30-03-2017

Deliverable D9.1
Market Analysis for Supporting Services for Campus Identity Providers

Deliverable D9.1

Contractual Date:	31-12-2016
Actual Date:	30-03-2017
Grant Agreement No.:	731122
Work Package/Activity:	JRA3
Task Item:	Task 1
Nature of Deliverable:	R
Dissemination Level:	PU
Lead Partner:	GARR
Document ID:	GN4-2-17-42C1B
Authors:	Ann Harding (SWITCH), Anass Chabli (RENATER), Tangui Coulouarn (DEIC), Marko Eremija (AMRES), Justin Knight (JISC), Jan Oppolzer (CESNET), Marco Malavolti (GARR), Mario Reale (GARR), Janusz Ulanowski (HEAnet) with valued input from the wider community

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

Abstract
This document provides a Market Analysis of the current offer on Campus IdP related services by the GÉANT NREN community and provides recommendations for features to be provided by a GÉANT Campus IdP platform.

Table of Contents

Executive Summary 3

1 Introduction 4
- 1.1 Background 4
- 1.2 Stakeholders 5
- 1.3 Approach 6

2 Requirements for IdP as a Service 7
- 2.1 Service Demand 7
- 2.2 Service Deployment Considerations 11
- 2.3 Service Features 13
  - 2.3.1 Overview of Existing Solutions 14

3 Recommendations for GÉANT to Address IdP Needs 18

Appendix A Overview of IdP Solutions 20
- A.1 AMRES 20
- A.2 GARR IdP in the Cloud 21
- A.3 CESNET's solution for eduID.cz participants 22
- A.4 JISC Managed IdP Service 22
- A.5 HEAnet 25
- A.6 SWITCH 26
- A.7 RENATER 26
- A.8 US - TIER 27

References 28

Glossary 29

Table of Figures

Figure 2.1: Barriers to the adoption of federated services 8

Figure 2.2: Current NREN/Federation support offerings to Home Organizations 9

Figure 2.3: Current NREN/Federation service offering to Home Organisations 9

Figure 2.4: Current NREN/Federation Hosted IdP offers 10
Figure 2.5: Institution interest in outsourcing IdP 10
Figure 2.6: Willingness to offer a GÉANT Campus IdP solution 12
Figure 2.7: Interest in a specific deployment model 12
Figure 2.8: NREN willingness to offer their Campus IdP to a wider community 13
Figure A.2.1: Architecture of the GARR IdP in the Cloud service 21

Table of Tables

Table 2.1: Overview of current Cloud IdP offers 16
Table 2.2: Required features for a GÉANT Campus IdP platform 17
Table A.1: JISC offer benefits and advantages 23
Table A.2: JISC offer support model 24

Executive Summary

The goal of JRA3 is to develop supporting services for campus identity providers. Based particularly on findings from AARC, TIER (Internet2) and NREN developments, JRA3 investigated the possibility of developing a Campus IdP extension to Federation-as-a-Service (FaaS) for those sites and regions that currently do not have the ability to support or offer a cloud IdP type of service to their campuses.

JRA3 T1 carried out a market analysis to identify relevant trends and needs in the market, to confirm whether its expectations in terms of demand were realistic and to establish the direction and approach for its development work.

This analysis showed that there is interest in solutions based on automated installation and configuration tools (e.g. Ansible, Puppet, etc.), and some NRENs have already developed a specific toolkit-based solution to support the provisioning of Campus IdPs. In addition, many NRENs deploy their own private cloud infrastructure to provide identity services to their customer organizations, while others rely on virtualization platforms from either commercial or local deployments.

Ensuring portability, independence from the specific underlying Cloud platform and scalability, and facilitating easier deployment are the key requirements for any solution for Campus IdP provided by the GN4-2 project for the GÉANT community.

This suggests that planning a set of supporting services requires an incremental approach, starting from providing a catalogue of existing solutions for Cloud-based Campus IdP, followed by a toolkit supporting, deployment and customisation, to then integrate this toolkit with cloud platforms would be expedient. A final step would include deployment on an existing GÉANT cloud platform for a fully managed option. However, this full as-a-Service approach does not alone address enough of the demand, therefore each increment should be made available to the community to adopt and integrate with their own solutions.

1 Introduction

This document provides a Market Analysis of the current offer on Campus IdP related services by the GÉANT NREN community and provides recommendations for features to be provided by a GÉANT Campus IdP platform.

This section provides background information on the current requirements and need for IdP services in the eduGAIN [eduGAIN]/Identity Federation environment, as well as the reasons for providing supporting services for Identity Providers in the GÉANT community. It also describes the Market Analysis approach adopted in this document and the stakeholders involved in the definition of the roadmap and implementation of supporting services for Campus IdPs.

Section 2 focuses on the high-level service requirements for Campus IdPs, describing the needs of the GÉANT community, including service deployment considerations. It also covers existing services offered by NRENs, global partners and commercial providers and gives an overview of the current offerings on the market. Based on these findings, common desirable features that could be provided by a GÉANT Campus IdP platform are identified.

Section 3 combines all findings to draw up some recommendations for GÉANT to address community needs for Campus IdPs, supporting product management decisions for commissioning development, deployment and operational work to provide a general solution for the community. It also gives recommended steps for Campus IdP to interact with closely related projects developments.

1.1 Background

Researchers and research activities have a need to access protected resources and services such as journals, databases, etc. Federated Identity Management (FIM) facilitates this by enabling researchers to use the same account to access resources from different services and research institutions.

In FIM, Identity Federations comprise groups of home organisations who operate as identity providers (IdPs) and service providers (SPs). These federation members operate within a consistent technical and policy framework, usually at a national level. At the international level, the eduGAIN service interconnects and facilitates service delivery between federations. The eduGAIN interfederation service consists of 45 federations located around the world, 40 of which are actively exchanging metadata[1] and this number continues to grow. For federations lacking knowledge and/or resources, GÉANT provides its own service called Federation as a Service (FaaS) to operate their central

[1] https://technical.edugain.org/status (January 2017)

federation infrastructure. This has been in production since GN4-1 and is typically used by emerging countries and federations to bootstrap their technical infrastructure.

2,200[2] of a total of about 3,500 known IdPs[3] currently participate in eduGAIN via their federations. While some of these federations (about one third) represent multiple campuses, the majority are individual campuses. The 2015 GÉANT Compendium [Compendium] estimates that GÉANT member NRENs provide a range of services to almost 4,500 Universities, Research Institutes and Further Education institutes alone. This number increases to almost 8,000 taking into account non-GÉANT NRENs, and not including figures from some major countries such as the US. This indicates that significant growth at IdP level is still possible.

The operators of mature identity federations often have enough knowledge and resources to help IdPs with configuration support and training so that they can provide the relevant information to SPs, or to offer managed services to their IdPs who do not wish to operate their own infrastructure. However, other federations still lack the knowledge and/or resources to provide the same level of support to their users. The objective of this analysis is to investigate the current state of the market for such services targeting IdPs (in terms of both supply and demand) and to make recommendations for service development by GÉANT in this area.

1.2 Stakeholders

Many individuals and organisations are involved in order for federations and eduGAIN to enable groups of people to share a set of resources using federated identity management. For GÉANT to develop and operate a hosted IdP, different stakeholders have to be considered, including:

- End users.
- Home Organisations (also *known as Home Institutions*).
- Identity federations.

End users are researchers, scientists, and other collaboration partners. Typically, they need to use several services for their work. In a federated identity model, users belong to a Home Organisation, typically a campus, which runs an Identity Provider (IdP). During authentication, the IdP and the Service Provider (SP) exchange information that enables the user to log in to a service with a single set of credentials, and where passwords are not stored or processed by the services. However, where a campus does not operate an IdP or does not have the skills or knowledge to configure needed attribute release policies or other technical mechanisms, end users can be excluded from using federated identities to access journals, scientific resources or collaboration platforms.

Home Organisations run an Identity Provider (IdP) for their users. Most often these are operated by campus IT departments on behalf of students and staff at an institution. The IdP is typically connected to a user directory implemented using technologies such as LDAP or an Active Directory containing end users' detailed information. The available skills, resources and level of engagement of institutions in operating the identity provider infrastructure vary widely, even within individual countries.

[2] https://technical.edugain.org/status (January 2017)
[3] https://met.refeds.org (January 2017)

Identity federations are groups of organisations operating services (Service Providers), IdPs (Identity Providers), and other relevant entities that agree to interoperate under a certain rule set. In the R&E environment, they are run by a Federation operator who provides processes and often tools to support their operation. The Federation operator is often but not necessarily a National Research and Education Network (NREN). The majority of mature national Identity federations in R&E are members of the eduGAIN inter-federation service. Federations offer various kinds of support to campuses to operate IdPs, from training and documentation to onsite and remotely managed services.

A crucial point when conducting a market analysis is to assess the willingness of campuses to outsource the role of IdP operator to other parties. In particular, given that the contractual relationship to the campus is several steps removed from GÉANT, it is essential to identify the ways in which federations/NRENs and GÉANT would interact to deliver this service to campuses.

1.3 Approach

This Market Analysis begins by looking at the need, environment and requirements for a hosted IdP service. Data was gathered from independent sources including:

- REFEDS annual federation survey and metadata exploration tool (MET).
- Previous GÉANT project results.
- Specific surveys carried out by the task (JRA3 T1).
- Targeted information requests to a subset of respondents.

It then continues with a review of the hosted IdP services or packages currently offered in Europe. A broad set of IdP-as-a-Service examples were studied, with information provided by the relevant NRENs/Federations or derived from available sales or contractual material in the case of commercial providers.

Finally, it combines the analysis of needs with available products and identifies which features and approaches would be most useful for a service offered by GÉANT in this area.

2 Requirements for IdP as a Service

2.1 Service Demand

This section investigates the opportunity or requirement for a hosted or managed IdP service that could be offered by GÉANT, focussing on any existing gaps at the campus and federation level.

As part of the development of GÉANT's Federation as a Service in 2013, issues relating to campus deployment were assessed[4]. The conclusion was that NREN member institutions generally fall under two categories:

- Higher education institutions (mostly universities) which are usually capable of adopting new technologies given sufficient interest.
- Other institutions that have a much smaller user base and smaller IT departments, and that would probably encounter problems in adopting federation technologies without their NREN's support.

More generally, some institutions in both categories were found to have the following problems:

- There is no interest on the part of the institution in deploying Identity Management (IdM), and they probably have no clear business case for the need for IdM.
- The institution has no available manpower for IdM or for managing user accounts and internal procedures.
- Institutions are lacking the knowledge needed for deployment of IdM.
- Institutions have some issues with the server infrastructure needed for operating an IdM (however this is not a serious issue).

The 2016 annual REFEDS survey[5] provided important information to support these 2013 findings. In particular, information gathered on staffing and funding at federations indicates that a significant number of these have very little resource and would not be able to offer much beyond a bare minimum federation registry. The majority have an annual budget below EUR 300,000 and staffing below 2.5 FTE. This poses a challenge to being able to support campuses where they are lacking in knowledge or infrastructure. Despite this, eight federations listed "hosted IdP" as a priority in 2017

[4] Milestone MS83 (DS5.4.1): Federation as a Service - Market Analysis and Pilot Service Definition, M. Veremezović (AMRES), 2013.

[5] https://geant.app.box.com/s/8f30ptw5houmauurfqfupw3ruz3x9enu

and Shibboleth IdP 3.0 installation was identified as a key training requirement. This is relevant for the adoption of Federations by the research community.

As well as using data from the wider REFEDS survey, the task also issued a specific survey to federation operators to determine if the 2013 concerns about meeting campus needs are still valid, and to what extent the existing services marketplace can address them. The survey aimed to collect information about current levels of awareness of and demand for IdP services on the part of Institutions and users, and their ability to support them. It also looked at any existing barriers to the services' adoption and acceptability of outsourced or hosted solutions, any solutions and support currently offered by the NRENs/Federations to their Home Organisations, and any interest shown in developing a GÉANT offering.

The survey was issued to both federation operators within FaaS and those operating their own infrastructure, with a request to circulate it more widely. By the end of November 2016, 23 responses had been received from 12 countries (plus answers from GÉANT).

The NRENs who responded include: ARNES, CANARIE, CESNET, GARR, GRNET, GÉANT, HEANet, Internet2, JANET, RedIRIS, RENATER, SURFnet and SWITCH. Other responses came from campuses and other organisations within the respondent countries.

The findings about the viability of service offerings based on survey responses to five questions are shown below.

Respondents were asked to identify barriers to adoption of federated services at campuses:

19/23 respondents provided an answer to this question. Results are shown in Figure 2.1 below.

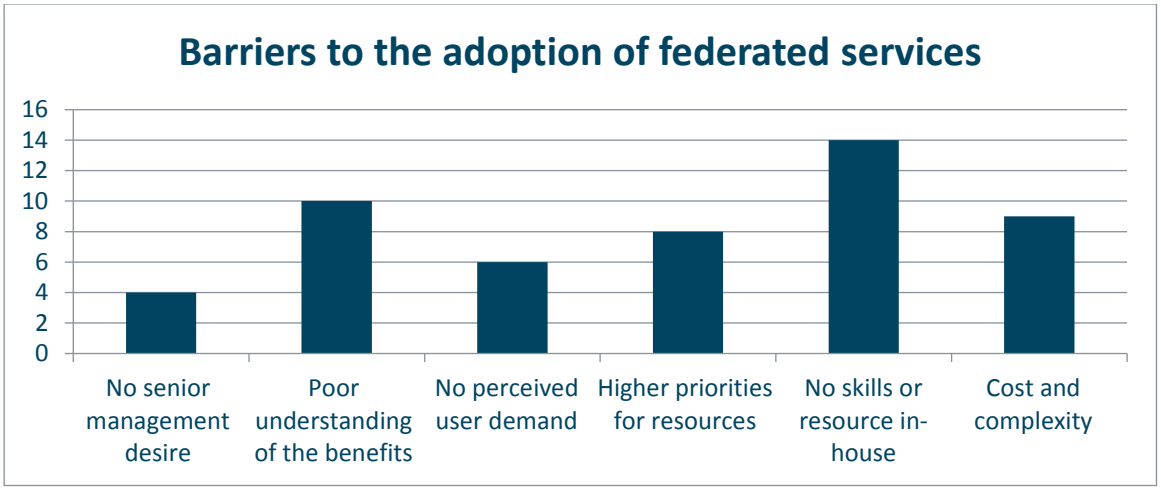

Figure 2.1: Barriers to the adoption of federated services

From this result, it is clear that the concerns about skills or resource that were noted in 2013 remain, with cost and complexity also being factors. It is possible to address both the latter concerns through a technical service offering. Understanding of benefits is also a significant factor, but is outside the scope of a technical service delivery.

Respondents were asked to note the current approach by NRENs to supporting IdP deployment for their Home Organisations, to assess to what extent market needs exist or are already covered: 17 respondents provided information (Figure 2.2).

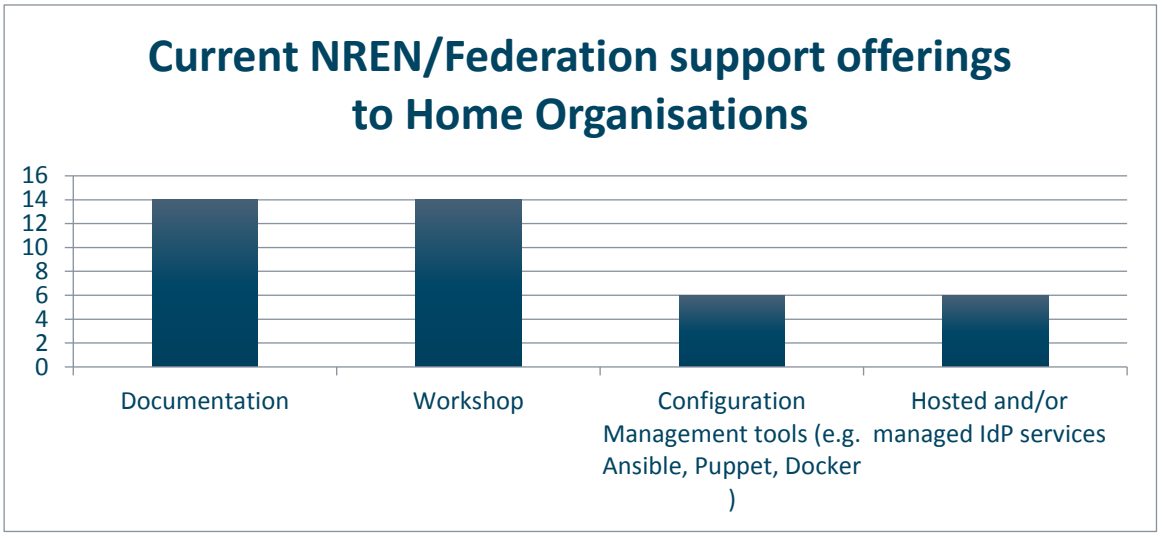

Figure 2.2: Current NREN/Federation support offerings to Home Organizations

In many cases NRENs are already providing management tools to support deployment. NRENs with some established systems would be less likely to adopt a hosted solution, but at the same time, given restricted budgets and staffing limitations at NRENs and federations, a coordination effort in this respect to facilitate federations working together on a smaller subset of common tools would provide some benefits.

Building on the previous question, respondents were asked to detail what support offerings are delivered to campuses, including the aforementioned documentation and training. (18 total respondents – Figure 2.3):

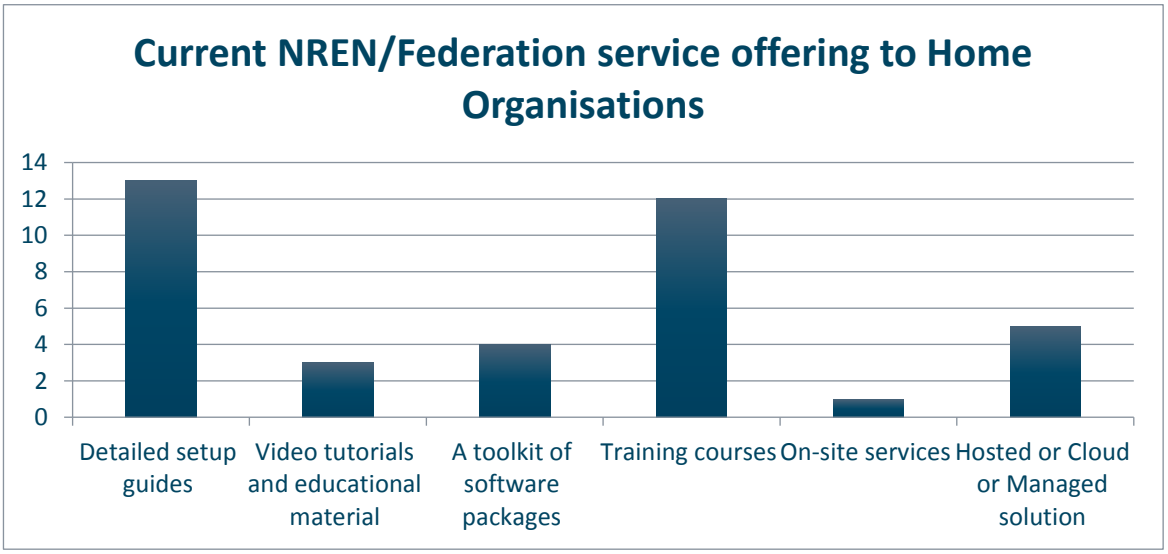

Figure 2.3: Current NREN/Federation service offering to Home Organisations

A more specific question asked if NRENs/Federations currently offer a hosted IdP solution to their Home Institutions, and if so, in what form and level of maturity (N. of Respondents: 20 – Figure 2.4):

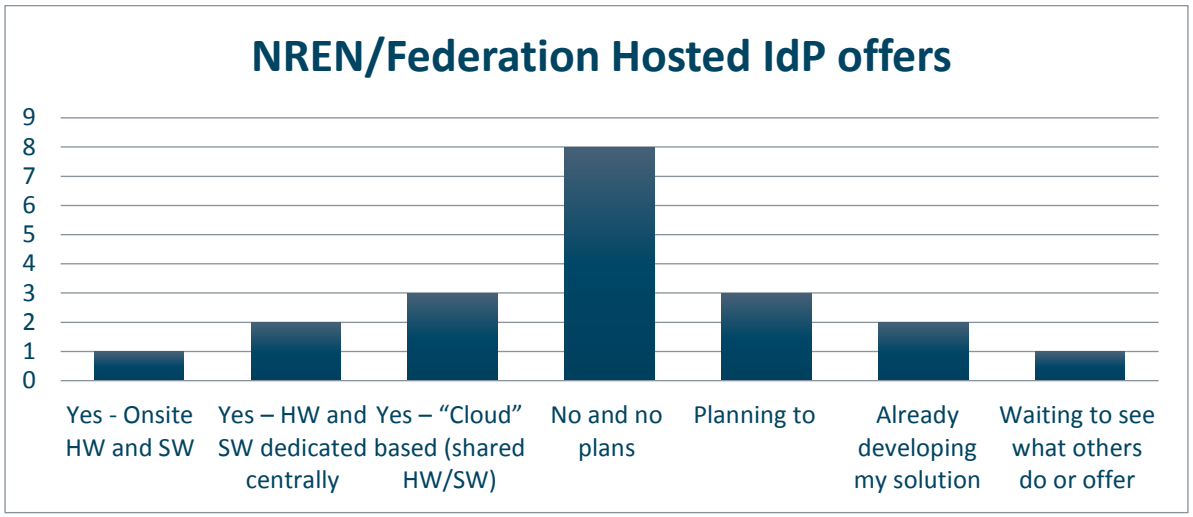

Figure 2.4: Current NREN/Federation Hosted IdP offers

This set of questions (Figure 2.2 to Figure 2.4) aimed to assess to what extent federations are already covering the skills or infrastructure gaps identified for campuses. The conclusions were that while federations currently offer support and documentation to their IdPs, only a minority have an IdP hosting option, with the provision of deployment guides, training and toolkits being the leading approach. When comparing these results with the REFEDS survey, it is reasonable to conclude that federations may themselves lack resources to deliver hosted IdP services on an ongoing basis, whereas toolkits, training and documentation have a lower operational cost.

Finally, one question assessed the interest from federations/NRENs in outsourcing an IdP solution: Results are shown in Figure 2.5 below.

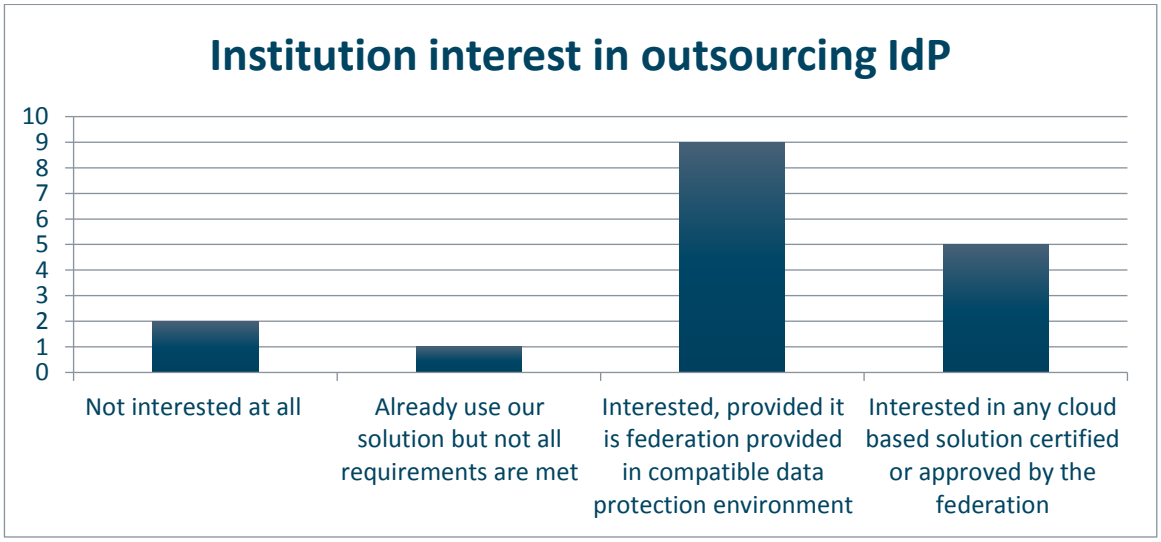

Figure 2.5: Institution interest in outsourcing IdP

This question investigated the willingness of campuses to outsource their IdP operation. It is noted that in many cases federations answered based on their opinion of what their campuses wanted, rather than giving a response directly from the campus, but this is acceptable within the service delivery context, where federations own the relationship to campuses. It is notable that although respondents indicated their campuses would have a significant wish to outsource their IdP operation, the leading response was that federations themselves did not have plans to provide this service. Where concerns were identified about outsourcing, the leading issues were security of data and integration of local directory services. Of the federations that currently deliver a hosted IdP service, only one currently makes this available beyond national borders by providing the outsourced service on behalf of the wider community.

Based on the combined results from these responses and the reviewed FaaS Market Analysis:

To address the common Campus IdP needs reported by the survey, it is recommended that GÉANT should develop, or obtain and package infrastructure to support federations (NRENs) in the provisioning of a Campus IdP offer to Home Institutions that would enable them to respond to the needs and willingness of the campuses to outsource their IdP operation.

What is less clear from these responses is what type of service delivery would be the best fit for each NREN/Federation environment. This indicates the need to implement an incremental, component-based solution that exploits automation tools for the installation and configuration of the IdP instances, rather than solely a fully managed service integrated with the GÉANT Federation as a Service offering. To address only the latter need would not see sufficient take-up to merit development. The following section will look at these issues in more detail.

2.2 Service Deployment Considerations

Having established that there is a need to support campuses to manage their IdPs, a series of questions investigated the form such a service would take, including some confirmation questions to validate previous answers.

When asked if a service to deliver IdP solutions provided by GÉANT would be acceptable or of interest (Figure 2.6), although a significant number of respondents excluded this completely, the majority of responses were positive, subject to conditions as to how this should be delivered, in particular if it would be natively branded and offered via the NREN's infrastructure (14 respondents). Of those who rejected the possibility completely, one respondent cited data protection legislation regarding hosting of personal data at a national level as an impediment, while the others did not specify any reason.

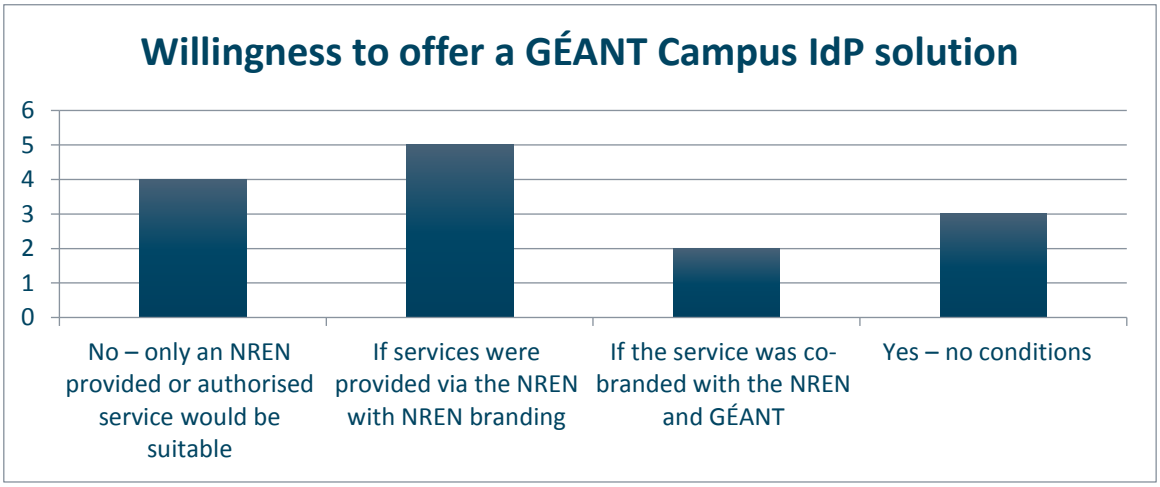

Figure 2.6: Willingness to offer a GÉANT Campus IdP solution

One specific question asked concerned the possible preference of a solution provided to NRENs to support their Home Organisations based on a deployment toolkit versus a Cloud approach: (Respondents:15). As shown in Figure 2.7, there was no clear determination as to whether a toolkit or a managed approach was preferred by respondents.

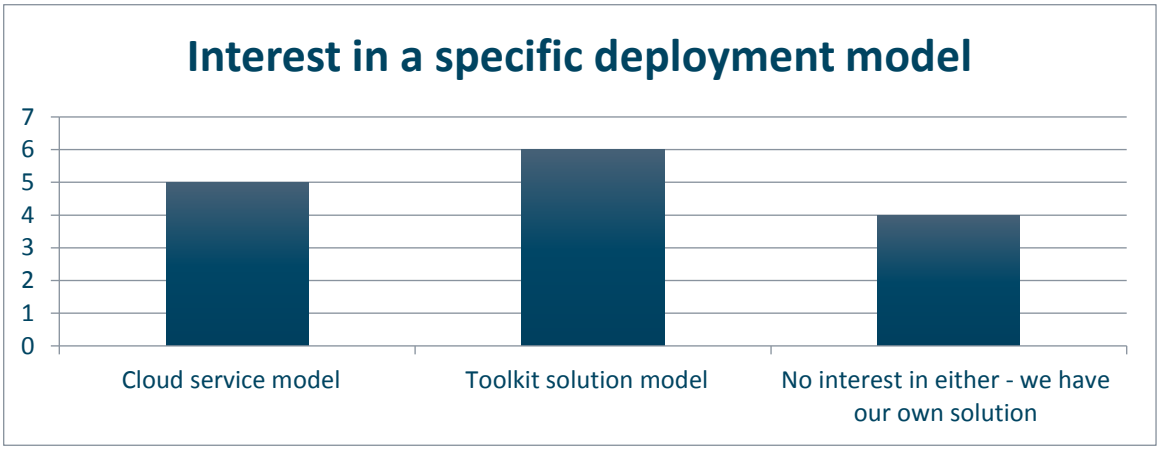

Figure 2.7: Interest in a specific deployment model

In view of the importance of preventing possible duplication of existing work or solutions, **NRENs/federations were also asked about their willingness to provide a Cloud IdP service to the community directly or on behalf of GÉANT** (15 respondents, Figure 2.8):

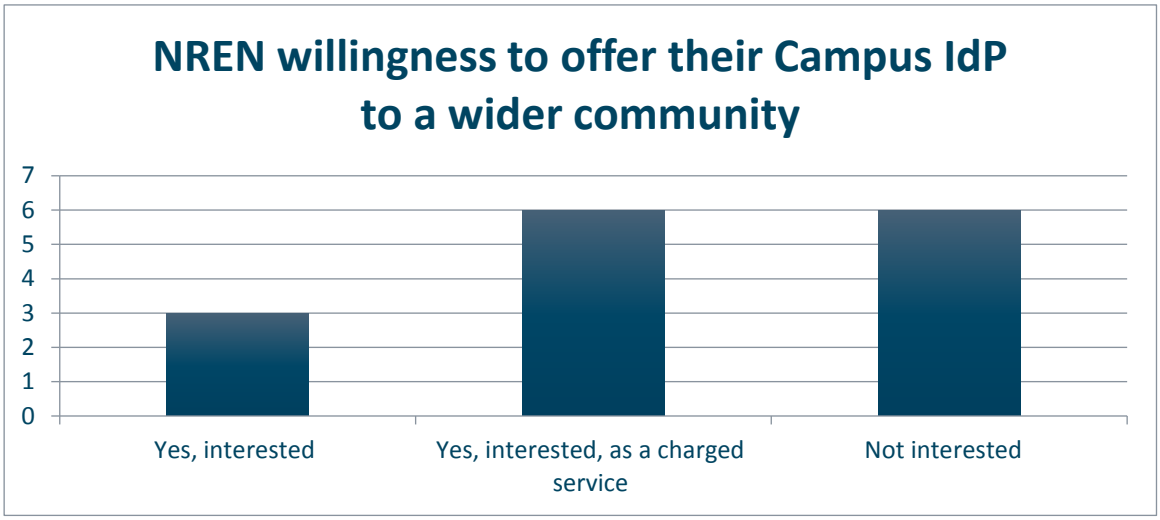

Figure 2.8: NREN willingness to offer their Campus IdP to a wider community

A number of federations expressed an interest in advocating their own solutions to scale to the GÉANT requirement. However, when compared to the solutions currently available (Section 0), only one federation has a service which it currently offers to non-members.

Based on these findings and the assessment work carried out by JRA3 task 1, it is probable that a combined approach to the service is required. Some NRENs would benefit from a simple toolkit, which would then be integrated into their own infrastructure. Others would benefit from automated configuration scripts to provision containers with federation-specific policies and tools. Flexibility in deployment scenarios is also required as there is no clear preference between enabling the home organisation to deploy their own instance in their own infrastructure or their own cloud environment, or have it hosted by the NREN. GÉANT should provide both an integrated solution for spawning IdP instances on a Cloud infrastructure on both Virtual Machines and containers that would ensure high portability for the provided solution, which is desirable given the different tools and platforms currently used by NRENs at the European level.

The survey reported that both NRENs and GÉANT have the trust of Home Organisations as valuable providers of a comprehensive Campus IdP solution, but subject to conditions in some cases as to how this is presented, i.e. the direct relationship for the campus is always with the NREN/Federation. The technical approaches under consideration are able to meet these requirements.

2.3 Service Features

As the survey indicated, within the GÉANT community several federations offer a cloud/hosted IdP solution. This service is typically offered to smaller institutions and universities that do not have enough manpower or other resources to operate an IdP themselves. In most cases it is a simple technical solution which allows them to participate in the federation or even in the eduGAIN inter-federation and does not include wider identity management features. Details of the offerings of six federations are provided in Appendix A. The majority of these are based on Shibboleth IdP [Shibboleth] software and are restricted to use by members of a federation's own community. Models

range from a 'light' approach where containers are delivered to a fully managed option. In almost all cases, user data and support remains at the campus, with infrastructure and platform management only being provided by the federation. The main exception is for a specific service to the HealthCare sector where LDAP is included. Several have a cost component separate to the default NREN or federation service.

2.3.1 Overview of Existing Solutions

In this section we provide an overview of solutions that currently exist within the GÉANT NREN community for providing Campus IdP services. More details are provided in Appendix A. Two offers by commercial providers (Gluu and Eduserv) with a footprint in R&E federations have been also taken into account, so as to have an indication of the available features and related costs.

Common aspects of the current offer on the Market are the use of Shibboleth IdP as reference product for providing SAML SSO, and to provide a Managed service to support those campuses that to not want to manage the IdP administration themselves.

A variety of technical solutions which differ in terms of underlying cloud or virtualisation platform, reference installation and configuration tools, as well as High Availability strategies have been implemented. As some federations already providing their own solutions have indicated that these do not meet all their requirements, the work of the task could also extend to supporting these existing solutions. However, this requires an approach that prioritises high portability and deployment scalability (i.e. into different environments rather than on a single platform).

A summary of the main features currently provided by the available offers is provided in Table 2.1 below.

Provider (NREN or commercial)	IdP S/W	Deployment Technology	High Availability Strategy	User Directories integration	Management degree levels	Scope of Offer
AMRES	SimpleSAMLphp	VMware	NA	LDAP	Fully Managed	AMRES only
CESNET	Shib	Ansible VMs on VMware	Local Fault Tolerance (Vmware) 2 DCs	LDAP AD MySQL	Fully Managed	eduID.cz only
GARR	Shib	Puppet VMs on Openstack Cloud	NA - Respawn based on Puppet recipes	LDAP	Fully Managed	GARR only

Provider (NREN or commercial)	IdP S/W	Deployment Technology	High Availability Strategy	User Directories integration	Management degree levels	Scope of Offer
HEANet	Shib	VMs on VMware Puppet for System update	HA available	LDAP AD	Fully Managed	HEANet only
JISC	Shib	VMs at commercial provider Custom deployment tools	Provider-based	LDAP AD at user premises (VPN)	Fully Managed	Available to any interested party at a cost (preferential tariff for NRENs and Public Sector)
RENATER	Shib	VMs on VMware + vRealize automation + Puppet, Ansible	NA	LDAP AD	Fully Managed	RENATER only
SWITCH	Shib	Puppet Ansible VMs on RHEV platform	IP anycast	Encrypted via TLS LDAP is default at HO	Fully Managed	SWITCHaai Federation only
TIER	Shib	Docker containers VirtualBox VMs pilot only)	--	Local at the site of HO	Unmanaged (s/w only)	Freely downloadable Customised for InCommon members
Gluu.org (Commercial - USA)	Shib	-	--	LDAP AD	Fully or User Managed (profiles)	Commercial Users

Provider (NREN or commercial)	IdP S/W	Deployment Technology	High Availability Strategy	User Directories integration	Management degree levels	Scope of Offer
				Gluu server		(6k$/srv/year)
Eduserv OpenAthens (Commercial - UK)	Shib	-	-	LDAP ADFS	Fully Managed	£5.40 per annum per user, volume discounts apply over 500 users

Table 2.1: Overview of current Cloud IdP offers

An important factor in favour of managed IdP instances is that they make it easier to deploy and manage policies and tools relating to attribute release and advanced features such as assurance profiles and entity categories which are required by research communities. These include the REFEDS Research and Scholarship Entity Category, the GÉANT Code of Conduct, and the SIRTFI framework for security incident response. At a national and international level, these requirements are very visible and solutions have been developed to meet them. However, for deployment in campuses demand is more fragmented and special configuration can be seen as an overhead and as lower priority where only a handful of campus users are affected. A managed approach enables these policies to be deployed without burdening the campus with the configuration work.

Based on the findings of this Market Analysis and the assessment of ongoing activities within NRENs in Europe, the common features for a Campus IdP platform that should be adopted on a wide scale to fulfil the needs and expectations of the largest possible set of European NRENs are:

- Automation in the installation and configuration of the SAML Shibboleth IdPs, providing hooks to configuration management tools such as ANSIBLE to carry out the process in a scalable, easy and reliable fashion on a running server.
- Possibility of providing several deployment scenarios including: improved Home Organisation deployment; NREN based (with the NREN acting as the Campus IdP Cloud provider); and an integrated deployment with FaaS. This allows for flexibility where data protection concerns require IdPs to be located within a particular jurisdiction.
- Possibility of integrating Metadata Registries/Resource Registries used by NRENs to host Campus IdP Entities Metadata. Based on the data in the registry, customisation of IdP instances for individual HOs should be provisioned, reducing the work time and skills required by both NRENs/federations and HO administrators.
- A new API service to manage configuration of IdPs from remote clients hosted on Web Interfaces (for example the Jagger Metadata Registry [Jagger]) would be required as a consequence of the integration of different Metadata Registry applications. This should be based on typical IdP configuration directives and standard message exchange protocols, to be

agreed upon and shared at the GÉANT and wider eduGAIN community level and beyond as appropriate.

- Possibility of interfacing in a safe manner with existing user databases at the Home Organisation premises or replicated databases hosted by the NRENs/federations (secure protocols and possible support for VPN connection between IdP instance and back-end database).
- Include support for High Availability of the IdP instances: resilience to the fault or unavailability of the individual instance so that a competitive SLA can be offered.
- Use of Containers, which appears a smart option to reduce costs and increase portability and manageability of the system. In particular, Docker Containers should be evaluated, to allow for lower hardware resource consumption and subsequent cost reduction, and high portability to Docker Engines hosted in different Cloud environment.

Required Feature	Proposed solution for the GÉANT Campus IdP platform	Notes
Support for IdP deployment	Automated IdP deployment e.g. ANSIBLE scripts for Shib 3.3.0+ IdP	
Security	Use of secure protocols and VPNs (where possible) –security patches applied and required upgrades made directly by the NREN	Home Organisations lacking skills and resources could address security management handing over to NREN
Ease of Configuration	Integration to IdP entities Metadata Registry – Development of API service to interface Resource Registry and Campus IdP cloud platform (e.g. Docker container Engine)	Jagger as initial reference Metadata Registry tool
Cost Reduction	Reduction of h/w consumed resources via Docker. Reduction in setup and configuration time per IdP	
Portability	Provision of IdP via containers	
Enforcement of advanced policy mechanisms e.g. assurance profiles, SIRTFI, CoCo, R&S, Multifactor etc.	Entity Category and other configuration support directly provisionable by system based on policies adopted.	

Table 2.2: Required features for a GÉANT Campus IdP platform

3 Recommendations for GÉANT to Address IdP Needs

Combining the outcome of the surveys with the analysis of the state of the art technology and market supply of IdP solutions, it is clear that while demand is broadly positive, it is also fragmented, i.e. no clear indicator for a single approach emerges.

An incremental approach has therefore been recommended where something of value to the community is delivered at each stage:

1. A first deliverable will be a public catalogue of IdP solutions that are available to be used beyond a single-federation context, with information about their suitability for use within an eduGAIN context e.g. support for entity categories etc. and terms of use. This will be initially based on information from this market analysis and survey but can be enhanced on an ongoing basis through community contributions.
    - The potential of enhancing the catalogue with service brokering between NRENs where they could charge a fee to users outside their own federation was also discussed. However it was agreed that, although the suggestion was thought very interesting, JRA3 lacks the required skills in this area, and would therefore ask the GÉANT organisation to address this separately within the wider context of inter-NREN service delivery.
2. Following this analysis, one of the existing approaches will be chosen as the basis for the GÉANT IdP service and implemented as playbooks and containers which will then be made generically available for download and customisation. Where this is based on open source, NREN or global partner developments, contributions will be made upstream wherever possible.
3. The next product iteration will be a platform to deploy the containers with a custom configuration to any infrastructure specified by the administrators, to enable NREN distribution in campuses (this could also serve non-campus requirements e.g. community IdPs for research communities).
4. A final product will be a managed service in FaaS, deploying to GÉANT infrastructure.

A GÉANT solution should address reduction of costs and complexity through automation of configuration and ease of administration, as well as integration with Metadata Management tools and eduGAIN. In addition, typical requirements such as availability and reliability should be addressed. Considerations on security of data and data protection requirements, as well as integration with local directories are also essential.

Each single product, rather than just the final aggregate product, can be provided individually by GÉANT, and demand reassessed for the next step at the end of each phase. This will allow for adaptation to changing environments and demand, and also enable meeting the conflicting demands of different groups as far as possible. The ongoing costs of operation for the earlier steps will thus be minimised, while benefits will still be delivered thanks to aggregating expertise.

A Cost Benefit Analysis for the phased delivery of these products will be developed based on these recommendations. The costs for development should be linked to KPIs to ensure that containerisation and service delivery scales are competitive in terms of cost with commercial offerings, while being more closely customised to R&E federation needs.

To align with R&E federation needs in particular, a strategy should be outlined for integrating with eduroam-managed IdPs and support the deployment of the eduKEEP model, where campuses provide attributes only and IdPs are centralised.

Common deployment modules for the eduroam radius-based identity provider and the SAML IdP are already being provided by some NRENs (CESNET), and it is recommended that the GÉANT Campus IdP platform provide a deployment option to interface the local IDM Directory in a joint deployment model for all scenarios foreseen by Campus IdP, including: toolkit, locally deployed container, and hosted container by the NREN on a private or hybrid Cloud platform.

Concrete mechanisms and approaches for this will be developed with JRA3 T4, which addresses eduroam development. Overall, there are two (non-exclusive) possible paths for synergy:

- eduroam-aaS becomes an SP to the Campus IdP: eduroam credentials are issued if the end user can log in using eduGAIN credentials. This would make manual IdM on the eduroam side obsolete.
- IdM is performed on the eduroam side; the resulting client credentials are X.509 certificates. The campus IdP can then authenticate users with (eduroam) client certificates in the browser.

These options will be assessed in the forthcoming months by both the Campus IdP and eduroam teams.

A global strategy for supporting Home Organisations in the adoption of Federated Identities should closely follow the eduKEEP progress in JRA3 T3 and periodically evaluate the possibility of providing eduKEEP as a central alternative to individual Home Organisations' IdPs. The eduKEEP approach implies campuses will operate attribute authorities and may benefit from managed services for this infrastructure. The architecture for Campus IdP should be flexible enough to extend to this use case.

Appendix A Overview of IdP Solutions

A.1 AMRES

At present, the AMRES federation is using a centralised architecture where it is responsible for providing a central SAML IdP. This solution was chosen in order to relieve AMRES members from the obligation of maintaining a SAML IdP. On the other hand, institutions which are using the central AMRES SAML IdP still need to maintain a valid and up-to-date user registry, as well as a RADIUS server which represents the authentication back end for central SAML IdP and which is at the same time used for eduroam. The current architecture may potentially be developed into a hybrid set up, should some of AMRES's members decide to run a SAML IdP on their own.

However, after a few years of fieldwork, AMRES engineers have come to the conclusion that most of its member institutions either did not have any kind of IdM in place, or were unwilling to move to another type of IdM system, or had multiple user registries that were not synchronised. Problems with RADIUS server installation and maintenance were also observed. This was due to of the lack of various resources, including hardware resources, human resources, knowledge or motivation. As a result, AMRES is working on a project that will enable smaller institutions (presumably with no more than two-digit numbers of users), as well as primary and secondary education institutes, to connect to AMRES's central SAML IdP by providing a fully hosted IdP solution [AMRES IdP].

This hosted IdP is envisioned as a central solution consisting of RADIUS (based on FreeRADIUS) and LDAP (based on OpenLDAP) servers. AMRES will be responsible for all the necessary OS updates, bug fixes, security updates etc., while the member institution is responsible for keeping the user registry (LDAP) up to date. Different HA scenarios are being considered at the moment, but all the critical elements will have some kind of replication in place.

In order to make IdM easier for institutions, a web application was developed for authorised institution personnel to create/suspend/remove users, add/remove attributes and create roles. The existing in-house web-based monitoring tool will be used to keep track of problems and for reporting (monthly SLA) for this centralised solution.

The service in question will be available to institutions at no charge, thanks to AMRES's financing model (fully funded by government).

A.2 GARR IdP in the Cloud

GARR provides Cloud-based IdP [GARR IdP] instances to customers in the HealthCare domain, namely Research Hospitals (IRCCS), in the context of a more general contract in place with the Italian national Ministry of Health. Other customers of the IdP in the Cloud service are the Ministry for Cultural Heritage and the Experimental Zooprophylactic Institutes. GARR's solution is based on Openstack as reference private Cloud platform, provided by the DataCenter GARR is hosting for its Cloud Department in Palermo. GARR provides fully hosted IdPs for the IRCCS institutes, including an LDAP backend, a PhPLDAPadmin administrative interface for user management, a basic web interface showing statistics based on log analysis (e.g. top ten peering SPs, etc.) and the Shibboleth IdP itself. The overall architecture is shown by the following figure.

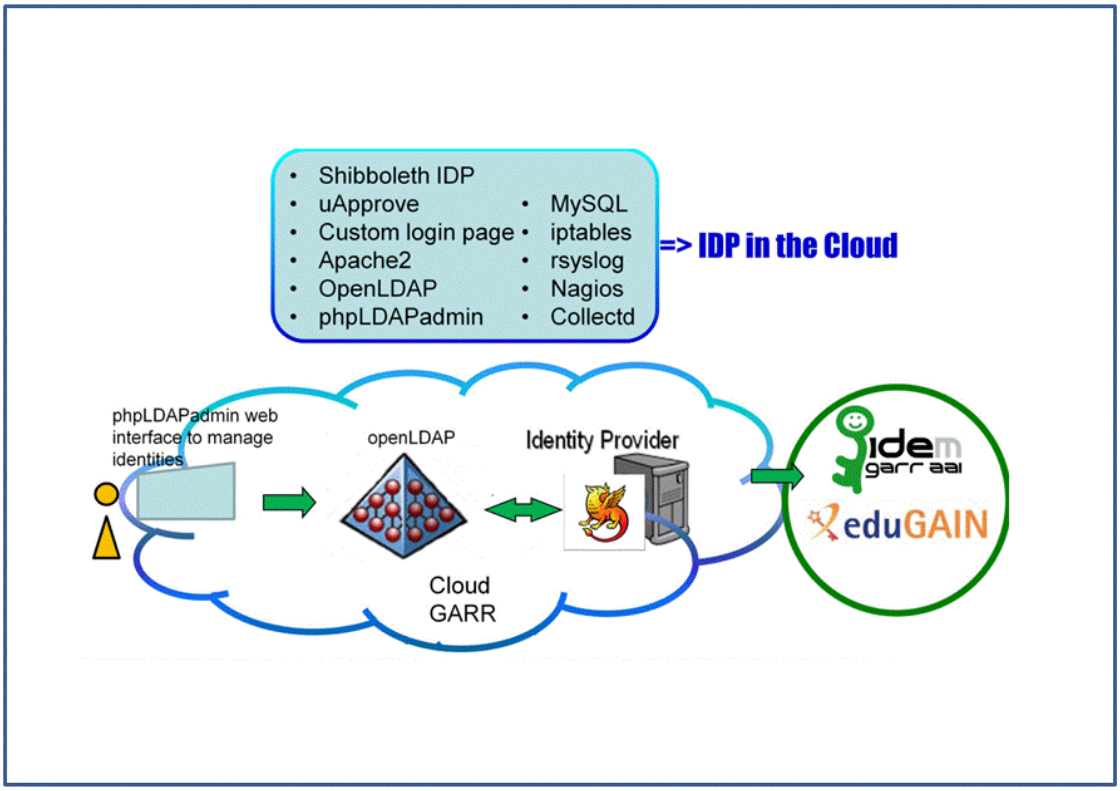

Figure A.3.1: Architecture of the GARR IdP in the Cloud service

IdP in the Cloud's deployment model is based on a VM provided by Openstack NOVA (Ubuntu), with installation and configuration of the IdP and related dependencies carried out using Puppet. Puppet recipes are kept up to date and stored in the infrastructure on the Puppet Master node. A set of monitoring tools, based on NAGIOS, ELK and bash scripts developed in house, keep the whole IDP infrastructure under the control of the Cloud operators.

Funding and sustainability are currently based on the contract in place with the Ministry of Health.

A.3 CESNET's solution for eduID.cz participants

CESNET has developed an automated way to install and configure Shibboleth IdP for small- to medium-sized customers [CESNET IdP] without the sufficient technical capacities to deploy and operate an IdP of their own. The IdP is run on CESNET's virtualisation platform, which is distributed in two data centres in two geographically distant locations. All that is required from participating organisations is a user directory -- LDAP, Active Directory or MySQL. Currently, this IdP deployment is being tested with one of the small organisations that recently joined, which has about 50 users, and discussions are also being held with another organisation regarding IdP deployment. Automation does not just involve the IdP, but also the firewall setup and operating system upgrades. As the participating organisation is a CESNET's customer, the home organisation can also be provided with an SSL certificate for CESNET's IdP using the GÉANT TCS service. Therefore CESNET does not just manage the IdP but also the whole underlying operating system. CESNET could also install and operate the IdP on any virtual platform or physical hardware chosen by the home organisation. However for this it would require a dedicated server without any other services run by the participant or any third party, in order to minimise disruption to other services. CESNET's IdP deployment is managed by a script (Ansible) and so the IdP is ready very quickly depending on the availability of the server (virtual or physical) and SSL certificate.

For the first 12 months, the service itself is provided for free. However, participants are required to pay for the virtual machine if the IdP is running on CESNET's virtual platform (15 € per month). After a 12-month trial run, the organisation then must decide whether to continue using the service (the price will be highly dependent on the number of hosted IdPs, most probably 15 to 20 € per month) or manage the IdP by their own means.

A.4 JISC Managed IdP Service

The requirement

Today Jisc offers three access management services [Jisc IdP]: the Access Management Federation (AMF), eduroam, and Assent. These services are used to manage access to web content, network connectivity, and research e-Infrastructure respectively.

Organisations wanting to use these services must obtain an Identity Provider (IdP). Typically, the IdP is either software that is deployed and operated by the organisation itself, or else a service provided under contract by a third-party provider. Generally, an IdP is required for each service because of the differences in the underlying technology and configuration.

The offer from Jisc

Jisc's Managed IdP Service is a Cloud-based offering that enables organisations to *reduce the cost of IdP provision* while uniquely offering an IdP that *supports all three access management services*. Customers are free to choose which of these to enable.

The system performs the following core functions for each of these services:

- Authentication of user credentials against the customer's Microsoft Active Directory, LDAP directory, or an LCF-compliant Library Management System.
- Authorisation of users via membership of Groups defined in Microsoft Active Directory or another LDAP directory.
- Provision of user attributes to services based on policies determined by Group membership.
- Accounting and reporting of user authentications and service use

The AMF capability also includes support for legacy IP-based authentication, for those web services that require it.

The Managed IdP service may also be used in other settings where the SAML 2.0, RADIUS, or ABFAB/Moonshot technologies are available; its application is not limited or constrained to the AMF, eduroam, or Assent environments.

Its key benefits and advantages are summarised in the following table.

Feature	Advantage	Benefit
A competitive tariff	Reduces the cost of IdP provision	Drive organisational cost efficiencies
Supports AMF, eduroam, and Assent	A single solution for IdP provision	Easy to administer identity provision for all three services
Simple integration with Microsoft Active Directory and other LDAP directories	Allows use of an organisation's existing identity management system	Quick and easy to deploy and use
Office hours' technical support	Help from the experts when you need it	Ensure a reliable service for your users
Designed and operated by leaders in access management	The service has the capabilities and reliability that you and your users need	Fit for purpose, today and tomorrow

Table A.1: JISC offer benefits and advantages

Adopting the service

The service is delivered from a public Cloud Provider using a platform developed and operated by Jisc. Located in Dublin, this is connected directly to Janet, Jisc's network. Jisc creates an IdP instance for each customer who subscribes to the service, and who can then decide which capabilities (AMF, eduroam and/or Assent) to enable. This can subsequently be changed at any time.

Before using the service, the customer deploys a VPN endpoint. This is used to protect data in transit between the customer's network and Jisc's service platform. The customer can use the VPN appliance provided by Jisc, or provide their own endpoint. Jisc then configures the IdP instance to connect to

the customer's Active Directory or another LDAP directory using its IP address and binding credentials, which are provided by the customer.

Using the service

Once the directory is connected, Jisc provides the customer with access to the service's management portal. This allows the customer to make changes to authorisation and attribute release policies, and to view usage reports.

The IdP instance will then need to be registered with the AMF, eduroam, and Assent services to make use of those. Once registered, the IdP can be used by the customer's end users for these services.

Support arrangements

The responsibility for support is shared by Jisc and the customer, as described in the table below. In brief, Jisc supports the customer in adopting the service and using its management portal, and the customer is responsible for end user support.

Support function	Responsibility of	Responsible for issues associated with
First line	Customer	End user account management (e.g., password resets, account locking, etc.) End user system configuration (e.g., eduroam Wi-Fi network configuration) End user documentation, training & assistance
Second line	Jisc	Connectivity issues (e.g., network, VPN or LDAP connections) Issues associated with using the service management portal (e.g., accessing it) Assistance in resolving user authentication issues Guidance in defining authorisation and attribute release policies
Third line	Jisc	Resolving technical issues with the platform (e.g., bugs, etc.) Processing and escalating requests for new features

Table A.2: JISC offer support model

Paying for the service

Organisations subscribe to the service for a minimum term of one year.

- For Jisc's Members, the tariff is structured around the Jisc Banding model; pricing is available on request.
- Other NRENs and Public Sector organisations receive a preferential tariff; pricing is available on request.
- Organisations from the Private Sector are welcome to use the service; pricing is available on request.

Depending on the status of the organisation, additional fees may be payable to register for AMF, eduroam, and Assent.

A.5 HEAnet

HEAnet is currently offering a double provisioning option for SAML Identity Providers to Home Organisations: the Standby Identity Provider and the Hosted Identity Provider.

The Standby Identity Provider is an instance at HEAnet premises, based on locally replicated User Directories, which takes over whenever HEAnet detects unavailability of the Home Organisation's locally hosted IdP.

User base replication is carried out via VPN and secure protocols, and makes use of LDAP or Active Directory as reference user database platforms.

The Hosted IdP Identity Provider is a Shibboleth IdP instance run at HEAnet premises on behalf of the Home Organisation, with no local replica of the user base.

The Hosted IdP connects to the original user base at the Home Organisation's premises via secure protocols, via either LDAPs or LDAP through VPN.

Both options are framed in the context of the Managed Identity Provider offer that includes monitoring, support for specific technical issues on the Shibboleth IdP for the Home Organisations (migrations, upgrades, changes in the user database backend)) and relies on 24/7 support for relevant issues/accidents (blocking problems, urgent issues).

The offer by HEAnet is described in the Identity Federations section of the HEAnet web site [HEAnet IdP].

A.6 SWITCH

SWITCHaai Identity Provider Hosting [SWITCHaai] allows organisations to outsource the operation and maintenance of an Identity Provider (IdP) to SWITCH. The service is primarily targeted at small and medium-sized institutions that are saving costs by mandating SWITCH to run their Shibboleth-based Identity Provider.

The Identity Provider Hosting service is available for SWITCH Community members and for other SWITCHaai Participants entitled to run their own IdP in the SWITCHaai Federation.

SWITCH currently uses two dedicated VMs per customer, with RHEL in two geographically distant locations in a hot standby setup with manual handover. For minimal user interference, the SWITCH approach uses IP anycast so that the IP address is always the same, independently of which instance the traffic gets routed.

The following information is from the SWITCH Information Brochure for potential users:

The SWITCH offer consists of the provisioning of IdP in redundant and secure environment;

Software and security updates are managed by SWITCH; Service monitoring and alerting are provided. Customers remain responsible for user directory as well as attribute management and release policy.

Connection to customer's user directory is usually by encrypted LDAP connection (other methods possible, e. g. relational database).

Primarily targeted at small and medium-sized institutions - Unbundled service with separate tariff /pricing.

A.7 RENATER

RENATER's IdP hosting as a service offer [RENATER Fed], includes deployment, configuration and hosting of Identity Providers. All the technical aspects (monitoring, updates) are included in the offer.

If an organisation is too small and does not operate a user directory, RENATER will provide a hosted directory which the organisation can access through a web interface that allows it to add and define access roles and attributes for multiple users.

Various methods and tools have been used to ensure the continuous availability of the service (BIG-IP f5 Load-Balancers, Firewalls, Nagios, etc.).

Management of updates has also been taken into account (bug fixes, security updates, use of the new features of the IdP, etc.). Ansible has been used wherever possible to automate setup and configuration.

The deployment model is based on VMs (Centos) managed by VMware vRealize Automation Appliance. Puppet is also used to configure the system part.

A.8 US - TIER

Internet2's Trust and Identity in Education and Research [TIER] program aims to simplify campus processes and advance inter-institutional collaboration and research. Rather than offer a managed service at this stage, the TIER programme instead is both an open-source toolset and a campus practice set. The toolset includes a set of critically important identity-related software components and development is aimed and making these tools easier to manage and deploy and to enhance them to meet campus-specific use cases provided by a range of US based campuses, large and small. It is funded directly by over 50 campus contributions.

TIER Release 1 took place in April 2016. It packages three open-source software components (Grouper, Shibboleth Identity Provider, and COmanage Registry) together and provides a first look at container-based distribution. As Shibboleth is also widely used within the GÉANT community at campus level, the sustainability, integration and improvement work done by I2 will additionally benefit European users. It may also make the work involved in developing and deploying managed IdP services simpler and more cost effective. It is therefore important to track the work of TIER and for GÉANT to arrange MoUs for contributions of use cases and effort to relevant components as needed.

References

[AMRES IdP]	https://www.amres.ac.rs/amres-hosted-idp
[CESNET IdP]	https://www.eduid.cz/cs/tech/join
[Compendium]	https://compendium.geant.org/compendium-2015-updated.pdf
[eduGAIN]	http://www.geant.org/Services/Trust_identity_and_security/eduGAIN
[GARR IdP]	https://tnc2014.terena.org/core/presentation/31
[HEAnet IdP]	https://www.heanet.ie/services/identity-access/hosted-standby-saml-identity-provider
[Jagger]	http://jagger.heanet.ie/
[Jisc IdP]	https://www.jisc.ac.uk/uk-federation
[RENATER Fed]	https://services.renater.fr/federation/index
[Shibboleth]	https://shibboleth.net/products/identity-provider.html
[SWITCHaai]	https://www.switch.ch/aai/
[TIER]	https://spaces.internet2.edu/display/TPD

Glossary

AAI	Authentication and Authorisation Infrastructure
AARC	Authentication and Authorisation for Research and Collaboration
AMRES	Serbian Research and Education Network
AP	Attribute Provider
API	Application Programming Interface
CA	Certification Authority
eduGAIN	EDUcation Global Authentication INfrastructure
FaaS	Federation as a Service (GÉANT)
FIM	Federated Identity Management
GARR	Italian National Research and Education Network
HA	High Availability
HO	Home Organisation
HEANet	Irish National Research and Education Network
IdM	Identity Management
IdP	Identity Provider
Jagger	Jagger Metadata Registry
LDAP	Lightweight Directory Access Protocol
NGI	National Grid Initiative
NREN	National Research and Education Network
RADIUS	The Remote Authentication Dial-In User Service
REFEDS	The REsearch and FEDerationS group
RENATER	French National Research and Education Network
SAML	Security Assertion Markup Language
SP	Service Provider
SWITCH	SWISS Research and Education Network
TLS	Transport Layer Security
VM	Virtual machine
VPN	Virtual Private Network