RESTENA
Réseau Téléinformatique de l'Education Nationale et de la Recherche

eduroam
Fondation RESTENA www.eduroam.lu

eduroam Luxembourg 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 registered trademark of GÉANT Association 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.
3. More information about *eduroam* is available at https://www.eduroam.org

2 Roles and Responsibilities

1. RESTENA Foundation (hereafter called "RESTENA") is the national *eduroam* organiser and acts as the *eduroam* National Roaming Operator (NRO) for Luxembourg.
2. The service is called "*eduroam* Luxembourg".
3. Organisations that participate in *eduroam* Luxembourg by providing their users credentials for authentication against the eduroam infrastructure are called "*Identity Providers"*, abbreviated as IdP.
4. Organisations that participate in *eduroam* by providing networking equipment that allows users to connect to the internet using *eduroam* are called "*Service Providers"*, abbreviated as SP.
5. An "*eduroam* Luxembourg participant" is an organisation which is an IdP, an SP, or both.
6. IdP and SP deployments need to have personnel which can be contacted via e-mail or telephone in case of technical problems or security incidents, the "*nominated contact*". The nominated contact(s) may be either a named individual (e.g. an individual email address) or an organisational unit (e.g. a role-account email address).

3 *eduroam* National Roaming Operator – RESTENA

1. RESTENA is the *eduroam* National Roaming Operator (NRO) for Luxembourg and is responsible for *eduroam* Luxembourg. RESTENA will act as the national *eduroam* policy authority, in accordance with the European *eduroam* confederation policy[1], the eduroam Service Definition[2] and the Global eduroam Compliance Statement[3].
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 and world-wide *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 SPs (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 provides an interface to the international roaming infrastructure. The infrastructure includes connections to the international root authentication servers (using the RADIUS/UDP and RADIUS/TLS protocol), regular monitoring and maintenance of the national servers and reporting of nationally aggregated statistics about the deployment details in Luxembourg.
6. 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.
7. 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.
8. 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)

eduroam identity providers can either operate as *stand-alone* IdPs (implementing all eduroam technical and security requirements themselves or via a third-party, a.k.a. "outsourcing") or as *RESTENA-hosted* IdPs (leaving all technical requirements to RESTENA), or as *Cloud-hosted* IdPs. The following items are valid for ALL of these variants:

B1. Only RESTENA customers can become *eduroam* Luxembourg identity providers; this is a necessary but not necessarily sufficient prerequisite. The final admission decision rests with RESTENA.

B2. The role of the IdP is to act as the credential provider for its users. It will also act as a technical and service support point for its users who want to access *eduroam* services at all SPs. Only nominated technical contacts can escalate technical support, service support or security issues on behalf of their users to RESTENA.

B3. 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, particularly to identify the correct server certificate of the IdP.

B4. IdPs MUST cooperate with RESTENA in case of security incidents, misuse etc.

B5. The eduroam IdP SHOULD announce the availability of eduroam for its users in the Domain Name System, DNS, to facilitate future service enhancements based on RFC 6614 (RADIUS/TLS).

B6. RESTENA reserves the right to modify certain RADIUS attributes while transporting them from the IdP to an SP. The attribute list includes, but is not limited to:

- attributes for VLAN assignment; removed to prevent accidental placement of the user into an inappropriate VLAN on the SP in question

The following items are valid for RESTENA-*hosted* IdPs only:

O1. IdPs MUST have a well-managed identity management system.

O2. The identity information MUST be deposited in RESTENA's institution account management system (a.k.a. "Mail-GUI").

The following items are valid for *stand-alone* IdPs only:

S1. IdPs MUST implement the technical requirements and SHOULD implement the technical recommendations as specified in section 6.3.2 of the European eduroam Service Definition [2].

S2. A secondary authentication server is RECOMMENDED for resilience purposes.

S3. The authentication server(s) SHOULD be reachable for and answer to ICMP Echo Requests sent by the RESTENA monitoring facilities.

S4. The identity provider SHOULD 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.

S5. The Identity Provider SHOULD report the total number of users in its authentication backend who are eligible for the *eduroam* service.

The following items are valid for *Cloud-hosted* IdPs only:

M1. The identity provider agrees to adhere to the "eduroam Managed IdP" system's Acceptable Use Policy.

5 *eduroam* service providers (SPs)

eduroam service providers can either operate as *stand-alone* SPs (implementing all eduroam technical and security requirements themselves or via a third-party, a.k.a. "outsourcing") or as *hosted* SPs (leaving parts of the technical requirements to RESTENA). The following items are valid for BOTH of these variants:

B1. The role of the SPs 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 SP authorises the use of any service it provides.

B2. The SP SHOULD provide support to users from other IdPs who are requesting *eduroam* services at his site.

B3. SPs MUST implement the technical requirements and SHOULD implement the technical recommendations for "Network Access Servers (NAS)" and for "Network" as specified in section 6.3.3 of the European eduroam Service Definition [2].

B4. Where user activity is monitored, the SP MUST clearly announce this fact including how this is monitored, stored and accessed so as to comply with legislation.

B5. The SP may offer any media; however as a minimum, wireless LAN according to IEEE 802.11 and any of its amendments is required.

B6. The deployment of the encryption schemes WPA/AES and WPA2/TKIP is strongly discouraged for interoperability reasons.

B7. The SP MUST provide RESTENA with the following basic information about its hotspot(s) and MUST allow RESTENA to publish this information:

- SSID
- geographic location or street address of hotspot(s)
- approximate number of Access Points per hotspot
- supported encryption levels
- whether or not there are significant port restrictions (Definition: a whitelist of open ports is a significant port restriction; a blacklist of closed ports is not a significant port restriction)
- whether or not a content-filtering proxy is installed at the hotspot
- whether or not IPv6 connectivity is provided at the hotspot
- whether or not the IP pool is behind a NAT gateway
- whether or not user activity is monitored; if so, the time span of retainment of such monitoring data
- if the use of the SPs network is governed by an Acceptable Use Policy (AUP) different from the default RESTENA AUP, a URL to this policy
- the fact that the SP is an eduroam participant and that the SP has declared to adhere to the eduroam Luxembourg policy

B8. The SP SHOULD implement a visitor virtual local area network (VLAN) for *eduroam*-authenticated users that is not to be shared with other network services.

B9. Only if no seperate guest VLAN is deployed, SPs 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 https://*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.

B10. The SP 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.

eduroam Luxembourg policy

B11. RESTENA reserves the right to modify certain RADIUS attributes while transporting them from the SP to an IdP. The attribute list includes, but is not limited to:

- Operator-Name [RFC 5580]; added to allow an IdP to identify the originating hotspot
- Chargeable-User-Identity [RFC 3748]; added to allow requesting of persistent user identifiers

The following items are valid for *hosted* SPs only:

O1. The requirements of the function "Local AAA Servers" in section 6.3.3 of the European eduroam Service Definition [2] are split between RESTENA and the hosted SP in the following way:

- Bullet points 1,2 and 4 (Authentication Request Forwarding, EAP-Message proxying, F-Ticks) are in the responsibility of RESTENA
- Bullet point 3 (Logging of layer 3 to layer 2 binding information) is in the responsibility of the SP.

O2. The recommendations of the function "Local AAA servers" in section 6.3.3 of the European eduroam Service Definition [2] are in the responsibiliy of RESTENA.

The following items are valid for *stand-alone* SPs only:

S1. SPs MUST implement the technical requirements and SHOULD implement the technical recommendations for "Local AAA servers" as specified in section 6.3.3 of the European eduroam Service Definition [2].

S2. If the SP is also an IdP, the SP is encouraged to report anonymised usage statistics with the amount of service usage of local users (i.e. users of their own realm at their own hotspot).

S3. When using RADIUS/TLS with dynamic discovery, reporting the number of national and international roaming users at the hotspot is MANDATORY; the reporting mechanism is F-Ticks.

6 Users

1. A user's role is in principle always a visitor who wants internet access at a site operated by an SP. The user MUST abide by their IdP's AUP or equivalent and respect the SP'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 (with configuration instructions as communicated 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 SP (where possible) and IdP of any faults with the *eduroam* service.

7 Logging

1. The log retention time for IdP and SP logs is at a minimum six months, and at a maximum twelve months. Sharing 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, and is subject to the laws of the Grand-Duchy of Luxembourg.

8 Communications

1. Both IdPs and SPs MUST provide RESTENA with communication details of their nominated contact(s); the information MUST include an email address and SHOULD include a phone number. Any changes to the nominated contact(s) MUST be notified to RESTENA in a timely manner.
2. 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)

9 Branding

1. Whenever an IdP or SP creates promotional material designed to signal the presence of the eduroam service to customers in the coverage area, the national branding of the eduroam Luxembourg service MUST be used.
2. The term to use to refer to the national eduroam service is "eduroam Luxembourg"; the logo is the eduroam Luxembourg logo, as seen for example on the national eduroam web page https://www.eduroam.lu. The logo MAY be augmented by the eduroam Luxembourg participant with additional local branding after negotiation with RESTENA. High quality digital sources for the logo are available from RESTENA at request.
3. When referring to the international roaming possibilities with eduroam, the term to be used to refer to the global eduroam service as a whole is "eduroam".
4. Promotional material dating from before the effective date of this policy does not need to be updated.

10 Authority, Compliance & Sanctions

1. The authority for this policy is RESTENA.
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, although a written confirmation is preferred. 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. SPs 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 SP may also be able to block a single visiting user, e.g. when a returning user has been identified via the RADIUS attribute Chargeable-User-Identity. 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 appropriately or by 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.

11 External References

[1] https://www.eduroam.org/wp-content/uploads/2016/05/GN3-12-194_eduroam-policy-for-signing_ver2-4_1_18052012.pdf

[2] https://www.eduroam.org/wp-content/uploads/2016/05/GN3-12-192_eduroam-policy-service-definition_ver28_26072012.pdf

[3] https://www.eduroam.org/wp-content/uploads/2016/05/eduroam_Compliance_Statement_v1_0.pdf

eduroam Luxembourg policy

The participating organisation declares to abide by this policy and follow RESTENA's service processes and guidelines listed herein. The participating organisation is:

(name or stamp of participating organisation)

participating as ☐ *eduroam* service provider (SP) (stand-alone / hosted)

☐ *eduroam* identity provider (IdP) for the following realm(s):

- ☐ stand-alone: realm(s) _____
- ☐ RESTENA-hosted
- ☐ Cloud-hosted

Contact 1: Name: _____

E-Mail: _____

Tel: _____

Contact 2: Name: _____

E-Mail: _____

Tel: _____

Signatures:

- for the participating organisation - - for RESTENA Foundation -