|  |  |
| --- | --- |
|  | Cost Benefit Analysis (CBA) |
| **Purpose:** | A cost-benefit analysis (CBA) is an analytical tool for assessing the advantages and disadvantages of moving forward with a business proposal or project. By using a cost-benefit analysis template, Activities can identify quantitative and monetary estimates to determine whether to pursue an initiative, tweak it or abandon it completely. This document is your template for producing a GEANT cost benefit analysis. The CBA is created for the GEANT PMO by a project sponsor, department or unit seeking funding, approval, or both for an activity, initiative, or project. |
| **Created by:** | The CBA is created and maintained by the GEANT Activity Leader. |
| **Submit to:** | projectdocumentation@geant.org (the GÉANT Project Office). |
| **CBA Information** |
| Project Name: | *eduroam Managed IdP* |
| CBA Author: | Ann Harding, Juha Hopia, Justin Knight |
| CBA Code: | JRA3 T4 |
| Project Type/Size | Medium |
| Date submitted |  |
| Activity (if applicable) | GN4-2 JRA3 |
| Task(if applicable) | T4 |
| **Gate Approval Meeting** |
| Decision: |  |
| Date of Meeting: |  |
| Comments: |  |

Table of Contents

1 Executive Summary

1.1 Background and work to date

1.2 Recommendation

1.3 Financial summary

2 Supporting Information

2.1 Organisational Overview

2.2 Community Need

2.3 Drivers for Change

2.4 Benefits and Impacts

2.5 KPIs

3 Description Of Alternatives Considered

3.1 Option 1 – Do Nothing

3.2 Option 2 – Catalogue of available commercial solutions

3.3 Option 3 – eduroam Managed IdP, subscription model, based on TCS

3.4 Option 4 - eduroam Managed IdP, Project-funded (initially)

4 Conclusion

# 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 over 90 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 based on the eduroam Service definition. 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 existing sites experience difficulties in deploying more than the simple basics. JRA3 have designed and piloted a managed alternative 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 monetary, technical or skills gaps. This Cost Benefit Analysis follows the pilot and transition to service phases and recommends taking the eduroam Managed IdP Service formally into production, enabling home organisations to operate their edroam IdP according to best practice standards.

## Background and work to date

The purpose of eduroam (education roaming) is to provide a secure, world-wide roaming access service for the international research and education community. The eduroam service architecture is based on a number of technologies and agreements, which together provide students, researchers and staff from participating institutions to obtain Internet connectivity across their campuses and when visiting other participating institutions without the need for guest wireless accounts.

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 CBA is based on the principles and technology of the eduroam consortium. Background information on the overall eduroam technical architecture can be found in the IETF RFC “eduroam Architecture for Network Roaming” [RFC7593], while the service definition for eduroam in Europe is described in the eduroam Service Definition[[1]](#footnote-1).

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 JRA3 have investigated, designed, developed and piloted 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.

In April 2017, approval was provided by the PLM to enter into a pilot. During this time the design and development of software components has been completed and undergone external testing via SA2 finding no critical issues. The pilot also engaged with a total of 11 NROs who created at least one Managed IdP instance.

In March 2018, in collaboration with the Partner Relations team, two Infoshare webinars were held inviting all GÉANT Members to a presentation on the pilot and proposed service. These Infoshare sessions asked participants as to their interest in taking up such a service; their anticipated user base; and amenability to being able to pass on costs to their constituencies should the service be subscription-based. A summary table is provided as Annex 1 at the end of this document. In brief:

* 18 NRENs (NROs) joined the sessions
* 10 expressed interest in taking the service
* 4 expressed interest pending investigation into the user base in their countries
* 1 stated they have their own alternative service so no interested
* 1 expressed interest in the underlying technology but not the managed service
* 2 gave no comment
* Additionally, 3 Pilot participants did not attend, 1 of which subsequently requested further information on the service.

The evaluation of the investigation into potential funding/cost model scenarios is that while several NROS indicated an ability to contribute to costs, an exclusively charged-for service would impede uptake due to an equivalent number of NROs’ inability to recoup their costs. As a result, the delivery model has been assessed against costs and qualitative benefits for the overall health of eduroam and it is proposed to offer the service on a Project-funded basis for the duration of GN4-2 and GN4-3. Funding is secured in GN4-2 for this, and the Trust and Identity White Paper for GN4-3 evaluation indicated that funding for eduroam, including such supporting services, is essential.

In this proposed model, NROs can take the service at no cost and on-board up to a maximum of 10,000 users. It is up to the NROs how those 10,000 users are spread across their institutions. For NROs with higher numbers of users expected, it is proposed to work with these NROs once the initial service is in production to establish a mutually feasible charging model, such as bringing the service into the Cost Share mechanism or offsetting some of the components into NRO operation to reduce the operational burden. An alternative consideration would simply be to increase the limit on the number of user if there is no practical implication on operational costs.

The exit-pilot gate was approved on 26.06.18, and transition to production formally began. A transition plan was prepared by SA2 and frequent tracking meetings were held between JRA3 and SA2.

## Recommendation

Based on the analysis of the pilot and proposal set out in this CBA, there are strategic and technical 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 participating institutions (i.e. end users), and qualitative, in that it would help to safeguard the quality of the eduroam experience, thereby protecting eduroam’s reputation.

The transition phase has progressed to plan, establishing a production-ready environment for the service.

The recommendation of this cost-benefit analysis is therefore to formally exit the transition phase and enter production of the eduroam Managed IdP service as described in this document. It is proposed that this service is provided on a Project-funded basis for the duration of GN4-2 and GN4-3, and further in service development take place with potential customers who exceed the limit of 10,000 users.

**1.3** **Financial summary**

|  |
| --- |
| Recommended Approach – Summary information |
| **Investment Information** |  |
| Total production cost Q3 2018 to Q4 2021 inclusive  | €391,975 (production costs) |
| **Funding stream requirements** |  |
| GN4-2 SA2 Funding | €41,665 |
| Required GN4-3 Funding | €350,310 |
| **Total Funding Required** | **€ 391,975** |
| Technical Annex Reference (if applicable) | GN4-JRA3 T2 funded developmentGN4-2-SA2 T2 will fund operations for the remainder of GN4-2. |

# Supporting Information

## Organisational Overview

The European eduroam service is built hierarchically. At the top level sits the confederation level service, which primarily provides the confederation infrastructure required to grant network access to all participating members of the eduroam service at any time. This confederation service is built upon the national roaming services, operated by the national roaming operators (NROs – in most cases, NRENs). National roaming services make use of other entities, for example, campuses and regional facilities. GÉANT, via NREN participation in GÉANT projects, operates the regional level service for members of the European eduroam Confederation, The confederation’s goal is to provide a secure, consistent and uniform network access service to its users.

In addition to operating the basic technical infrastructure for Europe, the GÉANT eduroam team also delivers a supporting services suite to support the widespread deployment of eduroam. This suite includes a central database with information about participating institutions, monitoring & metering tools and a Configuration Assistant Tool (CAT) for end users and campus administrators. The eduroam Managed IdP development has built on the experience and infrastructure of eduroam CAT to enable IdPs to offer a higher quality of service, and thereby meet the goal of a secure, consistent and uniform network access service

## Community Need

NRENs often have a lot of small customer organisations (other than big universities), that are eligible to join eduroam but not able to deploy and maintain the needed infrastructure. The reasons may vary, but mostly because they don’t have the resources or know-how to join. Such organisations, including schools, would therefore benefit from an eduroam Managed IdP by having a reduced cost and scope of adoption.

The requirement to adopt all of the improvements mandated by the eduroam community sets a higher threshold for participation than the simple deployment of an IdP/SP according to local policy. This service will therefore benefit organisations that do not currently participate in eduroam, or who would like to enhance the quality of their eduroam deployment to take advantage of these improvements.

## Drivers for Change

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 franchisee, i.e. the organisation of the SP or IdP). This simplistic view can spread rapidly 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 is 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.

## Benefits and impacts

By lowering the technology bar for organisations, significant further adoption of eduroam can be expected. Providing organisations with a service designed by eduroam experts will help organisations avoid problems with minimal effort on their part.

**Technical impacts:**

The service will enable Identity Provider operators of eduroam to deliver a safer and more effective service than the minimal baseline. In particular:

* To ensure a strong level of privacy and security for end user credentials
* To correctly handle VLAN assignments, thereby decreasing risk of accidental DoS
* To facilitate quick action in the case of malicious users
* To reduce the likelihood of man-in-the-middle attacks

**Benefits to GÉANT (Company and NRENs as Shareholders):**

* The reputation of eduroam is defended from improperly or badly configured Identity Providers which can lead to a poor user perception of eduroam in general.
* The proposed service aims to increase eduroam IdP footprint in the NROs’ service areas as new organisations will be enabled to join eduroam and therefore additional users will gain access to roaming. This increases the status of eduroam and its attractiveness to funding bodies to continue to provide innovation and operations funding.

**Benefits to NROs/NRENs:**

* NROs can obtain a managed eduroam solution on behalf of their community.
* The NRO’s internal helpdesk effort towards SPs and IdPs can be reduced because:
	+ Organisations using the managed service will benefit from a maintained, working, and actively managed platform developed and supported by eduroam experts, 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.

**Benefits to Campuses:**

* Campuses gain time and effort savings by outsourcing management of their IdP, while retaining necessary control of user data.
* Campuses benefit from specialist eduroam know-how in best practice without having to have permanent dedicated staff with this skillset

## KPIs:

The CBA for the Pilot set the below KPIs. Evaluation notes against these KPIs are in *italic* text.

* **KPI1: Acceptance by NROs**
	+ As a result of pilot, at least three eduroam NROs agree to promote eduroam Managed IdP to their constituency in production.

*14 NROs expressed interest in taking up the service in production during Partner Relations Infoshare webinars. It was clearly established that it would be the NROs, not GÉANT, who would hold the relationship with the end user institutions, so promotion is implicit in service uptake interest.*

* **KPI2: Uptake at campuses**
	+ During pilot, at least five Identity Providers enable the eduroam Managed IdP solution and provision at least one user account with it to verify quality

*During the pilot a total of 11 NROs created at least one Managed IdP instance.*

* **KPI3: service quality**
	+ NRENs/NROs’ evaluation of the quality of service from participant sites vs. their expected workload for independent deployment. - majority of participants must percieve that they had time/cost or skills savings from the product.
	+ Performance of infrastructure should be considered capable of meeting availability and performance targets that are suitable for an SLA e.g. min 99.99% availability outside of maintenance, once a fully resilient setup is deployed post pilot.

*This KPI has been moved to production service KPIs where it is more appropriate.*

* **KPI4: Positive evaluation by pilot participants**
	+ Qualitative evaluations from interview/survey of pilot participants at campus and NRO.

*Inforshare webinars were held in March 2018. Annex 1 provides the detailed feedback gathered. In summary::*

* *18 NRENs (NROs) joined the sessions*
* *10 expressed interest in taking the service*
* *4 expressed interest pending investigation into the user base in their countries*
* *1 stated they have their own alternative service so no interested*
* *1 expressed interest in the underlying technology but not the managed service*
* *2 gave no comment*
* *Additionally, 3 Pilot participants did not attend, 1 of which subsequently requested further information on the service.*
* **KPI5: Sustainability**
	+ Positive assessment of willingness to pay as per the business model by sufficient sites to sustain the service post GN4-2. Number to be quantified based on the price adopted as a result of pilot. System can automatically report and track progress.

*An assessment was carried out, via Partner Relations engagement with NROs, (both pilot, and non-pilot participants) as to ability to pay for the service and/or pass on a charge to their constituencies. This found that the introduction of a charge would substantially impede service uptake, as NROs do not have the capability to pass charges on to their constituencies. An alternative model utilising Project funding and introducing a user limit is therefore proposed, as described in this CBA.*

This CBA recommends the following KPIs for the production service:

* **KPI1: service quality**
	+ Performance of infrastructure should be considered capable of meeting availability and performance targets that are suitable for an SLA e.g. min 99.99% availability outside of maintenance.
	+ NRENs/NROs’ evaluation of the quality of service from participant sites vs. their expected workload for independent deployment. Majority of participants must percieve that they had time/cost or skills savings from the product. This evaluation will be carried out via regular engagement from Partner Relations.
* **KPI2: Service uptake**
	+ Based on the feedback from the Partner Relations Infoshare sessions, a KPI of uptake over three years is proposed:
		- 2018/19: 4 NROs join
		- 2019/20: 3 additional NROs join
		- 2020/21: 3 additional NROs join
* **KPI3: Tracking the cost of support by user**
	+ In order to record, and update if required, the level of cost associated with operating the service, and adjust funding levels if necessary.

# Description Of Alternatives Considered

## Option 1 – Do Nothing

eduroam could continue with the current model. In this option, the eduroam Managed IdP service would not be offered and users without the technical ability to deploy eduroam would not benefit from eduroam. In addition, the qualititative benefits of the eduroam Managed IdP for the eduroam service in general would not be recognised. This option is not recommended.

## Option 2 – Catalogue of available commercial solutions

In this option users could purchase or leverage available commercial solutions through GÉANT. One example is the evaluation of a commercial offer from Luxembourg made to a campus. The price for "one eduroam Managed IdP profile” (Cisco ISE server, VM environment, 150 users license, web frontend to manage users, without high availabily) was given as:

• setup costs: 2.450,00 EUR

• annual service: 7.356,00 EUR

This price point was considered unaccceptable by the campus but gives an indication of what the market provides vs. what campuses are prepared to pay. An option for GÉANT could therefore be to broker cheaper prices with commercial providers, on behalf of the community.

In this model, as with option 1, the qualititaitve benefits of the eduroam Managed IdP for the eduroam service as a whole would not be recognised. Furthermore, in this model, GÉANT’s efforts would be focused on brokering deals that generate revenue for commercial providers without safeguarding the reputation of eduroam or providing the best possible eduroam service to the community. As revenue generated could not be put into the sustainability of the eduroam service, whereas the eduroam Managed IdP does have this potential, this option is not recommended.

It is noted, though, that this option may be considered as a parallel or future activity to the recommended option. It requires commercial negotiation and contract development skills, and may therefore be considered by other activities e.g. JRA4, or the GÉANT organisation in the future.

## Option 3 – eduroam Managed IdP, subscription model, based on TCS

In this option users would get the eduroam Managed IdPservice through GÉANT, via their NREN/NRO in a model also used by the successful TCS service.

The business model would be that NROs pay GÉANT a set fee for a number of instances and distribute those within their region, using whatever cost recovery mechanism is most appropriate in their case. In the case of non GÉANT partners, such as regional development projects, commercial resellers and other global partners, a separate tariff(s) would need to be designed such as to differentiate from GÉANT partners.

As described in this CBA, evaluation of this potential model with GÉANT partners found that the introduction of a charging mechanism in the same vein as TCS would impede uptake of the service, due to NROs not being able to mechanistically pass on the charge to their constituencies, and financial incapability to cover the costs themselves. This option is therefore not recommended, however it is recommended to work with NROs with larger user bases to establish an appropriate and mutually feasible cost recovery model where usage of Managed IdP exceeds a sympathetically defined threshold. Any introduction of a charging mechanism would be subject to additional pilot, and is not part of the recommended initial production service.

## Option 4 – eduroam Managed IdP, Project-funded (initially)

This option proposes to offer the eduroam Managed IdP service on a Project-funded basis for the duration of GN4-2 and GN4-3. Funding is secured in GN4-2 for this, and the NREN evaluation of the Trust and Identity White Paper for GN4-3 explicity stated that funding for eduroam, including developments, pilots and production services, is essential. The risk that this funding will not be available is considered to be acceptable, and should this situation change, measures should be taken in Q4 to mitigate (limited offer to those who could pay while alternative funding is sought) rather than waiting to launch the service until this time.

In this proposed model, NROs can take the service at no cost and on-board up to a maximum of 10,000 users. It is up to the NROs how those 10,000 users are spread across their institutions. Based on the analysis of the Pilot, including the feedback gathered during the Partner Relations Infoshare webinars, this is the recommended option.

It is understood that during GN4-3 the cost sharing models of eduroam and similar services will be re-evaluated in the context of the NREN subscription and this would then be included in that exercise post production.

# Conclusion

Based on the analysis and proposal set out in this CBA, there are considerable benefits to offering the eduroam Managed IdP service in production. These benefits are both quantitative, as the service will enable the addition of 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.

The transition phase has progressed to plan, establishing a production-ready environment for the service, and so it is recommended to enter formally into a production service of the eduroam Managed IdP (on a project-funded basis initially).

Further work will be undertaken in GN4-3 with NROs with expected users greater than the limit of 10,000 to establish a mutually feasible sustainability model, possibly by bringing the service into the Cost Share model, offsetting some infrastructure into the large using NROs or alternatively increasing the user limit.

# Annex 1:

# Summary of Infoshare sessions 14.03.18 and 15.03.18, lead by Partner Relations

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | NREN | Piloting | Interest Y/N | Institution number/size | Comments |
| 1 | GRENA | No | No  |  | Already have solution as referenced above |
| 2 | HITSA | No | Yes – very interested | Schools potentially | Developing and soon be deploying identity management solution for Estonian schools. One part of this solution support and integration for eduroam. At one point we plan to offer eduroam users EAP-TLS certificates and seems that eduroam Managed IdP technical solution is something what we should integrate or copy. |
| 3 | CYNET | No | Possibly BUT depends on what user constituency say | Possibly a few small organisations | Happy to investigate amongst their community |
| 4 | Belnet | No | Possibly BUT depends on what user constituency say |  | Had some requests for a solution like this 3 years ago. They helped institutions to set up eduroam infrastructure at this time. There's now two thirds of all institutions in Belgium participating in eduroam. Demand for this service may be lower as a result, but happy to investigate. |
| 5 | GARR | No | Possibly – Claudio to comment further on Thursday | Possibly similar users to Shibboleth managed IdP  | They have a managed Shibboleth IdP service and can confirm the number of users for this. Similar institutions might be interested in eduroam managed too. |
| 6 | UoM | No | Yes  |  | Couple of institutions might be interested. One specifically asked for it a while back. Larger institutions which don’t have extended IT support team might be interested to – number of users for these would be more than 200 per institution |
| 7 | BASNET | No | Yes | One large institution | Unsure of interest from smaller institutions, but have had interest from one larger institution who wants to pass all things eduroam to BASNET  |
| 8 | ACOnet | No | Possibly BUT depends on what user constituency say |  | Would need to investigate with their community |
| 9 | RoEduNet | No | Possibly BUT depends on what user constituency say | Possibly smaller institutions | Not sure if an interest but smaller institutions might be |
| 10 | SWITCH | No | Interested in the technology behind it |  | Had cases in the past where would have been a solution but they teamed up with small institutions to support them. As part of larger scheme interest is in back end technology would welcome meeting to see if can use same infrastructure or clone CAT |
| 11 | RedIRIS | Yes | Yes |  |  |
| 12 | GARR | Yes | Yes | -8000 schools-research hospitals -1000s of sml research institutes None would be below 200 users. Average would be 700-800 users  | Run IdP in the cloud for eduGAIN. Can predict question from users: wonderful service but do I need to duplicate entries? Would like to work technically to integrate the two services for ease of use by the institutions Would look to house part of the service in-house (for the very big user groups) e.g. identical server in their system |
| 13 | SURFnet | Yes | Yes |  | Anticipate very low interest (1 or 2 users).Don’t see institutes small enough to use the service or many incapable of setting up an IdP. Group of schools that could be serviced but no financial support here |
| 14 | PSNC | Yes | Yes |  |  |
| 15 | FCCN | Yes | Yes |  | Would need to do analysis on potential number of institutions and users Discussions with users during pilot were very positive |
| 16 | MARNet | No | Yes | Unlikely to be below 200 more like several hundredSmaller state universities, private universities | State universities have their own infrastructure. Middle and high schools are being catered for by another initiative. |
| 17 | FUNET | Yes | Yes | Only x4 under 200 users – rest would be above this limit |  |
| 18 | URAN | No | No comments received |  |  |
| 19 | RENAM | Yes | No comments received |  |  |

1. https://www.eduroam.org/wp-content/uploads/2016/05/GN2-07-327v2-DS5\_1\_1-\_eduroam\_Service\_Definition.pdf [↑](#footnote-ref-1)