eduroam User/Device Onboarding requirements

Executive Summary

The User/Device Onboarding Working Group was chartered by the eduroam Advisory Committee to develop a set of requirements which Internet2 could use to evaluate solutions which will enable the onboarding of new eduroam users and devices in a secure, interoperable, scalable, and sustainable manner.

The rapid growth of eduroam into portions of the research and education community which are not as fully resourced as many larger institutions (which, to date, made up a majority of the eduroam community) has presented a number of challenges. One such challenge identified by the eAC is the question of how to provision eduroam at the individual level aligned with the Best Practices Guide for certificate based network authentication.

Having a solution in place will lower barriers to adoption, particularly in the K12 and smaller higher ed space. The work being done by state and regional organizations and Internet2 on statewide deployments of eduroam can be a powerful driver for the ubiquity which makes eduroam more valuable, but without solutions for onboarding they may not be able to bring up service.

The recommendation of this group is that Internet2 investigate a solution in which a provider (be that Internet2 or a 3rd party) hosts and manages the PKI infrastructure and Client Provisioning component, with the home institution being responsible for hosting and operating its own RADIUS infrastructure.

Summary of Work

eduroam User/Device Onboarding Models: Infrastructure Hosting and Maintenance

Assumptions

- Institution has an OpenID Connect or SAML 2.0 compliant identity provider
- Institutions can host cloud services in one or more of the following IaaS providers: Microsoft Azure, Amazon AWS, and/or Google Cloud Platform.

Components

There are 3 components required for basic eduroam connectivity: the RADIUS service, a public key infrastructure (PKI) service, and a client provisioning service (CPS).

The RADIUS service is responsible for authenticating institutional users, proxying requests to top-level eduroam servers or directly to institutions, and returning a basic access policy to the network infrastructure (access point, controller, or switch). This is the most critical runtime component and has the highest consumption cost but is not intrinsically incompatible with cloud-born identity stores leveraged by K12 and smaller deployments only capable of leveraging OIDC or SAML 2.0 .

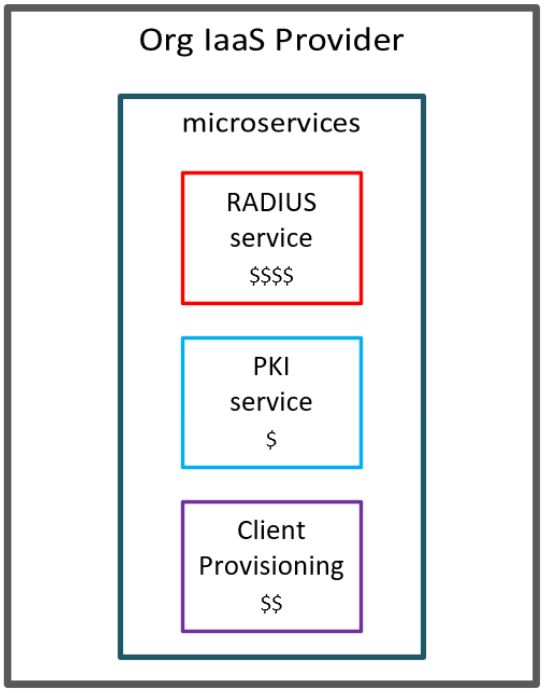
The PKI service is responsible for client certificate issuance in coordination with the CPS. This service has a medium to low consumption cost, depending on whether Certificate Revocation Lists - CRLs (low) or Online Certificate Status Protocol - OCSP (medium) are used for revocation checks. K12 and smaller deployments routinely lack any inherent PKI infrastructure for issuing and managing certificates with the complexities of PKI serving as a significant barrier to adoption of certificate based network authentication as Best Practices suggest. Consider how accounts could be deactivated. While certificate revocation can happen at PKI level, accounts could also be disabled at the local level (so even if a cert is still valid it could be associated with an account which has been deprecated and as such auth requests to that account would ultimately be rejected). Certificate lifetimes could default to four years, which is standard practice in Higher Education.

The client provisioning service (CPS) is responsible for authenticating a user against a federated identity provider via OpenID Connect or SAML and guiding the user through a provisioning process which requests a client certificate and configures a device's supplicant. This process varies by operating system.

In all 3 options below, the three services underlying codebase is maintained by <PROVIDER?>

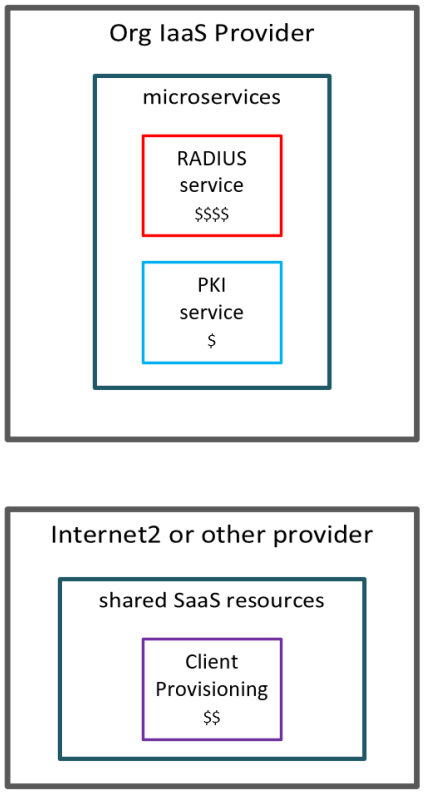
Option A: Institution hosts everything

In this option, the institution hosts all three components in their own cloud infrastructure as a service (IaaS) tenant, thus incurring all consumption costs. The 3 microservices would be packaged together as a marketplace app in Microsoft Azure, Amazon AWS, and Google Cloud Platform in an easily deployable package which can be upgraded as the solution evolves.



Option B: Institution hosts RADIUS and PKI services

For option B, the institution hosts both the RADIUS and PKI services in their own cloud IaaS tenant. These microservices would be packaged together as a marketplace app in Microsoft Azure, Amazon AWS, and Google Cloud Platform in an easily deployable package which can be upgraded as the solution evolves. The CPS would be a shared resource hosted by the <PROVIDER?> and integrated with the institution's RADIUS and PKI services.

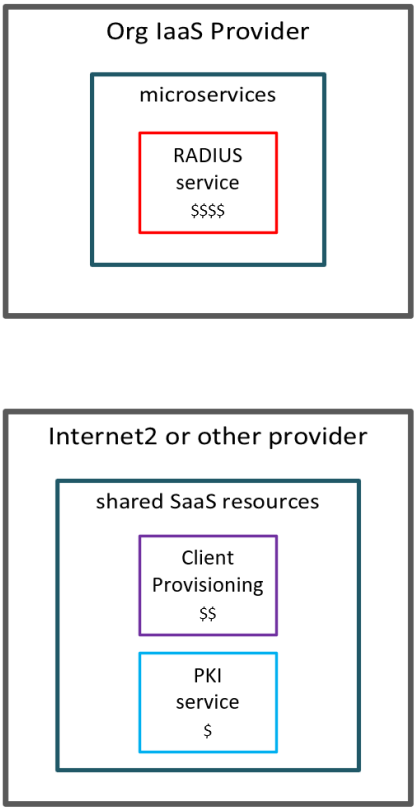


Option C: Institution hosts RADIUS service

This is the recommended deployment model as it balances consumption costs and ease of deployment/maintenance

For option C, the institution hosts only the RADIUS service in their own cloud IaaS tenant. This microservice would be packaged together as a marketplace app in Azure, AWS, and GCP in an easily deployable package which can be upgraded as the solution evolves. The PKI service and CPS would be shared resources hosted by the <PROVIDER?> and integrated with the institution's RADIUS service.

The PKI and client provisioning services have significantly lower operational cost as both are typically invoked once per device, per year. The most expensive component is the RADIUS service which is offloaded to the institution’s tenant.



Configuration Management

There are three potential options for configuration management.

Option A is to expose all configuration parameters to the IaaS platform. Initial configuration would be done during deployment from the marketplace, and any further configuration changes would be done via the IaaS provider's native methods.

Option B is to provide a fourth microservice that provides a GUI and API for configuration of the various components. The basic config would be done with the cloud platform during deployment, and the full configuration would be done via a GUI wizard exposed by the service.

Option C is to make all three services "headless" where they call home to the Provider's service to get their configuration. This allows for a single configuration interface for all services, regardless of their deployment model and provides portability across cloud providers and easy recovery. This is the recommended configuration management option.

The working group has concluded that option three is the most desirable approach for a community User/Device Onboarding service.

eduroam User/Device Onboarding Features

- Support TLS certificates
- Provides a hosted and managed PKI infrastructure.
- Provide some ability for institutions using an MDM platform to benefit from this service
- Leverage existing community resources such as CAT and geteduroam

Community Needs

Members of the eduroam community have expressed a need for a User/Device Onboarding Service which provides a consistent feature set and user experience. Because

- Note existing solution like CAT, limitations that lead to exploring additional options
    - Poor/no support for certificates
- Gear offerings or guidance toward different segments of the community, take into account a “spectrum of readiness”
- Include ability to adhere to K12 regulatory compliance (e.g. CIPA, COPPA, etc)

Recommendations for Internet2

The consensus of the working group is that Internet2 should investigate a solution in which a provider (be that Internet2 or a 3rd party) hosts and manages the PKI infrastructure and Client Provisioning components enabling K12 and smaller deployments to issue certificate based eduroam credentials using cloud identity and limited RADIUS skills (aka “Option C” outlined in the sections above). The institutions will be responsible for hosting and configuring their own RADIUS service as part of the overall solution.

To offset costs, Internet2 and representatives of the community could investigate the possibilities of low or no cost infrastructure which many large technology companies offer to educational institutions and/or not-for-profit organizations, leveraging those opportunities where feasible. Such cost offsets could be critical to making solutions possible, especially for smaller institutions.

The working group feels that there may be some degree of convergence in the mid-long term future between Onboarding services and Guest Access services and suggests looking for points where common infrastructure may be leveraged between the two services. For example, the CPS could leverage the existing CAT and/or geteduroam codebase. Again, leveraging existing

resources like these could lower the cost and lower barriers for adoption by organizations with lower levels of staffing and/or funding.

Finally, the working group strongly recommends that Internet2 consider upcoming technologies like OpenRoaming or Passpoint, and continue to track how they could impact the value proposition and/or functionality of eduroam.

Technical Requirements for User/Device Onboarding

Technical Requirement	**Relevant Standards/Guidelines**
Meets GEANT requirements for participation in eduroam	https://www.eduroam.org/wp-content/uploads/2016/05/eduroam_Compliance_Statement_v1_0.pdf
Conforms to community best practices	https://spaces.at.internet2.edu/display/eduroam/Consultation+on+eduroam-US+Best+Practices+Guide?preview=%2F174066029%2F174066124%2Feduroam-US+Best+Practices+Guide.pdf
Operates in a manner consistent with US eduroam subscribers	https://incommon.org/wp-content/uploads/2019/05/eduroam-connector-agreement-201711-Rvw-Copy.pdf
For K12 student use cases, comply with CIPA, COPPA. Consider other federal regulations may be a factor depending on use case	https://www.fcc.gov/consumers/guides/childrens-internet-protection-act https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule