Luxembourg 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 Background of this document

1. This document sets out guidelines that cover the control of the supply and receipt of roaming Internet access for educational purposes.

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.


2 Roles and Responsibilities

1. RESTENA Foundation (hereafter called “RESTENA”) is the national eduroam organiser, acts as the eduroam service provider for Luxembourg.

2. Organisations that participate in eduroam by providing their users credentials for authentication against the eduroam infrastructure are called Identity Providers, abbreviated as IdP.

3. Organisations that participate in eduroam by providing networking equipment that allows users to connect to the internet using eduroam are called Resource Providers, abbreviated as RP.

3 eduroam service provider – RESTENA

1. RESTENA is the eduroam service provider for Luxembourg and is responsible for the national eduroam service. RESTENA will act as the federation’s eduroam policy authority, in accordance with the European eduroam confederation policy.

2. RESTENA’s role is threefold:
   (1) to coordinate and support the eduroam service to nominated technical contacts of participating organisations 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.

3. RESTENA is responsible for maintaining and developing a national authentication server network that connects to participating organisations. RESTENA assumes no liability for any impact as a result of a loss or disruption of service. The eduroam IdPs and RPs (whether in the same or a different federation or confederation) accept no liability from each other.

4. RESTENA 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.

5. RESTENA is responsible for coordinating communications between participating organisations 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.

6. RESTENA will work with the nominated eduroam technical contacts of a participating organisation to test
one or more of the following aspects

1. initial connectivity,
2. authentication and authorisation processes and
3. the authorised services offered, and review of the logging activities and the relevant authentication server configuration for compliance with the policy.

7. RESTENA provides a monitoring facility to keep track of service availability. The results of this monitoring may be provided as a service to end users on the eduroam website.

4 eduroam identity providers (IdPs)

1. The role of the IdP is to act as the credential provider for registered staff and students, but not for pupils in secondary school classes. Also it will act as a technical and service support point for its users who want to access eduroam services at RPs. Only nominated technical contacts can escalate technical support, service support or security issues on behalf of their users to RESTENA.

2. IdPs MUST make their users aware of roaming conditions, especially of the user obligations in section 6. They MUST educate their users to follow security best practices, including how to identify the correct server certificate of the IdP.

3. IdPs MUST cooperate with RESTENA in case of security incidents, misuse etc.

4. IdPs MUST deploy an authentication server in accordance with the national eduroam technical and policy requirements as negotiated with RESTENA. A secondary authentication server is recommended for resilience purposes. The network equipment MUST comply to RFC 2865 (RADIUS) and SHOULD comply to RFC 2866 (RADIUS Accounting).

5. The IdP’s authentication server(s) MUST be reachable from RESTENA’s national authentication and accounting servers for authentication and accounting purposes. They MUST also be reachable for and answer to ICMP Echo Requests sent by the RESTENA monitoring facilities.

6. The identity provider MUST create an eduroam test account (eduroam username and password credential) that will be made accessible to RESTENA to assist in pre-connection testing, ongoing monitoring support and fault finding activities. If the test account's password is changed, RESTENA MUST be notified by the IdP in a timely manner. RESTENA MAY require an IdP to change the test password to proactively work against leakage of the test credential.

5 eduroam resource providers (RPs)

1. The role of the RPs is to supply internet access to users via eduroam (based on trusting that the user’s identity provider authentication check and response is valid). The RP authorises the use of any service it provides.

2. Where user activity is monitored, the RP MUST clearly announce this fact including how this is monitored, stored and accessed so as to comply with legislation.

3. The RP MUST abide by this policy and follow RESTENA’s service processes and guidelines listed herein.

4. The RP may offer any media; however as a minimum, wireless LAN IEEE 802.11b is required whilst 802.11g is also recommended.

5. The RP MUST deploy the SSID ‘eduroam’ (except in cases where multiple resource providers overlap physically; in this case a custom SSID is to be negotiated with RESTENA) 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” MUST be broadcasted if the networking equipment allows for that.

6. The RP MUST implement IEEE 802.1X and MUST provide WPA/TKIP encryption scheme, or better. If the networking equipment allows simultaneous use of both WPA1 and WPA2 with TKIP and AES-CCMP encryption, both options SHOULD be activated. If a choice between WPA/TKIP and WPA2/AES-CCMP has to be made, WPA2/AES-CCMP has preference over WPA/TKIP. The networking equipment MUST comply to RFC 2865 (RADIUS) and SHOULD comply to RFC 2866 (RADIUS Accounting).

7. The RP SHOULD 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

8. The RP SHOULD give public IP addresses to its visitors. Where available, IPv6 connectivity SHOULD be provided.

9. The RP SHOULD implement a visitor virtual local area network (VLAN) for eduroam-authenticated users that is not to be shared with other network services.

10. Only if no separate guest VLAN is deployed, RPs MAY deploy content filtering mechanisms, but MUST announce this fact to the users on-site as well as to RESTENA. RESTENA will note that the institution uses content filtering on the national eduroam webpage on www.eduroam.lu. The filtering MUST be transparent to the user, i.e. it has to be usable without configuration changes on the user's device.

11. The RP MUST NOT charge for eduroam access. This service is based on a shared access model where eduroam participants supply and receive Internet access for their users.

6 Users

1. A user’s role is in principle always a visitor who wants internet access at a site operated by an RP. The user MUST abide by their IdP’s AUP or equivalent and respect the RP’s AUP or equivalent. Where regulations differ the more restrictive applies. Users MUST as a minimum abide by relevant law of the country where they are physically situated while using the service.
2. The user is responsible for taking reasonable steps to ensure that he is connected to a genuine eduroam service (as directed by their IdP) prior to entering their login credentials. The primary means to achieve this is to validate the server certificate that is presented to the user upon login.

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

4. If credentials are thought to have been compromised, the user MUST immediately report back to his IdP.

5. The user is obliged to inform the RP (where possible) and IdP of any faults with the eduroam service.

7 Logging

1. Both RPs and IdPs 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 authentication result returned by the authentication backend or upstream server;
   (3) For IdPs: The inner identity of the request
   (4) The value of the request's accounting status type.
   (5) The value of the User-Name attribute in accounting requests.
   (6) The value of the Accounting-Session-Id in accounting requests.

2. The RP MUST either
   
   a) 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
   
   b) log MAC address to IP address bindings by other means that are at least as reliable as DHCP logs

   An RP may provide its service geographically distributed, i.e. a single, central RADIUS server instance may serve various hotspots (coherent sets of access points) which are distributed throughout the country. In this case, the logging obligations in this stanza 7.2 MAY be delegated to the hotspot locations.

3. The eduroam resource provider MUST keep the logs from section 7.2 for a minimum of six months and a maximum of twelve months. Co-operation about the content of these logs will be restricted to the eduroam technical contacts and RESTENA's technical contact to assist in resolving specific security or abuse issues that have been reported to RESTENA.

4. All relevant logs MUST be created with synchronisation to a reliable time source.

8 Support

1. The IdP MUST provide support to their users requesting access at an eduroam resource provider.

2. The RP SHOULD provide support to users from other IdPs that are requesting eduroam services at his site.

3. The RP MUST publish local information about eduroam services on a dedicated part of RESTENA's eduroam website (http://www.eduroam.lu) containing the following minimum information:
   (1) Text that confirms adherence to this policy document as published on www.eduroam.lu;
   (2) A URL link to eduroam resource providers' acceptable use policy or equivalent;
   (3) A list or map showing eduroam access coverage areas and the number of Access Points deployed;
(5) Details of the authentication process and authorised services offered;
(6) Details about the use of a transparent application proxy/content filter (if applicable);
(7) 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.
(8) The contact details of the appropriate technical support that is responsible for eduroam services.

9 Communications

1. Both IdPs and RPs MUST provide RESTENA with contact details of two nominated technical contacts that can be contacted via e-mail or telephone. The contact may be either a named individual or an organisational unit. Any changes to contact details MUST be notified to RESTENA in a timely manner.

2. IdPs 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.

3. Participating organisations MUST notify RESTENA 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)

10 Authority, Compliance & Sanctions

1. The authority for this policy is RESTENA who will implement this policy.

2. Any changes to this policy will be made in consultation with participating organisations and RESTENA.

3. Connecting to RESTENA's authentication servers will be deemed as acceptance of this policy. Any organisation that is currently connected will be given a period of one month's grace from the official ratification date of this policy by RESTENA, 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.

4. In cases where immediate action is required to protect the integrity and security of the eduroam service, RESTENA has the right to suspend the eduroam service or restrict eduroam access to only those participating organisations that can comply with the required changes. To do so, RESTENA will notify participating organisations of such incidents, outages and remedial.

5. RESTENA will notify by email to the nominated technical and/or security contact of the participating organisation 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, RESTENA has the right to block eduroam access to that organisation.

6. RPs may prevent use of their networks by all users from a particular IdP by configuring their authentication server(s) to reject that realm if a security breach or abuse case can not be resolved in a timely manner with the technical contact(s) of the corresponding IdP; in some cases an RP may also be able to block a single visiting user. All user or realm blocking actions have to be reported to RESTENA as soon as possible.
7. IdPs may withdraw an individual user’s ability to use eduroam by configuring their own authentication server or removing that user from their authentication database.

8. IdPs have to 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.
Luxembourg eduroam policy

Participating organisation:

participating as  □ resource provider (RP)
□ identity provider (IdP) for the following realm(s):

_________________________
_________________________

Technical Contact 1:
Name: _____________________________________
E-Mail: _____________________________________
Tel: ________________________________________

Technical Contact 2:
Name: _____________________________________
E-Mail: _____________________________________
Tel: ________________________________________

Security Contact (IdP only):  □ same as technical contact  □ dedicated contact below
Name: _____________________________________
E-Mail: _____________________________________
Tel: ________________________________________

Signatures:

- for the participating organisation -
- for RESTENA Foundation -