**15.02.06**

# Deliverable DJ5.1.3:
# Roaming policy and legal framework document Part 2: Policy document

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 the 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.

# Document Revision History

| Version | Date | Description of change | Person |
|---|---|---|---|
| 1 | dd-mm-yy | First draft issued as separate documents | D. Simonsen |
| 2 | 15/11/05 | GN2 style doc version 01 | J. Rauschenbach |
| 3 | 28/11/05 | Second draft issued as one doc, changes in structure of policy as well as content | D. Simonsen |
| 4 | 16/12/05 | New mgmt. structure and many editorial | J. Rauschenbach |
| 5 | 23/12/05 | Third draft, new organisational structure introduced, technical corrections | D. Simonsen |
| 6 | 28/12/05 | Editorial and mgmt. Structure changes | J. Rauschenbach |
| 7 | 19/01/06 | eduroam definition, new organisational structure, technical corrections, based on Cambridge discussion | D. Simonsen |
| 8 | 15/02/06 | Changes based in TF-mobility meeting, Zagreb, Feb. 2006. | D. Simonsen |
| 9 | 15/02/06 | Small editorial changes and changes to the roles of the various eduroam bodies. | K. Wierenga |
| | | Review | |

| REVIEW | | **Main reviewer** | N. Surname |
|---|---|---|---|
| **Summary of suggested changes** | | | |
| **Recommendation** | 1) Major revision[1] ☐ | | 2) Minor revision[2] ☐ |
| **Re-submitted for review - if 1)** | DD/MM/YY | | |

---

[1] Deliverable must be changed and reviewed again before submission to the EC can be considered
[2] Deliverable may be submitted to the EC after the author has made changes to take into account reviewers' comments as appropriate

| **Final comments** | |
|---|---|
| **Approved[3]:** | DD/MM/YY |

# Table of Contents

---

[3] For submission to EC

# 1 Executive Summary

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

JRA5 is considering the established national roaming infrastructures as federations. Therefore a European roaming infrastructure will be seen as a federation of federations and hence 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 is less detailed than the national documents. We presume these rules are in place and under deployment on the national level, so that only basic and static features 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. This can be considered as a blueprint for establishing national roaming federations.

Both the eduroam-next generation (*eduroam-ng*) technology as well as the policy documents are being developed by JRA5 under the name *eduroam*-ng. In order to minimize the potential confusion about what *eduroam* is, the name *eduroam*-ng should not reach the end user. This is the reason why the policy only mentions '*eduroam*' even though the work in progress has been regarded as '*eduroam*-ng' in JRA5.

We are aiming on a one year test period together with TF Mobility community for collecting feedback and practical experience on this rather new field of federated co-operation as a step stone for more complex AAI solutions.

# 2   Introduction

Part 1 of the document DJ5.1.3 "Roaming policy and legal framework" illustrated the roaming service functionality and explained in which points 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 their credentials provided by their identity provider (i.e. home institution) to get access to network resources. This means that communication between the resource provider (visited institution) and the identity provider will occur. This communication will cross both administrative domains and national borders. The user credentials are generally perceived critical by both the institutions and the users as they often give access to email, course management systems etc. via single sign on systems at the home institutions. They should most likely be thought of as referring to 'natural persons' and as a concequence be treated as 'personal data'.

The development status of roaming infrastructures varies 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 organizer* (the NREN) and the participating institutions (in this document called 'federation members'). A blueprint for a national roaming policy document is appended to this document.

For the period of the on-going construction of national or other roaming infrastructures and services the confederation will be established with more loose requirements than intended in the long run. This shall make it easier to join even for JRA5 partners not providing a full service to its federation participants (who may not even have a federation established in a formal manner). It seems important to provide this option to get a broad and real European experimental roaming infrastructure.

The general roaming environment and best practice security considerations (see also the Roaming Requirements Document DJ5.1.2) now point to a quite narrow set of technologies that form the basis of the present educational roaming solution, *eduroam*.

Much effort is now being spent on paving the way for *eduroam* towards a mature and robust service. There is a need for a federated service to guarantee the level of trust in an eduroam confederation. Questions on the scope of user groups, policy management rules, national and

international trust relations, service levels, technical set-ups etc. must be answered and defined in order to manage 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 as well as between participating institutions and roaming users as the federation participants.

# 3 European *eduroam* confederation policy

## 3.1 Main part of policy document

### 3.1.1 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.

### 3.1.2 eduroam definition

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.

### 3.1.3 European *eduroam* confederation policy

This document and its associated documents (definitions, policy management procedures, service level agreement including confederation and federation level technical requirements) define the European *eduroam* confederation policy.

### 3.1.4 European *eduroam* confederation purpose

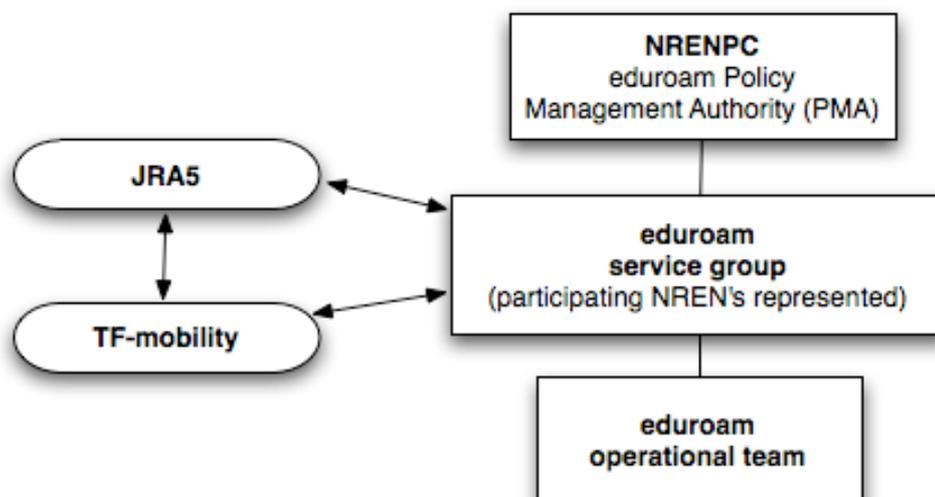The purpose of the European eduroam confederation is to provide mutual roaming network access to its members: European eduroam federations, their participating institutions and the end users. The confederation MAY peer with other roaming infrastructures. The appropriate policy rules SHALL be defined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

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

### 3.1.5   European *eduroam* confederation members, structure and scope

The members of the European eduroam confederation are national research and educational networks (NRENs) that coordinate the national eduroam services.



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

The European eduroam confederation therefore consists of the following levels:

1) National Research and Educational Networks Policy Committee (NRENPC) as the Policy Management Authority (PMA) for the European eduroam confederation

2) The working group consists of representatives from all participating federations. Non-members can be invited as observers

3) The Operational Committee will be appointed by the eduroam working 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 working group as well as receive and further disseminate input and developments from the eduroam working group. TF-mobility and JRA5 will also fuel future development of the service.

### 3.1.6 Joining requirements

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

- they are in conformance with the European eduroam security requirements (associated with this document),

- they are in conformance with the European eduroam service level agreements (associated with this document),

- they accept the European eduroam confederation policy

When the European eduroam operational committee (see policy management procedures) can confirm that the federation adheres to 1) and 2), and 3) is acknowledged by signing the present 'European eduroam confederation policy', the prospective member will be approved and the working group will be notified about this. After approval the federation becomes an official 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 operational commitee. Substantive disagreements will be referred to the NRENPC for arbitration.

### 3.1.7 European *eduroam* security requirements

The security of the user credentials must be preserved and the privacy regulations must be obseved. See the European eduroam conferation service level agreement for technical details.

*eduroam* MUST always provide the means for 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 to ensure that they will only be utilized by the user and his identity provider (see European eduroam confederation service level agreement).

Confederation members (NRENS) and federation participants (institutions) taking part in eduroam MUST make sure that eduroam servers and services are maintained according to server build, configuration and security best practices to ensure a generally high security level and thereby trust in the European eduroam confederation (see European eduroam confederation service level agreement). The confederation members MUST ensure that the participating institutions are aware on their responsibility to establish an appropriate security level at the participating institutions.

### 3.1.8 *eduroam* marketing

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.

# 4  Definitions

| | |
|---|---|
| Authentication | Process of proving the identity of a previously registered end user |
| Authorization | 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 | An organization that consists of a number of parties or groups united in an alliance or league |
| Credentials | Evidence or testimonials concerning one's right to credit, confidence, or authority |
| *eduroam* server | 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 *eduroam* resource providers |
| Federation | A federation is an association of organizations that come together to exchange information as appropriate about their users and resources in order to enable 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 |

# 5 European eduroam confederation policy management procedures

### 5.1.1 European *eduroam* confederation policy management authority

The role of the European eduroam policy management authority (PMA) will be fulfilled by the NRENPC. The PMA only approves changes to the policy as put forward by the eduroam working group. The NRENPC delegates the task of the operational maintenance and development of eduroam to the working group.

### 5.1.2 European eduroam working group

The European eduroam working group approves new members of the confederation, negotiates and recommends policy decisions to be approved by the NRENPC. 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 committee'. The European eduroam working group is the point of contact for TF-mobility and JRA5.

### 5.1.3 European *eduroam* operational committee

The European eduroam Operational Committee will be appointed by the European eduroam working group to work on behalf of the working group to gain flexibility in the operational part of operating eduroam. The day to day running of the confederation business will be handled by the 'eduroam operational committee. The operational commitee reports to the eduroam working group.

The European eduroam operational committee will assist in the dissemination of eduroam and connecting new confederation members as well  as connecting to other eduroam confederations. Incidents will be handled by the European eduroam operational commitee according to the incident handling procedures.

### 5.1.4 Confederation members, institutions and end users

The confederation members MUST act as policy enforcing authority towards its constituency, as the federation participants (institutions) will towards the end users. The European eduroam operational committee is obligated to ensure the enforcement of the present policy either proactively, reactively or both with the hereunder-described incident handling procedures at hand. This MUST be done in corporation with the relevant confederation members. Decisions of a strategic nature will be escalated to the eduroam working group and, if needed, to the NRENPC.

### 5.1.5 Incident handling procedures

In case of abuse of eduroam or any serious policy violation escalation procedures MUST be undertaken in a timely manner. The European eduroam operational committee has the right and is obliged to react in the following ways and to escalate to the eduroam working group (which might escalate further to the NRENPC), depending on the level of violation:

- notice of the policy breach and initiate evaluation process (operational committee level)

- decision about temporary quarantine period (eduroam working group level/NRENPC level)

- decision on disqualification from confederation (NRENPC level)

- confirmation and announcement of termination with grievance process (NRENPC level)

Operational and detailed incident handling procedures are provided by the European eduroam Operational Commitee.

# 6 European *eduroam* confederation service level agreement

## 6.1.1 Confederation level

The European eduroam operational committee guarantees that the necessary infrastructure to run the official European eduroam confederation services is operational and that it is maintained according to server build, configuration and security best practices. The European confederation server MUST be replicated and placed in geographically separate locations to ensure high resilience and robustness of the European eduroam service.

The European eduroam operational committee also ensures that reported incidents concerning the European eduroam confederation will be handled in a timely manner. All such incidents SHALL be logged and presented in an aggregated form to the eduroam working group and the NRENPC.

## 6.1.2 Federation level (confederation members)

Each confederation member joining eduroam MUST establish the necessary infrastructure to support eduroam services and ensure that it is maintained according to server build, configuration and security best practices.

Confederation members MUST ensure that their federation participants obey to the security requirements of the European eduroam confederation policy.

The confederation member MUST act as eduroam authority towards its federation participants (universities etc.).

The federation participants are responsible for proper user management and that they are authenticating only allowable users.

Misuse and breaches of the European eduroam confederation policy MUST be reported to the European eduroam operational committee and SHALL be presented to the eduroam working group and the NRENPC.

Each confederation member MUST establish and maintain a website informing about participating institutions and practical information about 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>.

### 6.1.3 Confederation member level technical requirements

#### 6.1.3.1 Technical contact

Confederation members MUST designate a technical contact that can be contacted using email and telephone. 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.

#### 6.1.3.2 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 MUST ensure that logs are kept of all *eduroam* RADIUS *authentication* requests exchanged; the following information MUST 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 MUST log all *eduroam* RADIUS accounting requests; the following information MUST 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.

#### 6.1.3.3 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.

### 6.1.3.4 *Resilience*

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

### 6.1.3.5 *Network addressing*

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

eduroam resource providers MUST log all DHCP transactions; 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.

### 6.1.3.6 *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 Caller-Station-ID attribute.

### 6.1.3.7 Application and interception proxies

eduroam resource providers deploying application or interception proxies must publish information about application- and intercept proxies on the 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.

### 6.1.3.8 IP filtering

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

### 6.1.3.9 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.

### 6.1.3.10 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 proxy transparently proxy any EAP-type for visiting users.

### 6.1.3.11 Website

Confederation members 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

### 6.1.3.12     *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.

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**

**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* resource 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.

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.

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[4], 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 coorporate 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 users 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 announce this fact including how this is monitored, stored and accessed so as to comply with state or national legislation[5].

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

---

4

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 they are 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, 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;
(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.  Coorporation 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. (David: does this make sense?)

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[6], 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 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.