lead to a complete denial of service (a service malfunction) to the affected end user.

However, it cannot be completely ruled out that a given pair of identity and service provider have an agreement about common VLAN tags. This makes it imperative that VLAN attributes are not filtered automatically on any level of the infrastructure.

To minimise possible malfunctions due to VLAN attributes, the OT monitors packets en route for the existence of VLAN tagging attributes, namely

- Tunnel-Type.
- Tunnel-Medium-Type.
- Tunnel-Private-Group-ID.

The OT notifies the federation from where these packets originate. Participating federations are encouraged to do the same, and to investigate whether the sender is sending these attributes inadvertently or not, and then take appropriate action. A ticket on the TTS is used to communicate these cases from the OT to participating federations.

5.6 Handling Membership

National roaming federations can join the European eduroam confederation only if the NRO (on behalf of the national roaming federation) accepts and signs the European eduroam policy, thus committing to provide the eduroam service inside its federation and contribute to the European eduroam service.

If the OT, on request of the prospective member, confirms that the federation adheres to the Policy, the NREN PC may approve the membership of the federation.

If an institution belonging to the NROs constituency cannot be routed through the NRO's servers for any technical reason, the NRO may request to SA5 that the respective institution is added to the TLRS instead. Upon such a request by the respective federation, SA5 asks the OT to check the technical reasons and, if justified, approves the request. OT shall then modify configuration on TLRSs and report back on the execution of the configuration change.

The NREN PC approves roaming with other confederations upon the proposal from SA5.

SA5 may temporarily establish peering connection in relation to the international liaisons with other roaming confederations or federations, for development and testing purposes. SA5 must inform the NREN PC prior to this action.

Whenever peering with other confederations is set-up, SA5 should establish the same security conditions as those governing the European eduroam confederation.

Any member of the European eduroam confederation can at any time leave the confederation by giving three months' notice of their intention to leave. This notice period is required to ensure that all the resultant practicalities of the member leaving can be taken care of in a timely manner (updating web sites, top level servers, user notification, and so on.)

In the case of severe violation of the eduroam policies, the NREN PC may exclude a member from any further participation in the eduroam confederation.

The list of members is publicly available on the eduroam web site. Changes in membership are announced using the SA5 list.

5.7 Service Reports

The OT prepares the eduroam service report every six (6) months.

The report should provide information on:

- Number of member federations.
- Estimated coverage inside each member federation.
- Number of successful international roaming sessions.
- Number of successful roaming sessions inside the member federations.
- Number of security incidents and malfunctions.
- Report on maintenance activities.
- Confederation service up-time.
- Data collected by the monitoring system.
- Service improvements.

NROs must provide the respective data to the OT.

6 Requirements on confederation members

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" used in this chapter are to be interpreted as described in RFC 2119:

6.1 Policy

The eduroam policy enables the establishment of the eduroam confederation by formalising the organisational and technical requirements.

The Policy MUST be signed by an NREN and the NRO (when the national roaming service is not maintained by the NREN). By signing the policy, NRO and NREN commit to offer the eduroam service inside their federation in line with the eduroam policy.

This Policy is also to be signed by DANTE on behalf of consortium..

Violation of the Policy MUST be reported to the OT and MUST be presented to the SA5 group and escalated to the NREN PC in serious cases.

6.2 Operational requirements for confederation members

6.2.1 General requirements for confederation members

Each federation joining the eduroam confederation MUST:

- Establish the necessary infrastructure for eduroam, and ensure that it is maintained according to the eduroam service requirements and best practices.
- Establish user support service for its end users as explained in 5.1 “User Support” on page 17.
- Participate in the work of the SA5 group.
- Provide the following information to the OT and SA5 group:

- Email and telephone details of a designated technical contact that can be reached during working hours. The contact can be either a named individual or an organisational unit. Arrangements MUST be made to cover for absence owing to such things as illness and holidays.
- Information about their connected service providers:
  - Name of the connected service provider.
  - Geographical position of cohesive hotspot areas of the service provider.

- Act as the eduroam authority towards its federation participants, ensuring that:
  - Its identity providers exercise proper user management and only authenticate and authorise eduroam-eligible users.
  - Both their identity providers and their service providers implement the security requirements of the eduroam service policy.
- Establish and maintain a website including information with respect to the participating institutions as well as practical information on how to use eduroam. The web page MUST be available in English.

In addition to the requirements above, the following set of commitments is RECOMMENDED:

- The website mentioned should also be accessible in a local language.
- The website should be found at http://www.eduroam.org.
- An extended set of information about the connected service providers should be communicated to the SA:
  - Network name (SSID).
  - An indication whether or not the network name is broadcasted.
  - The levels of in-air data encryption that are supported.
  - A list of blocked ports.

6.2.2 eduroam security requirements

The basic security principle that governs the eduroam infrastructure is:

The security of the user credentials MUST be preserved when travelling through the infrastructure, and all partners providing the service MUST observe privacy regulations.

Relevant technical details are listed in the next section.

The following requirements apply:

All eduroam participants (OT, confederation members, connected institutions in federations) MUST:

- Always provide trustworthy and secure transport of all private authentication credentials (i.e. passwords) that are traversing the eduroam infrastructure.
- Ensure that user credentials stay securely encrypted end-to-end between the user's personal device and the identity provider (home institution) when traversing the eduroam infrastructure. A rationale for this requirement can be found in Appendix A.

- Ensure that eduroam servers and services are maintained according to the specified best practices for server build, configuration and security, with the purpose of maintaining a generally high level of security, and thereby trust in the eduroam confederation.

An additional task for confederation members is to ensure that the participating institutions are fully aware of their responsibility to establish an appropriate level of security.

The OT guarantees that the necessary infrastructure to run the confederation services is operational and maintained according to server build, configuration and security best practices. The OT also ensures that it will start resolving reported incidents concerning the eduroam confederation not later than two (2) working hours after the incident has been discovered. All such incidents will be logged, aggregated and presented to the eduroam service group and to the NREN PC.

6.3 Technical requirements for confederation members

6.3.1 Relevant specifications

All the components in eduroam need to have, or provision, access to the internet. Therefore, in general the equipment needs to provide all the functionalities for standard internet access (for example an IP stack, optional VLANs, and so on). In addition to the general networking requirements, eduroam makes use of a number of protocols for user authentication. These authentication-specific requirements are listed below. Details regarding the extent of usage of these specifications are also given.

Conformance, in whole or in part, to the following specifications is **required** for eduroam equipment.

- AAA Servers:
  - RFC2865 (RADIUS).
  - RFC3580 (EAP over RADIUS).
  - RFC4282 (User name format).
  - At least one EAP payload protocol capable of mutual authentication.
- Network Access Servers:
  - RFC2865 (RADIUS).
  - RFC3580 (EAP over RADIUS).
  - IEEE 802.1X.
- User devices:
  - IEEE 802.1X.
  - At least one 802.1X payload protocol capable of mutual authentication.

The following specifications are optional, but recommended:

- AAA Servers:
  - RFC2866 (RADIUS Accounting).
  - RadSec (RADIUS over TCP and TLS).

- RFC3588 (Diameter Base Protocol).
- Network Access Servers:
  - RFC2866 (RADIUS Accounting).
  - RadSec (RADIUS over TCP and TLS).
  - RFC4005 (Diameter NAS Application).
  - RFC4072 (Diameter EAP Application).
- Confederation member level AAA servers:
  - AAA proxies MUST supportRFC2865 (RADIUS) and RFC2866 (RADIUS Accounting).
  - All relevant logs MUST be created with synchronisation to a reliable time source (GPS or in its absence NTP).
  - Confederation members' AAA proxy servers MUST be reachable from the confederation AAA proxy servers via RADIUS for authentication and accounting. They MAY additionally be reachable using other AAA protocols. The ports under which the servers are reachable are to be negotiated with the Operational Team. They default to UDP/1812 (RADIUS), UDP/1813(RADIUS-ACCT), TCP/2083 (RadSec), TCP/3868 and SCTP/3868 (Diameter).
  - Confederation members' AAA proxy servers MUST respond to ICMP Echo Requests sent by the confederation infrastructure and confederation monitoring service.
  - Confederation members MUST ensure that logs are kept of all eduroam authentication and accounting requests exchanged; the following information SHOULD be recorded. The minimum log retention time is six months, unless national regulations require otherwise. A rationale for logging this data is provided in Appendix B.
    - The time the authentication or accounting request was exchanged.
    - The value of the user name attribute in the request ('outer EAP-identity').
    - The value of the Calling-Station-Id attribute in authentication requests.
    - The value of the accounting session ID.
    - The value of the request's accounting status type.
  - Confederation members SHOULD deploy a secondary eduroam federation server for resilience purposes.

6.3.2 Connected federations' infrastructures

Connected federations MUST make sure that their infrastructure and connected institutions can provide the following items:

- Service Providers:
  - Authentication requests that originate from their service providers and carry a realm that is outside the scope of this federation MUST be forwarded through the federation infrastructure to the federation's eduroam federation server.
  - Service providers MUST keep sufficient logging information to be able to correlate between a client's layer 2 (MAC) address and the layer 3 (IP) address that was issued after login if public addresses are used. They SHOULD log all DHCP transactions; if they do, the following information MUST be recorded:
    - The time of issue of the client's DHCP lease.
    - The MAC address of the client.
    - The IP address allocated to the client.

- Service providers MUST deploy NASes that use IEEE 802.1X and symmetric keying using keys provided within RADIUS Access-Accept packets, in accordance with section 3.16 of RFC3580 on their eduroam SSID. An encryption level SHOULD be WPA/TKIP or better.
- Service providers MUST deploy NASes that include the supplicant's MAC address within the Calling-Station-Id attribute.
- The eduroam service provider MUST deploy the SSID “eduroam” (unless overlapping wireless coverage conflicts with other eduroam networks) and IEEE 802.1X Extensible Authentication Protocol (EAP) authentication to ensure a consistent service and minimum level of security. The SSID “eduroam” SHOULD be broadcasted.
- Service providers MUST transparently proxy any EAP-type for visiting users.
- Service providers SHOULD provide open network access to eduroam users. Where this is not possible, the number of filtered protocols SHOULD be kept as low as possible.
- Service providers SHOULD provide visitors with publicly routable IPv4 addresses using DHCP.
- Service providers MAY configure additional realms to forward requests to other internal RADIUS servers, but these realms MUST NOT be derived from any domain in the global DNS that the participant does not administer.
- Service providers MAY configure additional realms to forward requests to external RADIUS servers in other organisations, but these realms MUST be derived from domains in the global DNS that the recipient organisation administers (either directly, or by delegation).
- Service provider MAY offer any media; however as a minimum, wireless LAN IEEE 802.11b is required whilst newer standards (for example 802.11a, 802.11g and 802.11n) are also recommended.
- Service provider MAY implement a visitor virtual local area network (VLAN) for eduroam-authenticated users that is not to be shared with other network services.
- eduroam service providers SHOULD NOT deploy application or interception proxies. Service providers deploying application or interception proxies MUST publish information about these proxies on their eduroam website. If an application proxy is not transparent, the service provider MUST also provide documentation on the configuration of applications to use the proxy.

For a consistent user experience it is crucial that a common set of services is available throughout the infrastructure. While the following list of desirable open ports is not a requirement, it serves as a guideline for service, and service providers are asked to strive to open at least these ports:

- Standard IPSec VPN: IP protocols 50 (ESP) and 51 (AH) both egress and ingress; UDP/500 (IKE) egress only.
- OpenVPN 2.0: UDP/1194.
- IPv6 Tunnel Broker service: IP protocol 41 ingress and egress.
- IPsec NAT-Traversal UDP/4500.
- Cisco IPSec VPN over TCP: TCP/10000 egress only.
- PPTP VPN: IP protocol 47 (GRE) ingress and egress; TCP/1723 egress only.
- SSH: TCP/22 egress only.
- HTTP: TCP/80 egress only.
- HTTPS: TCP/443 egress only.
- IMAP2+4: TCP/143 egress only.
- IMAP3: TCP/220 egress only.
- IMAPS: TCP/993 egress only.

- POP: TCP/110 egress only.
- POP3S: TCP/995 egress only.
- Passive (S)FTP: TCP/21 egress only.
- SMTPS: TCP/465 egress only.
- SMTP submits with STARTTLS: TCP/587 egress only.
- RDP: TCP/3389 egress only.

- For Identity Providers:
- All eduroam user names MUST conform to RFC4282 (Network Access Identifier specification). The realm component MUST conclude with the eduroam identity providers' realm name, which MUST be a domain name in the global DNS that the identity provider administers, either directly or by delegation.
- Identity providers MUST configure their Extensible Authentication Protocol (EAP) server to authenticate one or more EAP types.
- Identity providers MUST select a type, or types, for which their EAP server will generate symmetric keying material for encryption ciphers, and configure their RADIUS authentication server to encapsulate the keys, in accordance with section 3.16 of RFC3580 (IEEE 802.1X RADIUS Usage Guidelines), within RADIUS Access-Accept packets.
- Identity providers MUST log all authentication attempts; the following information MUST be recorded:
  - The time the authentication or accounting request was exchanged.
  - The user identity corresponding to the request (so that the actual user can be properly identified if it is required)
  - The value of the Calling-Station-Id attribute in authentication requests
- The minimum log retention period is six months, unless national regulations require otherwise.

7 Continuous Service Improvements and liaisons

The SA5 group shall actively participate in the activities of TF-mobility/JRA5 and follow their results. Upon SA5 decision OT will test and implement improvements. These improvements include not only the implementation of the new technologies but also the service elements' enhancements.

The OT should inform SA5 about the results of tests and new feature implementations.

OT and SA5 should initiate research and development activities for potential service improvements.

Work on RadSec integration into eduroam infrastructure is one the first service improvements planned.

Other areas for further improvement include monitoring and diagnostics tools, user support processes, eduroam database and statistics presentation.

7.1 Liaisons

The eduroam service is a result of the innovation chain envisaged right from the beginning of the GÉANT2 project: from Task Force, through Joint Research Activity, to the service:

- Task Force TF – Mobility, established by TERENA, started its work with some initial meetings in 2002. TF is composed not only of members of NREN organisations, but also from networking researchers of wider provenance, for example universities and industries and from different world regions.
- Joint research Activity JRA5, as a part of the developments in the GN2 project carried out the necessary concrete studies and improved the pilot project, which has grown to the pre-operational stage.
- SA5 as the final link in this chain.

The R&D activity in the eduroam area (roaming) will continue in JRA5, as the SA5 group only governs the *service.* Input from the Mobility Task Force will continue to be sought.

Also worldwide liaisons with other, non-GÉANT2 or non-European roaming federations will be maintained through the activities of SA5, JRA5 and TF-Mobility.

8 Service transition and Implementation plan

The Service transition and Implementation plan will follow the overall plan of the SA5 activity.

Transition from pilot to regular service is due in project month 48 (August 2008).

In order to achieve that goal all planned service elements must be put to the operation, as follows:

1. Policy.
2. Monitoring system.
3. TTS.
4. eduroam database.
5. eduroam web site.

8.1 Policy

Final policy acceptance is planned for project month 41 (January 2008.).

In order to avoid discontinuation of the service for the end users, an NREN/NRO that cannot sign the Policy for organisational or technical reasons may send a signed **Letter of Intent** (LOI) to the NRENPC, clearly stating the date when they will be able to sign the Policy. The LOI should not specify a date later than the end of project month 48 (August 2008).

It is important to understand that Policy acceptance does not force an NRO to ban legacy roaming systems inside its federation. More information on security problems regarding the web-based roaming systems and reasons for the selection of 802.1X as the only eduroam technology is provided in Appendix C.

8.2 Monitoring system

- First version of production monitoring system is planned to be operational by the end of the project month 44 (April 2008).
- Monitoring system will be continuously improved.

8.3 TTS

- First version of production TTS is planned to be operational by the end of the project month 42 (February 2008).
- TTS operations will be continuously improved.

8.4 eduroam database

- First version of production eduroam database is planned to be operational by the end of the project month 42 (February 2008).
- It is planned NROs will provide the needed data by the end of project month 44 (April 2008).
- eduroam database will be enhanced continuously.

8.5 eduroam web site

- Current version of eduroam web site is available at http://www.eduroam.org/.
- New version is planned to be in production by the end of project month 41 (January 2008). Nevertheless as the other service elements (for example TTS, monitoring, eduroam database) are finished, the web site will be updated accordingly.

9 Potential risks

The short list of potential risks given below represents a basic description of the potential issues.

9.1 Issue 1: Legal regulations

Potential issues might come from national legal regulations in the fields of data protection and data preservation. As an example, the Anti-Terror Law in Italy demands a photo document before network access can be granted. This is not possible with the current eduroam infrastructure.

9.2 Issue 2: Sufficient high number of participants

The value of the eduroam service depends very much on a good coverage of the:

- Federations participating in the confederation.
- Institutions participating in the federations.

While almost all NRENs are participating in the eduroam pilot already, the percentage of potential eduroam enabled institution varies. There are also the institutions that act only as IdP and do not provide the eduroam access point to the other participants. Substantial effort by all involved in eduroam service provision is needed to reach a critical mass for eduroam to succeed as a service.

9.3 Summary Risk Analysis

The following table summarises the hypothetical risks that have been taken into account, their probability of occurrence and impact area (Cost (C), Schedule (S), Performance (P)). The response to each risk is outlined, clarifying the impact of the risk, its probability, and potential response.

The responses to risks are classified as:

- Avoid: The risk is already eliminated, or we have a plan how to deal with it.
- Transfer: Ensure that the consequences of the risk only impact the respective federation participant.

ID	Description	Impact	Probability	Impact Area	Response to risk
1	Signing policy; NRO commitment to the eduroam service	high	medium	S, P	Avoid: an effort on information dissemination is done; help for new eduroam members is provided
2	OT not performing well	high	low	S,P	Avoid: OT already proved to function well. Inside the OT one partner can backup the work of the other
2	Confederation RADIUS servers delayed	high	low	S, P	Avoid: The servers are already in place as part of the eduroam pilot.
3	Federation RADIUS servers delayed	medium	medium	S, P	Transfer: Implementation of Federation RADIUS servers is within the responsibility of the respective federation. JRA5, eduroamSA, and the operational team are only involved providing support in the form of cookbooks. Many of the Federation RADIUS servers are already in place as part of the eduroam pilot.
4	Institutional RADIUS servers delayed	low	medium	S, P	Transfer: Implementation of Institution RADIUS servers is within the responsibility of the respective Institution. JRA5, eduroamSA, and the operational team are only involved providing support in the form of cookbooks.
5	Confederation RADIUS server fail	high	low	S, P	Avoid: The Confederation RADIUS servers are completely redundant
6	Federation RADIUS servers fail	medium	medium	S	Avoid: The Federation RADIUS servers are completely redundant as required by the policy
7	Institutional RADIUS servers fail	low	medium	S	Transfer: The Institutional RADIUS servers are solely in the responsibility of the respective institution

Table A A-1: Risk Analysis table

10 Liability and branding

10.1 Liability

The Article 8 of the Consortium Agreement regulates the liability issues arising between the Parties participating in the SA5.

10.2 Branding

eduroam and the eduroam logo are registered trademarks of the Trans-European Research and Educational Networking Association, TERENA.

For further information see the web page of TERENA (www.terena.org).

All locations providing eduroam should clearly indicate so in order to promote user awareness and ensure a high level of trust in the brand and service.

11 Conclusions

The European eduroam confederation is based on the set of defined organisational and technical requirements that members of the European eduroam confederation must accept and follow.

As part of GEANT2, the European eduroam service is managed by the National Research and Educational Network Policy Committee (NREN PC), which in turn delegates the supervision of the European eduroam service to the SA5 group. In turn, SA5's eduroam Operational Team (OT) carries out the day-to-day operations of eduroam, and runs the eduroam confederation service.

The technologies and organisational structures described in this document show that the confederated eduroam service encompasses all the elements necessary to support the European service. Aside of the confederation infrastructure itself, these include:

- Establishing trust between the member federations.
- Monitoring and diagnostic facilities.
- Central data repository providing information about the eduroam service.
- Confederation level user support (i.e. support for member federations).

12 References

GN2-07-328	“eduroam policy - for signing
DJ5.1.4	“Inter-NREN Roaming Architecture: Description and Development Items
DJ5.1.5,2:	“Inter-NREN Roaming Infrastructure and Service Support Cookbook - Second Edition”

13 Acronyms

AAA	Authentication, Authorization and Auditing
EAP	Extensible Authentication Protocol
eduroam	EDUcation ROAMing
FLR	Federation level RADIUS server
IdP	Identity Provider
JRA	Joint Research Activity
NA	**Networking Activity**
NREN	National Research and Educational Network
NRO	national roaming operator
OT	Operational Team
PAP	Password Authentication Protocol
PC	Policy Committee
PEAP	Protected Extensible Authentication Protocol
RADIUS	Remote Authentication Dial In User Service
SA	Service Activity
SP	Service Provider
TLR	Top-level RADIUS server
TLS	Transport Layer Security
TTLS	Tunnelled Transport Layer Security
TTS	trouble-ticketing system
VLAN	Virtual Local Area Network

Appendix A End-to-end encryption of user credentials

This ensures that no intermediate party, be it an eduroam infrastructure operator or external parties, can steal the digital identity of an eduroam user. This enables the eduroam SA to make an important assertion: using eduroam never exposes the credentials to anyone in the infrastructure except the home institution, which makes sure that the confederation infrastructure operators are neither responsible nor liable for password theft.

Since no AAA infrastructure available today provides end-to-end encryption in itself, end-to-end security has to be established by the two ends of the authentication chain: the end-user device (Laptop, PDA, etc.) and the home authentication server. This is achieved by using mutual-authentication protocols such as TTLS-PAP, PEAP or EAP-TLS. Most notably, authentication methods in use by web-redirect portals such as PAP do NOT provide end-to-end security.

Appendix B Logging of authentication and accounting packets

Authenticating a user and the subsequent establishing of the user session is a transaction between the identity provider and the resource provider. The intermediate infrastructure acts only as conveyor of their data. As such, no liabilities for the confederation members or the operational team are involved. Still, logging this data provides an audit trail that may help connected institutions resolve conflicts. Furthermore, the data is useful if debugging a problem is required. Because of that, it is recommended that confederation members, and the confederation infrastructure itself, keep logs of the data flowing through the infrastructure. Since national regulations may require time frames for data retention, it is not possible to give a general recommendation on the duration.

Appendix C Web-redirect systems

eduroam implements the 802.1X-protocol, creating secure channels for authentication to the users' home institution, and when the user is visiting other institutions (including abroad). A legacy installed base of insecure web-based roaming systems, stemming from the initial eduroam pilot, also carry the name eduroam and must be phased out. Why two different systems are still called eduroam, and why this is not viable, is explained below.

eduroam provides, in a secure manner, internet network access for a closed, international user group: education and research The network must be restricted to the community in order to keep the level of trust sufficiently high for institutions to give users from the “outside” access to their networks.

The advantage of the 802.1X protocol is that the user is authenticated before they are handed an IP-address and then in turn can connect to the Internet. This method ensures that no users can harm the local network installations before being authenticated.

This is unlike web-redirect systems, where the (unknown) user is initially given an IP-address in order to authenticate using a web-browser. Not only will the user be able to interfere with the network before getting authenticated, but also the authentication session is not secure, since the user name and password are traversing the underlying (RADIUS) infrastructure unencrypted.

Furthermore there is no way of telling if a web-login page is a genuine or rogue eduroam-page. Fake web-login-pages can easily be set up by copying the original html-code to a web-server, which then grants the user internet access and collects user credentials.

Finally, even after being authenticated with web-redirects, there is no security context established for the wireless connection that prevents malicious users to take over the session of a valid user (“session hijacking”).

The historic reason for having two systems called eduroam goes back to the days of TERENA's Task-force on Mobility, which investigated both of the above mentioned roaming approaches as well as a VPN-based solution (which was ruled out because of scaling problems).

Both the 802.1X and the web-redirect based roaming systems rely on a hierarchy of RADIUS servers to route the authentication requests back to the users' home institution. Both systems were installed under the name eduroam, as it took time to get consensus on the fact that web-redirects are too insecure and would quickly undermine the trust in the system as a whole, as eduroam grew internationally.

Meanwhile, several countries have installed national roaming services, based on web-redirect systems, which can exist in parallel with eduroam (and simultaneously use the same RADIUS infrastructure as eduroam). Only the name of the service as well as logo, network name and so on, must be different to eduroam, to avoid confusion.

Most of today's wireless access points can run multiple separate networks at the same time and thereby support several (roaming) systems.

Appendix D Resources

This Appendix describes the resources needed for running the European eduroam service. Please refer to Section 2 “Service Elements” for a description of Service Elements, and Section 4 “Service Organisation” for a description of Service Organisation.

Service fees from participating NROs/NRENs for the service are not planned at this stage. The principle of mutual support of the visiting users will be applied. However, below are the resources (equipment and man power) needed for the efficient working of the OT.

Necessary hardware and software are listed below:

Type	Number of pieces	Expected Cost
Monitoring workstations	4	8 K€
Servers (TLRS)	3	9 K€
Software licences	2	4,4 K€

Table D-1: hardware and software costs

The expected budget for software is planned assuming that Open Source software (as well as software tools developed inside JRA5 and SA5 activities) will be used where appropriate

Listed hardware and software needs cover all the service elements that must be provided by the OT.

For manpower, the following funding is required:

- SA5 leader.
- OT members.
- SA5 participants.

It is planned and expected that funding in the magnitude of 0,5 FTE to the SA5 leader and 3,5 FTE for the eduroam operational team will be sufficient for Year 4 of the project. In addition, we plan that each SA5 participant will need around 1,5 MM for active participation in the SA5 activities. Based on the experiences and current plans, the required manpower for Year 4+ 6 months is as described in the table below:

Purpose	Year 4	+ 6 months	Total y4+6M (18 months)
SA5 leader	0,5 FTE (6 MM)	0,25 FTE (3 MM)	0,75 FTE (9 MM)
Operational team (for 4 members)	3,5 FTE (42 MM)	1,75 FTE (21 MM)	5,25 FTE (63 MM)

SA5 members (for 30 members)	3,75 FTE (45 MM)	1,875 FTE (22,5 MM)	5,625 FTE (67,5 MM)
Summary	7,75 FTE (93) MM	3,875 FTE (46,5 MM)	11,625 FTE (139,5 MM)

Table D-2: Personnel costs

Note: This plan is done with the calculation of 30 participating members in the SA5 that are eligible for funding; currently there are 29 NROs/NRENs eligible for funding their activity in SA5.