26 July 2012

eduroam Policy Service Definition

Version 2.8

Date of Issue:	26-07-2012
Document Code:	GN3-12-192
Authors:	M. Milinović, Srce / CARNet, Stefan Winter, RESTENA and members of the SA3 T2 group
Description:	eduroam Policy Service Definition for SA3, Task 2

Table of Contents

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 and following the eduroam policy declaration).[1]

As part of GÉANT, 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 eduroam Steering Group (SG). The eduroam Operations 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.

[1] European eduroam Confederation Policy Declaration, ver. 2.0 (May 2012).

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 his/her home institution using the institution’s specific authentication method. The authorisation required to allow access to local network resources is carried out by the visited network.

The European eduroam service provides this facility as a confederated service, built hierarchically. At the top level sits the confederation level service, which 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 Remote Authentication Dial-In User Service (RADIUS) servers is used to transport the authentication request of a user from the visited institution to his/her home institution, as well as the authentication response. 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 in the form of institution.TLD, where TLD is the country code), 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 (gTLD) (for example, terena.org) requires different handling and MUST be requested via the eduroam OT.

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 (through which the actual authentication information (username/password, etc.) is carried (e.g. via EAP-TTLS or PEAP)) from the user’s computer to his/her home institution is established, or mutual authentication by public X.509 certificates is used (EAP-TLS). The three authentication methods previously mentioned establish a secure TLS session from the end-user device to its home authentication server so users' private credentials are not subject to eavesdropping by intermediate parties. Other EAP methods may be designed in the future and they may depend on security mechanisms other than TLS exchange. Those methods may be used as long as they provide effective protection against eavesdropping for critical user data (such as passwords).

The confederated eduroam service encompasses all the necessary elements to provide a service to the users. Aside from the confederation infrastructure itself, these elements include:

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

These elements are described in more detail in the following sections.

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 website 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. There are various transport protocols to carry RADIUS payloads, as of May 2012, the following protocols exist: RADIUS/UDP, RADIUS/TCP, RADIUS/DTLS and RADIUS/TLS.

eduroam supports transport over RADIUS/UDP and RADIUS/TLS, and recommends the use of RADIUS/TLS. Routing of RADIUS messages, independently of the transport used, is implemented in two ways: a baseline-routing model, based on a hierarchy of RADIUS servers, and a dynamic-routing model, based on DNS service discovery. The dynamic-routing model is only supported over RADIUS/TLS.

The routing models and infrastructure elements are described in more detail in the following sections.

2.1.1 Routing Models

2.1.1.1 *Baseline RADIUS Routing (Hierarchy)*

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 federation-level RADIUS proxy server (FLRS). See Figure 2.1.

HI = Home Institution
VI = Visited Institution
IdP = Identity Provider
SP = Service Provider
(network access service
provided by an institution)

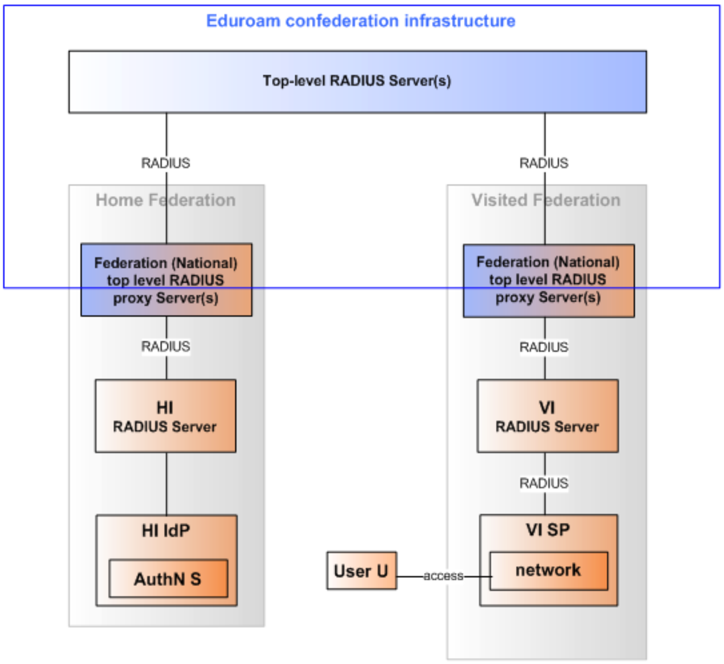
Eduroam confederation infrastructure
Top-level RADIUS Server(s)
RADIUS
RADIUS
Home Federation
Visited Federation
Federation (National) top level RADIUS proxy Server(s)
Federation (National) top level RADIUS proxy Server(s)
RADIUS
RADIUS
HI RADIUS Server
VI RADIUS Server
RADIUS
HI IdP
AuthN S
User U
access
VI SP
network

Figure 2.1: Current eduroam confederation structure

The eduroam European Top-level RADIUS Servers (ETLRS) interconnect the participating eduroam federations. They provide the means to find the correct federation-level RADIUS server of a given users' federation, and to transport all information in a secure way. eduroam ETLRS are maintained by the OT.

2.1.1.2 *Dynamic RADIUS Routing*

In dynamic routing, eduroam Identity Providers (IdP) announce their responsible RADIUS server over DNS. eduroam Service Providers (SPs), which need to authenticate a user, look up the appropriate RADIUS server by querying the Domain Name System (DNS) for a special eduroam server record.

This routing model does not require any intermediate RADIUS infrastructure, but can be used even in the presence of intermediates. In particular, if an eduroam IdP does not wish to deploy its own RADIUS/TLS enabled RADIUS server, it can connect to the FLRS via a static uplink (hierarchical routing), and announce in the DNS record that the RADIUS/TLS endpoint is the IdP's FLRS. Similarly, an eduroam SP, which does not wish to perform its own DNS lookups, can statically connect its infrastructure to the FLRS, which, in turn, can carry out the DNS lookups for that SP.

eduroam IdPs and SPs always need to have a static route to their FLRS configured as a "default" fallback routing mechanism, because the publishing of DNS records for eduroam IdPs is optional. As a result, a default routing decision needs to be available should a DNS not yield the routing information.

2.1.2 European Top-level RADIUS Servers (ETLRS)

Currently, the European Top-level RADIUS Servers (ETLRS) for the European Confederation are located in the Netherlands and Denmark. Each server has a list of connected, federation top-level domains (.nl, .dk, .hr, .de etc.) serving the appropriate NRENs. The servers also maintain exception rules for domains whose federation membership is not immediately identifiable in the realm (typically gTLD realms such as '.edu', '.eu', '.net', etc.). The servers accept requests for the federation domains they are responsible for, and subsequently forward them to the associated RADIUS server for that federation, and transport the response (i.e. result of the authentication request) back. Requests for the federation domains that the servers 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 (ETLRS), although these NRENs are not members of the European confederation.

2.1.3 Federation-level RADIUS Server (FLRS)

A federation RADIUS server has a list of connected eduroam IdP servers and their associated realms, as well as the connected eduroam Service Providers within a federation. It is connected to the ETLRS.

The purpose of the FLRS is to receive requests from the ETLRS and eduroam SPs, and forward these requests to the responsible eduroam Identity Provider (either using static routing, or by performing DNS lookups for dynamic request routing).

2.1.4 eduroam Identity Providers (IdPs)

An eduroam IdP's 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. The Identity Management System contains information on end users (for example, usernames and passwords). They must be kept up-to-date by the eduroam Identity Provider.

Note that the eduroam Identity Provider's RADIUS server has the most complex task of all. Whereas the other RADIUS servers merely proxy requests, the Identity Provider's server also needs to actually authenticate users, and therefore, needs to be able to terminate EAP requests and perform identity management system lookups.

2.1.5 eduroam Service Providers (SPs)

An eduroam Service Provider's (SP) RADIUS server is responsible for forwarding requests from users visiting this SP to the responsible eduroam IdP, either by forwarding the request along the hierarchy, or by discovering the responsible server with DNS. Upon proper authentication of a user, the eduroam SP's RADIUS server may assign a VLAN to the user.

Small SPs that do not require VLAN assignment do not necessarily need their own RADIUS server, and can instead connect their network access elements (see below) to the respective FLRS.

In most cases, an educational institution participating in eduroam acts as an IdP and SP at the same time.

2.1.6 Network Access Elements

eduroam is not dependent 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.

2.1.6.1 *Supplicants*

A supplicant is software on an end-user's computing device that uses the IEEE 802.1X protocol to send authentication information, using the EAP protocol. Supplicants are often built into the operating system, but can also be a separate program.

In order to use the eduroam service and access the network, the supplicant software on users' devices must be appropriately configured. This configuration is valid throughout the eduroam confederation.

2.1.6.2 *Access Points*

Access points are only required for wireless access to the network.

Access points need to be IEEE 802.1X capable. They must also be able to forward access requests coming from a supplicant to the SP’s RADIUS server, to allow network access upon proper authentication. Access points may also possibly assign users onto 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 and to ensure encryption of user payload data on the wireless medium.

2.1.6.3 *Switches*

Switches are used for wired access to the network.

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

These switches need to be able to forward access requests coming from a supplicant to the SP's 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, Diagnostics and Metering

The basic purpose of the eduroam monitoring, diagnostics and metering service is:

- to test the functionality of the FLRSs, TLRSs and the whole confederation infrastructure.
- to collect information about the authentication traffic from the FLRSs.

The design of the monitoring and diagnostics element allows implementation of different monitoring scenarios in order to test various operational aspects of the eduroam service. It can also complement other (e.g. national-level) monitoring services.

The eduroam monitoring and diagnostics element reports the results of the tests, both as a colour-coded map and as graphs showing the response-time behaviour. Information has been provided via the monitoring website [Monitoring] An alert system is also implemented in order to inform responsible staff about any malfunctions in the service as soon as they occur.

The metering element relies on the F-Ticks tool. Information about F-Ticks, as well as the collected data, is available via the F-Ticks website [F-Ticks].

The website also provides various information from the eduroam monitoring, diagnostics and metering service. Some of those are public, while others are restricted to predefined user groups. The decision on the availability of the information lies with the eduroam Steering Group (SG).

The eduroam monitoring, diagnostics and metering service is run and maintained by the Operations Team (OT).

2.2.2 eduroam Website

The eduroam website [eduroam] is run and maintained by the OT.

It is the central information point for eduroam users at the same time providing information and links for all user groups (see Section 3, Users).

2.2.3 eduroam Database

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

- NRO representatives and respective contacts.
- eduroam SP and IdP official contacts.
- Information about eduroam Service Providers (SP location, technical info).
- Monitoring information.
- Information about the usage of the service.

Information about the eduroam database design and data collection practice is available via the website [eduroam Database].

A web interface to the database is implemented, which allows various views of the database content. Some of these are public, while others are restricted to predefined user groups. The decision on the availability of the information lies with the eduroam SG.

Data exchange with other applications related to the eduroam service is subject to prior approval by the eduroam SG.

The eduroam database and its web interface is run and maintained by the OT.

2.2.4 Trouble Ticketing System (TTS)

The OT runs and maintains a Trouble Ticketing System (TTS) [TTS] in order to document its work, and to allow authorised users from the predefined user groups to report any irregularities in the eduroam service.

2.2.5 Mailing Lists

Two mailing lists are provided:

- eduroam SG list (eduroam@geant.net).
- eduroam Operations Team (OT) list (eduroam-ot@geant.net).

Both lists are 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, either at their home institution or while 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 device to use eduroam. The latter ("consumers") require more assistance. In terms of the current service portfolio, no distinction is made between these two categories and, for now, they are addressed in the same way. Table 3.1 shows that end users have access to the eduroam website, database for accessing general information and access to basic monitoring tools. It is recognised that over time, a more refined distinction between end-user categories should be made, with corresponding refinement of the service portfolio mapping.

3.2 Administrative Personnel

Administrative personnel are those users who are running parts of the eduroam infrastructure that are not handled directly by the OT: 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 level of skill 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 Operations 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 for an identity management system. Given that identity management systems are quite diverse, it is impossible for eduroam OT and SG 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 handle day-to-day user support. They should be supported by the respective NRO. eduroam OT and SG 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	**Institution--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 website	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
SG/OT Mailing lists	No	No	Yes
Support form OT	No	No	Yes

Table 3.1: Service elements

4 Service Organisation

As part of the GÉANT 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 eduroam steering group (SG).

The organisation of the European eduroam service is aligned with the overall organisation of the GÉANT project, and will be adjusted in case of future changes in the project organisation.

The SG consists of representatives of all federations connected to the eduroam confederation. Official members of the SG group are the representatives of those roaming federations that have signed the eduroam policy. SG may also accept unofficial members, who are either representatives of other roaming federations that liaise with the European eduroam service or are technical experts in the field.

Day-to-day operations are carried out by the eduroam Operations Team (OT). It is approved by the SG and the NREN PC. The SG leader manages and oversees the work of the OT.

The eduroam service model is illustrated in Figure 4.1:

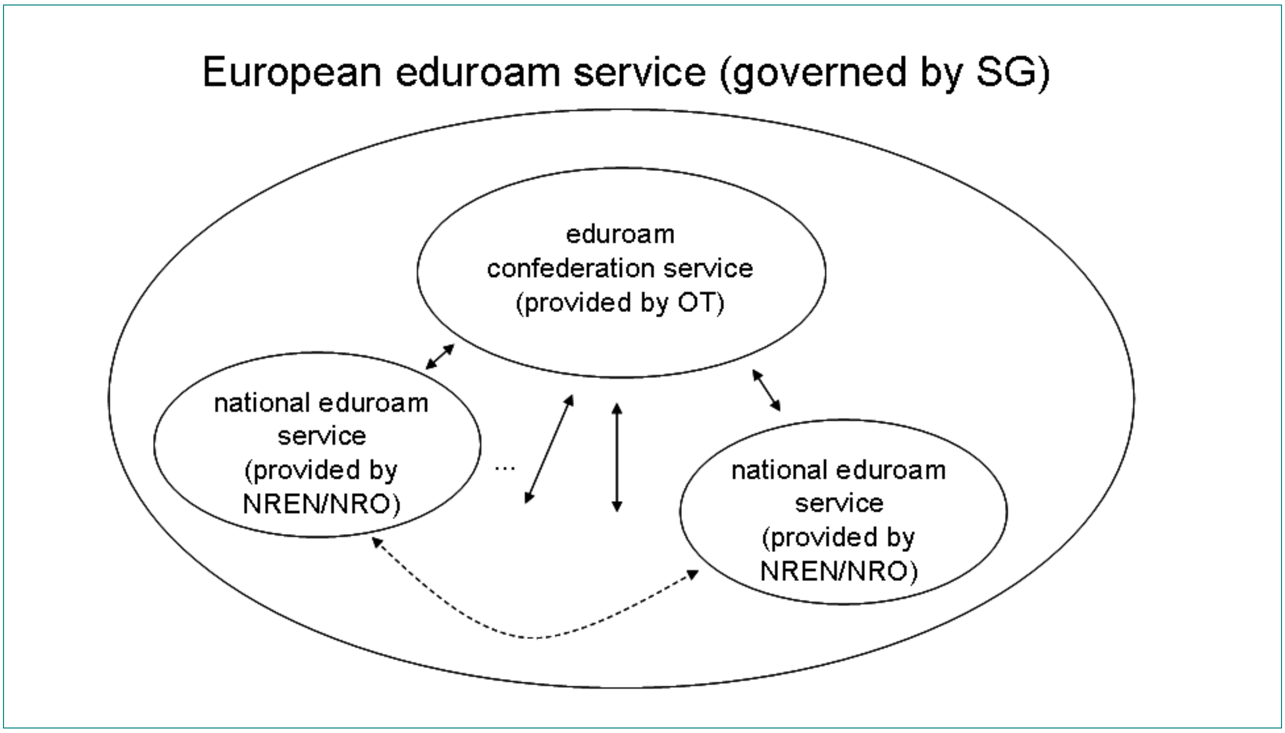
European eduroam service (governed by SG)
eduroam confederation service (provided by OT)
national eduroam service (provided by NREN/NRO)
...
national eduroam service (provided by NREN/NRO)

Figure 4.1: eduroam service model

4.1 Roles and Responsibilities

This section describes the specific roles and responsibilities, including those of the:

- NREN Policy Committee (NREN-PC).
- eduroam confederation members: National Roaming Operators (NROs).
- eduroam Steering Group (SG).
- eduroam Operations Team (OT).

4.1.1 NREN PC

The NREN PC coordinates the cooperation of the European NRENs in the GÉANT project, and approves the budget plans. The NREN PC delegates supervision of the European eduroam service to the SG.

The NREN PC is responsible for approving basic service items (for example, appointment of SG leader), the composition of the OT and the eduroam policy proposed by the SG. The NREN PC also handles disputes that cannot be resolved by the SG.

4.1.2 eduroam Confederation Members (NROs)

NROs should appoint at least one representative to the eduroam SG.

The tasks of the eduroam Confederation members include:

- Participating in the work of the SG.
- Assuring adherence to the eduroam policy.
- Provisioning of necessary support and information to the OT.
- Provisioning of the support to the respective roaming users.

4.1.3 eduroam Steering Group (SG)

The SG manages the eduroam service. It is the responsibility of the SG to manage the work of the OT and provide it with necessary input.

The tasks of the eduroam SG include:

- Supervising the Operations Team.
- Formulating recommendations on monitoring and diagnostic tools, and supporting scripts that should be used in providing service.
- Further policy development.
- Handling membership matters.
- Integrating future research results.
- Formulating recommendations related to establishing trust between member federations.

- Participating in the dissemination work (providing material for web pages, enhancement of the visibility of the Confederation, including the provision of promotional material).
- Evaluating usage-related data and publishing of corresponding graphs and statistics.
- Improving of eduroam service definition and procedures.
- Participating in organisation of the training events.
- Providing support for the Confederation members (including providing a federation web presentation in English, with appropriate access information, exchange of technical knowledge, motivating events, etc.).
- Liaising on technical matters with other non-GÉANT or non-European roaming (con-) federations.

4.1.4 eduroam Operations Team (OT)

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

The tasks of OT include:

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

4.1.5 Service-level Definition

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

- Confederation infrastructure (explained in Section 2.1).
- Monitoring and diagnostic facilities.
- eduroam database.
- eduroam website.
- Confederation trouble ticketing system.

The goal for the availability of these services is in the range of 99%.

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.

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

5 Service Operation

This section defines basic operational procedures for the eduroam service.

The OT and SG will use the following communication tools:

- Mailing lists (see Section 2.2.5).
- Trouble Ticketing System (TTS).
- eduroam website.
- 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 is delivered primarily by the home 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 and use 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 visiting users, regarding the use of eduroam service.

The OT primarily provides 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 within their home federation, the federation's user support rules are applied.

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

If needed, respective federation-level personnel are contacted along with the OT. Regardless of this, end users should only contact 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 deals with the basic eduroam technology.
  - Contact other involved federations 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*

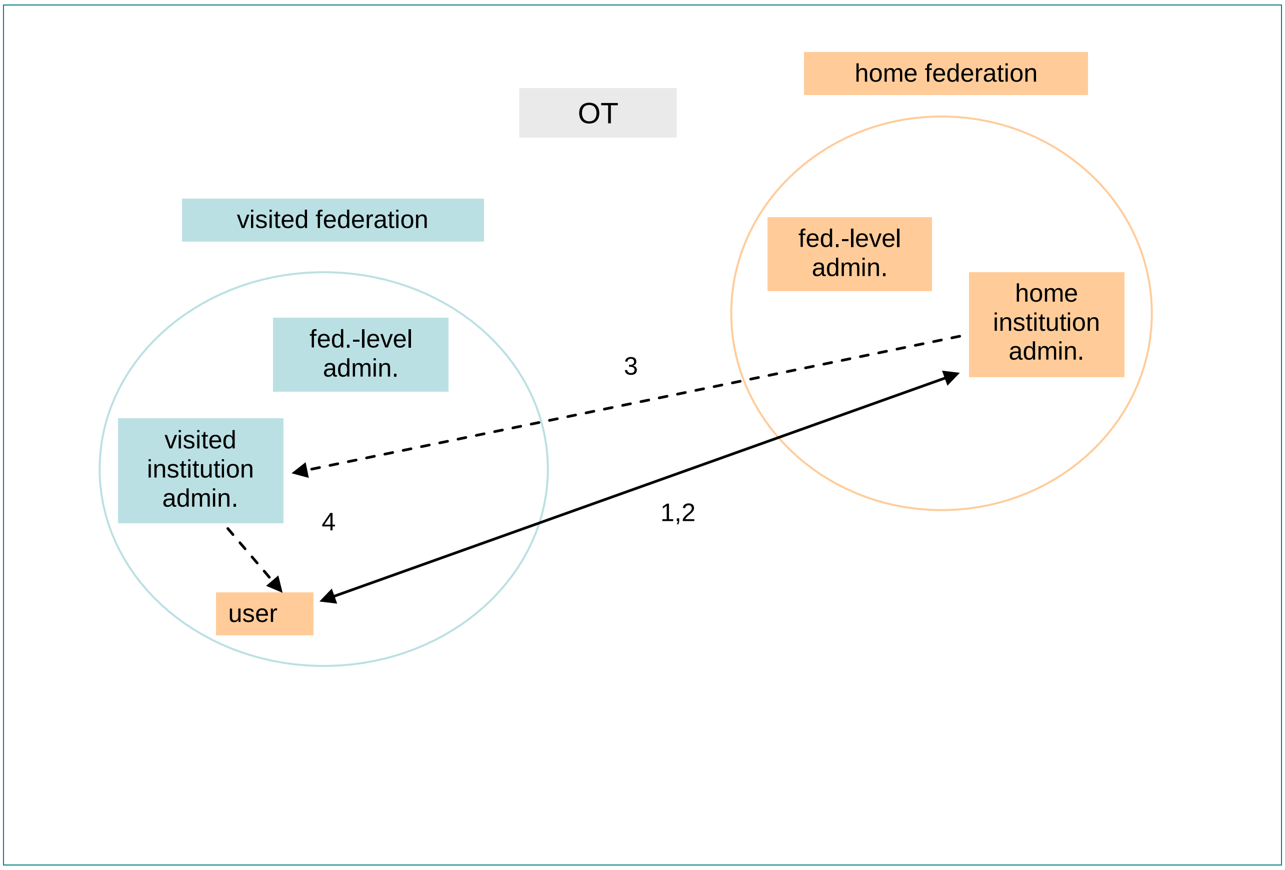

Figure 5.1: Problem escalation scenario, user and institution personnel

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

1. The user calls his/her home institution, and asks for help from administrative personnel.
2. 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. Personnel 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 administrative personnel at the user's home institution discover problems receiving a proper authentication request from the visited site, they should contact 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, 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*

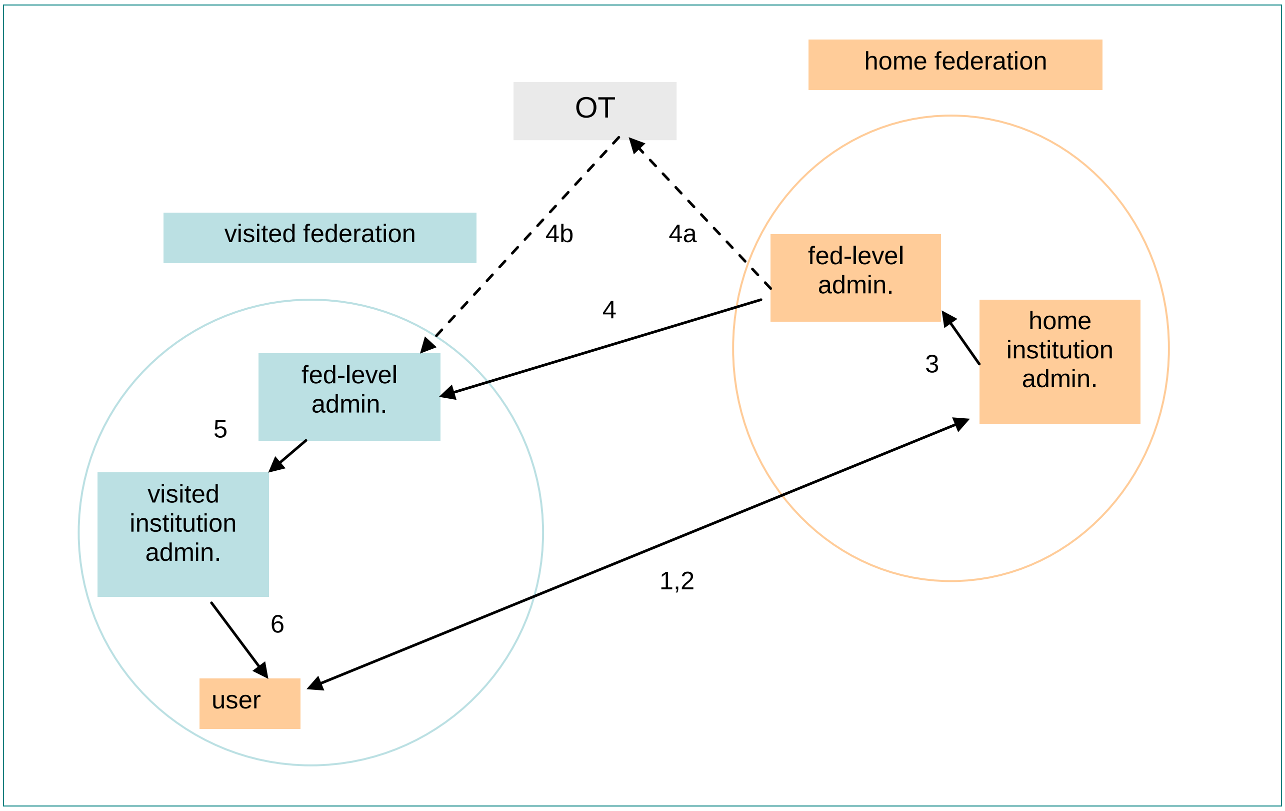

Figure 5.2: Problem escalation scenario, user, institution and federal-level personnel

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

1. The user must call his/her home institution and ask for help from administrative personnel.

2. Administrative personnel at the user's home institution will check the validity of the user's credentials and help to set 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 administrative personnel at the user's home institution discover the problem is in receiving authentication requests from the visited site, and they cannot resolve the problem by contacting administrative personnel at the visited institution, they should contact administrative personnel of their federation.

4. The end user's federation administrative personnel should carry out further checks, and if needed, contact the visited federation's administrative personnel. In response, the federation's administrative personnel should provide necessary information in order to resolve the problem. If the OT is involved in resolving the problem, (see Steps 4a and 4b in Figure 5.2), the 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. Administrative personnel at visited institution should inform the visiting user that the problem has been resolved.

5.2 Maintenance Procedures

This section outlines main maintenance procedures. Detailed procedures including the working hours are defined by the OT and approved by SG.

5.2.1 Scheduled Maintenance

Scheduled maintenance of 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 SG mailing list. Scheduled maintenance should be scheduled from Tuesday to Thursday, 06:00–08:00 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 TLRS must be planned to avoid any break in the service.

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

5.2.2 Unscheduled Maintenance

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

Unscheduled maintenance of 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 SG 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 SG 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

In the case of any security incidents, the GÉANT multidomain services security incident handling procedures must be followed [Security Incidents].

In general, whenever necessary and appropriate, incidents should be handled by the respective Computer Emergency Response Team (CERT). In addition there are some further actions (explained below) that 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 the NRO's respective official contacts in the eduroam SG.

NROs should regularly report to the OT about the number and type of these incidents.

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 the SG, if appropriate (which might result in further escalation to the NREN PC), depending on the level of violation:

- Issue a notice on the SG 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 required are handled on a case-by-case basis).
- Propose (through SG) 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 SG 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 SG 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 providers 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.

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 SG 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 make a request to OT to add the respective institution to the TLRS instead. Upon such a request by the respective federation, OT checks the technical reasons and, if justified, modifies configuration on TLRS and reports back on the execution of the configuration change.

The European eduroam confederation peers with all roaming confederations or federations who signed the Global eduroam compliance statement defined by the Global eduroam Governance Committee (GeGC) [GeGC]..

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 (updating websites, top level servers, user notification, and so on) can be taken care of in a timely manner.

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

An excluded member or the NRO whose application has been turned down by the SG has right to appeal to the NREN PC. NREN PC decisions on membership are final.

The list of members is publicly available on the eduroam website. Changes in membership are announced using the eduroam website and SG 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 Confederation Member Requirements

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 Declaration

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

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

Violation of the Policy declaration MUST be reported to the OT, and MUST be presented to the SG 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 Section 5.1, “User Support Processes”.
- Participate in the work of the SG.
- Provide the information for the eduroam database (see Section 2.2.3).
- Establish and maintain a website, including information with respect to the participating institutions, as well as practical information on how to use eduroam. The webpage SHOULD be available in English.

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.

The 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 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 no 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

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, etc.). In addition to the general networking requirements, eduroam makes use of a number of protocols for user authentication and service provisioning. These authentication-specific and service-specific requirements are listed below. Details regarding the extent of usage of these specifications are also given.

6.3.1 Specifications and Operational Requirements: Federation Level

Adherence to the following specifications is REQUIRED:

- AAA Servers:
  - RADIUS datagram processing to and from the ETLRS, as per RFC 2865 or any other of the recommended transports (e.g. RADIUS/TLS).
    The server MUST be able to proxy RADIUS datagrams to other servers based on contents of the User-Name attribute.

  - RFC 3580 (EAP over RADIUS).
    The server MUST proxy EAP-Message attributes unmodified, in the same order as it received them, towards the appropriate destination.

  - F-Ticks [F-Ticks].
    The server MUST generate F-Ticks and send them to the monitoring infrastructure. If dynamic RADIUS routing (see Section 2.1.1.2) is used by the individual SPs, then it is the responsibility of the respective NRO to ensure that appropriate F-Ticks are sent to the monitoring infrastructure, either by enforcing that the SPs send them to the monitoring infrastructure themselves, or by collecting information of the authentication events and sending these on to the monitoring infrastructure on the SP’s behalf.

  - The server MUST be set up to allow monitoring requests from the monitoring service.

  - All relevant logs MUST be created with synchronisation to a reliable time source (GPS or in its absence NTP/SNTP).

  - The server(s) MUST respond to ICMP/ICMPv6 Echo Requests sent by the confederation infrastructure and confederation monitoring service.

- Web server:
  - NRO MUST set-up a web server in order to publish information about the eduroam service. The address of that server SHOULD be www.eduroam.<tld>.

  An NRO’s web server MUST provide data in XML format, based on the specification defined by the SG, and available at http://monitor.eduroam.org/database.

Adherence to the following specifications is RECOMMENDED:

- AAA Servers:
  - ○ RFC 2866 (RADIUS Accounting).
    The server SHOULD be able to receive RADIUS Accounting packets if a service provider opts to send that data.
    If RADIUS Accounting is supported, RADIUS Accounting packets with a destination outside the

federation MUST NOT be forwarded outside the federation, and MUST be acknowledged by the FLRS.

- ○ A RADIUS/TLS endpoint open for connections from all other eduroam participants to enable the receiving end of RADIUS/TLS dynamic discovery.
- ○ A DNS-based discovery module for outgoing RADIUS/TLS dynamic discovery.
- ○ Servers SHOULD be highly available, for example, by deploying multiple separate servers in a failover configuration in different IP subnets on different physical locations.
- ○ Logs of all authentication requests and responses SHOULD be kept. The minimum log retention time is six months, unless national regulations require otherwise. The information in the requests and responses SHOULD as a minimum include:
  - The time the authentication 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 result of the authentication.
  - The value of Chargeable-User-Identity (if present in Access-Accept message).

6.3.2 Specifications and Operational Requirements: Identity Providers

Adherence to the following specifications is REQUIRED:

- AAA Servers:
  - ○ RADIUS datagram processing as per RFC 2865 or any other of the recommended transports (e.g. RADIUS/TLS). The server MUST be configured to receive authentication traffic from its FLRS and send appropriate replies.
  - ○ EAP server endpoint as per RFC 3580.
  - ○ A well-managed identity management backend system.
  - ○ All relevant logs MUST be created with synchronisation to a reliable time source (GPS or in its absence NTP/SNTP).
  - ○ At least one EAP type, which is capable of mutual authentication and capable of generation of keying material for use with IEEE 802.1X in accordance with Section 3.16 of RFC 3580 (IEEE 802.1X RADIUS Usage Guidelines).
  - ○ The outer EAP identities (and with it, RADIUS User-Name attributes) for the IdP MUST be in the format of arbitrary@realm, The realm component MUST be a domain name in the global DNS (without the trailing . sign) that the identity provider administers, either directly or by delegation. The part to the left of the @ sign is arbitrary; in particular, anonymity support is possible and encouraged.
  - ○ The server-side EAP credentials MUST be communicated to the user base, and end-user documentation needs to be precise enough to allow users the unique identification of their EAP server.
  - ○ The appearance of the Operator-Name attribute (RFC 5580) in Access-Requests MUST NOT cause these requests to be treated as invalid.
  - ○ Logs of all authentication requests and responses MUST be kept. The minimum log retention time is six months, unless national regulations require otherwise. The information in the requests and responses MUST, as a minimum, include:
    - The time the authentication 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.
- If tunnelled EAP types are used, the actual user name in the request ('inner EAP-identity').
- If the IdP opts to generate a Chargeable-User-Identity, the value of this attribute.
- The result of the authentication.

An IdP MUST provide sufficient configuration instructions for their end users so that a unique identification of the IdP is possible for the end user at all times.

Note: the list of supported EAP types as configured by the IdP in Section 6.3.2, and the list of supported EAP types in the supplicant software in Section 6.3.4 MAY have an empty intersection. In such cases, the combination of end-user device and IdP configuration will leave the user without service. To minimise the probability of this, eduroam IdPs are encouraged to configure as many EAP types as they can possibly support, and to announce the full list of supported EAP types to their end users.

Adherence to the following specifications is RECOMMENDED:

- AAA Servers:

  - Generation of a Chargeable-User-Identity (RFC 4372) response if solicited by a Service Provider and on the condition that the Service Provider's Access-Request contains a non-empty Operator-Name attribute. The value of Chargeable-User-Identity attribute returned in the response MUST have a constant value for one user and one Operator-Name attribute value. The value of Chargeable-User-Identity attribute MUST be generated in a way which ensures that the matching of this value to the actual user identity is possible only at the Identity Provider.

6.3.3 Specifications and Operational Requirements: Service Providers

Adherence to the following specifications is REQUIRED:

- Network Access Servers (NAS):
  - Construction and processing of RADIUS datagrams as per RFC 2865 or any other of the recommended transports.
    The NAS MUST send its RADIUS datagrams either to the SPs local RADIUS server or, in its absence, to the federation's FLRS.
    The generated RADIUS datagrams MUST include the attribute Calling-Station-Id, and the attribute value MUST contain at least the MAC address of the connecting end-user device.
  - RFC 3580 (EAP over RADIUS).
  - IEEE 802.1X.
  - All relevant logs MUST be created with synchronisation to a reliable time source (GPS or in its absence NTP/SNTP).
  - Wireless NASs MUST support WPA2/AES, and MAY additionally support WPA/TKIP as a courtesy to users of legacy hardware. Exceptionally, an SP established before January 1, 2012, MAY support only WPA/TKIP, but not longer than January 1, 2013.

- Wireless NASs MUST deploy the SSID "eduroam" and MUST broadcast the SSID "eduroam", unless there is more than one eduroam SP at the same physical location and the signal overlap would create operational problems, in which case an SSID starting with "eduroam-" MAY be used.
- local AAA Servers (in its absence, NAS or the FLRS):
  - Authentication requests MUST be forwarded towards the responsible eduroam Identity Provider via the eduroam infrastructure.
  - The server MUST proxy EAP-Message attributes unmodified in the same order as it received them towards the appropriate destination.
  - Sufficient logging information MUST be kept 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. This requirement is void if NAT is used.
  - If dynamic RADIUS routing (see Section 2.1.1.2) is used, appropriate F-Ticks MUST be sent to the monitoring infrastructure, either directly or through the NRO services (see Section 6.3.1).
- Network:
  The following set of ports MUST be made available to roaming visitors:

Service	Protocol / Port	Direction
Standard IPSec VPN	IP protocol 50 (ESP) IP protocol 51 (AH) UDP port 500 (IKE)	incoming and outgoing incoming and outgoing outgoing
OpenVPN 2.0	UDP port 1194	incoming and outgoing
IPv6 Tunnel broker service	IP protocol 41	incoming and outgoing
IPSec NAT-Traversal	UDP/4500	incoming and outgoing
Cisco IPSec VPN over TCP	TCP/10000	outgoing
PPTP VPN	IP protocol 47 (GRE) TCP port 1723	incoming and outgoing outgoing
SSH	TCP port 22	outgoing
HTTP	TCP port 80 TCP port 443 TCP port 3128 TCP port 8080	outgoing outgoing outgoing outgoing
Mail sending	TCP port 465 TCP port 587	outgoing outgoing
Mail reception	TCP port 143 TCP port 993 TCP port 110 TCP port 995	outgoing outgoing outgoing outgoing
FTP (passive)	TCP port 21	outgoing

Adherence to the following specifications is RECOMMENDED:

- NAS or local AAA Servers:
  - Inclusion of hotspot location information with the Operator-Name attribute in authentication requests as per RFC 5580.
  - Requesting a Chargeable-User-Identity value from the IdP, as per RFC 4372.

- local AAA Servers (in its absence, FLRS):
  - Logs of all authentication requests and responses SHOULD be kept. The minimum log retention time is six months, unless national regulations require otherwise. The information in the requests and responses SHOULD, as a minimum, include:
    - The time the authentication 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.
    - If present, the value of the Chargeable-User-Identity attribute.
    - The result of the authentication.

- Network:
  - network access to roaming visitors SHOULD not be port-restricted at all (i.e. in addition to the minimum list of open ports from above, allow all outgoing communication). Where this is not possible, the number of filtered protocols SHOULD be kept as low as possible.
  - The use of NAT SHOULD be avoided.
  - IPv6 connectivity SHOULD be supplied.
  - Service providers SHOULD NOT deploy application or interception proxies. Service providers deploying application or interception proxies MUST NOT use the proxy to require users to submit personal information before gaining access to the Internet, and 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.

6.3.4 Specifications and Operational Requirements: End-user Devices

- Requirements for user devices:
  - IEEE 802.1X.
  - Supplicant software with support for at least one EAP type capable of mutual authentication.

7 Liability and Branding

7.1 Liability

The Article 9 of the GEANT Consortium Agreement regulates the liability issues arising between the Parties participating in the European eduroam service.

7.2 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 this, in order to promote user awareness and ensure a high level of trust in the brand and service.

References

[eduroam]	http://www.eduroam.org
[eduroam Database]	http://monitor.eduroam.org/database.
[IEEE 802.1X]	http://www.ieee802.org
[F-Ticks]	http://monitor.eduroam.org/f-ticks/howto.php http://monitor.eduroam.org/f-ticks/
[GeGC]	http://www.eduroam.org/downloads/docs/eduroam_Compliance_Statement_v1_0.pdf
[Monitoring]	http://monitor.eduroam.org/.
[Security Incidents]	http://www.geant.net/service/multidomainsecurity/Security_Incidents/Pages/
[TTS]	http://tts.eduroam.org

Glossary

AAA	Authentication, Authorisation and Accounting
AH	Authentication Headers
CERT	Computer Emergency Response Team
CET	Central European Time
DNS	Domain Name Server
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol Transport Layer Security (StB IETF)
eduroam	EDUcation ROAMing
ESP	Encapsulating Security Payloads
ETLRS	European Top-Level RADIUS Server
FLRS	Federation-Level RADIUS Server
FTP	File Transfer Protocol
GeGC	Global eduroam Governance Committee
GPS	Global Positioning System
gTLD	generic Top Level Domain
HI	Home Institution
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IdP	Identity Provider

IKE	Internet Key Exchange
IPSec	IP Security (StB IETF)
MAC	Media Access Control
NAS	Network Access Servers
NAT	Network Address Translation
NREN	National Research and Educational Network
NREN PC	National Research and Educational Network Policy Committee
NRO	National Roaming Operators
NTP	Network Time Protocol
OT	Operations Team
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-In User Service (StB IETF)
RI	Remote Institution
RI	Remote Institution
SA5	Service Activity 5
SG	Steering Group
SNTP	Simple NTP
SSH	Secure Shell
TCP	Transmission Control Protocol
TLD	Top-Level Domain
TLRS	Top-Level RADIUS Server
TLS	Transport Layer Security
TTS	Trouble Ticketing System
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WPA2	Wi-Fi Protected Access, version 2

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 service 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 (notebook, PDA, smartphone, tablet, etc.) and the home authentication server. This is achieved by using mutual-authentication protocols such as EAP-TTLS, 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 Operations 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 IEEE 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 IEEE 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”).