IRANET eduroam Compliance Statement

This document outlines the minimum technical and organizational standards for academic organizations in Islamic Republic of Iran, to join IRANET eduroam National Federation (IEF) in order to provide the global eduroam service inside Iran.

This document is subject to change by the IPM / IRANET eduroam Governance Committee (IPMGC), subject to feedback from IEF members or individual eduroam users.
Any feedback regarding this document should be directed to <eduroam@iranet.ir> for consideration.
In case of a dispute regarding the status of a member in the eduroam service that cannot be resolved by the responsible IEF member or IRANET eduroam operation team, the IPMGC will give the final ruling.

1. Terminology

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 RFC2119.

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. Roaming Identity Provider (RIDP)

A RIDP, also known as "Home Institutions" is an academic organization in Iran, approved by the Ministery of Science, Research and Technology that is responsible for user credentials and operation of an authentication server for eduroam access.

1.3. eduroam Service Provider (eduroam SP)

A SP, also known as "Visited Institutions" is an academic organization in Iran, approved by the Ministery of Science, Research and Technology that operates an access network on which eduroam users are admitted to access Internet services following successful authenticated by their RIDP.

1.4. IRANET eduroam National Federation (IEF)

IEF is overseen by the networking operations unit (IRANET) of the Institute for Research in Fundamental Sciences (IPM) and is responsible to operate the eduroam services in IRAN at Federation Level. The IEF is recognised as such by the TERENA Roaming Confederation.

1.5. APPLICANT
APPLICANT is an academic organization in Iran, approved by the Ministery of Science, Research and Technology that is requesting to become a member of IEF by accepting the policies of eduroam services and signing form in section **5** of this document.

Each applicant will act as RIDP for its own users, and as eduroam SP for visiting users from other members of global eduroam community.

1.6. IRANET eduroam National Federation Member (IEFM)
A IEFM is approved APPLICANT by IEF to use and provide eduroam services inside their organization.

1.7. Roaming Confederation (RC)
An entity that consists of a cohesive set of Roaming Operators serving a geographical region and that is recognized as such by the Global eduroam Governance committee.The “European eduroam Confederation” is one example.

1.8. 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.

2. User identification process

2.1. eduroam uses technologies that allow the identification of every individual user which joins an eduroam SP network.The user identification process is defined via an out-of-band communication between the eduroam SP and the user's RIDP 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 RIDP 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. A RPS operated by an RC, IEF, APPLICANT **MUST** forward EAP-messages it receives, destined for eduroam participants, unmodified to the appropriate RADIUS server (be it RC, IEF or APPLICANT) as determined by the eduroam routing mechanism defined and agreed by the Global eduroam Governance committee.

4. Administrative and technology compliance for APPLICANTs

4.1. The IEFM is responsible for ensuring the eduroam service operation within a particular educational organization.

4.2. The IEFM **MAY** also be responsible for ensuring the eduroam service operation within another educational organization, if no appropriate entity exists in that organization that is able and willing to operate the eduroam service for that organization. Each case of this kind requires explicit approval from the IEF for the geographic region of Islamic Republic of Iran.

4.3. The IEF has the authority to determine the eligibility of APPLICANTs, being organisations engaged in research and/or education, in Iran.

4.4. The IEF has the authority to determine the eligibility APPLICANTs acting as eduroam SPs in Iran. 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 IEF **MUST** establish communication channels to all other IEFMs. IEF MUST be reachable within a reasonable time on this channel.

4.6. The IEF **SHOULD** publish information about the available points of presence of eduroam (SP sites) in Iran in an adequate manner defined by the Global eduroam Governance committee.

4.7. The IEF **MUST** establish communication channels to IEFMs in Iran to be able to communicate changes in requirements and resolve problems.

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

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

4.9. The IEF **MUST** make sure that the IEFMs in Iran 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. APPLICANTs **MUST** agree to follow policies in “IRANET eduroam National Federation Policy” and “eduroam Policy Service Definition”.

5. Administrative and technology compliance for eduroam IdPs and SPs

5.1. The requirements for APPLICANTs are listed in the Appendixes A and B of this document. Those requirements are subject to technology changes and feedback from IEFMs, RC or individual eduroam users. Any changes agreed by the IPMGC 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 APPLICANT unilaterally declares to implement and adhere to the rules set forth herein.
By signing this document, IEF commits to ensure that the APPLICANT implement and adhere to the rules set forth herein.
Failure to adhere may result in the removal of an entity's recognition as a IEFM, including removal of the right to use the eduroam services.

Acting as APPLICANT for: (Organization name / Address)

Signed by: (Name of organization representitive)

Signature: Date:

eduroam Compliance Statement Appendixes

A. Administrative and technology compliance for eduroam Identity Providers

A.1. APPLICANTs **MUST** implement a RADIUS interface to connect to the eduroam routing fabric.
A.2. APPLICANTs **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. APPLICANTs **MUST** send a RADIUS accept message for valid authenticated local users for which they receive an access request.
A.4. APPLICANTs **MUST NOT** send a RADIUS accept message for invalid users or those who are not authenticated.
A.5. APPLICANTs **MUST** provide support to their users. Any support matters may be escalated to the IRF to coordinate and resolve.
A.6. APPLICANTs **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.
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 IEF.
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 stripping 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 changed 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 happening (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.