eduroam Compliance Statement

This document outlines the minimum technical and organisational standards for roaming operators (RO) and roaming confederations (RC) in order to provide the global eduroam service. Implementing the minimum standard requires the coordination of roaming operators (RO) and roaming confederations (RC). This document is subject to change by the Global eduroam Governance committee (GeGC), based on feedback from ROs, RCs or individual eduroam users. Any changes will be managed via version control and relevant TERENA change control processes.

The TERENA co-ordinated GeGC comprises of representatives from ROs and RCs; they have written this document. Any feedback regarding this document should be directed to <gegc@terena.org> for consideration.

In case of a dispute regarding the status of an entity (IdP, SP, RO) in the eduroam service that cannot be resolved by the responsible RO or RC, the GeGC will give the final ruling.

1. Terminology

1.1. eduroam

eduroam is a federated roaming service that provides secure network access by authenticating a user with their own credentials issued by their IdP.

1.2. eduroam Identity Provider (eduroam IdP)

An entity that is responsible for user credentials and operation of an authentication server for eduroam access for these
users. IdPs are in some regions also known as “Home Institutions”.

1.3. eduroam Service Provider (eduroam SP)

An entity that operates an access network on which eduroam users are admitted to access Internet services once they are successfully authenticated by their IdP. SPs are in some regions also known as “Visited Institutions”.

1.4. Roaming Operator (RO)

The entity that operates the eduroam service for a country or economy and that is recognised as such by the RC to which it belongs or, in case the country or economy is part of a geographic region for which no RC is established, by the GeGC. The RO may be a National Research and Education Network operator, for example. ROs are sometimes referred to as the “eduroam operators”.

1.5. RADIUS Proxy Server (RPS)

RPSs are established and maintained in order to provide the technical infrastructure (i.e., RADIUS server hierarchy) for the global eduroam service. Top-level RPSs for a geographic region are run by the corresponding RC. In cases where no RC is established for a specific region, the GeGC, advised by the ROs of that region, appoints the ROs that will run the top-level RPSs for the region.

1.6. Roaming Confederation (RC)

An entity that consists of a cohesive set of ROs servinga geographical region and that is recognised as such by the GeGC. The “European eduroam Confederation” is one example.

2. User identification process

2.1.eduroam uses technologies that allow the identification of every individual user which joins an edu roam SP network. The user identification process is defined via an out-of-band communication between the eduroam SP and the user's eduroam IdP to identify the inner EAP identity of an end-user. The user identification process requires sufficient logging information to be recorded at both the eduroam SP and eduroam IdP. The result of the user identification process is for the responsible eduroam IdP to uniquely identify the user who triggered a particular use of an eduroam SP network.

The user identification process expressly does not include that this user identification is transmitted to the eduroam SP.

3. Technology compliance for eduroam EAP packet transfer

3.1. An RPS operated by an RC, RO, eduroam IdP or SP MUST forward EAP-messages it receives, destined for eduroam participants, unmodified to the appropriate RADIUS server (be it RC, RO or IdP)as determined by the eduroam routing mechanism defined and agreed by the GeGC.

4. Administrative and technology compliance for ROs

4.1. The RO is responsible for ensuring the eduroam service operation within a particular country or economy.

4.2. The RO may also be responsible for ensuring the eduroam service operation within another country or economy, if no appropriate entity exists in that country or economy that is able and willing to operate the eduroam service for that country or economy. Each case of this kind requires explicit approval from the RC for the geographic region that the country or economy is part of, or, in case the country or economy is part of a geographic region for which no RC is established, from the GeGC.

4.3. The RO has the authority to determine the eligibility of eduroam IdPs, being organisations engaged in research and/or education, in its country or economy.

4.4. The RO has the authority to determine the eligibility of eduroam SPs in its country or economy. There are no restrictions for the eligibility of eduroam SPs as long as the eduroam SP technical requirements are met and access is provided to all eduroam users, irrespective of their origin and without charge.

4.5. The RO MUST establish communication channels to all other ROs. This can be via an RC or via the eduroam regional operators list. An RO MUST be reachable within a reasonable time on this channel.

4.6. The RO SHOULD publish information about the available points of presence of eduroam (SP sites) in its country or economy in an adequate manner defined by the GeGC.

4.7.The RO MUST establish communication channels to the eduroam SPs in its country or economy to be able to communicate changes in requirements and resolve problems.

4.8. The RO MUST publish information about eduroam services on dedicated web pages containing the following minimum information:

- Text that confirms adherence (including a url link) to an RC policy (if applicable);
- A list of IdPs and a list or map showing eduroam access coverage areas with links to each eduroam SPs web page;
- The contact details of the appropriate technical support that is responsible for eduroam services and mailing list(s).

4.9. The RO MUST make sure that the eduroam IdPs and eduroam SPs in its country or economy maintain sufficient logging information to allow the user identification process to terminate successfully. Means to achieve this goal are set forth in the appendices A and B.

4.10. The RO MUST register the eduroam name and logo as trademarks in its country or economy, if the eduroam name and logo have not been registered there as trademarks of TERENA. If an entity is no longer recognised as an RO by the RC of the geographic region that its country or economy is part of, or, in case no RC is established for that region, by the GeGC, then the entity MUST transfer the ownership of the trademarks to TERENA.

5. **Administrative and technology compliance for eduroam IdPs and SPs**

5.1.The requirements for eduroam IdPs and SPs are listed in the Appendices A and B of this document. Those requirements are subject to technology changes and feedback from ROs, RCs or individual eduroam users. Any changes agreed by a majority of the GeGC will be managed via version control and will take effect for all parties that have signed an earlier version of this document. By signing this document, an RO or RC unilaterally declares to implement and adhere to the rules set forth herein. By signing this document, an RC commits to ensure that the ROs that make up the RC implement and adhere to the rules set forth herein. By signing this document, an RO commits to ensure that the eduroam IdPs and eduroam SPs in its country or economy implement and adhere to the rules set forth herein.

Failure to adhere may result in the removal of an entity’s recognition as an RC or RO, including removal of the right to use the eduroam name, logo and trademark.

eduroam Compliance Statement
Appendixes

A. Administrative and technology compliance for eduroam Identity Providers

A.1. eduroam IdPs MUST implement a RADIUS interface to connect to the eduroam routing fabric.

A.2.eduroam IdPs MUST implement an EAP method for all local users that is suitable for wireless networks as well as wired, and supports mutual authentication and end-to-end encryption of credentials.

A.3. eduroam IdPs MUST send a RADIUS accept message for valid authenticated local users for which they receive an access request.

A.4.eduroam IdPs MUST NOT send a RADIUS accept message for invalid users or those who are not authenticated.

A.5. eduroam IdPs MUST provide support to their users. Any support matters may be escalated to the RO or RC to coordinate and resolve.

A.6.eduroam IdPs MUST log all authentication attempts; the following information MUST be recorded:

- timestamp of authentication requests and corresponding responses
- the outer EAP identity in the authentication request (User-Name attribute)
- the inner EAP identity (actual user identifier)
- the MAC address of the connecting client (Calling-Station-Id attribute)
- type of authentication response (i.e. Accept or Reject).

The minimum retention time is six months, unless national regulations require otherwise.

B. Administrative and technology compliance for eduroam Service Providers

B.1.eduroam SPs networks MUST implement 802.1X with a RADIUS interface to connect to the eduroam infrastructure.

B.2. eduroam SPs IEEE 802.11 wireless networks MUST broadcast the SSID "eduroam". If there is more than one eduroam SP at the same location, an SSID starting with "eduroam-" MAY be used.

B.3.eduroam SPs IEEE 802.11 wireless networks MUST support WPA2+AES, and MAY additionally support WPA/TKIP as a courtesy to users of legacy hardware. Exceptionally, an SP established before January 1, 2012, MAY support only WPA/TKIP but not longer than January 1, 2013.

B.4.eduroam SPs networks MUST provide IP address and DNS resolution auto-configuration infrastructure.

B.5.eduroam SPs networks SHOULD provide routable IP addresses, and MAY provide NAT translation.

B.6.eduroam SPs SHOULD forward all EAP-messages, destined for eduroam participants, unmodified to the eduroam infrastructure.

B.7. eduroam SPs MUST NOT charge users or their eduroam IdPs for being admitted on the eduroam SP's access networks.

B.8.eduroam SP services are based on SP local policies. However, modifying the content of user connections (e.g., access lists or firewall filter rules to deny arbitrary ports or application-layer proxies) is strongly discouraged and MUST be reported to the respective RO.

B.9. eduroam SPs SHOULD keep sufficient logging information to be able to identify the responsible Identity provider for the logged-in user, by logging:

- timestamp of authentication requests and corresponding responses
- the outer EAP identity in the authentication request (User-Name attribute)
- the MAC address of the connecting client (Calling-Station-Id attribute)
- type of authentication response (i.e. Accept or Reject)
- correlation information between a client's layer 2 (MAC) address and the layer 3 (IP) address that was issued after login if public addresses are used (e.g., ARP sniffing logs or DHCP logs)

The minimum retention time is six months, unless national regulations require otherwise.

Compliance Statement FAQ

Q: According to 3.1, EAP
-
Messages MUST be transferred unmodified. Does that restrict an operator from
strippin
g out VLAN attributes, or stopping brute
-
force attacks?
A: The RADIUS packets contain the EAP
-
Message and other attributes like VLAN assignment attributes alongside. It is only
the EAP
-
Message that needs to remain unmodified; the VLAN attributes can be cha
nged or stripped as needed
-
if need
be.
Note also that the clause applies to proxy servers only. If a brute
-
force attack is mounted, it will come from a hotspot, i.e.
from an eduroam SP network. The eduroam SP has the possiblity to stop this from happenin
g (the relevant clause is B.6,
which is a SHOULD). If an SP has decided it wishes to forward the requests to an IdP, any procy
which sits in between is
not supposed to interfere.
The intent of this clause in the Compliance Statement is to make sure that a
proxy server does not terminate an EAP
session itself (i.e. not send it forward, but terminate the tunnel). This behaviour is not allowed.
Q: In 4.6, it is prescribed that the Access Point information needs to be in a certain format. Why is
adhering
to a
well
-
known format required?
A: The information is used to compile several pieces of end
-
user documentation, like a global hotspot map. It is not
-
or
only with great technical difficulty
-
possible to create a cohesive map for the entire planet if the info
rmation about the
hotspots is fragmented and partitioned in several different formats.
Q: In 5.1 ,it states "By signing this document, an RO commits to ensure that the eduroam IdPs and
eduroam
SPs in its country or economy implement and adhere to the rule
s set forth herein." What would be an
appropriate way for an RO to honour this commitment?

A: A good way for an RO to honour this commitment would be to have the eduroam IdPs and eduroam SPs in its country
or economy sign a statement in which they commit t
o implement and adhere to the rules. If and when it would come to
the attention of an RO that an eduroam IdP or eduroam SP in its country or economy is not adhering to the rules, then the
RO is expected to take appropriate action towards that IdP or SP.