24-02-2016

Deliverable D9.3 Service Approach Specification to Small Site eduroam Adoption

Deliverable D9.3

Contractual Date:	31-10-2015
Actual Date:	24-02-2016
Grant Agreement No.:	691567
Work Package/Activity:	9/SA5
Task Item:	Task 7
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	SRCE/RESTENA
Document Code:	GN4-1-16-10AEFF

Author:	Stefan Winter (RESTENA)
Co-editors:	Ann Harding (SWITCH), Miroslav Milinovic (SRCE)
Contributors:	Marko Eremija (AMRES), Scott Armitage (JISC), Alan Buxey (JISC), Stelios Sartzetakis (GRNET), Hideaki Goto (Tohoku University & NII), Rok Papez (ARNES), Janos Mohacsi (NIIFI), Phillippe Van Hecke (Belnet), Raimundas Tuminauskas (LITNET)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

Abstract

This deliverable investigates the requirements to support the deployment of eduroam at smaller, less well-resourced or experienced eligible sites. It assesses the benefits and value proposition of providing an 'as-a-Service' model of deployment for these users and outlines potential products for Identity Provider and Service Provider deployment.

Table of Contents

Table of Figures

Executive Summary

The eduroam service provides secure, consistent and uniform roaming network access. Since its beginnings in Europe, eduroam has gained momentum throughout the research and education community and is now available in 74 countries. GÉANT operates the regional level service for members of the European eduroam Confederation which comprises 44 members. The confederation is a group of autonomous roaming services, who agree to a set of defined organisational and technical requirements by signing and following the eduroam Policy Declaration [POLDEF] based on the eduroam Service definition [SERVDEF]. After more than ten years of operation, eduroam has a global footprint of around 15 000 service locations, more than 3 000 Identity Providers and an estimated 10 million active users. This is evidence that the benefits of the service are well known and widely appreciated by the R&E community.

However, some remaining eligible sites have yet to implement eduroam and some experience difficulties in deploying more than the simple basics. This report defines a recommended approach for extending the eduroam service to smaller sites that have not yet adopted it or that wish to enhance the quality of their eduroam deployments but are not currently able to do so due to technical or skills gaps.

1 Introduction and Background

The purpose of eduroam (**edu**cation **roam**ing) is to provide a secure, world-wide roaming access service for the international research and education community.

The eduroam service allows students, researchers and staff from participating institutions to obtain Internet connectivity across their campuses and when visiting other participating institutions by simply switching on their laptops. The architecture that enables this is based on a number of technologies and agreements, which together provide the essential eduroam user experience: "open your laptop and be online".

The basic principle underpinning the security of eduroam is that the authentication of a user is carried out at his/her home institution using the institution's specific authentication method. The authorisation required to allow access to local network resources is carried out by the visited network.

The recommended approach described in this deliverable is based on the principles and technology of the eduroam consortium. Background information on the overall eduroam technical architecture can be found in the eduroam Architecture for Network Roaming paper [RFC7593], while the service definition for eduroam in Europe is described in the eduroam Service Definition [SERVDEF].

In business terms, the eduroam operational model is similar to a franchise in that the main service and some auxiliary services' specifications are defined centrally, while the actual service delivery to end users is managed by participating institutions in the NREN constituency. Institutions may either take on the role of eduroam Identity Providers (IdPs), issuing accounts to their own users and maintaining their own authentication infrastructure, or of eduroam Service Providers (SPs), providing internet access to valid eduroam users, or both roles at once. IdPs and SPs are aggregated on a national level and governed by eduroam National Roaming Operators (NROs), which are either the NRENs themselves or third parties that have been assigned the role by their NRENs, where an NREN exists. NROs are governed by the Global eduroam Governance Committee (GeGC).

For all aspects of service delivery, i.e. IdPs, SPs, NROs and the GeGC, the overall service specifications strike a balance between items which require uniform handling – and thereby central control – and items which can be left to service implementers in the field.

Historically, the level of centralisation of eduroam was low, and most aspects of the service were managed by the participants at the NRO or IdP/SP level. As the service evolved over time, it became apparent that service levels and end-user experiences varied significantly across NROs, as well as between individual SPs and IdPs within an NRO. Therefore, the service specifications have been refined over time and now contain a set of "MUST" requirements for baseline service delivery and

"SHOULD" items for enhanced quality of service. To further improve service levels, central monitoring and configuration assistance tools were devised which allow assessment of operational status and compliance with many of the requirements as set forth in the service definition in its current form.

The requirement to adopt all of these improvements sets a higher threshold for participation than the simple deployment of an IdP/SP according to local policy. Therefore this deliverable investigates the possibility of offering an 'as-a-Service' option for deploying eduroam targeted at organisations that do not currently participate in eduroam, or that would like to enhance the quality of their eduroam deployment to take advantage of these improvements.

2 Value Proposition for eduroam Small Site Adoption

2.1 Compelling Reason to Act

Field experience has shown that, despite clear service definitions, some IdPs and SPs fail to meet even the baseline service level and deliver an inconsistent roaming experience. Additionally, an unknown number of potential Identity or Service Providers do not participate in eduroam at all. A contributing factor in this is that, as quality criteria are enhanced and excellence is promoted over minimum compliance, they perceive that the burden placed on smaller sites is too high compared to that of simply operating a basic IdP and SP.

The following two sections illustrate the negative consequences of a suboptimal implementation of the service. These are more likely to be encountered in deployments where no eduroam specialists, or even designated Wi-Fi or permanent IT experts, are available to support and operate the service. Providing them with a service designed by eduroam experts can help these sites avoid these problems with minimal effort on their part.

2.2 eduroam Identity Provider Reasons

The requirements for eduroam Identity Providers within Europe are set out in the eduroam Service Definition [SERVDEF].

Failure to adhere to the "REQUIRED" set in the specification in most cases leads to immediate authentication failure on a technical level. Once those basic requirements are cleared and users are able to log in, the IdP service may appear acceptable upon superficial observation. However, there are many points in service delivery which differentiate an excellent eduroam Identity Provider from a mediocre or even a poor one. A non-exhaustive list of examples includes:

- **An IdP does not inform its users of the applicable security parameters which allow identification of the genuine authentication server (this information is required for compliance with the eduroam Service Definition but cannot be automatically monitored or addressed).**

Failure to comply with this requirement makes users susceptible to man-in-the-middle attacks and rogue “evil twin” networks, increasing the risk of credential theft.

- **An IdP does not keep the authentication server up-to-date with the relevant security patches (this is required for compliance with the eduroam Service Definition but can only be partially monitored or addressed).**

  Failure to comply with this requirement puts the account credentials and any other sensitive information on the authentication server at risk of compromise or abuse.

- **An IdP does not respond to requests for Chargeable-User-Identity for new user sessions (this is a recommendation which allows for better incident handling).**

  Failure to implement this recommendation means that users acting maliciously cannot be singled out by Service Providers, who in this case may need to block all users from the IdP just to prevent one malicious user from gaining access.

- **An IdP sends VLAN assignment attributes for its authenticated users regardless of whether they are using the local campus network (where the VLAN attributes are understood) or a roaming network (where those VLAN attributes are almost never understood).**

  This item is not regulated as there are only few legitimate uses for these attributes in a roaming scenario. However, great care needs to be taken to implement correct handling of these attributes, as failure to apply filtering on VLAN assignment attributes may lead to a Denial of Service for the end user at the remote roaming hotspot.

- **An IdP does not allow users to make use of anonymous outer identities in their client configurations (this item is not regulated: it is acceptable where it was implemented intentionally by the IdP administrator, but is suboptimal where it is the result of unintentional misconfiguration).**

  A suboptimal configuration may decrease the level of privacy for the end users of the Identity Provider.

2.3 eduroam Service Provider Reasons

The requirements for eduroam Identity Providers within Europe are set out in the eduroam Service Definition [SERVDEF].

Currently, failure to comply with the requirements and recommendations may compromise an individual user’s session, but go largely undetected outside the hotspot itself. For example, a lack of addresses in a DHCP pool due to too many users at a hotspot may result in a Denial of Service for one user who cannot get an IP address, but leaves no traces beyond the local network which could be monitored and remedied.

Many of the local hotspot issues are specific to the Wi-Fi layer and require additional monitoring insight using probes, however this topic is outside the scope of this deliverable.

Many other Service Provider setup issues however are the result of improper configuration of the local authentication server and infrastructure. Typical examples of configuration aspects which may lead to a suboptimal level of service on the Service Provider side are:

- **The Service Provider does not synchronise the authentication server clock to a reliable time source (this is required for compliance with the eduroam Service Definition, but cannot be satisfactorily monitored).**

  Failure to implement this requirement makes it impossible to link a user login on the SP side to an actual end user on the IdP side, which goes against one of the eduroam cornerstone principles, i.e. the identifiability of users.

- **The Service Provider decides to filter certain user realms (e.g. '.com' domains) mistakenly believing they are not eligible for eduroam. It is a requirement of the eduroam Service Definition to forward authentication attempts to the eduroam infrastructure without discriminating any realm (except in reactive blocking following fraudulent use).**

  Failure to forward all realms leads to Denial of Service situations for users who actually do have a username in such realms.

- **The Service Provider does not send its hotspot identification inside the Operator-Name attribute as recommended in the eduroam Service Definition.**

  Not sending the Operator-Name makes debugging user problems on the IdP side more difficult because the originating Service Provider and the matching user session cannot be identified.

- **The Service Provider does not request the Chargeable-User-Identity attribute when originating new login requests as recommended in the eduroam Service Definition.**

  Not requesting CUI information means missing the opportunity to single out specific users should they misbehave and need to be blocked from using the Service Provider's network. This means the Service Provider may need to take overly drastic measures to exclude such a user, such as blocking all users from the realm, effectively resulting in widespread Denial of Service.

- **The Service Provider fails to filter incoming RADIUS attributes from the IdP.**

  This leads to potential network and/or authentication issues as the irrelevant attributes are acted on by the RADIUS server and/or wireless infrastructure. e.g. VLAN override attributes.

- **The Service Provider fails to send the RADIUS attribute Calling-Station-Id in its requests as required in the eduroam Service Definition.**

  This can cause issues identifying devices at the NRO or IdP, or even lead to rejection of the user at the IdP because the request is malformed.

2.4 Benefits

2.4.1 eduroam NRO Benefits

There are numerous benefits for eduroam National Roaming Operators in terms of service participation and quality of deployments.

One obvious benefit is the increased eduroam footprint in the NRO’s service area when new organisations are enabled to join eduroam.

Another significant benefit is that the NROs’ internal helpdesk effort towards SPs and IdPs can be reduced. This because:

- IdPs and SPs using the outsourced solution will benefit from a maintained, working, and actively managed platform developed by eduroam experts in GÉANT, leading to reduced likelihood of service failures.
- Incident handling is simplified as more SPs and IdPs perform at a better level, leading to increased prevention and/or decreased severity of incidents.

2.4.2 eduroam Service Quality Benefits

The end users’ perception of the service is fundamental to eduroam. Failure at a single SP or IdP can lead to significant brand damage for eduroam overall, because the typical conclusion when something does not work is “eduroam is broken” (rather than a nuanced view that considers that the mistake may be of the organisation of the SP or IdP), and this simplistic view can spread worldwide via social media channels etc.

By providing high-quality SP and IdP building blocks, many potential problem sources in service delivery to end users can be eliminated, as greater centralisation of these components will ensure any issues can be quickly identified.

The quality of incident resolution will also improve internally when the outsourced IdP or SP functions are on the critical path of an incident. This because the corresponding functions are administered by a known team (eliminating the need to search for a responsible person), and the functions themselves are built to include all possible desirable properties for expedited incident resolution.

2.4.3 eduroam Adoption Benefits

eduroam’s visibility depends both on the number of users who have an account and know how to use it, and on the number of hotspots where these accounts can be put to use.

By lowering the technology bar for future IdPs and SPs, a significant positive effect in the growth of eduroam can be expected.

3 Product Descriptions

Educational and research institutions are eligible for adding their own user base to eduroam, and so typically assume the roles of Identity Provider and Service Provider simultaneously. However some organisations which are ineligible to create eduroam user accounts could still benefit from being an eduroam Service Provider only, i.e. allowing eduroam users onto their networks while not having users themselves. The operational model of delivery assumes an acceptance of centralisation for key elements but does not fully relieve NROs and campuses of all responsibilities. In particular, the NRO must still have an overview of the Identity Providers, regardless of where they are hosted, and an Identity Provider organisation must still hold responsibility for identity management, i.e. adding, changing and deleting users as appropriate.

3.1 eduroam IdP Functions as-a-Service

3.1.1 Target Groups and Market Size

A typical example of an eduroam Identity Provider would be a university that needs to manage several thousand student accounts and hundreds of staff accounts. Organisations of this size can be expected to have a well-operated identity management backend and an IT department that can run its own authentication servers. As the majority of these Identity Providers have already successfully deployed eduroam to a high standard of quality, they are not the target group of the solutions presented in this deliverable.

However, there are a number of other organisations of various sizes that are eligible to join eduroam but may be missing out for various reasons. Some large organisations for example do not have a sufficiently staffed IT department to master their own authentication servers (e.g. large secondary schools), while other organisations are too small to warrant the effort of server maintenance (e.g. a research organisation with only a low, two-digit number of employees).

These organisations are the target group for the solutions presented in this deliverable, given one precondition, as follows:

The organisation’s user management must ensure that only its current users can use eduroam, and that the data relevant to eduroam about this user base can be queried automatically by the solutions proposed in this deliverable (e.g. via SAML assertions).

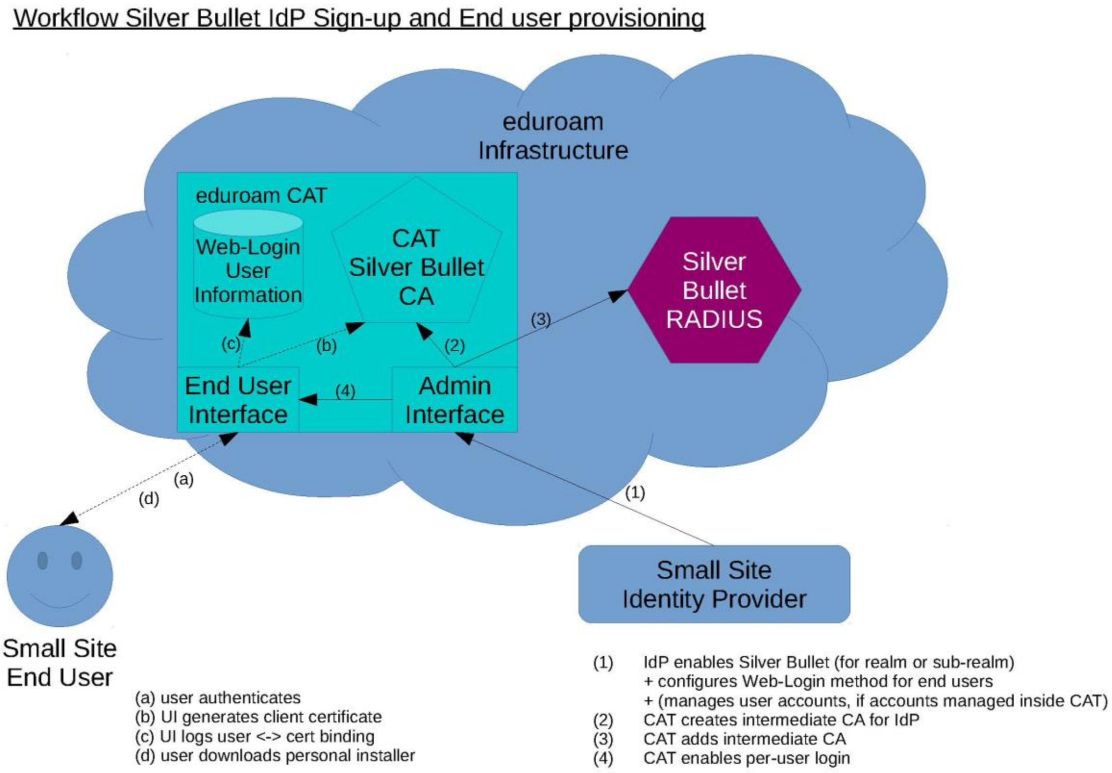
This means that the requirement for eduroam Identity Providers in section 6.3.2 of the service definition [SERVDEF], “A well-managed identity management backend system”, needs to be fulfilled.

3.1.2 Technical Description

3.1.2.1 *Scope of Technical Solution*

The general goal of the “IdP-as-a-Service” solution is to implement and operate as many of the requirements and recommendations of section 6.3.2 of the service definition [SERVDEF] for the target group as is possible without sacrificing security and operational capability.

The overall architecture of the solution is depicted in Figure 3.1 below.



(a) user authenticates
(b) UI generates client certificate
(c) UI logs user <-> cert binding
(d) user downloads personal installer

(1) IdP enables Silver Bullet (for realm or sub-realm)
+ configures Web-Login method for end users
+ (manages user accounts, if accounts managed inside CAT)
(2) CAT creates intermediate CA for IdP
(3) CAT adds intermediate CA
(4) CAT enables per-user login

Figure 3.1: IdP-as-a-Service solution architecture

IdP-as-a-Service comprises three main elements:

1. A RADIUS server which handles EAP authentication. The RADIUS realm should be managed by the organisation. This means that the request routing to the IdP-as-a-Service RADIUS server needs to be established across several NROs involved (and should also be published in DNS NAPTR records). This is however no different than for all other realms. At the RADIUS level, NROs should consider the IdP-as-a-Service solution as “third-party outsourcing” of the technical setup of their participants.

2. A web interface which delivers all the configuration information for users of the RADIUS authentication server, including all the details needed to verify the server's authenticity.
3. An administrator interface where the institution's administrator can manage the eduroam accounts under their control, including:
   - Connecting IdP-as-a-Service to the pertinent identity management backend;
   - Ability to add and remove eduroam accounts, including specification of lifetime of those accounts;
   - Ability to block/disable user accounts without fully removing them;
   - Ability to create short-lived guest accounts;
   - Possibility to query authentication server logs to help the administrator identify actual users (in cases of debugging and incident management);
     - List of all Chargeable-User-Identity mappings for each of the users,
     - Given a timestamp and MAC address, identify the authentication session for a specific user.

The responsibility for proper management of the provisioned identities stays with the IdP. If the identity management functions within the IdP are rich enough, and if an interface to exchange the user data can be created, then user accounts and possibly default account lifetimes can be created semi-automatically. As an example, if the IdP has a SAML interface a username can be validated using SAML authentication assertions. The lifetime of the corresponding account can be determined by a user attribute e.g.: if the role is "staff", then a long-lived TLS certificate will be created; a "user" role has shorter lifetime to account for per-semester churn in student registers; and an "other" role would only qualify for a short-lived guest account.

Depending on the ease of use of the developed solution and its IdM interfacing capabilities, the system may also be attractive to larger IdPs. In an initial phase, while operational experience is gathered, the service will actively restrict the usage by such IdPs. This restriction will take the form of a user count limit that can be administered via the user interface. Since positive field experiences with a similar solution have already been recorded in large organisations in Japan (DEAS), the size limit may be softened or lifted entirely at a later stage.

3.1.2.2 *Technical Realisation*

The solution will implement the EAP type EAP-TLS, using a CAT module for administrators, a CAT module for end users, a Certification Authority operating in the eduroam CAT backend, and a RADIUS server for actual user authentication. The following building blocks will be put in place:

- eduroam CAT administrator interface:
  - addition of the "Silver Bullet EAP-TLS" choice in the Profile/EAP-Type selection;
  - eduroam CAT administrator interface – dedicated Silver Bullet management page, which allows administrator to:
    - specify the SAML endpoint where users authenticate,
    - specify other IdM interfaces (LDAP?),
    - add user accounts and web login passwords without external mapping.

        - — specify if accounts should reside in a sub-realm (allowing own user accounts besides Silver Bullet) or the entire realm of the institution,
        - — delete provisioned EAP-TLS client credentials (triggers revocation of all certificates associated with the user account);
- eduroam CAT user interface:
    - ○ when selecting a Silver Bullet Identity Provider, authenticates end user as specified by the administrator (SAML, …);
    - ○ after authentication, creates installation programs/profiles per user, each with its own client certificate, crafted on demand;
    - ○ permanently stores mapping between authenticated username and opaque identifier of the client certificate;
    - ○ keeps track of number of authenticated users who are in possession of a valid certificate; denies creation of new installers when the user limit is reached (and informs administrator when remaining accounts are low or zero);
    - ○ issuing reminders regarding certificate expiry and/or automatic renewal of the certificate directly from the configured device are out of the scope of this solution.
- eduroam CAT CA backend:
    - ○ an offline root CA is created with the sole purpose of creating/revoking intermediate CA certificates per Silver Bullet institution;
    - ○ the per-institution intermediate CAs are online CAs; certificates are created on the fly for each authenticated user whenever an installer is being downloaded;
    - ○ the private key to the user certificate is not retained; further downloads of installation programs by the same user generate a new certificate and private key;
    - ○ client certificate identifiers take the form of <opaquehash>@<adminchoice>.realm.tld or <opaquehash>@realm.tld.
- RADIUS server (FreeRADIUS 3.x):
    - ○ Is configured exclusively for EAP-TLS;
    - ○ Accepts user logins with valid certificate from the root CA (and all its intermediates);
    - ○ Consults CRL for intermediate and root CA;
    - ○ implementation may take the form of one EAP configuration and virtual server per realm in order to reduce CRL lookup complexity to two CRLs per virtual server;
    - ○ implementation will configure all “MUST” and “SHOULD” requirements from the eduroam Service Definition;
    - ○ there may be multiple instances of this RADIUS server. Specifically, one copy per NRO may be in place to authenticate users in a national context more quickly, or one copy may also reside at the IdP to authenticate local users in a streamlined way.

For the solution to work in an international roaming context, the realms which are enabled in the system need to be routed correctly to the RADIUS server, i.e.:

- If the administrator chose to let Silver Bullet handle the entire institution's realm, the NRO will need to forward that realm to the Silver Bullet RADIUS server.

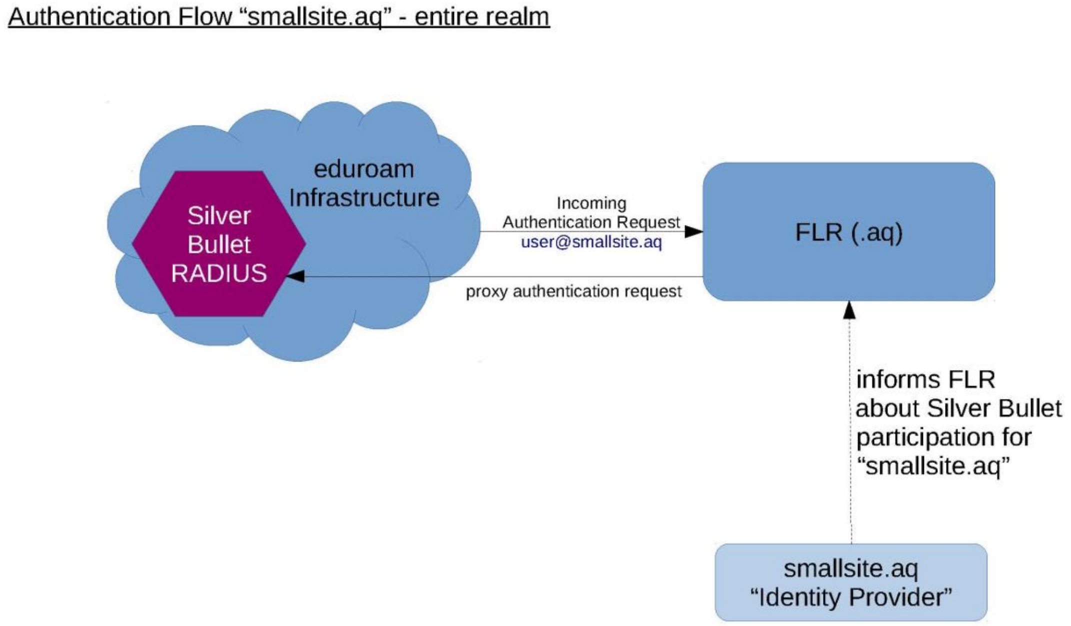

Authentication Flow "smallsite.aq" - entire realm
eduroam Infrastructure
Silver Bullet RADIUS
Incoming Authentication Request
user@smallsite.aq
FLR (.aq)
proxy authentication request
informs FLR about Silver Bullet participation for "smallsite.aq"
smallsite.aq "Identity Provider"

Figure 3.2: Authentication flow – entire realm

- If the administrator chose to only dedicate a sub-realm to the solution, the NRO forwards requests for the entire realm to the organisation, and the RADIUS server of the organisation needs to forward the sub-realm in question to the Silver Bullet RADIUS server. Alternatively, the NRO may create two distinct forwarding rules: redirect the sub-realm to the Silver Bullet RADIUS server; or, redirect all other requests to the IdP.

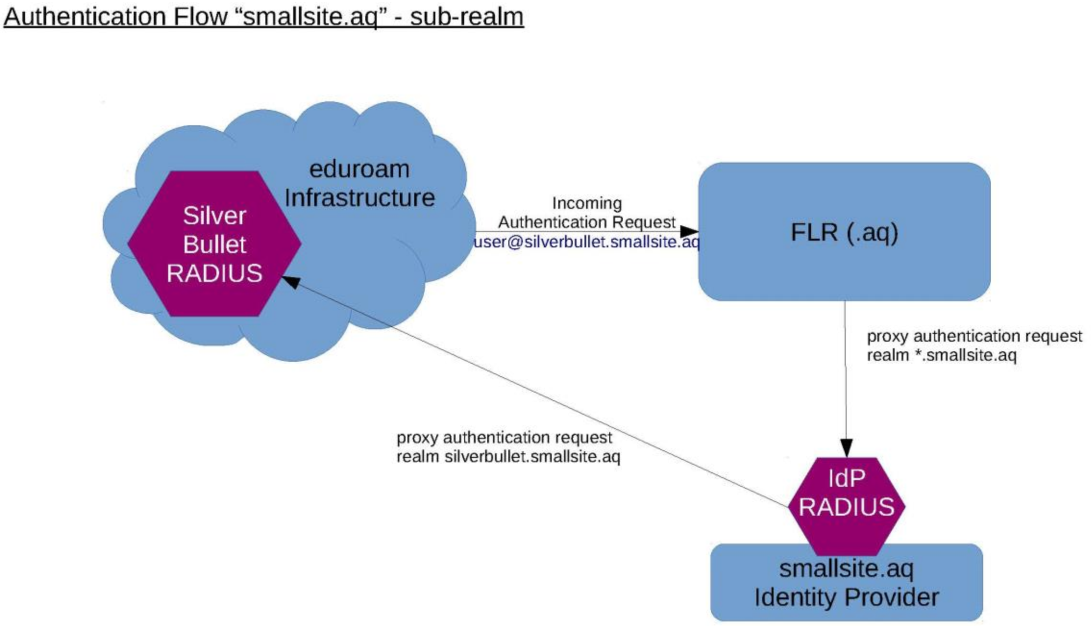

Authentication Flow "smallsite.aq" - sub-realm
eduroam Infrastructure
Silver Bullet RADIUS
Incoming Authentication Request user@silverbullet.smallsite.aq
FLR (.aq)
proxy authentication request realm *.smallsite.aq
proxy authentication request realm silverbullet.smallsite.aq
IdP RADIUS
smallsite.aq Identity Provider

Figure 3.3: Authentication flow – sub-realm

- The use of NAPTR records for the realm or sub-realm directly to the Silver Bullet RADIUS server is RECOMMENDED.

3.1.3 Suggested KPIs

- **KPI1: Acceptance by NROs**

  Within one year after launch, at least three eduroam NROs promote Silver Bullet to their constituency.

- **KPI2: Uptake at campuses**

  Within one year after launch, at least five Identity Providers enable the Silver Bullet EAP-TLS solution and provision at least one user account with it.

- **KPI3: Positive evaluation by pilot participants**

  Qualitative evaluations from interview/survey of pilot participants at campus and NRO.

- **KPI4: service quality**

  NRENs/NROs evaluation of the quality of service from participant sites vs. their expected workload for independent deployment.

3.2 eduroam SP Functions as-a-Service

eduroam Service Providers need to be able to provide Wi-Fi at their premises. In principle it is possible to centralise deployment of IEEE 802.11 layer 2 equipment, but this is hard to do at scale and requires intimate knowledge of the network on campus. Accordingly, any outsourcing is best placed near the Service Provider for administrative and technical purposes, i.e. aggregated at the NRO level at most.

For this reason, the provisioning and management of the layer equipment at eduroam Service Providers is considered out of scope for this solution. However, failures on this “last mile” of a local campus are also those that can result in the most significant reputational damage to the eduroam brand, because all failures of an eduroam hotspot are typically attributed to eduroam at large, not to the Wi-Fi setup of the specific campus.

A managed solution for eduroam Service Providers thus should include as many functions as possible, and at least enable some monitoring of the performance of the hotspot in question.

Care must be taken to define interfaces at the point where local responsibility for managing the service begins, so as to prevent any possible interruptions in the audit trail for incident resolution.

Additionally, even though an outsourcing solution for an SP does not necessarily need to involve its NRO on a technical level, it will still need to allow the NRO to maintain an overview over its SP deployments.

3.2.1 Target Groups and Market Size

The initial target market is identical to that for Identity Providers, i.e. mainly universities and educational institutions, which eduroam according to its founding principle aims to enable to participate fully in the exchange of resources. eduroam also provides significant value to the R&E community with Service Provider locations outside institution campus venues (e.g. at airports, train stations, tourist locations, etc.). However, deploying eduroam has complex technological implications for these entities. Reducing that complexity may enable the addition of new Service Providers in these non-traditional locations.

3.2.2 Technical Description

3.2.2.1 *Scope of Technical Solution*

The envisaged solution outsources the authentication and authorisation endpoint for hotspots (i.e. the RADIUS outbound interface) towards one or more aggregation points operated by the eduroam Operational Team. Multiple, and possibly anycasted, instances of the service, evenly distributed geographically, may be required to reduce latency towards the hotspots. All other aspects pertaining to deployment and operation of a Wi-Fi hotspot remain the responsibility of the hotspot or the NRO including, but not limited to:

- Site survey.
- Procurement of layer 2 devices.

- Configuration of layer 2 devices.
- Provisioning of DHCP servers for the end user network.
- Access control of payload traffic on layer 3 and above (firewalling) for the end user network.
- Traffic backhaul from the hotspot to the internet.

Given that the RADIUS interface is disjoint from the hotspot’s layer 2 topology, it is difficult to include user separation (VLAN assignment) into the resulting system. A coarse-grained administrator-level control which allows VLAN assignment by realm of the outer identity is envisaged, but this is considered to be of secondary importance.

Given that DHCP and ARP/Neighbor Discovery traffic remain contained in the hotspot network, the solution cannot provide the most crucial element for proper incident resolution that is, mapping from the authenticated MAC address to the IP address in a session. Its scope is consequently limited to maintaining RADIUS logs of the authentication sessions. Logs of layer 2 and layer 3 user bindings are out of scope.

The scope of the solution is entirely technical. The hotspot operator remains a customer of the NRO in question; accounts for the RADIUS interface are issued only following an invitation by the NRO (an operational model comparable to the eduroam CAT invitation system). Therefore, there are no particular policy considerations on the side of eduroam Operations. It remains the decision of the NRO whether or not to consider a partly outsourced eduroam SPs as a special case (needing additional local policy provisions).

The solution will include the requirement to monitor the deployed hotspot to allow for sufficient insight by eduroam Operations on the service quality of the hotspot. To that end, one of the existing NRO “probe” systems will be selected, and the hotspot will be equipped with one such probe. This means that a deployment of the probe equipment will induce actual hardware and shipping and handling costs, the allocation of which has yet to be decided.

This solution roughly corresponds to the category “Authorisation-only by NREN” as defined in the GN3plus JRA1 Task 3 Deliverable [GN_JRA_NETARCH].

3.2.2.2 *Technical Realisation*

The system should be realised with at least three RADIUS servers strictly in a proxy-only role. The RADIUS servers will be FreeRADIUS 3.x installations. The three servers will be physically located in the Netherlands (near ETLR1), Denmark (near ETLR2) and in Croatia (near European Monitoring) respectively to achieve significant geographical spread.

The servers will be configured identically with all servers sharing and synchronising the same client list; where required, the system can scale horizontally (more servers, maintaining the global client list, possibly spanning the globe) or vertically (partitioning the client list, creating local clusters of servers - e.g. per NRO).

In a non-anycast scenario, hotspots can select two or more IP addresses of servers from the pool in a classic failover configuration; if an anycast group is created, then hotspots can select any one IP address and will reach the nearest available server.

The template configuration for each server – which implements all the "MUST" and "SHOULD" items for eduroam Service Provider RADIUS servers of the European eduroam Service Definition – will be maintained in a revision control repository so as to enable all deployed instances of the server to be updated with configuration changes when and if eduroam best practices change over time.

A web interface, possibly integrated in the administrator interface of eduroam CAT, will be created to allow provisioning, settings maintenance and deprovisioning of new hotspots.

3.2.3 Suggested KPIs

- **Acceptance by NROs**
- **Uptake at campuses (slightly out of scope) and off-campus**
- **Positive evaluation by pilot participants**
- **Measurements related to service quality e.g. % drop in issues**

4 Conclusions and Recommendations

Based on the analysis and proposal set out in this deliverable, there are considerable benefits to offering an 'as-a-Service' enhancement to stimulate eduroam adoption in the future. These benefits are both quantitative, in terms of the opportunities such a service offers for adding more service locations and participating institutions, and qualitative, in that it would help to safeguard the quality of the eduroam experience, thereby protecting eduroam’s reputation.

It is therefore recommended to proceed with service development based on the product lifecycle management of GÉANT and to finalise the strategy phase by completing a Cost Benefit Analysis and Business Case. Funding should be allocated in future projects to complete the design and pilot the service. It is also strongly recommended that global collaborations should be undertaken during the development phase and to include potential funding/cost model scenarios for use within the European Confederation and beyond in the analysis. The experience in producing this study has shown that although there is interest and demand on the user side, it is only by aggregating interested parties more widely that enough dedicated expertise can be made available to complete the work. Cost models and operational models must also be considered in this context.

Appendix A National-Level Approaches by NROs

There are various approaches to outsourcing of IdP and/or SP functions by NRENs. The following list is the result of a survey involving national operators, both European and world-wide.

A.1 Belgium

- **IdP small:** yes
- **IdP big:** no
- **SP:** no
- **Special Policy:** unknown

No operational service is currently in place, however there are plans for the implementation of such a service.
The focus of the solution considered will probably be small institutions, as most large organisations have all the required knowledge to implement the service themselves.
It is envisaged that identity management will be provided in several different ways, including access to existing institutional databases (LDAP, AD, etc.) or via a direct user database at the NREN level. Deployment of the system will probably be via cloud-compute services as an appliance.

A.2 Greece

- **IdP small:** yes
- **IdP big:** yes
- **SP:** yes
- **Special Policy:** no

GRNET is providing managed IdP and SP RADIUS services for institutions that cannot afford to run such services and/or have a strong preference or other practical reasons to outsource this function to GRNET. This service is primarily used by beneficiary institutions of the Wi-Fi infrastructure that was procured by GRNET through recent projects. For the IdP function, the service currently requires a previously established user database and authentication backend (typically LDAP), which is normally used as a backend also for other federated services; therefore user management remains beyond the scope of this service.

A.3 Hungary

IdP small:	yes (primary and secondary schools)
IdP big:	no
SP:	yes (primary and secondary schools)
Special Policy:	yes

NIIFI is providing hosted IdP and managed SP for primary and secondary schools.

Hosted IdP:

The NIIF Institute is running the user database on a redundant LDAP system with a redundant RADIUS server. A user management interface for school administrators has been developed in-house which covers user management, affiliation, mail addresses and aliases; mass user management is also possible. The user management interface is integrated with the centralised mail systems for the schools. Both the mail system and eduroam are optional for every school. Schools that enrol in eduroam have to sign a simplified eduroam/eduID contract. Schools are solely responsible for updating their user database and where not compliant can have their capabilities to access eduroam removed.

Hosted SP:

The NIIF Institute was awarded the tender to install Wireless APs in schools, for which it developed an integrated service management solution that enables school administrators to configure some basic settings for the Wireless network parameters in addition to the non-configurable eduroam services.

A.4 Japan

IdP small:	yes
IdP big:	yes
SP:	no
Special Policy:	no

The following centralised IdP services have been in operation for several years in Japan. Both systems are open to any institutions, including larger ones. They are not exclusive and some institutions are using multiple IdPs in addition to their own. Some use the centralised IdP for guest account service only.

- **Delegate Authentication System (DEAS):**

  DEAS is fully-independent of the institution's database. It is equipped with an online sign-up extension that uses an email address for pre-authentication. More details can be found in the corresponding presentations given at the 32nd and 33rd TF-Mobility and Network Middleware meetings [TF-MNM]. In addition, the national IdP has also been found useful for guest account support.

One of DEAS's design decisions was to include the institution's name in the realm (e.g.: @<inst_name>.eduroam.jp) to make it clearer who the responsible bodies are. This design has proven quite successful and provides some additional benefits, such as support for Dynamic VLAN assignments, as an institution can enable Dynamic VLAN by checking whether or not the realm matches their own.

- **Shibboleth-based eduroam account issuing system (eduroam-shib)**

  eduroam-shib uses a common, fixed realm (@upki.eduroam.jp) and does not provide an attribute, making the use of Dynamic VLAN impossible. This is expected to be improved in the next generation: the system is currently under revision following discussions at the APAN40 meeting (see [APAN40]).

Using these two systems, IdPs can provision accounts either automatically (using a SAML connection to the identity management system) or manually, via a web frontend. The RADIUS accounts are EAP-TLS client certificates. Revocation is possible with CRLs upon the administrator's request.

There is no special policy regarding these IdPs. Whichever IdP system is used, the user institution is responsible for account issuing for their members/visitors.

A.5 Lithuania

- **IdP small:** yes
- **IdP big:** yes
- **SP:** yes
- **Special Policy:** unknown

A proof of concept exists for outsourcing of both IdP and SP functions. Several classes of service are envisaged:

- **Colleges with an existing non-eduroam Wi-Fi infrastructure, Identity Management and RADIUS infrastructure.**

  These colleges are being equipped with more Access Points to allow additional provisioning of eduroam. The new Access Points are managed jointly by the NREN and the colleges; eduroam traffic is placed on a distinct VLAN. Colleges are responsible for logging, DHCP and all other aspects of local service delivery.

- **Colleges without existing Wi-Fi infrastructure and RADIUS, but with a functional identity management system.**

  In these cases, the NREN will augment local campuses' setup with a locally installed RADIUS server, a Wi-Fi controller, and sufficient Access Points for full coverage. The NREN will manage DHCP, NAT and logging for the colleges.

- **Schools with no functioning identity management system.**

  In addition to the services provided in the previous case, here an NREN-operated identity management system is being put in place where administrators can provision and deprovision accounts. All local traffic is forwarded to an aggregation point in the local municipality where NAT, DHCP and logging take place. Access to eduroam for such institutions is currently limited to members of staff, and not extended to end users.

A.6 Luxembourg

IdP small:	yes
IdP big:	no
SP:	yes
Special Policy:	yes

RESTENA operates an identity management system for small organisations. The system was originally designed to manage mail accounts (hence its name “MailGUI”), but has been extended to other services, including eduroam. Identity management is limited in size to an absolute maximum number of accounts which the organisation administrator is allowed to provision. MailGUI-provisioned eduroam accounts are connected to RESTENA’s RADIUS infrastructure for the purposes of user authentication. The responsibility of the organisation’s administrator is limited to keeping the list of accounts current and accurate; all technical authentication and authorisation processes are outsourced.

RESTENA does not procure physical infrastructure (i.e. Access Points or Wi-Fi controllers), but eduroam Service Providers can make use of a central RADIUS server. Configuration of the on-site physical infrastructure is then limited to AP/Controller deployment and configuration of a shared secret on the central server. For secondary schools, a dedicated entity of the education ministry (CGIE) does procure access points and provides configuration assistance for participants in a project known as eduWIFI.

RESTENA’s eduroam policy makes a distinction between “stand-alone” and “hosted” IdP/SP deployments; this clearly separates which requirements and recommendations in the European eduroam Service Definition remain the responsibility of the participant and which are transferred to RESTENA as the operator of the hosted parts.

A.7 Slovenia

IdP small:	yes
IdP big:	yes
SP:	yes
Special Policy:	no

ARNES is offering "eduroam-as-a-Service", which contains AP registration, DHCP, RADIUS, LDAP and IdM-as-a-service. The service provides both SP and IdP functionality.

On the SP side, currently it provides the services but not the hardware. However, there are plans to buy wireless equipment and buy and/or manage the L2 network, which, coupled with its existing L3 management, will enable ARNES to provide Network Services Orchestration (NSO).

On the IdP side, institutions can choose between an LDAP interface for local identity management, or a hosted identity management solution. An LDAP monitoring and reporting tool is in place that administrators can run on demand to obtain status reports. The system used to be restricted to institutions of up to 5 Access Points in size, but this restriction was recently lifted.

From the policy point of view participating institutions are standard SPs/IdPs, however sign-up to hosted services requires an additional contract. Security-wise, there is general uneasiness because centralised identities present a "bigger target". The centralisation is however required due to resource shortage.

References

[APAN40] https://www-lk.apan.net/meetings/KualaLumpur2015/Sessions/session.php?id=8

[GN_JRA_NETARCH] Deliverable D12.2 (DJ1.3.1) “Network Architectures for Aggregation of High-Speed Mobile Networking”. Raimundas Tuminauskas (editor), et. al.

[POLDEF] https://www.eduroam.org/downloads/docs/GN3-12-194_eduroam-policy-%20for-signing_ver2%204_1_18052012.pdf

[RFC7593] Wierenga, K., Winter, S., and T. Wolniewicz, "The eduroam Architecture for Network Roaming", RFC 7593, DOI 10.17487/RFC7593, September 2015, http://www.rfc-editor.org/info/rfc7593.

[SERVDEF] https://www.eduroam.org/downloads/docs/GN3-12-192_eduroam-policy-service-definition_ver28_26072012.pdf

[TF-MNM] https://www.terena.org/activities/tf-mobility/meetings/

Glossary

ARP	Address Resolution Protocol
CAT	Configuration Assistant Tool
CRL	Certificate Revocation Check
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
eduroam OT	eduroam Operations Team
eduroam SG	eduroam Steering Group
EAP	Extensible Authentication Protocol
ETLR	European top-level RADIUS server
FLRS	Federation-level RADIUS proxy server
GeGC	Global eduroam Governance Committee
IdM	Identity Management
IdP	Identity Provider
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
MAC address	Media access control address
NAPTR	Name Authority Pointer
NAT	Network address translation
NREN	National Research and Education Network
NRO	National Roaming Operator
RADIUS	Remote Authentication Dial-In User Service
SAML	Security Assertion Markup Language
SP	Service Provider
TLS	Transport Layer Security