

08.11.06

Deliverable DJ5.1.3,2: Roaming Policy and Legal Framework Document - Part 2



Deliverable DJ5.1.3,2

Contractual Date: 30/11/05
Actual Date: 08/11/06
Contract Number: 511082
Instrument type: Integrated Infrastructure Initiative (I3)
Activity: JRA5
Work Item: WI 1 (Roaming)
Nature of Deliverable: R (Report)
Dissemination Level: PU (Public)
Lead Partner: SURFnet
Document Code: GN2-06-080v5

Authors: D. Simonsen (UNI-C), J. Rauschenbach (DFN), J. Howlett (Ukerna), R. Papez (ARNES), R. Castro (RedIRIS), T. Wiberg (University of Umea), K. Wierenga (SURFnet), S. Winter (RESTENA), JRA5 team

Abstract

While Part 1 of this document provided an overview on the legislation background of roaming infrastructures, Part 2 defines the policy rules for a European roaming confederation.

Table of Contents

0	Executive Summary	iv
1	Introduction	1
2	European eduroam confederation policy	3
2.1	Main part of policy document	3
2.1.1	Notation (as defined in RFC 2119)	3
2.1.2	European <i>eduroam</i> confederation purpose	3
2.1.3	European <i>eduroam</i> confederation members, structure and scope	3
2.1.4	Prerequisites for joining the confederation	5
2.1.5	Leaving the confederation	5
2.1.6	Liability	5
2.1.7	<i>eduroam</i> branding	6
3	European eduroam confederation policy management procedures	7
3.1	European <i>eduroam</i> confederation policy authority	7
3.2	European eduroam service group	7
3.3	European <i>eduroam</i> operational team	7
3.4	Confederation members, institutions and end users	8
3.5	Incident handling procedures	8
3.6	Policy change announcement	8
4	Operational requirements for participating federations	9
4.1	European <i>eduroam</i> security requirements	9
4.2	General requirements on confederation level	9
4.3	General requirements for federations (confederation members)	10
4.4	Technical requirements for confederation members	10
4.4.1	Technical contact	10
4.4.2	Confederation member level RADIUS servers	11
4.4.3	RADIUS forwarding	11
4.4.4	Resilience	11

4.4.5	Network addressing	12
4.4.6	802.1X Network access server (NAS)	12
4.4.7	Application and interception proxies	12
4.4.8	IP filtering	13
4.4.9	User name format requirements	13
4.4.10	EAP authentication general requirements	13
4.4.11	Website	13
4.4.12	Service Set Identifier (SSID)	14
4.4.13	Web redirect login transition period	14
Appendix A	Definitions	15
Appendix B	Best Current Practice: A National Roaming Policy	16

0 Executive Summary

The architecture of the European pilot infrastructure *eduroam-ng* (technical part) is currently being investigated in JRA5 and will be documented in DJ5.1.4 “Roaming architecture”. In parallel, there are discussions in progress both in Europe and world-wide to define a policy for a roaming infrastructure for education and research. While several National Research and Education Networks (NRENs) in Europe and other regions have already defined technical and usage *eduroam* guidelines on the national level in order to provide a roaming service for their own users, this is still not true for the European level.

JRA5 considers the established national roaming infrastructures as separate federations. Thus, a European roaming infrastructure is a federation of federations; therefore it is called: the European *eduroam* Confederation. The members of the confederation are the NRENs. This document outlines the rules and guidelines for the confederation and its members.

The confederation policy and service description are less detailed than the national documents. It is assumed that these rules are already in place on the national level, and consequently only the most fundamental properties of the roaming infrastructure are needed in the main part of the confederation policy. Where national documents are not yet ready we expect the confederation members – even if just a few institutions are participating - to act along the guidelines in the confederation service level agreement or in the “best current practices” document that can be found in the appendix of this document. The appendix can be considered as a blueprint for establishing a national roaming federation.

In order to differentiate the operational part and the part under development, these are identified as *eduroam* and *eduroam-ng* (next generation) respectively. Once the development is mature enough to be incorporated into the operational environment the next generation identifier will be stripped off. The policy developed in JRA5 is discussed with the whole TF mobility community and will be applied to *eduroam*.

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

JRA5 is working together with the TF Mobility subscribers as the current best eduoam representing community. After applying the policy it is planned to have a one year test period to collect feedback and practical experience on this rather new field of federated co-operation.

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

1 Introduction

Part 1 of the document DJ5.1.3 “Roaming policy and legal framework” illustrated the roaming service functionality and explained how it handles sensitive data and which information has to be protected.

Users that roam between institutions within the GÉANT2 community will be able to use the credentials provided to them by their identity provider (i.e. their home institution) to get access to network resources. This means that communication will occur between the resource provider (the visited institution) and the identity provider. This communication will cross both administrative domains and national borders. User credentials are generally perceived as highly sensitive by both institutions and users as they often facilitate access to email, course management systems etc. using single sign-on systems at home institutions. User credentials typically refer to 'natural persons' and consequently must be treated as 'personal data'.

At the time of writing, there exists some variation in the development status of the roaming infrastructures in the different NRENs participating in the GÉANT2 JRA5 project. In some countries a roaming service is already available and the necessary trust is established by appropriate rules and guidelines. These are based on contractual agreements between the national *eduroam organiser* (usually the NREN) and the participating institutions (called in this document 'federation members'). A blueprint for a national roaming policy document is appended to this document.

The confederation will, for the period of the construction of national or other roaming infrastructures, be established with less rigorous requirements than those intended in the longer term. This will make it easier for interested parties, who may not have a federation established in a formal manner, to participate while only providing a limited service to its federation partners. This flexibility is necessary to facilitate an inclusive European experimental roaming infrastructure.

The technologies required by the general roaming environment and by the best practice security considerations (see also the Roaming Requirements Document DJ5.1.2) form a rather narrow subset of the present educational roaming solution, *eduroam*, pointing exclusively to IEEE 802.1X compatible technologies in the longer run.

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

Much effort is now being expended on paving the way towards a mature and robust *eduroam* service. There is a need for a federated service to realise the required level of trust between the partners in the eduroam confederation. Some questions exist as well regarding the scope of user

groups, policy management rules, national and international trust relations, service levels, technical set-ups etc.; these must be answered and defined in order to fulfill the expectations of users, system administrators and developers.

The policy document seeks to answer these questions in order to maintain and further establish trust between the members of the confederation, the participating institutions and their roaming users.

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

2 European eduroam confederation policy

2.1 Main part of policy document

2.1.1 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.

2.1.2 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.

2.1.3 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 can be outsourced to an institution working on behalf of the NREN.

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

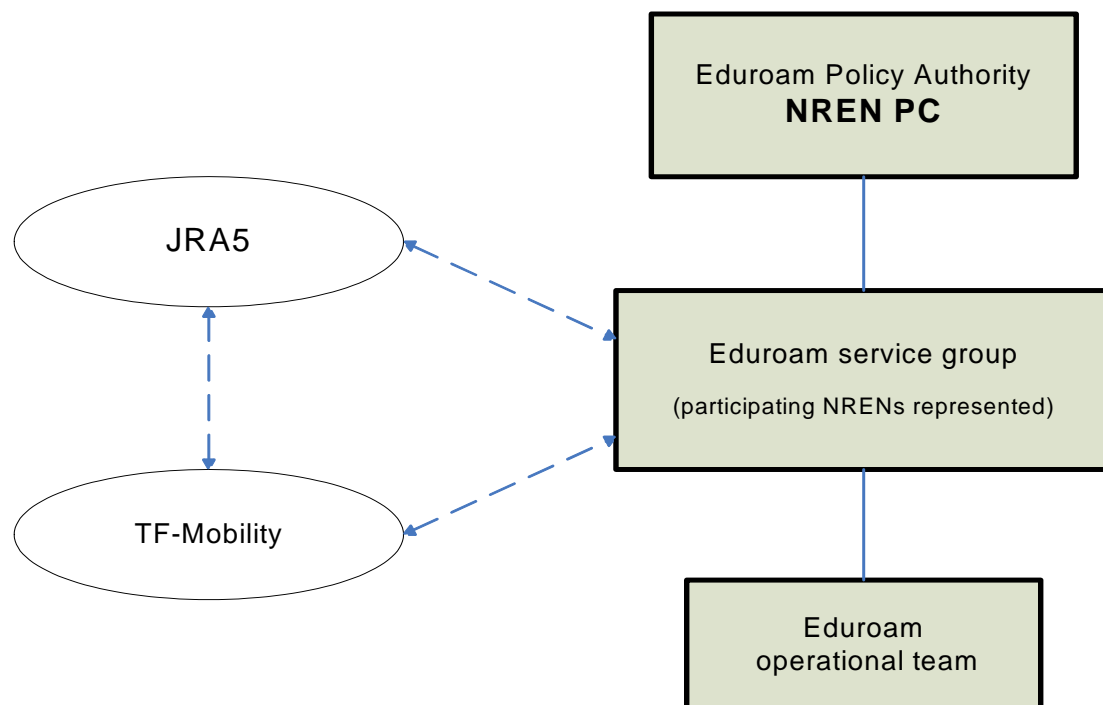


Figure 1: European eduroam confederation levels

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 No 5 (JRA5) will provide expertise to the eduroam service group as well as receive and further

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

disseminate input and developments from the eduroam service group. TF-mobility and JRA5 will also fuel future development of the service.

2.1.4 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 5).

When the European eduroam operational team (Part 4.1.3 of the chapter on policy management procedures) 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 will 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.

2.1.5 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.)

2.1.6 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.

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

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.

2.1.7 *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.

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

3 European eduroam confederation policy management procedures

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 Policy change announcement

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

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

4 Operational requirements for participating federations

4.1 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.

4.2 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.

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

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.

4.3 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>.

4.4 Technical requirements for confederation members

4.4.1 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.

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

4.4.2 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.

4.4.3 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.

4.4.4 Resilience

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

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

4.4.5 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.

4.4.6 802.1X 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.

4.4.7 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.

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

4.4.8 IP filtering

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

4.4.9 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.

4.4.10 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.

4.4.11 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

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

- Confederation member acceptable use policy (AUP) if available
- The eduroam logo and link to www.eduroam.org

4.4.12 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.

4.4.13 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 DDMMYYYY, ending DDMMYYYY+1) web redirect MAY be used. After this time web redirect MUST NOT be associated with the eduroam name, logo etc.

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

Appendix A Definitions

Authentication	Process of proving the identity of a previously registered end user
Authorisation	Process of granting or denying access rights to a service for an authenticated end user
Best practice	The generally acknowledged and agreed best way of doing things
Confederation	A co-operation of federations through means of legally binding arrangements
Credentials	Evidence or testimonials concerning one's right to credit, confidence, or authority
<i>eduroam</i>	Eduroam provides Internet access for roaming users of research and education networks. The access is based on secure authentication by the home organisation of the user.
<i>eduroam server</i>	An authentication server of the eduroam infrastructure
End User	A student, an employee, or a person otherwise affiliated with a home organization, using services provided by <i>eduroam</i> resource providers
Federation	A co-operation of organizations through legally binding arrangements, in the purpose of enhancing collaborations and transactions.
Identity provider (home organization)	A participant of an eduroam federation, responsible for authentication of end users and maintenance of their attributes
Identity	Abstraction of a real person in an information system. Consists of a set of attributes describing him/her.
NREN	National Research and Educational Network
Resources	Material to which access is granted, e.g. network, applications, websites, databases, systems, etc.
Resource Owner	The entity owning a resource and offering resource access to end users
Resource provider	A federation participant or partner that provides network services to end users

Appendix B **Best current practice: A national roaming policy**

To ease the task of setting up national *eduroam* federations, a template for national federation policies is here provided. It is inspired by the Australian *eduroam* policy. It is the hope that providing this template will help harmonize the policy landscape of European *eduroam* federations joining the confederation.

[Country name] *eduroam* policy

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.

1.0 Background to this document

- 1.1 This document sets out guidelines that cover the control of the supply and receipt of roaming Internet access for educational purposes
- 1.2 *eduroam* is a TERENA registered trademark and is an abbreviation for "educational roaming" that originated from a European national education and research networks project to deliver a user-friendly, secure and scalable internet access solution for visitors.
- 1.3 More information about *eduroam* is available at www.eduroam.org

2.0 Roles and Responsibilities

- 2.1 [Name of national *eduroam* organizer]
 - 2.1.1 This policy will be ratified by **[Name of national *eduroam* organizer]**.
- 2.2 ***eduroam* service provider**
 - 2.2.1 [Name of national *eduroam* organizer] is responsible for the national *eduroam* service. [Name of national *eduroam* organizer] will act as the federation's *eduroam* policy authority, in accordance with the European *eduroam* confederation policy.

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

- 2.2.2 [Name of national *eduroam* organizer]'s role is three fold, (1) to coordinate and support the *eduroam* service to nominated technical contacts of participating organizations only, and (2) to maintain links with the European *eduroam* community and their authentication servers, and (3) contribute to the further development of the *eduroam* concept.
- 2.2.3 [Name of national *eduroam* organizer] is responsible for maintaining and developing a national authentication server network that connects to participating organizations. The *eduroam* service provider assumes no liability for any impact as a result of a loss or disruption of service. The *eduroam* identity and resource providers (whether in the same or a different federation or confederation) accept no liability from each other (see also the liability statement in the main policy document).
- 2.2.4 [Name of national *eduroam* organizer] is responsible for managing a second line technical support function covering pre-connection and ongoing technical support and maintenance of a dedicated website containing technical, service, policy and process information, and mailing lists.
- 2.2.5 [Name of national *eduroam* organizer] is responsible for coordinating communications between participating organizations so that policies and procedures contained herein are adhered to in a timely manner and as a matter of last resort has the right to impose technical sanctions.
- 2.2.6 [Name of national *eduroam* organizer] will work with the nominated *eduroam* technical contact of a participating organization to test one or more of the following aspects (1) initial connectivity, (2) authentication and authorization processes and (3) the authorized services offered, and review of (1) the logging activities and (2) the relevant authentication server configuration for compliance with the policy.

2.3 Identity providers

- 2.3.1 The role of the identity provider (home organization) is to act as the credential provider for registered staff and students. Also it will act as technical and service support function for its user's who want to access *eduroam* services at *eduroam* resource providers (visited sites). Only nominated technical contacts can escalate technical support, service support or security issues on behalf of their users to the [Name of national *eduroam* organizer].
- 2.3.3 Identity providers must cooperate with [Name of national *eduroam* organizer] in case of security incidents, misuse etc.

2.4 *eduroam* resource providers

- 2.4.1 The role of the *eduroam* resource providers is to supply internet access to users via *eduroam* (based on trusting that the user's identity provider (home organization) authentication check and response is valid). The *eduroam* resource provider authorizes the use of any service it provides.
- 2.4.2 Where user activity is monitored, the *eduroam* resource provider must clearly

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

announce this fact including how this is monitored, stored and accessed so as to comply with legislation.

2.4.3 The *eduroam* resource provider must abide by this policy and follow [name of national *eduroam* organizer]'s service processes and guidelines listed herein.

2.4.4 The *eduroam* recourse provider must cooperate with [name of national *eduroam* organizer].

2.5 User

2.5.1 The users are responsible for usage of their credentials

2.5.2 A user's role is in principle always a visitor who wants internet access at an *eduroam* resource provider. The user must abide by their identity providers (home organisation's) AUP or equivalent and respect the visited organization's AUP or equivalent. Where regulations differ the more restrictive applies. Users must as a minimum abide by relevant law of the country where he is physically situated, home or abroad.

2.5.3 The user is responsible for taking reasonable steps to ensure that he is connected to a genuine *eduroam* service (as directed by their home organization) prior to entering their login credentials.

2.5.4 The user is responsible for their credentials and the use of any service they might provide.

2.5.5 If credentials are thought to have been compromised, the user must immediately report back to his home organization.

2.5.6 The user is obliged to inform the visited organization (where possible) and home organization of any faults with the *eduroam* service.

3.0 Base service

3.1 Identity providers must deploy an authentication server in accordance with *eduroam* technical and policy guidelines available at [federation-urlA] secondary authentication server is recommended for resilience purposes.

3.2 The *eduroam* identity provider authentication server(s) must be reachable from the *eduroam* resource provider's authentication servers for authentication and accounting purposes.

3.3 The identity provider must create an *eduroam* test account (*eduroam* username and password credential) that will be made accessible to [Name of national *eduroam* organizer] to assist in pre-connection testing, ongoing monitoring, support and fault finding activities. If the test account's password is changed, [Name of national *eduroam* organizer] must be notified by the home organisation in a timely manner. No authorised services should be accorded to the test account.

3.4 The *eduroam* resource provider may offer any media; however as a minimum,

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

wireless LAN IEEE 802.11b is required whilst 802.11g is also recommended.

3.5 The eduroam resource provider must deploy the SSID '*eduroam*' and IEEE 802.1X Extensible Authentication Protocol (EAP) authentication (excluding EAP-MD5) to promote a consistent service and minimum level of security. The SSID "*eduroam*" should be broadcasted.

3.6 The eduroam resource provider must as a minimum implement IEEE 802.1X and WPA/TKIP, or better.

3.7 The eduroam resource provider must as a minimum offer:

- Standard IPsec VPN: IP protocols 50 (ESP) and 51 (AH) both egress and ingress; UDP/500 (IKE) egress only
- OpenVPN 2.0: UDP/1194
- IPv6 Tunnel Broker service: IP protocol 41 ingress and egress
- IPsec NAT-Traversal UDP/4500
- Cisco IPsec VPN over TCP: TCP/10000 egress only
- PPTP VPN: IP protocol 47 (GRE) ingress and egress; TCP/1723 egress only
- SSH: TCP/22 egress only
- HTTP: TCP/80 egress only
- HTTPS: TCP/443 egress only
- IMAP2+4: TCP/143 egress only
- IMAP3: TCP/220 egress only
- IMAPS: TCP/993 egress only
- POP: TCP/110 egress only
- POP3S: TCP/995 egress only
- Passive (S)FTP: TCP/21 egress only
- SMTPS: TCP/465 egress only
- SMTP submit with STARTTLS: TCP/587 egress only
- RDP: TCP/3389 egress only

3.8 The eduroam resource provider should implement a visitor virtual local area network (VLAN) for *eduroam*-authenticated users that is not to be shared with other network services.

3.9 The visited organisation must not charge for *eduroam* access. This service is based on a shared access model where eduroam resource providers supply and receive Internet access for their users.

4.0 Logging

4.1 eduroam resource providers must log all authentication and accounting requests; the following information must be recorded

- (1) The date and time the authentication request was received;
- (2) The RADIUS request's identifier;
- (3) The authentication result returned by the authentication database;
- (4) The reason given if the authentication was denied or failed.
- (5) The value of the request's accounting status type.

4.2 The eduroam resource provider must log all DHCP transactions; including

- (1) The date and time of issue of the client's DHCP lease;
- (2) The MAC address of the client;

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

(3) The client's allocated IP address.

4.3 The eduroam resource provider must keep a log of DHCP transactions for a minimum of three months and a maximum of six months. Co-operation about the content of these logs will be restricted to the *eduroam* technical contacts and [Name of national *eduroam* organizer] technical contact to assist in resolving specific security or abuse issues that have been reported to [Name of national *eduroam* organizer].

5.0 Support

5.1 The identity provider must provide support to their users requesting access at an eduroam resource provider.

5.2 The eduroam identity provider should provide support to users from other eduroam identity providers that are requesting *eduroam* services at their eduroam identity provider campus.

5.3 The eduroam resource provider must publish local information about *eduroam* services on dedicated web pages on their organization website containing the following minimum information,

- (1) Text that confirms adherence (including a url link) to this policy document published on www.eduroam.TLD;
- (2) A url link to eduroam resource providers' acceptable use policy or equivalent;
- (3) A list or map showing *eduroam* access coverage areas;
- (4) Details of the broadcasted or non-broadcasted SSID as *eduroam*;
- (6) Details of the authentication process and authorized services offered;
- (7) Details about the use of a non-transparent application proxy including user configuration guidelines (if applicable);
- (8) A url link to the website www.eduroam.TLD and posting of the *eduroam* logo and trademark statement;
- (9) Where user activity is monitored, the eduroam resource provider must clearly announce this fact including how this is monitored so as to meet with state or national legislation, including how long the information will be held for and who has access to it.
- (10) The contact details of the appropriate technical support that is responsible for *eduroam* services.

6.0 Communications

6.1 The eduroam identity provider must provide [Name of national *eduroam* organizer] with contact details of two nominated technical contacts. Any changes to contact details must be notified to [Name of national *eduroam* organizer] in a timely manner.

6.2 The eduroam identity provider must designate a contact and their contact details to respond to security issues, this may be the same person designated as the nominated technical contact.

6.3 Participating organizations must notify [Name of national *eduroam* organizer] in a timely manner of the following incidents; (1) security breaches; (2) misuse or

Project:	GN2
Deliverable Number:	DJ5.1.3,2
Date of Issue:	08/11/06
EC Contract No.:	511082
Document Code:	GN2-06-080v5

abuse; (3) service faults; (4) changes to access controls (e.g. permit or deny of a user or realm)

7.0 Authority, Compliance & Sanctions

- 7.1 The authority for this policy is [Name of national *eduroam* organizer] who will implement this policy.
- 7.2 Any changes to this policy will be made in consultation with participating organizations and [Name of national *eduroam* organizer].
- 7.3 Connecting to [Name of national *eduroam* organizer] authentication servers will be deemed as acceptance of this policy. Any organization that is currently connected will be given a period of one month's grace from the official ratification date of this policy by [Name of national *eduroam* organizer], to either continue to connect as a statement of acceptance of this policy or the removal of their authentication server connection(s) to indicate an inability to accept this policy at the present time.
- 7.4 In cases where immediate action is required to protect the integrity and security of the *eduroam* service, [Name of national *eduroam* organizer] has the right to suspend the *eduroam* service or restrict *eduroam* access to only those participating organizations that can comply with the required changes. To do so, [Name of national *eduroam* organizer] will notify participating organizations of such incidents, outages and remedial .
- 7.5 [Name of national *eduroam* organizer] will notify by email to the nominated technical and/or security contact of the participating organization of any technical or policy breach or incident that requires resolution. Where such notifications are not acted upon in a timely manner, or where the breach or incident may impact on the security and integrity of *eduroam*, [Name of national *eduroam* organizer] has the right to block *eduroam* access to that organization.
- 7.6 *eduroam* resource providers may prevent use of their networks by all users from a particular *eduroam* identity provider by configuring their authentication server(s) to reject that realm; in some cases a *eduroam* resource provider may also be able to block a single visiting user.
- 7.7 *eduroam* identity providers may withdraw an individual user's ability to use the *eduroam* by configuring their own authentication server or removing that user from their authentication database.
- 7.8 *eduroam* identity providers must also ensure that their computing regulations enable users who breach this policy to be subject to an appropriate internal disciplinary process irrespective of their location at the time.