eduroam User/Device Onboarding - Articulation of Community Requirements

FINAL DRAFT of the eduroam User/Device Onboarding working group, chartered by the eduroam Advisory Committee

1 Summary

eduroam US is increasingly seen not just as a way to roam on Wi-Fi, but as a way to securely and privately configure authorized individual’s wireless devices that can roam within and between eduroam subscriber Service Locations. As the broader eduroam community begins to adopt eduroam, as described in the Requirements for eduroam Growth paper [REGP], broad access, and by extension, ease of support and deployment become critical goals for the service. These goals are accompanied by a need for the service deployment on the part of eduroam subscribers, and Internet2 itself, to be performed in a cost viable manner.

In the summer of 2021, the eduroam Advisory Committee (eAC) sponsored a working group to review the community's needs for additional user device onboarding assistance. The subsequent report, the eduroam User/Device Onboarding Requirements [EUDOR] document was provided for community input in December 2021. The eAC felt the report accurately described the several components of end user onboarding and suggested an option for Internet2 to pursue. In March 2022, the eAC requested additional clarification on the drivers of the proposal and an articulation of requirements and priority of the needs identified. This document is designed to extend upon that work and provide a set of requirements to which the Internet2 team can respond and address the identified need.

2 Problem Statement

The User/Device Onboarding Requirements described in this document is intended to address the seven problems set out in the table below.

ID	Name	Description	Undesirable Consequences
1	Device configuration	It is hard for End Users to configure their devices for eduroam, impeding use of the service, even with the use of mobile device management solutions.	End User uptake is reduced. The value of eduroam to Subscribers is reduced if End Users cannot use the service.
2	Subscriber support burden	It is time consuming for Subscribers to support End Users in configuring their devices for eduroam.	The cost to Subscribers of supporting End Users is elevated.
3	Insecure device configuration	Insecure device configurations can result in security issues.	The compromise of End User privacy, data, and credentials damages perceptions of the service.
4	Compromise of primary credentials	Insecure configuration and/or unwise End User behavior can lead to compromise of their primary organizational credentials	Misuse of an End User’s primary credential can be costly to the Subscriber.
5	IDP implementation	Prospective Subscribers may be deterred from adopting eduroam if they are required to implement a RADIUS IDP	Subscriber uptake is reduced.
6	Internet2 support burden	Subscribers often contact Internet2 for support with operational issues that are caused by misconfigured End User devices.	Internet2 cost of supporting eduroam is elevated.
7	Spurious authentications	Device configurations can persist longer than End User entitlement, resulting in an ever-increasing number of spurious authentication attempts.	Increases operational costs by adding load to systems. Distorts service metrics by inflating authentication attempts and failures.

3 Stakeholders

There are two types of stakeholders that Internet2 should consider in the design of a solution that addresses these problems: Subscribers and End Users.

3.1 Subscribers

A Subscriber is an organization that is enrolled in the eduroam service as an eduroam IDP.

As discussed in the User/Onboarding Requirements document, there are different types of subscribers that might benefit from a User/Device Onboarding solution. In this document, we have classified Subscribers into three different personas, as follows:

1. **Classic Subscribers**: medium- to large-sized universities and research institutions that constitute the majority of Subscribers today. These can be characterized as either:
    a. **“Relief Seekers”**: Subscribers who are content with their eduroam implementation, but are seeking to reduce the cost of providing the service;
    b. **“Secondary Credentialers”**: Subscribers who, in addition to seeking cost reduction, want their End Users to use secondary credentials for eduroam authentication, instead of the primary credentials issued by their organization.

2. **New subscribers without RADIUS and eduroam Support Organization constituents “Newbies”**: the new wave of Subscribers consisting of organizations such as K-12 school systems, libraries, and museums. For these Subscribers, the requirement to operate an eduroam IDP constitutes a significant barrier to implementation, especially when implementing with certificate based authentication.

The differing characteristics of these persona, which are outlined below, may affect their requirements and appetites for a solution.

3.1.1 Classic Subscribers seeking greater efficiency (“Relief Seekers”)

This persona includes those Subscribers that are content with their current eduroam implementation (for example, their RADIUS server and the authentication methods they are using). They are primarily interested in a solution that reduces their costs by addressing problems 1, 2, and 3 (“Device configuration”, “Insecure device configuration”, and “Subscriber support burden”).

Typical organization: Medium to Large Universities & Research Institutions.
Onboarding volume: Thousands to tens of thousands of new End Users per year, with a high churn throughout the academic year.
Human resource: Highly-skilled IT professionals, often with significant relevant technical depth.

State of deployment: ~1000 fully-deployed institutions, many with >10,000 End Users, and mature, established systems that can make them slow to change.
Incommon federation: Likely to be Incommon Federation participants.
Typical infrastructure: Vast, complex infrastructure including commercial IAM solutions, pre-existing RADIUS servers (FreeRADIUS, Cisco ISE, Microsoft NPS, ClearPass, and others), many WiFi access points wireless controllers across a wide geographical area.

Their key challenges include:

- large volume and churn of End Users
- the need for a solution to work with existing infrastructure choices and configurations
- cost of onboarding and supporting large numbers of End Users, and
- discontent with the rising costs and changing business models of commercial solutions.

3.1.2 Classic Subscribers wanting a second credential (“Secondary Credentialers”)

Classic Subscribers are increasingly moving toward Single Sign-On (SSO) solutions that enable their End Users to use a single, primary credential for most or all of their access needs. These systems are typically web-based and leverage the InCommon federation, Shibboleth, and Grouper technology stack.

When these credentials are shared across multiple services, and especially across services with different security models, it increases the likelihood and impact of the compromise of primary credentials. This issue can be alleviated, at least in part, by providing End Users with a secondary credential (which is generally linked to their primary credential) for a specific service. These secondary credentials can then be used to access this service subsequently.

In the eduroam context, many Subscribers are using their End User’s primary credentials for authentication. This use of credentials can secure against compromise, subject to the End User’s device being correctly configured. However, configuring a device for eduroam can require multiple steps and so End Users are prone to inadvertently configuring their devices in ways that make them susceptible to credential compromise.

This persona are those Subscribers that are concerned about the compromise and misuse of End Users’ primary credentials. Their profile is also similar to the “Relief Seekers” defined previously, and so they will also be seeking a solution to problems 1, 2, and 3. However, they prioritize a solution to problem 4 (“Compromise of primary credentials”), to reduce the likelihood of a credential compromise from a misconfigured device.

Their key challenge, in addition to those noted for “Relief Seekers”, is concern about the cost to the organization and the impact on End Users of providing End Users with secondary credentials.

3.1.3 New subscribers without RADIUS and eduroam Support Organization constituents (“Newbies”)

This persona includes those recent or prospective Subscribers that are concerned about the cost of implementing a RADIUS IDP, and managed device management. They are primarily interested in a solution that facilitates their adoption of eduroam by addressing problem ID5 (“IDP implementation”) and ID3 (“Insecure device configuration”).

This persona is differentiated from the Classic Subscribers by two distinguishing features: most do not have an existing RADIUS implementation and are not members of the InCommon Federation.

This persona makes extensive use of cloud-hosted productivity platforms such as Google Workplace (featuring 80% adoption) and Microsoft 365. These platforms provide user directories and web federation, which these organizations use for identity and access management (IAM), but do not tend to include RADIUS. They are often sensitive to costs, and rarely use other IAM tools nor have any specialist IAM resources, and so the implementation of a RADIUS IDP creates a barrier to adoption.

This persona also tends to make extensive use of mobile device management solutions to deploy end user devices. These mobile device management solutions tend to be responsible for installing end user wireless credentials on the device, rather than the end user configuring it for themselves. These credentials either may be shared by all devices deployed at a Subscriber with a mobile device configuration applied, or may be device specific credentials tied to an individual user. Mobile device management paired with secondary credentials is being explored to address K-12 specific device management and traffic filtering needs associated with the Children's Internet Protection Act (CIPA).

Typical subscribers: K-12 Schools.
Onboarding volume: Hundreds to thousands of new end users per year, mostly stable throughout an academic year.
Human resource: Generalist IT professionals, often with less relevant technical depth, and non-IT professionals in a part-time capacity.
State of Deployment: Some existing deployments, but there is still time to influence how eduroam is deployed for the bulk of these Subscribers.
InCommon Federation: Unlikely to be InCommon Federation participants.
Typical Infrastructure: Internet connectivity, relatively small numbers of access points and wireless controllers, eduroam-specific RADIUS Server (often Microsoft NPS), cloud-hosted IAM.

Their key challenges include:

- lack of IT resources having depth of relevant knowledge
- limited budget and resources to adopt new IAM solutions, infrastructure, or services, and

- few resources to support End Users.

3.2 End Users

End Users are people (staff, students, researchers, affiliates, etc.) who are entitled to access eduroam through their affiliated Subscriber. An End User may own or be issued several devices (phone, laptop, tablet, IoT devices, etc.) that are capable of accessing a WiFi network, some of which may already be configured to access eduroam. Many End Users who are entitled to use eduroam do not currently have eduroam configured on their devices.

In many (but not all) cases, End Users own these devices and may want to control if and how eduroam is configured on their personal devices. In other cases, the Subscriber owns these devices and centrally manages their configuration to access eduroam.

End users are primarily interested in a solution that addresses problem ID1 (“Device configuration”).

3.3 Problem Prioritization

The table below suggests the prioritization given to each problem by these stakeholders.

	Subscribers			**End Users**
Problem	**“Relief Seekers”**	**“Secondary Credentialers”**	**“Newbies”**	
Device configuration	High	Medium	High	High
Subscriber support burden	High	Medium	High	Low
Insecure device configuration	High	High	High	Low
Compromise of primary credentials	Medium	High	Medium	Low
IDP implementation	Low	Low	High	Low
Internet2 support burden	Low	Low	Low	Low
Spurious authentications	Medium	Medium	Low	Low

4 Requirements

This section sets out the requirements of a solution meeting the stated problems and priorities of the different stakeholders.

4.1 Non-functional Requirements

The table below lists the non-functional requirements for the solution.

ID	Name	Stakeholder(s)	Description
1	Community control of solution	All	The community should have technical, legal, and practical points of control of all components of the system, so that there is no irreplaceable reliance on third parties.
2	Long-term sustainability model	Subscribers	If successful, the solution will be used by thousands of Subscribers and perhaps millions of End Users. They must be able to depend on it.
3	Reuse of ecosystem FOSS	Internet2, All	As noted in the Requirements for eduroam Growth paper [RFGP], where appropriate, Internet2 would like to leverage the FOSS that already exists in the eduroam ecosystem. This could reduce costs and reduce the time needed to deliver a solution.
4	Subscriber ease-of-adoption	Subscribers	Subscribers can adopt this solution without the need to make any IDP configuration changes, deploy additional infrastructure, or obtain new IT expertise.

4.2 Functional requirements

The table below lists the functional requirements for the solution.

ID	Name	Stakeholder(s)	Description
5	Subscriber ease-of-use	Subscribers	The solution should be easy to use for Subscriber’s administrators. The need to make any configuration changes, deploy additional infrastructure, or obtain new IT expertise must be minimized.

6	Provision of secondary credentials	“Secondary Credentialers”	Subscribers can choose to provision secondary credentials to End Users. Subscriber can also choose to configure a mobile device management solution to consume secondary credentials on behalf of the End User as part of mobile device profile deployment.
7	Authentication of secondary credentials	“Secondary Credentialers”	Subscribers can easily authenticate their End User’s secondary credentials
8	Integration with cloud-hosted user directories	“Newbies”, potentially others	Subscribers can leverage identities stored in cloud-hosted user directories for issuing certificates and non-certificate authentication
9	End User ease-of-use	Subscribers, End Users	Using eduroam should be as easy as installing any other app on a phone or other device.
10	Subscriber opt-in	Subscribers	Subscribers must opt into the solution because they may not wish to use it (e.g., they have another solution).
11	Validation of End User affiliation	Internet2	Prevents End Users from obtaining configuration intended for another Subscriber
12	Provision of device configuration	Subscribers, End Users	This must include support for devices widely used by End Users (e.g., iOS, Android, Windows, MacOS, Linux, ChromeOS, etc).
13	Secure device configuration	All	The solution should only provision secure configurations to protect against well-known misconfigurations (e.g., to protect from MITM attacks by rogue APs advertising “eduroam” SSID). EAP method choice and configuration must comply with [RFC4017] and GeGC compliance statement [GeGC-CS].
14	Protection of user privacy	Subscribers, end users	To whatever extent possible, promote the use of anonymized user identities, hide personally identifiable information, and discourage/prevent user tracking (cyber or physical).
15	Automatic configuration deprovisioning	All	End users’ device configurations must be deprovisioned when term of authorization ends

16	Reporting	All	Subscribers should be able to track downloads of installers, both in aggregate and by user

5 References

[EUDOR] eduroam User/Device Onboarding Requirements, September 2021. https://spaces.at.internet2.edu/pages/viewpage.action?pageId=210796656&preview=/210796656/210796671/eduroam%20User_Device%20Onboarding%20requirements.pdf

[REGP] Requirements for eduroam Growth paper, https://spaces.at.internet2.edu/x/1JMTD

[GeGC-CS] GeGC eduroam Compliance Statement, October 2011. https://www.eduroam.org/wp-content/uploads/2016/05/eduroam_Compliance_Statement_v1_0.pdf

[RFC4017] D. Stanley, J. Walker, B. Aboba; RFC 4017: EAP Method Requirements for Wireless LANs, March 2005. https://datatracker.ietf.org/doc/html/rfc4017