

05.04.07

Deliverable DJ5.0.1: Plan for Transition of JRA5 Roaming (eduroam) into Production Service



Deliverable DJ5.0.1

Contractual Date:	31/07/06
Actual Date:	05/04/07
Contract Number:	511082
Instrument type:	Integrated Infrastructure Initiative (I3)
Activity:	JRA5
Work Item:	0
Nature of Deliverable:	R (Report)
Dissemination Level	PU (Public)
Lead Partner	DFN
Document Code	GN2-06-257v3

Authors: J. Rauschenbach (DFN), T. Kersting (DFN), M. Milinovic (CARNet/Srce), M. Stanica (DFN), K. Wierenga (SURFnet), S. Winter (RESTENA), T. Wolniewski (NCU), JRA5 group

Abstract

This deliverable provides a short overview of service related JRA5 documents and addresses the next steps and a roadmap towards an eduroam service.

Table of Contents

0	Executive Summary	1
1	Introduction	2
2	Service Definition	4
2.1	Generic service description	4
2.2	Service Scope	6
2.3	Service Level Agreement (SLA)	6
2.3.1	Service Availability	6
2.3.2	Service contacts	7
2.3.3	Service Reporting	7
2.3.4	Service participation and subscription	7
2.4	Information on roaming service participants	8
2.5	Service elements under development	8
2.5.1	RadSec integration	8
2.5.2	Monitoring	9
2.5.3	Test support (end-to-end testing)	9
2.6	End User Support	10
3	Organisational Structure, Roles and Responsibilities	11
3.1	The NREN PC	11
3.2	The eduroam service activity	11
3.3	The eduroam operational team	12
4	Service Rollout (roadmap)	14
4.1	Rollout Checklist	14
4.2	Timetable and Process of Transition	15
4.2.1	Main Stages of Transition	15
4.2.2	Conduct and Sequence of Transition	16

4.2.3	Roll-out support for federations	16
5	Possible Issues (Risk Analysis)	17
5.1	Issue 1: Legal regulations	17
5.2	Issue 2: Sufficient high number of participants	17
5.3	Summary Risk Analysis	18
6	Relationship to other groups	20
6.1	Relationship to NREN based federations	20
6.2	Relationship to JRA5 and TF Mobility	20
6.3	International relationship	20
7	Resources	22
7.1	Transition Process (JRA5)	22
7.2	Service Operation	22
7.3	Funding	24
8	Conclusions	26
9	References	28
10	Acronyms	29
Appendix A	European eduroam Confederation Policy Agreement	30
1.1	Main policy part	32
1.1.1	Notation (as defined in RFC 2119)	32
1.1.2	European eduroam confederation purpose	32
1.1.3	European eduroam confederation members, structure and scope	33
1.1.4	Prerequisites for joining the confederation	34
1.1.5	Leaving the confederation	34
1.1.6	Liability	34
1.1.7	eduroam branding	35
1.2	European eduroam confederation policy management procedures	36
1.2.1	European eduroam confederation policy authority	36
1.2.2	European eduroam service group	36
1.2.3	European eduroam operational team	36
1.2.4	Confederation members, institutions and end users	37

2.5	Incident handling procedures	37
2.6	Policy change announcement	37
3.	Operational requirements for participating federations	38
3.1	European eduroam security requirements	38
3.2	General requirements on confederation level	38
3.3	General requirements for federations (confederation members)	39
3.4	Technical requirements for confederation members	39

Table of Figures

Figure 2.1: eduroam confederation structure

5

0 Executive Summary

The JRA5 work item “Roaming” started with a certain level of practical experience already available. As part of the eduroam pilot, an infrastructure was created that could already be used for authentication of a user with the home institution from a different location. While evaluating the eduroam architecture based on practical experience, areas for improvement have been identified and technical alternatives investigated and tested (see also deliverable “Inter-NREN architecture”, [DJ5.1.4]).

Roaming services are available in a number of NRENs by now. From the JRA5 point of view these services are provided by federations established on a national (NREN) level. A roaming confederation has the purpose of interconnecting these national federations by means of a common infrastructure, which facilitates interoperability and exchange of data between them. A policy document for this confederation concept was developed as a pre-condition to moving eduroam to a European wide service [DJ5.1.3,2]. The policy agreement defines rules and organisational structures that are required for operating the eduroam service on a confederation level.

One element which still needs to be added to the current eduroam architecture is a monitoring and diagnostic capability on the confederation level. Corresponding tools must be provided in order to strengthen the infrastructure and to detect failures. Once these features are available and tested, Service Level Agreements (SLA) may be refined and a certain quality of service can be provided. This constitutes another pre-condition to launching an eduroam confederation service. The present document outlines the necessary steps in the eduroam transition to service process and provides a roadmap until the service start in April 2007.

In the past two years of the project, JRA5 has attempted to convey knowledge from the experienced partners to those having just started these services in their home organisations. A few JRA5 participants have reached an almost complete coverage in their user community or provide roaming services to the majority of the higher education institutions, while others are connected to eduroam with only a low number of test institutions. Parallel to the operation of the eduroam confederation service, the proposed service activity is supposed to provide financial and technical support to all participants for a limited time (end of GN2), in order to support the rollout and to push roaming to a higher penetration level.

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

1 Introduction

This deliverable outlines the installation process and operational principles of the eduroam confederation service. The following documents provide a sound technical basis for the future eduroam service. It is strongly recommended to study these documents mentioned below before joining the eduroam confederation service.

- Deliverable DJ5.1.2 describes the requirements of a roaming infrastructure.
- DJ5.1.4 provides the technical description in the architecture document.
- DJ5.1.5 provides information such as installation guidelines for the administrator of a campus or for a federation - "Roaming cookbook"
- The two parts of deliverable DJ5.1.3 provide a policy framework.
 - While DJ5.1.3,1 contains a collection of legal regulations in a number of countries of eduroam federations,
 - DJ5.1.3,2 contains the eduroam confederation policy, offering in addition a blueprint for a national eduroam policy.

The main part of the last deliverable is separately available as a policy agreement to be signed by the NRENs participating in the eduroam confederation and by the respective eduroam service provider (if it is a different organisation from the NREN). By signing this policy agreement they agree to the specified organisational and technical rules.

The eduroam confederation service will be based on the pilot, which is already in an pre-service but operational state, together with the policy outlined in DJ5.1.3,2. New architecture elements (RadSec) will be introduced, and monitoring means as well as diagnostic tools will be evaluated and installed. A more detailed description of these elements is outlined in this document. The service start is planned for April 2007. A roadmap is provided in chapter 5.

To handle the organisation and operation of the service, a GN2 service activity (eduroamSA) will be created and an operational group (eduroam operational team) will be launched.

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

The eduroamSA will be a part of the GN2 Project structure and will be managed in accordance with the Consortium and GN2 Contract with the EC. The eduroam service activity will address the planning of eduroam service-related improvements (eduroam confederation service development).

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

2 Service Definition

2.1 Generic service description

The vision of JRA5 is to grant network access to all participating members of the eduroam confederation service, at any given location within the confederation and at any time, providing nearly equivalent conditions for network access in any institution of any federation as in the home institution (local services like printing might be not available). The JRA5 goal is to create a confederation of autonomous roaming infrastructures based on open standards, where the trust level is indicated by the requirements for each member of the confederation (see the policy document DJ5.1.3,2). The authentication of a user takes place at their home institution based on the electronic identity maintained there.

The confederation service will be built upon the existent federations, in most cases organised by the NRENs. Generally the RADIUS hierarchy for a federation ends with a national top level RADIUS proxy. To interconnect several federations, an additional infrastructure is needed for providing the means to find the top level proxy of the involved federation and to transport all information in a secure way (see Figure 2.1).

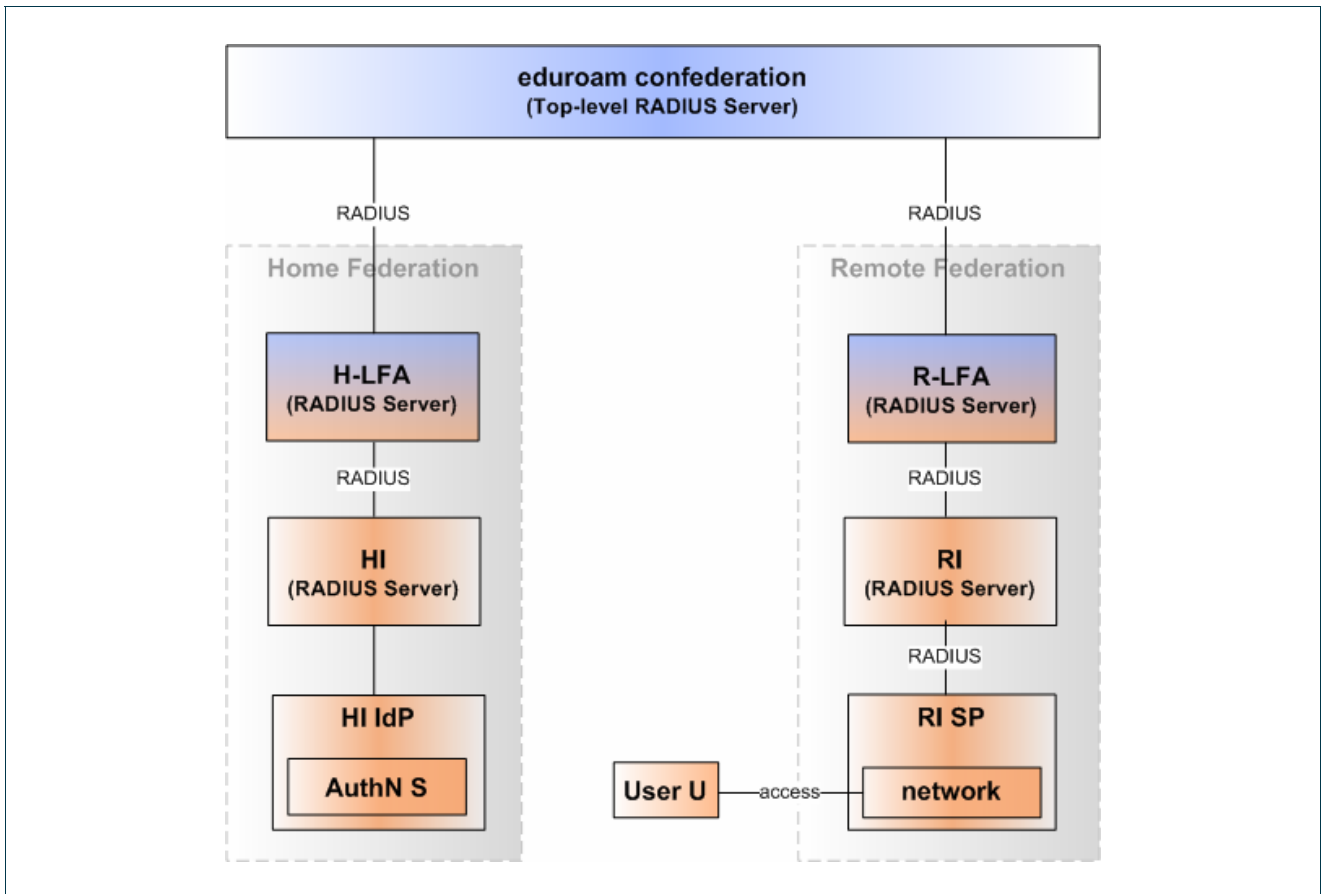


Figure 2.1: eduroam confederation structure

The confederation service

- provides the confederation infrastructure consisting of top level RADIUS proxies, and of the confederation part (the one interacting with a top level proxy) of the federation proxy servers; the latter are called Local Federation Adaptors (LFAs) in JRA5, as they serve to establish the link between the local federations and the confederation;
- establishes trust between the confederation top level RADIUS proxy and the federation level proxies;
- ensures the operability and high availability of the infrastructure by means of diagnostic and test facilities.

The notations HI and RI stand for home, respectively remote institution from the user's perspective.

2.2 Service Scope

This document is focussed on the European eduroam confederation service. The main goal is to provide a stable infrastructure to transport access requests and assertions between the participating federations. The currently involved eduroam devices are the federation top level RADIUS proxies, the confederation level servers and a small number of monitoring devices provided to the eduroam operational team.

The coverage (number of participating institutions) on the federation level influences the usefulness of the service at the confederation level. The more institutions are connected, the better are the chances to use roaming in the real world. The operation of the federation is under the autonomy of the appropriate NREN or national eduroam operator.

2.3 Service Level Agreement (SLA)

In this section a number of SLA related items are covered. This is not yet a complete SLA definition though. It is seen as an initial proposal that will be discussed and refined within the eduroamSA, and provided in a more complete form in a later version of this document.

2.3.1 Service Availability

The eduroam operational team (see chapter 3.3) will be in charge of ensuring the availability of the service at the federation top level and confederation level RADIUS servers. Therefore monitoring tools will be evaluated by the JRA5 group and installed by the eduroam operational team on appropriate computers. As most of the components are under federation control, it will be difficult to secure an acceptable service availability solely by the activity on the confederation level. A close cooperation with the (local) federation administrators, including the provision of test accounts and troubleshooting in the event of an error or abuse, is essential and must be organised in order to provide a stable service.

The goal set for the availability of the confederation infrastructure is in the range of 99%. The service pilot phase will be used to get a better estimate of the exact figure, which will be fixed for the full service establishment at the end of 2007.

To reach the high service availability on the confederation level the eduroam operational team will specify the details of the fault resolution process as part of the operational procedure. A continuous monitoring will be organised, however the working hours of operational team members will be the standard working hours only.

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

2.3.2 Service contacts

In case of a failure in the confederation service, which consists of the confederation level RADIUS and the federation top level RADIUS servers, an eduroam operational team member will contact the operator of the involved federation.

In case of a failure detected by an eduroam end user, the local support (network administrator) will help to identify the cause. Failures caused by configuration errors on a user machine are out of the scope of the confederation service. In case of a problem with the RADIUS communication, the technical contact responsible for the concerned federation will be informed by the local administrator.

The details of the technical contacts must be provided when joining the confederation and maintained accordingly. The contact data must be accessible at least by the eduroam operational team and by the federation eduroam service administrators. The federation operator, on the other hand, must know how to contact the institution network administrators. Links should be provided on the federation web pages.

2.3.3 Service Reporting

The planned reports will provide statistics on the service usage, the number of connected NRENs, the number of institutions belonging to a certain NREN, which provides roaming service to their users, the number of successful roaming events and an overview of failures that happened in a certain time period.

Monitoring results and status reports will be made available on the eduroam web site.

2.3.4 Service participation and subscription

All European NRENs are potential participants of the confederation service, independent of whether they are already participating in the eduroam pilot or not. The value provided by the eduroam service to the research and education community grows with the number of federation members, and therefore with the availability of network access for end users at as many locations as possible.

The condition for participation in the eduroam pilot was the provision of at least one operational top level RADIUS proxy and one connected institution tested against the confederation level RADIUS proxy (root). The intention was to make it possible for federations to join the pilot with minimum effort.

In the next step, beginning with the service start, participation will additionally require signing the policy document by the federation in order to raise the level of trust in the confederation. By signing the policy document, the federation agrees to fulfil the specified requirements such as proper user identity management for their roaming federation participants, and the technical and operational conditions formulated in the confederation policy. This will significantly raise the level of trust. However, a different treatment of NRENs that

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

have signed the policy agreement and those, not signing yet is not foreseen in the migration phase until the next version of the policy document is provided.

The NREN PC needs to approve a request for participation if the requestor is not a GÉANT2 consortium member. The communication between pilot participants and service participants will be supported until full establishment of the confederation service, including the updated policy, by the end of 2007.

2.4 Information on roaming service participants

An overview of the federations participating in the eduroam pilot is given in the maps that can be found on the eduroam web page www.eduroam.org. The clickable maps often provide more detailed federation-specific information like the connected institutions; in case where the federations provide this information. A more fine-grained presentation would be very useful in order to find out where eduroam access points are located, but this requires substantial support from the connected federations and is not yet generally available. At the time of writing 29 national European research networks are connected as federations to the pilot, with more than 500 institutions. Just a few NRENs achieved full national coverage of their member institutions by now. Other participants are running the RADIUS federation level proxy with just a few institutions connected. Most of the participants are currently between these 2 positions. Some institutions within national federations act as an IdP while not offering the service to visiting users, some do not offer a similar service at all. It remains a primary task of the service activity to improve the situation.

2.5 Service elements under development

Some service elements are still missing in the eduroam pilot. This is partially due, as in the case of RadSec, to the on-going standardisation process and the test of a second implementation, or as for the monitoring elements in the need for further development work.

2.5.1 RadSec integration

One of the promising eduroam architectural extensions, which JRA5 classified as a candidate for production is RadSec (for a static configuration only, dynamic peer-to-peer functionality will be added later on, see DJ5.1.4). This improves the RADIUS protocol related to security by using Transport Layer Security (TLS) and by using TCP instead of UDP.

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

RadSec is available on the Radiator product, based on a white paper. JRA5 is seeking to implement a second implementation based on ANSI-conformant C code. The aim is to create a lightweight proxy that can be installed alongside arbitrary RADIUS implementations, thus providing RadSec capabilities to each RADIUS device, independent of vendor, computing capacities or platform. A prototype is already available and proven to interoperate with Radiator. The JRA5 goal is to fulfil the roaming requirement of using standard-compatible solutions. Work is in progress to bring RadSec to a standard level in the IETF. The latter is not feasible in the short time frame until the service start, but is mentioned as justification for the RadSec integration into the confederation service.

Part of the federation RADIUS infrastructure will be RadSec enabled until the service start in April 2007. The integration will be done by at least three participants of the eduroam pilot; others are expected to follow.

2.5.2 Monitoring

The purpose of monitoring the eduroam infrastructure on the confederation level is to have sufficient information about the availability and quality of service, so that failures can be discovered and repaired as fast as possible. A collection of data showing the service availability is considered useful.

Almost every eduroam partner has a number of monitoring tools selected or developed in order to provide information about availability and functionality of elements of the infrastructure. The challenge is to find the best suited monitoring solution for the confederation infrastructure.

As initial step a weather map showing the actual state of the confederation service infrastructure would be sufficient. A good example of federation server availability can be found here:

<http://radius-rap.a3.surf.net/reports/radius-check-eduroam/stateoverview.html>

The eduroam operational team will be in charge of providing a similar overview tool for the confederation service until end of April 2007.

2.5.3 Test support (end-to-end testing)

An additional maintenance application is end-to-end testing of a path through the infrastructure. This can be organised in several steps. Having a test account installed at every national RADIUS top level proxy will be useful for checking the upper part of the hierarchy (national federation level RADIUS server – confederation level RADIUS server – federation level RADIUS server). Tests down to an institutional user involves the federation eduroam operator and the institutions' administrators, and will most likely happen on a less regular time scale, when a new participant joins, or when a failure occurs.

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

From the point of view of the confederation service, it would be very helpful to enable end-to-end testing based on facilities from federation members such as universities and research institutes. A test account similar to a real user's account should be configured and used for carrying out tests at the participant institutions, in order to report potential problems. This should provide good indicators for the usability of the eduroam confederation infrastructure. The test account should be available for the eduroam operational team, but would be helpful for the local operator as well. End-to-end testing requires a strong coordination between the participants of the confederation.

2.6 End User Support

The confederation service does not directly deal with end users. The end user in a federation is normally connected to a roaming service. The ability of an end user to connect to the roaming service is therefore based on the decision and the support of his home institution, which itself is a federation participant. The home institution is also the first address for the end user support, helping with the configuration of clients and the provision of information and trouble-shooting. These issues are thus out of scope of the confederation service and of this document. However, this function can be supported by the expert knowledge in the whole community, as well as by the documents and cookbooks such as [DJ5.1.5] developed in the GÉANT2 research and service project parts.

3 Organisational Structure, Roles and Responsibilities

3.1 The NREN PC

The NREN PC is the policy authority for the European eduroam confederation and has the responsibility for all high-level decisions and for the overall management of the Service Activity: reviewing and/or amending the work programme, allocation or re-allocation of funding, approval of the annual budget and definition of use of the infrastructure. The NREN PC is responsible for accepting new confederation members, if they do not belong to the GÉANT2 consortium. The policy agreement needs to be signed by the NREN (and additionally by a national eduroam service provider if different from the NREN) willing to become a member of the eduroam confederation. The GÉANT2 coordinator will store these signed documents.

The NREN PC might be approached in case of a conflict between two member federations as part of the de-escalation procedure.

Appendix A contains the policy agreement that needs to be signed by the NRENs which are applying for a membership in the European eduroam confederation. This policy agreement contains the essential requirements that need to be fulfilled by the applicants. A Letter of Intent is requested by those federations unable to sign the policy agreement at the present time, in order to become a voting member of the eduroamSA. In this letter the future confederation member must express the will to comply with the policy agreement as well as a date for the migration.

3.2 The eduroam service activity

As defined in the DJ5.1.3,2, the European eduroam Service Activity (eduroamSA) prepares the integration of new members to the confederation, and recommends policy decisions which need to be approved by the NREN PC. The eduroamSA decides on technological matters concerning the eduroam service. It is composed

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

of representatives from the confederation members (voting rights) and non-members (observer status). Eduroam confederation members, who do not belong to the GÉANT2 consortium can have only observer status in eduroamSA.

The eduroamSA delegates the task of executing the European eduroam confederation mission to the 'European eduroam operational team'. The eduroamSA is the point of contact for TF-mobility and JRA5.

The NREN PC will approve the activity leader of the eduroamSA based on the proposal of the eduroamSA initial meeting. The activity leader is a member of the Technical Committee.

The list of eduroamSA tasks includes:

- Supervision of the operational team
- Recommendations on diagnostic tools and supporting scripts
- Further policy development (in coordination with JRA5/TF Mobility)
- Integration of further research results from JRA5/TF Mobility
- Application of trust means (operation of the JRA5 eduGAIN CA)
- 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
- Definition and improvement of incident handling procedures
- Organisation of training events for the operational personnel (wherein eduroamSA provides the content and NA8 assists in organisational matters)
- Provision of a virtual home for the operational team
- Support of the roaming federations (provision of federation web presentation in English and with appropriate access information, exchange of technical knowledge, motivating events etc).

3.3 The eduroam operational team

The daily operation will be delegated to the eduroam operational team, which was appointed in the initial set-up by the eduroam service activity meeting. This needs to be approved by the project management to ensure the budget/funding.

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

The eduroam SA leader will be as well the operational team leader.

The list of eduroam operational team tasks includes:

- Running the confederation part of the eduroam infrastructure, incl. the top level servers
- Monitoring the confederation/federation level servers (root and country top level)
- Handle fault resolution procedures (including a trouble ticket system)
- Support for new member federations (providing relevant documentation in cookbook form to assist in the configuration, serving as possible test partner in the set-up phase)
- Coordination of trust means (eduGAIN CA usage, CRLs)
- 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 confederation web pages.

The confederation level RADIUS servers (two at the time of writing) are run by TERENA with technical support from SURFnet and Uni-C. Therefore people working in those organisations having the appropriate technical experience are suggested to work in the operational team. The eduroamSA suggested CARNet/Srce based on technical knowledge collected in one of the biggest eduroam regions and TERENA with a special focus on the maintenance of the eduroam web pages as additional eduroam operational team members.

4 Service Rollout (roadmap)

The eduroam confederation service rollout plan consists of several elements:

- a) A checklist of points that have to be addressed before the service start can be considered;
- b) A description of the stages of the transition.

4.1 Rollout Checklist

The following tasks have to be accomplished before the rollout can be considered complete:

- Approval of the policy (NREN PC): done, August 06
- Derivation of a condensed policy document from DJ5.1.3,2: done, October 06
- Providing the policy document to the NRENs for signing: done, November 06
- Establishment of the eduroamSA and eduroam operational team: January 07
- Collecting the signed policy documents: from November until end of March 07
- Collection of the commitments by the eduroam SA members, development of the work plan and budget proposal along the lines of the plans in the GN2 Technical Annex
- Technical improvements (monitoring, RadSec): March/April 07
- Service start: April 07 (after technical conditions are met as well)

4.2 Timetable and Process of Transition

4.2.1 Main Stages of Transition

The main stages of transition are outlined below.

4.2.1.1 Stage 1: Organisational set-up

The organisational set-up is sketched in the policy document (DJ5.1.3,2) and in the chapter 3 of this document. Two different methods are envisioned for the distribution of the policy document to be signed: via mailing lists and via the NREN PC. This document provides additional information for the service participants. Collecting signatures from the federation partners will be organised by the JRA5 chair until the eduroamSA is launched, and then handed over.

The eduroamSA will be open for all eduroam participants. The APM (Access Point Manager) model seems to be well suited (compare with <http://www.geant2.net/server/show/nav.759>). A limited amount of funding (in the range of 2 man months) will be planned for every SA partner for the service roll-out support in their federations. The tasks of the eduroam SA are listed in 3.2. The nomination of an eduroam federation representative by each member is crucial for active participation in the service development. The establishment of the eduroam operational team before the service starts is essential.

JRA5 stays responsible for the preparation of the eduroam service until the eduroamSA will be operational. The establishment date is defined in the roadmap. JRA5 is not supposed to run the production service, its role being limited to service preparation and further development work. The establishment of the eduroam operational team is not equivalent to the service start date. The new team should be given time to adopt the results from JRA5 and add other operational and support means.

4.2.1.2 Stage 2: RadSec integration

With the integration of RadSec, trust relations between proxies will be based on certificates. The eduGAIN CA will be used for this purpose and is already available for tests.

A number of volunteers (RESTENA, SURFnet, FCCN, ARNES, Nicholas Copernicus University of Torun, DFN) are identified, but the list is open and other eduroam participants are invited to join. For the commercial RADIUS product Radiator (OSC) the possession of an appropriate licence is required for the participation in the pilot. The new developed RadSec implementation does not imply usage limitations and can interoperate with different RADIUS products.

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

4.2.1.3 Stage 3: Monitoring of the infrastructure

Stage 3 will involve several tools on diagnostics and monitoring. The evaluation of available software, its adaptation or new development is on the agenda of the JRA5 work plan for the next couple of months (in cooperation with eduroamSA and eduroam operational team after successful launch). The goal is to have a monitoring tool available according to the example given in chapter 2.5.2 by end of March 2007.

4.2.1.4 Stage 4 Service activity tasks and service start

Stage 4 will be the official start of the pilot service with the Service Level Agreements described in chapter 2. More details will be provided by the eduroamSA based on practical experience.

4.2.2 Conduct and Sequence of Transition

Stage 1 has already started. Stages 2 and 3 are on going in parallel. The final one (service start) is based on the successful completion of the other 3 stages and is planned for April 2007.

4.2.3 Roll-out support for federations

In order to help the eduroam service gain more members and to develop the service inside of the federation in an appropriate way, it is opportune to provide a small funding for a limited time (a couple of person months until end of GN2). This can be used to help deploying or advancing the eduroam infrastructure on the federation level in terms of availability and stability. The funding will be addressed in a separate budget proposal.

5 Possible Issues (Risk Analysis)

5.1 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.

5.2 Issue 2: Sufficient high number of participants

The value of the eduroam confederation 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. Big efforts are needed to reach a critical mass.

5.3 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 how probability and/or impact of the risk are dealt with.

The responses to risks are classified as:

- Avoid: the risk is already eliminated
- Transfer: ensure that consequences of risk only impacts the respective federation participant

ID	Description	Impact	Probability	Impact Area	Response to risk
1	Confederation RADIUS servers delayed	high	low	S, P	Avoid: The servers are already in place as part of the eduroam pilot.
2	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.
3	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.
4	Confederation RADIUS server fail	high	low	S, P	Avoid: The Confederation RADIUS servers are completely redundant
5	Federation RADIUS servers fail	medium	medium	S	Avoid: The Federation RADIUS servers are completely redundant as required by the policy
6	Institutional RADIUS servers	low	medium	S	Transfer: The Institutional RADIUS servers are solely in the responsibility of the respective

	fail				institution
--	------	--	--	--	-------------

6 Relationship to other Groups

6.1 Relationship to NREN based federations

The interaction with the federations will be organised via their representatives in the eduroamSA. An appropriate mailing list will be created. The basic idea is that every participating NREN or eduroam operator on behalf of an NREN should nominate a person for the eduroamSA.

Items of this interaction are technical support at the federation level including failure recovery, coordination in abuse cases, exchange of experience and cooperation in the operation of the confederation.

6.2 Relationship to JRA5 and TF Mobility

JRA5 and TF Mobility are continuing to work on the development of eduroam. The main JRA5 work items of this development activity are new protocol elements, improvements of the eduroam architecture and the integration of SAML into the roaming infrastructure (DAMe). TF Mobility provides support in dissemination and in broadening the discussion platform based on a bigger list of interested people, thus providing feedback and ideas for future technologies. Both groups will not be directly involved in the service operation, but can assist the eduroamSA whenever this is needed.

6.3 International relationship

The eduroam service aims at the provision of a roaming service for the research and education community in Europe as part of a global roaming concept covering also other parts of the world. However, like technical solutions, roaming operator requirements and policies might differ between Europe and other regions.

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

Therefore a harmonisation of the rules will be necessary for the global service. The harmonisation process is out of scope of this document. The eduroam service described here is focussed on Europe only.

The European representation in the global eduroam cooperation will consist most likely of chairs of JRA5, eduroamSA and TF Mobility. The cooperation between confederations will require a common policy document or special agreements in the long run. The coordination and strategic development might be the scope of the existing global working group (eduroam gwg), however this group will probably need reactivation and reconsolidation.

7 Resources

7.1 Transition Process (JRA5)

The service preparation is in the responsibility of JRA5 based on the resources of work item 1 (Roaming). The following partners will be involved in the preparation work:

Stage 1: Organisational set-up: Uni-C, SURFnet, DFN, RESTENA and CARNet/Srce

Stage 2: RadSec integration: RESTENA, SURFnet, FCCN, ARNES and DFN

Stage 3: Monitoring the Infrastructure: RESTENA, CARNet/Srce, ARNES, CESNET, Uni-C and SURFnet

7.2 Service Operation

The eduroamSA will take over the responsibility for the service operation with the official start of the pilot service in April 2007. The following partners will be involved in the operation and maintenance of the production eduroam services, with the following manpower and other resources (the list below is the set of potential participants in Europe known by now, (Yes) indicates already received approval of interest in participation in the eduroamSA):

Austria: ACONET

Belgium: BELNET

Bulgaria: ISTF

Croatia: CARNet/Srce (Yes)

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

Czech Republic: CESNET (Yes)

Denmark: Uni-C (Yes)

Estonia: EENet

France: Renater/CRU

Finland: Funet/CSC (Yes)

Germany: DFN (Yes)

Greece: GRNET

Hungary: HUNGARNET

Ireland: HEANet (Yes)

Italy: GARR (Yes)

Latvia: LATNET/LANet

Lithuania: LITNET

Luxembourg: RESTENA (Yes)

Malta: UoM

Netherlands: SURFnet (Yes)

Norway: UNINETT

Poland: PSNC/Nicholas Copernicus University of Torun NCU (Yes)

Portugal: FCCN (Yes)

Romania: RoEduNet

Slovakia: SANET

Slovenia: ARNES (Yes)

Spain: Red.es/RedIRIS (Yes)

Sweden: Sunet/SWAMI

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

Switzerland: SWITCH (Yes)

UK: Ukerna

Note: In some cases the roaming federation is not operated by the “official” GN2 partner (examples: Poland, Latvia, France, Croatia). It is expected that the eduroam operator is acting on behalf of the NREN in these cases. An additional check for funding possibility will become necessary in some cases.

The following participants have already signed the policy agreement: RedIRIS, CSC, GARR, RESTENA and HEANet.

7.3 Funding

Service fees from participating NRENS for the confederation service are not planned at the current state. The principle of mutual support of the visiting users will be applied. However, every service has a cost. The obvious parts involving costs are the eduroam root proxy servers (we will use the existing ones from the pilot infrastructure), the monitoring workstations (one per eduroam operational team member) and the operation of the service (manpower for maintaining the infrastructure; monitoring and error discovery).

Equipment type	Number of pieces	Costs
Monitoring workstations	4	8 K€
Additional eduroam root server	1	2 K€

Table: Equipment costs

For the live team of the GN2 project manpower funding is needed:

- for the eduroamSA leader,
- for the eduroam operational team members,
- for the eduroamSA participants.

It is planned to provide funding in the magnitude of 0,5 FTE to the eduroamSA leader and to each of the eduroam operational team members in the remaining project time. The initial idea for funding involves about 0,1 FTE (1-2 person months) for every partner of the SA (see roll-out support). A request for funding will be provided to the GN2 management (EXEC) by the JRA5 chair. Based on the experiences and the actual need an appropriate funding will be incorporated in the year 4+ budget.

Purpose	FTE (summary p.a.)	Cost y3 (6 month)	Costs y3 in K€	Cost y4+ (18 months)	Costs y4 in K€
EduroamSA leader	0,5	0,25	12	0,75	36
Operational team member (4)	2,0	1,0	40	3,0	120
EduroamSA member (30)	3,0	1,5	60	4,5	180
Summary	5,5	2,75	112	8,25	336

Table: Personal costs

The positions eduroamSA leader and operational team member are the basic personal costs of an eduroam service. The funding for eduroamSA members will be needed in the rollout phase only.

8 Conclusions

This document outlines the process of transition to service. It describes the current state as starting point and how to proceed. The important next steps are the consolidation of the eduroam confederation and the eduroamSA, putting the eduroam operational team into work and developing initial technical support (monitoring etc). Every NREN from the consortium interested in participating in eduroam as a federation, shall delegate one person as a representative for the eduroamSA. Signing the policy agreement is an essential requirement to join the eduroam confederation. If this is not yet possible due to the level of development of the federation, a Letter of Intent to sign the policy agreement, once the conditions are met, is sufficient to join the eduroamSA for the migration phase. Letter of Intent should clearly state the deadline for signing the policy. Without the above mentioned commitments the representative of the NREN might still participate in the eduroamSA, but voting rights and funding will not be provided (observer status). Eduroam confederation members, who do not belong to the GÉANT2 consortium can have only observer status in eduroamSA.

The eduroamSA will be set-up in compliance to the GÉANT2 guidelines.

The service is expected to start in project year 3 (around April 2007) under the name of “European eduroam confederation pilot service”. Once it has been running successfully for a number of months, the term “pilot” will be removed from the service name. Technical and policy related feedback will be collected and incorporated in new versions of the appropriate documents.

The eduroamSA leader, the JRA5 work item leaders and the GN2 project management will monitor the transition process.

Following the experience gathered during the pilot phase, an informal, second version of this deliverable will be produced within 6 months. It will include but not be limited to the elements listed below:

- Methods to assess the degree of conformance to the eduroam operational requirements, to be applied on those federations requesting to join or to interoperate with the eduroam confederation.
- Methods to re-evaluate the conformance on a regular basis, or triggered by complaints/trouble ticketing information.

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

- Strategy for indicating and evaluating the coverage, which may include the number of institutions, the number of provided identities and the number of access points, related to the size, history of eduroam provision and development level of the R&D networking at the respective NREN.
- The decision-making procedures in the eduroamSA group. (Present considerations point to a solution, by which the official representatives of GN2 members which have joined the eduroam confederation or have sent a Lol to join, have voting rights, while other participants act as observers).
- Interactions between the eduroamSA and Operational Team, described in a form of workflows. The authority/responsibility of the relationship will be examined.
- Development of operational procedures regarding the relation between the confederation (represented by the eduroamSA), the Operational Team and the federations, including the trouble ticketing procedures.
- Means to coordinate with NA8 for education and training and with NA2 for dissemination of information on eduroamSA progress.

9 References

- [DJ5.1.1] <http://www.geant2.net/upload/pdf/GN2-04-111Final.pdf>
- [DJ5.1.2] <http://www.geant2.net/upload/pdf/GN2-05-71v6.pdf>
- [DJ5.1.3,2] <http://intranet.geant2.net/server/show/conMediaFile.4550>
- [DJ5.1.4] http://www.geant2.net/upload/pdf/GN2-06-137v5-Deliverable_DJ5-1-4_Inter-NREN_Roaming_Technical_Specification_20060908164149.pdf
- [DJ5.1.5] http://www.geant2.net/upload/pdf/GN2-06-258v8-DJ5-1-5_Inter-NREN_Roaming_Infrastructure_and_Service_Support__Cookbook_1st_Version.pdf

10 Acronyms

In JRA5 used acronyms can be found in the JRA5 Glossary of Terms [DJ5.1.1]. Additional terms are listed below.

CRL	Certificate Revocation List
DAMe	Deployment of AA Mechanisms in eduroam (JRA5 subproject)
eduGAIN CA	eduGAIN Certificate Authority
eduroam gwg	eduroam global working group

Appendix A **European eduroam Confederation Policy Agreement**

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

European eduroam confederation policy

Version 1.1



This version corresponds with the GÉANT2 JRA5 deliverable “Roaming Policy and Legal Framework Document – Part 2”

http://www.geant2.net/upload/pdf/GN2-06-080v4-Deliverable_DJ5-1-3_2_Roaming_Policy_and_Legal_Framework-Part2_20060719163405.pdf

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

1. Main policy part

1.1 Notation (as defined in RFC 2119)

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

1.2 European eduroam confederation purpose

The purpose of the European eduroam confederation is to provide mutual roaming network access to its members: European eduroam federations, their participating institutions and the end users. The confederation MAY peer with other roaming infrastructures. The appropriate policy rules SHALL be defined in a confederation peering document.

The goal of the confederation is to increase the coverage of eduroam in European research and educational networks and to establish eduroam as a long-term service that SHALL be maintained and further developed.

1.3 European eduroam confederation members, structure and scope

The members of the European eduroam confederation are the organisations responsible for national roaming infrastructure (NRENs). The technical operation MAY be outsourced to an institution working on behalf of the NREN.

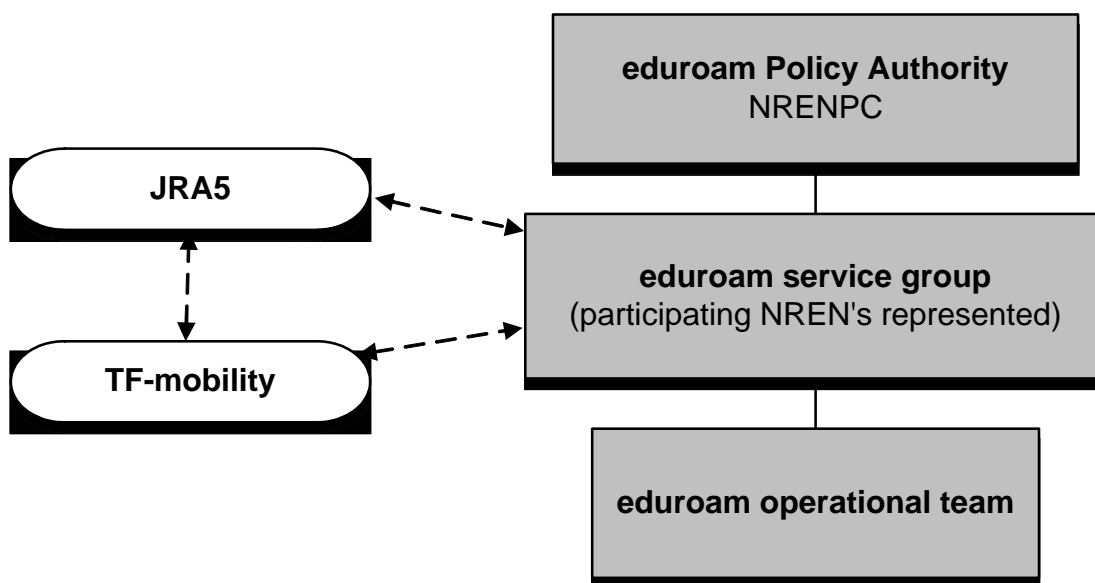


Figure 1: European eduroam confederation levels

The European eduroam confederation will be organised under the umbrella of the National Research and Educational Network Policy Committee (NREN PC), which in turn delegates the management of the European eduroam confederation to the 'eduroam service group' where all participating federations are represented. The day to day running of the confederation business will be delegated to the 'eduroam operational team' which will be appointed by the eduroam service group.

The European eduroam confederation therefore consists of the following levels:

- 1) National Research and Educational Networks Policy Committee (NREN PC) as the Policy Authority for the European eduroam confederation.
- 2) The eduroam service group consists of representatives from all participating federations. Non-members can be invited as observers.
- 3) The operational team, appointed by the service group.

The TERENA Task Force Mobility (TF-mobility) as well as the Géant2 Joint Research Activity 5 (JRA5) will provide expertise to the eduroam service group as well as receive and further disseminate input and developments from the eduroam service group. TF-mobility and JRA5 will also fuel future development of the service.

1.4 Prerequisites for joining the confederation

National eduroam federations can join the European eduroam confederation under the following conditions:

1. The national eduroam federation accepts the European eduroam confederation policy.
2. The national eduroam federation conforms with the operational requirements for participating federations (see chapter 3).

When the European eduroam operational team (see chapter 2.3) confirms that the federation adheres to (1) and (2), and when (1) is acknowledged by signing the present 'European eduroam confederation policy', the prospective member MAY be approved by the NREN PC. Following approval, the federation becomes member of the confederation. This will be announced at the official web page of the confederation. The physical signed document will be kept by the eduroam service group.

1.5 Leaving the confederation

Any member of the European eduroam confederation can at any time leave the confederation with a three months notice. This is necessary to ensure that all practicalities can be taken care of in a timely manner (updating web sites, top level servers etc.)

1.6 Liability

The European eduroam confederation is not liable for any damages, including but not limited to loss of profit, loss of savings and incidental or consequential damages resulting from its activities including the operation of the European eduroam confederation. Accreditation of an authority does not imply any assumption of liability by the European confederation.

The European eduroam confederation is not responsible for the actions or faults of any of its members AND will not accept any liability caused by the violation of any national or international laws or rules or AUPs by its members and their users.

Indemnity regarding other confederation members or end users is explicitly excluded. The confederation shall not

be liable for damage caused to the confederation member or its end user and the confederation member shall not be liable for damage caused to the confederation due to the use of the roaming services, service downtime or other issues relating to the use of the roaming services.

1.7 eduroam 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.nl).

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.

2. European eduroam confederation policy management procedures

2.1 European eduroam confederation policy authority

The role of the European eduroam policy authority will be fulfilled by the NREN PC. The NREN PC will approve new members and changes to the policy suggested by the eduroam service group and act as a clearing house for all policy and management related problems in eduroam. The NREN PC delegates the task of the operational maintenance and development of eduroam to the service group.

2.2 European eduroam service group

The European eduroam service group prepares the integration of new members of the confederation, and negotiates and recommends policy decisions to be approved by the NREN PC. It coordinates activities with relevant forums and groups active in the network roaming field. It decides on technological matters concerning eduroam. It delegates the authority of enforcing the European eduroam confederation policy on an annual basis to the 'European eduroam operational team'. The European eduroam service group is the point of contact for TF-mobility and JRA5.

2.3 European eduroam operational team

The eduroam operational team will be appointed by the eduroam service group to work on its behalf in the purpose of gaining flexibility in the operational part of eduroam, and handling the day to day running of the confederation business. The operational team reports to the eduroam service group.

It also has the task of assisting with the dissemination of eduroam and the connection of new confederation members, as well as with connecting to other eduroam confederations. Incidents will be handled by the eduroam operational team according to the corresponding procedures.

2.4 Confederation members, institutions and end users

The confederation members **MUST** act as the policy enforcement authorities for their federation participants (institutions). The federation participants **MUST** likewise act as the policy enforcement authorities for their end users. The eduroam operational team is obliged to enforce the present policy either proactively, reactively or both, according to the incident handling procedures described below. This **MUST** be done in co-operation with the relevant confederation members. Decisions of a strategic nature will be escalated to the eduroam service group and, if needed, to the NREN PC.

2.5 Incident handling procedures

In the case of an abuse of eduroam, or any serious policy violation, escalation procedures **MUST** be undertaken in a timely manner. The European eduroam operational team will react in the following ways, including, where appropriate, an escalation to the eduroam service group (which might further escalate to the NREN PC), depending on the level of violation:

- issue a notice of the policy breach and initiate an evaluation process (operational team level)
- decide on a temporary quarantine period (eduroam service group level/NREN PC level)
- decide on a disqualification from confederation (NREN PC level)
- confirmation and announcement of termination with grievance process (NREN PC level)

Operational and detailed incident handling procedures are defined (determined) by the eduroam operational team.

2.6 Policy change announcement

All policy changes will be announced in writing to all confederation members with at least 3 months notice before becoming effective.

3. Operational requirements for participating federations

3.1 European eduroam security requirements

The security of the user credentials **MUST** be preserved and privacy regulations **MUST** be observed. The European eduroam confederation service level agreement contains the relevant technical details.

Eduroam **MUST** always provide trustworthy and secure transport of all messages traversing the eduroam infrastructure.

User credentials **MUST** stay securely encrypted end-to-end between the personal device and the identity provider (home institution) when traversing the eduroam infrastructure. This ensures that they will only be used by the end users and their identity providers.

Confederation members (NRENs) and federation participants (institutions) taking part in eduroam **MUST** ensure that eduroam servers and services are maintained according to the specified best practices for server build, configuration and security. This has the purpose of maintaining a generally high level of security, and thereby trust in the eduroam confederation (see European eduroam confederation service level agreement). The confederation members **MUST** ensure that the participating institutions are aware of their responsibility to establish an appropriate level of security.

3.2 General requirements on confederation level

The European eduroam operational team guarantees that the necessary infrastructure to run the official confederation services is operational and maintained according to server build, configuration and security best practices. The European confederation server **MUST** be replicated at least one time and placed in geographically separate locations to ensure a resilient and robust European eduroam service.

The eduroam operational team also ensures that reported incidents concerning the eduroam confederation will be handled in a timely manner. All such incidents **SHALL** be logged and presented in an aggregated form to the eduroam service group and to the NREN PC.

3.3 General requirements for federations (confederation members)

Each member joining eduroam MUST establish the necessary infrastructure to support eduroam services and to ensure that these are maintained according to the specified best practices.

Each confederation member MUST act as the eduroam authority towards its federation participants, and ensure that they observe the security requirements of the European eduroam confederation policy.

The federation participants are responsible for proper user management and the authentication and authorisation of eligible users only.

Misuse and breaches of the European eduroam confederation policy MUST be reported to the European eduroam operational team and SHALL be presented to the eduroam service group and escalated to the NREN PC in serious cases.

Each confederation member MUST 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 in English and SHOULD be in local language(s) as well. The webpage SHOULD be found at <www.eduroam.TLD>.

3.4 Technical requirements for confederation members

10.1.1.2 *Technical contact*

Confederation members MUST designate a technical contact that can be reached using email and telephone during working hours. The contact MAY be either a named individual or an organisational unit. Arrangements MUST be made to cover for absence owing to eventualities such as illness and holidays.

10.1.1.3 *Confederation member level RADIUS servers*

1. RADIUS clients and servers MUST comply with RFC2865 (RADIUS) and RFC2866 (RADIUS accounting).
2. All relevant logs MUST be created with synchronization to a reliable time source.

3. Confederation members' RADIUS proxy servers **MUST** be reachable from the confederation RADIUS proxy servers on ports UDP/1812 and UDP/1813, or ports UDP/1645 and UDP/1646, for authentication and accounting respectively.
4. Confederation members' RADIUS proxy servers **MUST** respond to ICMP Echo Requests sent by the confederation RADIUS proxy servers.
5. Confederation members **SHOULD** ensure that logs are kept of all eduroam RADIUS authentication requests exchanged; the following information **SHOULD** be recorded.
 - a. The time the authentication request was exchanged.
 - b. The value of the user name attribute in the request ('outer EAP-identity').
 - c. The value of the Calling-Station-Id attribute in the request.
6. Confederation members **SHOULD** log all eduroam RADIUS accounting requests; the following information **SHOULD** be recorded.
 - a. The time the accounting request was exchanged.
 - b. The value of the user name attribute in the request.
 - c. The value of the accounting session ID.
 - d. The value of the request's accounting status type.

10.1.1.4 *RADIUS forwarding*

eduroam resource providers **MUST** forward RADIUS requests containing user names with unknown realms to the national eduroam federation server.

eduroam resource 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.

Resource 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).

Resource providers **MUST NOT** otherwise forward requests to other eduroam participants.

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3

10.1.1.5 *Resilience*

Confederation members SHOULD deploy a secondary eduroam federation server for resilience purposes.

10.1.1.6 *Network addressing*

eduroam resource providers SHOULD provide visitors with publicly routable IPv4 addresses using DHCP.

eduroam resource 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. 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.

10.1.1.7 *802.1X Network access server (NAS)*

eduroam resource providers MUST deploy NASes that support IEEE 802.1X and symmetric keying using keys provided within RADIUS Access-Accept packets, in accordance with section 3.16 of RFC3580.

eduroam resource providers MUST assign a single user per NAS port.

eduroam resource providers MUST deploy NASes that include the following RADIUS attributes within Access-Request packets.

- The supplicant's MAC address within the Calling-Station-Id attribute.

10.1.1.8 *Application and interception proxies*

eduroam resource providers deploying application or interception proxies MUST publish information about application - and intercept proxies on their eduroam website.

If an application proxy is not transparent, the resource provider MUST also provide documentation on the configuration of applications to use the proxy.

10.1.1.9 *IP filtering*

eduroam resource providers SHOULD provide open network access to eduroam users.

10.1.1.10 *User name format requirements*

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.

10.1.1.11 *EAP authentication general requirements*

eduroam identity providers MUST configure their Extensible Authentication Protocol (EAP) server to authenticate one or more EAP types.

eduroam 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.

eduroam identity providers MUST log all authentication attempts; the following information MUST be recorded:

- The authentication result returned by the authentication database
- The reason given if the authentication was denied or failed

eduroam service providers MUST transparently proxy any EAP-type for visiting users.

10.1.1.12 Website

Every Confederation member MUST publish an eduroam website, which MUST be generally accessible from all hosts on the Internet on TCP/80. The website MUST include the following at a minimum.

- Information and links to the local federation participants
- Confederation member acceptable use policy (AUP) if available
- The eduroam logo and link to www.eduroam.org

10.1.1.13 *Service Set Identifier (SSID)*

All eduroam resource providers SHOULD implement the SSID 'eduroam'. The SSID SHOULD be broadcasted.

Overlapping IP-subnets with same SSID is known to be a problem. If this situation occurs the SSIDs of those institutions involved can be changed to 'eduroam-[inst]' (where [inst] is an easily understandable indication of institutions name). If this solution is applied the SSIDs MUST be broadcasted.

10.1.1.14 *Web redirect login transition period*

To enable a smooth transition from already installed web redirect applications to the herein described eduroam requirements, the following rule applies:

For one year (starting 01/10/2006, ending 30/09/2007) web redirect MAY be used. After this time web redirect MUST NOT be associated with the eduroam name, logo etc.

This policy document is modified only after an agreement with the NREN PC and comes into force with the signature of the representatives of the European eduroam confederation member.

Signed on behalf of the NREN by:

Signed on behalf of the roaming operator:

Name:

Name:

Signature:

Signature:

Date:

Date:

Project:	GN2
Deliverable Number:	DJ5.0.1
Date of Issue:	05/04/07
EC Contract No.:	511082
Document Code:	GN2-06-257v3