eduroam Compliance Statement

Introduction

1.1 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).

1.2 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 GÉANT change control processes. This document may be extended or replaced by a more specific agreement.

1.3 The GÉANT co-ordinated GeGC is composed of representatives from ROs and RCs; they have written this document. Any feedback regarding this document should be directed to <gegc@lists.geant.org> for consideration. The relationship between the GeGC and GÉANT is further described in the GeGC Charter.

1.4 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.

1.5 On occasion it MAY be necessary to remove an IdP, SP, RO or RC in order to comply with external legislation or legal requirements placed on the eduroam core Operational Team or Roaming Operators. The eduroam community will be informed of any such decisions.

1.6 All eduroam SP, IdPs, ROs and RCs MUST comply with applicable data protection regulations.

1.7 The keywords “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 [RFC2119].

1.8 The following definitions are used:

eduroam	eduroam is a federated roaming service that provides secure network access by authenticating a user with their own credentials issued by their IdP.
eduroam core Operational Team	Team responsible for elements of the eduroam service operated on behalf of all Roaming Operators. The core Operational Team is appointed by GÉANT.
eduroam Identity Provider (IdP)	An entity that is responsible for user credentials and eduroam access for these users. IdPs are in some regions also known as “Home Institutions”.
eduroam Service Provider (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”.
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”.
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.
Roaming Confederation (RC)	An entity that consists of a cohesive set of ROs serving a geographical region and that is recognised as such by the GeGC. The “European eduroam Confederation” is one example.

2. Administrative and technical compliance for ROs, RCs, IdPs and SPs

2.1. eduroam uses technologies that allow the identification of every individual user which joins an eduroam SP network. It is the responsibility of the RO to ensure that users can be uniquely identified.

2.2 The authentication mechanism is defined between the user and eduroam IdP to verify the identity of an end-user by means of mutual authentication. It's the responsibility of the eduroam IdP to deliver credentials in a secure manner (possibly out-of-band) such that the user remains uniquely identifiable, and make sure the user verifies the IdP authenticity by means of mutual authentication.

2.3 The user identification process requires sufficient logging information be recorded at the Roaming Operator, the eduroam SP and eduroam IdP. This process expressly does not include that user identification is present or transmitted to the eduroam SP. (An anonymous outer identity or EAP-mechanism that preserves the user's privacy is encouraged.)

2.4. An RPS operated by an RC, RO, eduroam IdP or SP MUST forward EAP-messages (including outer identities) 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.

3. Administrative and technology compliance for ROs

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

3.2. 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.

3.3. 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.

3.4. The RO has the authority to determine the eligibility of eduroam SPs in its country or economy. There are no restrictions on 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.

3.5. 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 ensure that their data within the eduroam database is complete and up-to-date (https://monitor.eduroam.org/). An RO MUST be reachable within a reasonable time on appropriate channels.

3.6. 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.

3.7. 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.

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

> **3.8.1.** Text that confirms adherence (including a url link) to an RC policy (if applicable);
> **3.8.2.** A list of IdPs and a list or map showing eduroam access coverage areas with links to each eduroam SPs web page;
> **3.8.3.** The contact details of the appropriate technical support that is responsible for eduroam services and mailing list(s).

3.9. 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.

3.10. 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 GÉANT. 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 GÉANT.

4. Administrative and technology compliance for eduroam IdPs and SPs

4.1. 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, IdPs, SPs or individual eduroam users. Any changes agreed to by a majority of the GeGC will be managed via version control, and notice of such changes MUST be provided to ROs and RCs via email ten (10) days prior to such changes taking effect. Such changes will apply to all relevant parties (e.g., ROs, RCs, IdPs, SPs) using eduroam.

4.2 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. By signing this document, an RO or RC agrees that this eduroam Compliance Statement supersedes all prior eduroam Compliance Statements agreed to by the RO or RC.

4.3 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.

Acting as RC/RO for: (country, economy / multiple of)

Signed by: (Name of RO / RC)

Signature: Date:

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 infrastructure.

A.2. eduroam IdPs MUST implement an EAP method for all affiliated 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 Access-Accept message for valid authenticated affiliated users for which they receive an Access-Request.

A.4. eduroam IdPs MUST send a RADIUS Access-Reject for invalid users or those who are not authenticated.

A.5. eduroam IdPs MUST support 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)
- the visiting SP for the user via the Operator-Name attribute, if present
- the visiting country of the request via the eduroam-SP-country attribute, if present
- type of authentication response (i.e. Accept or Reject).

The minimum retention time is three months, unless national regulations require otherwise.
The eduroam IdP SHOULD provide a Chargeable-User-Identity (CUI RADIUS attribute) to assist with the user identification at an eduroam SP visiting network.

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.

If the eduroam SP is not a home network for an IdP (e.g., part of another roaming infrastructure) the network MAY be provided via Passpoint / Hotspot 2.0 using a Roaming Consortium Organisation Identifier (RCOI) of GÉANT in 001BC50460 or one specifically assigned by GÉANT for a particular roaming network.

B.3. An eduroam SP SHOULD forward all authentication for eduroam Passpoint / Hotspot 2.0 clients towards the eduroam infrastructure, but MAY choose to rely on dynamic peer discovery (via NAPTR records) to find the infrastructure.

B.4. eduroam SPs IEEE 802.11 wireless networks MUST support WPA2+Enterprise (possibly via backwards compatibility).

B.5. eduroam SPs networks MUST provide IP address and DNS resolution auto-configuration infrastructure.

B.6. eduroam SPs networks SHOULD provide routable IP addresses, and MAY provide NAT translation.

B.7. eduroam SPs MUST forward all EAP-messages including outer identities, destined for eduroam participants, unmodified to the eduroam infrastructure.

B.8. eduroam SPs MUST NOT charge users or their eduroam IdPs for being admitted on the eduroam SP's access networks.

B.9. eduroam SPs 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.10. eduroam SPs SHOULD keep sufficient logging information to be able to identify the responsible Identity Provider for the logged-in user, by logging and/or sending:

- 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).
- the MAC address and SSID of the connected access point (Called-Station-Id attribute, not always available).
- the SP identifier in the Operator-Name attribute (MAY be provided by the RO).
- type of authentication response (i.e. Accept or Reject).
- Chargeable-User-Identity (CUI attribute) if the IdP returns it.
- 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., DHCP logs).

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