31-10-2013

Milestone MS83 (DS5.4.1): Federation as a Service - Market Analysis and Pilot Service Definition

Milestone MS83 (DS5.4.1)

Contractual Date:	31-10-2013
Actual Date:	31-10-2013
Grant Agreement No.:	605243
Work Package/Activity:	WP9/SA5
Task Item:	MS83
Nature of Deliverable:	R
Dissemination Level:	PU
Lead Partner:	NORDUnet
Document Code:	GN3PLUS13-557-42
Authors	M. Veremezović (AMRES)
Contributors	L. Hämmerle (SWITCH), V. Nordh (NORDUnet), P. Schober (ACOnet), B. Schofield (TERENA), N. Sluer (TERENA)

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013) under Grant Agreement No. 605243 (GN3plus).

Abstract

Federation as a Service (FaaS) is the SA5 T4 Task aimed at assisting NRENs, individual institutions and Large Projects to gain or provide access to federated services. This report presents the Market Analysis undertaken to evaluate the services that could be offered by a Pilot Service for these three entities. A definition of the FaaS Pilot Service is also presented.

Milestone MS83 (DS5.4.1):
Federation as a Service - Market Analysis
and Pilot Service Definition
Document Code: GN3PLUS13-557-42

Table of Contents

Table of Figures

Table of Tables

1 Service Objectives and Work Plan

An NREN is a specialised Internet Service Provider and as with other ISPs, expectations about the range of services have grown over the years. While once it was only expected that an NREN would provide a reliable national network, today's user expects a range of additional facilities such as access to pan-European federated services. Providing such services becomes easier with an Identity Federation that enables NRENs to participate in eduroam and eduGAIN.

Large international research projects are another specific group with strict requirements for an Authentication and Authorisation Infrastructure (AAI). NRENs are facing the demand to provide services such as access to large data sets to an expanding user base in shifting collaborations that need to ignore organisational and national boundaries. These "Large Projects" often have many service providers deployed in different countries, which presents a challenge to federating these services.

Federation as a Service (FaaS) is the SA5 T4 Task within GN3plus aimed at assisting NRENs, individual institutions and Large Projects to gain or provide access to federated services. The FaaS task will assess the means of offering the benefits of the eduroam Federation, the WebSSO Identity Federation and potentially Moonshot as a service to Service Providers (SPs) who choose not to, or are unable to, operate these services themselves. The goal is of running a pilot for this service by the end of the GN3plus project. FaaS has liaised with its target groups to understand the issues they have today and how GÉANT can effectively engage in order to obtain Federation services for them. The final goal is to develop the necessary policy and technical infrastructures required to offer a FaaS pilot according to the best practices currently available.

The first quarter of the FaaS timeline (to 31 September 2013) was focused on Market Analysis: this is presented in Section 2 of this document. The types of services that could be offered by a FaaS pilot are outlined in Section 4, and these allow a FaaS Pilot Service to be defined in Section 5 of this document.

2 Market Analysis

FaaS should assist NRENs, relevant institutions and Large Projects to make use of Identity Federation technologies. For FaaS it was important to start with a thorough understanding of the potential obstacles, in terms of technology, the availability of knowledgeable and skilled personnel, and political, financial and funding issues. FaaS have three target groups and it was important to perform a market analysis for each of them.

To understand the NREN's requirements, FaaS interviewed those NRENs which are not running a Federation. Interviews were performed in cooperation with the GN3plus SA5 T3 Federation Support eduGAIN subtask, whose aim is to help emerging and existing federations on their road map to a full operational federation. Given the overlapping working fields and target groups, FaaS and eduGAIN worked together closely during the first six months of GN3plus and jointly entered into dialogues with the NRENs involved to get a clearer picture of the issues hindering Federation deployment. The results of these interviews are summarised in Section 2.1.

The second FaaS target group were individual institutions. Because of their potentially large number and as the institutions are in most cases represented by their NRENs, the most efficient approach was to ask the NREN representatives about institution requirements to adopt federation. The results of these interviews are summarised in Section 2.2.

The third, and very specific FaaS target group were Large Projects. SA5 T5 Enabling Users task's objective is to act as an expert partner for large pan-European projects with AAI requirements and to set priorities for the other AAI tasks in SA5, so it was natural for FaaS to collaborate closely with the Enabling Users task. Task 5 already coordinates at least three collaboration projects between GÉANT and specific user communities, addressing their federated-identity concerns. The knowledge and experience gained will be documented in a knowledge database that will serve other projects that have similar needs. The requirements for Large Projects are summarized in Section 2.3.

2.1 NRENs: Market Analysis

European National Research and Education Federations are usually run by NRENs themselves[1]. Of the 43 partners in GN3plus, there are currently two NRENs that are without an eduroam federation[2] and 21 NRENs that are without a WebSSO Federation[3]. For the eduroam service, SA5 T2 is aiming to support these NRENs in building their eduroam federation, which will result in full eduroam service coverage among GN3plus partners. However, even where an NREN does operate an eduroam service, there may

[1] A list of existing European SAML federations can be found at https://refeds.org/europe_map.html

[2] The countries without eduroam are Georgia and Ukraine.

[3] The countries without SAML Identity Federation are: Armenia, Azerbaijan, Belarus, Bulgaria, Cyprus, Georgia, Iceland, Israel, Lithuania, Luxembourg, Macedonia FYRo, Malta, Moldova, Montenegro, Poland, Romania, Russia, Serbia, Slovakia, Turkey and Ukraine.

still be problems in increasing the participation with NREN institutions and it is this aspect which was covered in the market analysis. Consequently, for the market analysis, all 21 NRENs without a Federation were contacted. Six of them answered the invitation and were interviewed.

As for the means of conducting the NREN market analysis, it was decided to talk directly to selected NREN representatives rather than send them a survey to complete. This way it was possible to talk actively about the deployment status of their Federation, discuss the issues that are standing in their way and concentrate on specific circumstances in a country that might otherwise be overlooked in a general survey. To be able to compare, analyse and summarise, these interviews were structured with an outline list of topics and questions, consisting of the following groups:

- **General** – investigates the status of Federation deployment. NRENs were asked if there are existing or planned web services, or if they were candidates for the WebSSO Federation.
- **Issues** – NRENs were asked to grade the problems they have with Federation deployment, grading the issues by difficulty: these results are presented in Section 2.2
- **Support** - the ways that NRENs can be supported by FaaS in their way of joining or providing a Federation.

The analysis of responses is presented in the following Sections.

2.1.1 General status of Federation deployment in NRENs

NRENs were asked if they had already started to build their own WebSSO Federation and what is the progress until now. The summary of responses is presented in Figure 2.1.

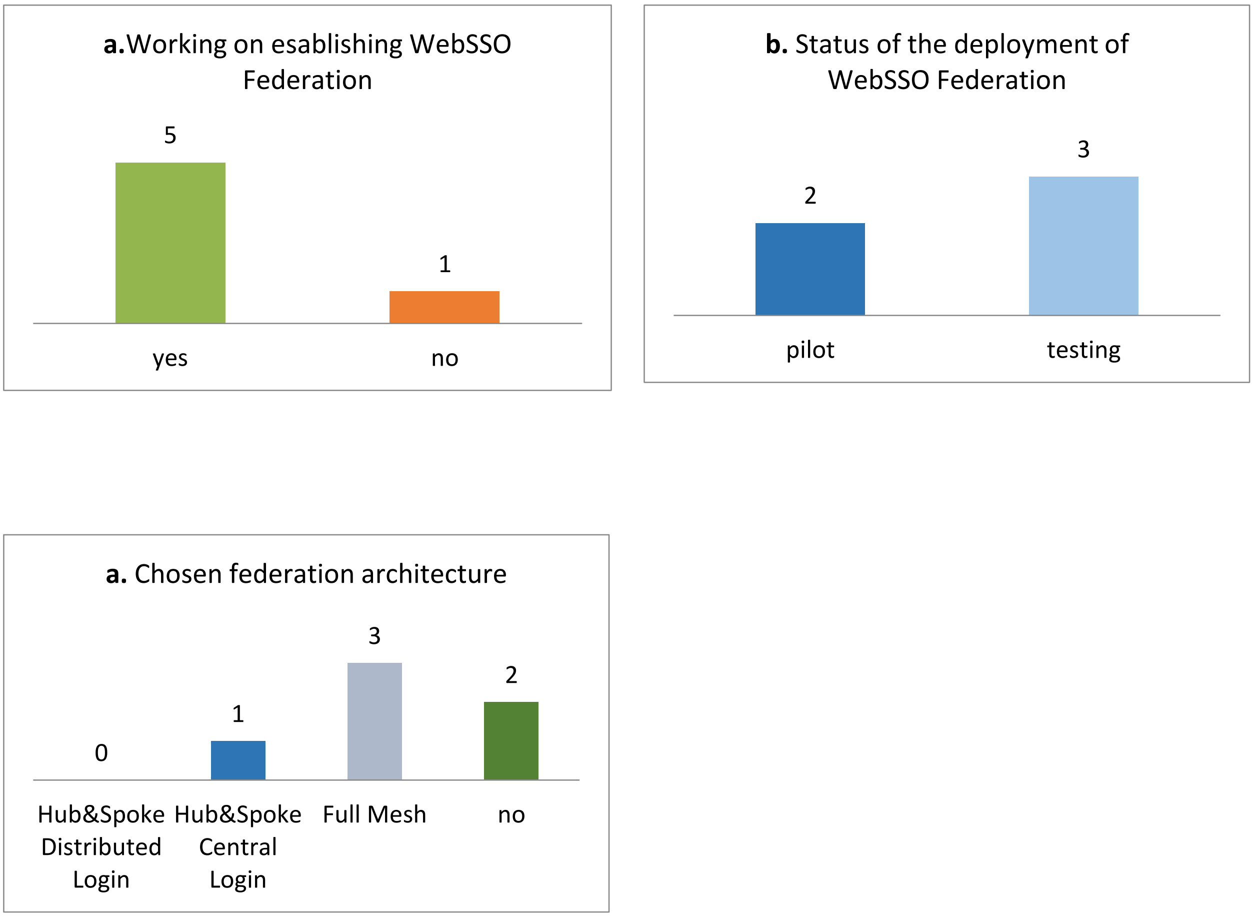


Figure 2.1: Status of WebSSO Federation deployments in NRENs

The answers received are surprising. Interviewed NRENs showed that they already had the knowledge about federations and were aware of its benefits. Most of them had already made some progress in building their own federation, with some being in pilot status. However, these results should be taken with caution as the NRENs that were interviewed are mostly the same ones who had already participated in the Building Identity Federation workshops organised by EuroCAMP. When it came to deciding the federation architecture, most of the NRENs chose the mesh architecture, one chose a central IdP architecture, with two NRENs undecided about the architecture for their WebSSO Federation.

For the interviewed NRENs it was challenging to give more information about candidate web services for WebSSO federation. This could be because there are few services in need of AAI or that some NRENs are not aware of the benefits of operating an AAI. When asked if an NREN's institutions have services that would have inter-institutional usage, or if there are services outside their country that their users showed interest in, with the exception of one service, they knew of no such cases. A list of services NRENs mentioned in the interviews is shown in Table 2.1, together with the number of occurrences of the same service in different interviews.

Existing services	
Library Access to scientific information	5
Filesender	3
Confusa for TCS personal certificates	1
Grid services	1
Okeanos	1
School e-diaries	1
Microsoft Dreamspark	1
Wiki pages	1
Confusa for TCS personal certificates	1
Document delivery service	1

Planned services	
Web video-conferencing	2
Tool for Surveys	1
Confusa for TCS personal certificates	1
BigBlueButton	1
Filesender	1
Trusted cloud drive by TERENA	1

Table 2.1: List of services candidates for WebSSO Federation

There is one service that took a clear lead in this list. Almost all countries have nationally-procured library access to scientific information; this is not commonly not provided by the NRENs. In some cases, this service is enabled though the EIFL program [EIFL]. Access to this service is IP-based which denies access to the service when users are not at the place they work or study. Some NRENs use a VPN service mainly to resolve this issue. Also, because NRENs do not operate the service, most of them agreed that they would first have to talk to institutions that are in charge of the service.

Discussions during these interviews revealed one more factor in NRENs status that turns out to be important: the way a NREN is constituted is a significant aspect when planning how to deploy Federation. Two cases were encountered:

- The NREN is constituted as legal body and has the manpower delegated to do work within the NREN. This constitution enables the NREN to host central services, to define the policy and technology for the service that institutions have to follow, and to provide institutional support.
- The NREN is a consortium of Universities. This constitution makes it more difficult to provide central services and to centrally govern them. In this situation it is difficult to support or influence the adoption of new services at other Universities.

The consequence is that NRENs that are consortia of Universities would prefer a solution which doesn’t have centralised services. Deploying new services is strictly at the discretion of each institution and there are less means of driving them into adopting new services.

2.1.2 Issues NRENs have in deployment of Federation

NRENs were asked to grade the problems they have when deploying WebSSO and the eduroam Federation. The list of issues was predefined and NRENs were given a scale from 3 to 0 to grade them;

3 represented a very significant issue, 0 was not an issue at all, with 2 and 1 for the grades in-between. An even-number scale was chosen to remove any bias towards a middle, neutral grade.

In the first group of questions, NRENs were asked to grade the relevance of problems they have with deploying WebSSO Federation. Full results are presented in Appendix A, Figure A.1 with the average scores in Figure 2.2, below.

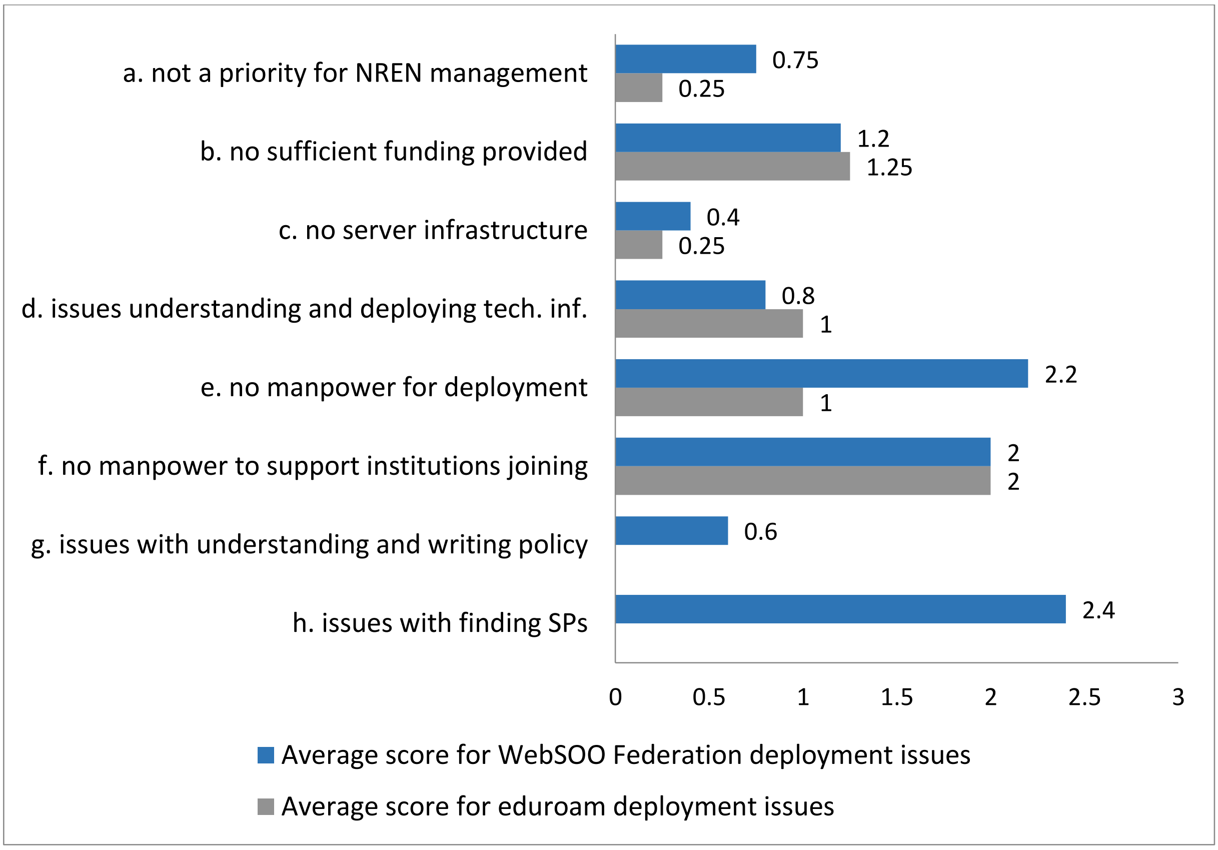


Figure 2.2: Average scores for problems NRENs have deploying eduroam and WebSSO Federaton

These grades highlight certain issues:

- There are funding issues (based on **b**);
- There is an issue with finding SPs that have AAI requirements (based on **h**);
- There is not enough manpower for WebSSO Federation and for supporting institutions joining (based on **e** and **f**).

These issues are shown in diagram form in Figure 2.3. The equation shows that a prerequisite for successfully building a WebSSO Federation is to have manpower dedicated to this task. The amount of manpower is related to the available funding and the perceived need for the service. In this case, with funding problems and with no urge for the WebSSO Federation (less SPs with AAI requirements), much less manpower is dedicated. The end result is delay in building a WebSSO Federation. If either the funding or the need of a WebSSO federation were higher, more manpower would be provided.

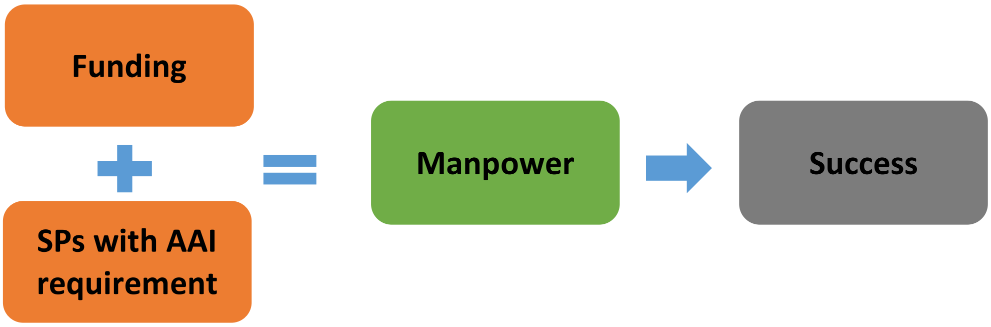


Figure 2.3: Diagram for successful deployment of WebSSO Federation

Figure 2.4 shows the NREN staffing figures in target NRENs taken from the TERENA 2012 Compendium [Compendium]. This chart shows that roughly one third of these NRENs have less than 10 full-time staff members, one third have between 10 and 20, and one third between 20 and 30. These numbers also include administrative staff and there is wide variation in the service portfolios that they support. It is likely that few of these NRENs could provide additional technical staff for federation duties from their current manpower resources.

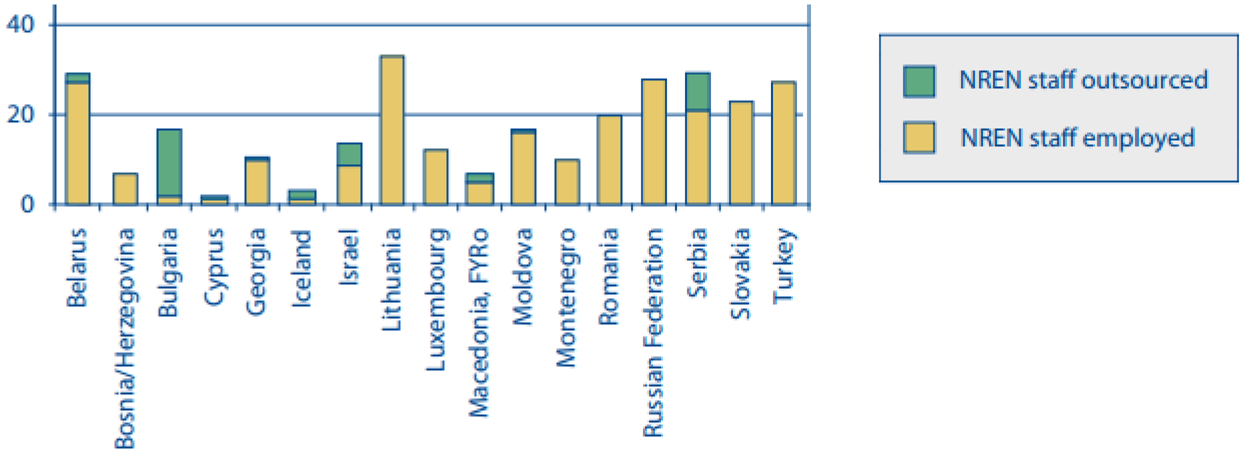


Figure 2.4: NREN staffing statistics (from TERENA Compendium 2012)

The other grades in Figure 2.2 show that there are some issues in understanding the technical solution (based on d) and creating a policy (based on g), but these issues are certainly not critical. With slightly more manpower, adequate training and readily available information resources, NRENs could overcome these obstacles. NRENs have the necessary technical infrastructure to deploy a WebSSO Federation (based on c). NRENs generally give a reasonably high priority to deploying a WebSSO Federation, although some NRENs marked “Don’t know” as the response, which could indicate that this matter has not been discussed with their management.

In the second group of questions, NRENs were asked to grade the relevance of problems they have with deploying the eduroam Federation. Source figures are presented at Appendix A, Figure A.2 and average scores at Figure 2.2.

The results again show that the biggest issue for these NRENs is lack of manpower (based on e and f). However, there is one significant difference between eduroam and WebSSO federation, which is reflected in services provided in those federations. Namely, the eduroam federation provides network access, which is a widely known and established commodity service. There is a suspicion that when deploying eduroam, the NRENs were motivated to join the eduroam federation as they had wireless to be federated and the benefits for their users of being able to use wireless when visiting other institutions were obvious. Returning to Figure 2.1, with probably the same funding issues, we can understand why those NRENs managed to deploy eduroam federation – they had SPs with AAI requirements. In addition, favouring eduroam adoption could be because the people who were interviewed mostly work with the network and eduroam is more familiar to them.

The other grades show that there are some issues of understanding and deploying a technological solution (based on **d**), but these were certainly not alarming.

2.1.3 Support for NRENs by FaaS

NRENs were asked how, in their opinion, FaaS could help them with federation deployment. At the time of these interviews, FaaS did not have a precise list of what FaaS services would include, so it was difficult for NRENs to answer this question accurately, so the responses should be interpreted with caution. Once the FaaS task creates its portfolio, it would be wise to send out a follow-up survey to these NRENs in order to get an accurate picture of what they would choose from the FaaS services list. When NRENs were asked about support for WebSSO Federation, the responses are listed in Table 2.2.

Support for NREN
Funding for the manpower
Policy framework
Best practice documents and Deployment Cases
Consulting with expert
Workshops and Hands on help
Identity Management best practice

Table 2.2: List of support that NRENs expressed an interest for

When asked if they would be interested in using the FaaS services if the NREN Federation infrastructure was hosted and operated by GÉANT, two NRENs expressed interest in using a centrally-hosted Metadata Management tool, one NREN gave an explicit “no” and the others were “Don’t know”.

From the perspective of sustainability of the FaaS, it was important to know if NRENs were willing to pay in the future for some FaaS services. The attitudes towards paying for FaaS support are presented in Figure 2.5.

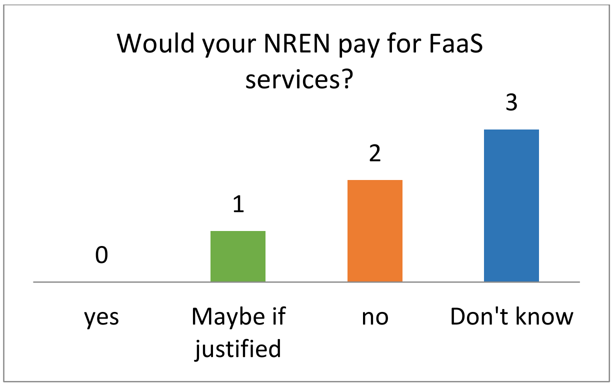


Figure 2.5: NRENs disposition towards paying for a FaaS support

The responses, though the sample is small, show a reluctance by NRENs to pay for FaaS support. This should be taken into account when planning for the FaaS Pilot, so that the services offered for NRENs are sustainable without monetary support coming from NRENs.

2.2 Individual Institutions: Market Analysis

As previously stated, NREN representatives were interviewed in order to learn about the issues standing in the way of adoption of federation technologies by individual institutions. The overall impression was that NRENs do not have good insight about these services in their member institutions. The status in the largest Universities is usually known because they are the institutions with a large user base, they have identity management systems and good IT support that adequately delivers IT services. The conclusion was that NREN member institutions can in general be divided into two groups:

- Higher education institutions i.e. Universities which are usually capable of adopting new technologies given sufficient interest;
- Other institutions that have a much smaller user base, small IT departments and that would probably have problems in adopting federation technologies without the NREN’s support.

As before, NRENs were asked to grade the relevance of problems their member institutions have in regard to the federation.

Properly managed Identity Management systems (hereafter referred to as IdM) are a central component on which an AAI relies and it is crucial to understand if institutions are capable of running them. In the first group of questions, NRENs were asked to grade the relevance of problems their member institutions have in deploying IdM system and maintaining user identities. Source figures are presented in Figure A.3 and average scores in Figure 2.6.

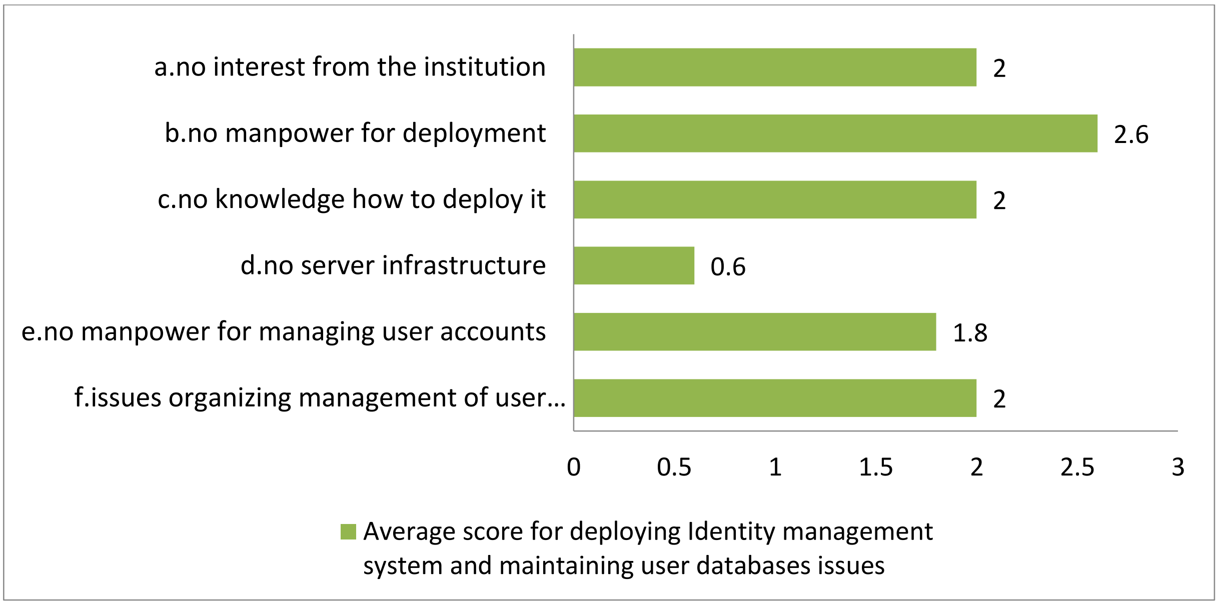


Figure 2.6: Average scores for problems institutions have deploying Identity management system and maintaining user identities

Results show that institutions in general have the following problems:

- There is no interest by the institution in deploying IdMs (based on **a**). This shows that they probably don't have clear business case for having IdM;
- There is no manpower available for IdM, managing user accounts and managing internal procedures (based on **b**,**e** and **f**);
- Institutions are lacking the knowledge needed for deployment of IdMs (based on **c**);
- Institutions have some issues with the server infrastructure needed for operating an IdM, but this is not a serious issue (based on **d**).

In the second and third group of questions, NRENs were asked to grade the relevance of problems institutions have or potentially would have in adopting the WebSSO and eduroam federation respectively. Summary results are presented in Figure A.4 and Figure A.5 and average scores in Figure 2.7.

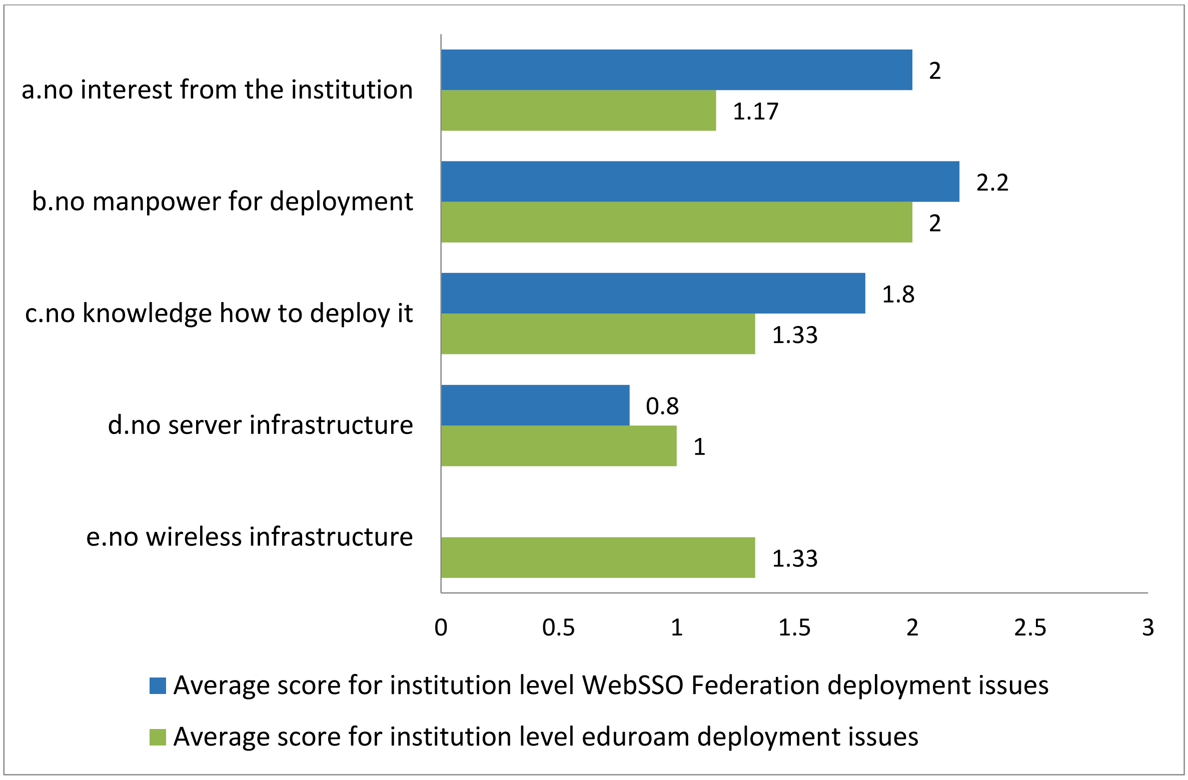


Figure 2.7: Average scores for problems institutions have or potentially would have in adopting the eduroam and WebSSO federation

Analysing WebSSO and eduroam federation issues together, we can conclude the following:

- NRENs in general think that their institutions don't have a strong interest in deploying a WebSSO Federation. The figures are more in favour for eduroam Federation (based on **a**). Again, this can be explained by eduroam having a much clearer business case and set of benefits for institutions. Another reason could be that the people interviewed mostly work with the network, so eduroam is more familiar to them;
- NRENs perceive that institutions have a lack of manpower for deployment of both federation technologies (based on **b**);
- Institutions do not possess the necessary knowledge to adopt federation technologies, where the figures are slightly in favour of eduroam (based on **c**);
- Infrastructure needed for the deployment of these services is lacking for both federation technologies (based on **d**);
- In the case of eduroam, institutions are struggling to provide wireless infrastructure (based on **e**).

2.3 Large Projects: Market Analysis

Large Projects are another very specific FaaS target group. In contrast to other target groups, Large Projects mainly have a number of web SPs which are, to complicate things, deployed internationally. They may have an IdP instance which is used as a guest IdP (a “home for the homeless”) and an Attribute Authority to store additional attributes for users who are using identities from their federation.

As before, we relied on the SA5 T5 Enabling Users task as our interface towards Large Projects use cases [UseCases]. The Enabling Users task requested that research communities submit federated identity management use-cases in May 2013. In total, 11 projects submitted their use cases. The Enabling Users participants then reviewed the submitted use-cases in order to identify two or three with which they will work together more closely. The use-cases were examined in order to identify those that promise the best results regarding: reproducibility, complexity, time frame, existing SAML-usage/SAML-know-how and other aspects. Task 5 decided to initially work closely together with the following communities on their eduGAIN-related use-cases:

- DARIAH, www.dariah.eu
- ELIXIR, www.elixir-europe.org
- CRISP/PaNdata (Umbrella), www.pan-data.eu

Another resource that we used for the Large Projects market analysis is ‘Federated Identity Management (FIM) for Research Collaborations’ paper [FIMpaper], which describes the needs of the research communities and the status of their activities in the Federated Identity Management domain. This paper was written by various e-Research projects and infrastructures driven by the interest in using federation technologies. In response to this paper, REFEDS and eduGAIN groups prepared the ‘Addressing e-Research Requirements’ [FIMresponse] which analyses requirements and issues identified in the FIM paper with the purpose to define a roadmap to address them.

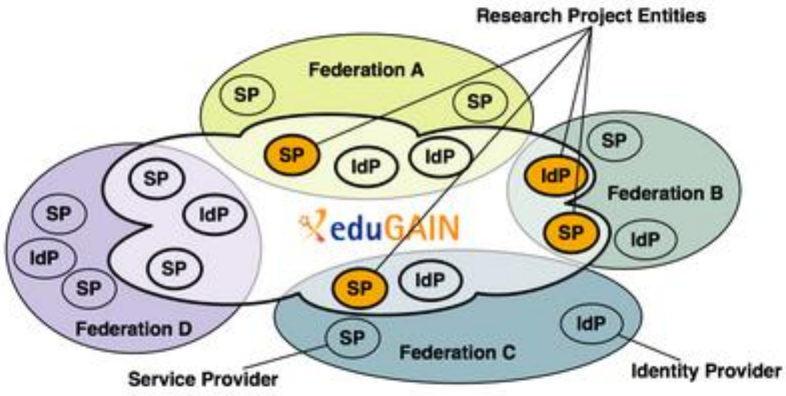
From the resources outlined above, one can draw a conclusion that Large Projects are facing many challenges in order to make use of R&E Federations which are providing the WebSSO services for most of their user base. Some of these challenges are:

- **IdPs not always release attributes:** it is well known that SPs in R&E Federations are reporting the same problem, but Large Projects are dealing with one more fact that makes this more difficult to resolve: IdPs have a presence in different countries. Large Projects are facing IdPs from different federations which are regulated by different policies and country regulations regarding personal data protection. In addition, IdPs have to decide if and how to release the user attributes across national border. It is anticipated that Code of Conduct document [DataProtection] developed by eduGAIN and REFEDS will have positive influence to this problem;
- **IdPs for guest users:** there are certain groups of users who nowadays cannot be easily supported by Federations, e.g. users whose home organisation has not joined a Federation, users who are affiliated with multiple institutions or persons who move from one institution to

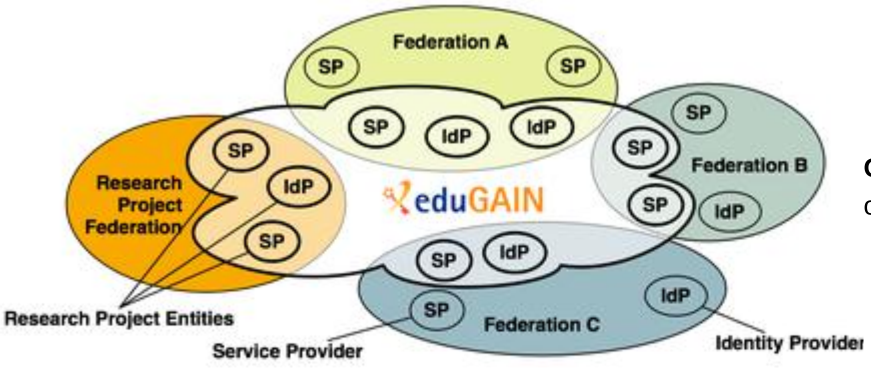
another (so called “nomadic users”). Some Large Projects are resolving this issue by catering themselves guest IdPs;

- **Attribute authorities that handle attributes for specific communities:** Federated IdPs cannot take the role of managing service-specific user attributes. This task naturally falls on the community which is providing the service: most Large Projects have a need for Attribute Authority specific for their services;
- **Deployment of large numbers of SAML SPs:** Each implementation of a service needs to be protected by SAML SP and the registration procedures differ from country-to-country. Therefore, projects with many services are confronted with different procedures to register the SPs with a federation and with eduGAIN.

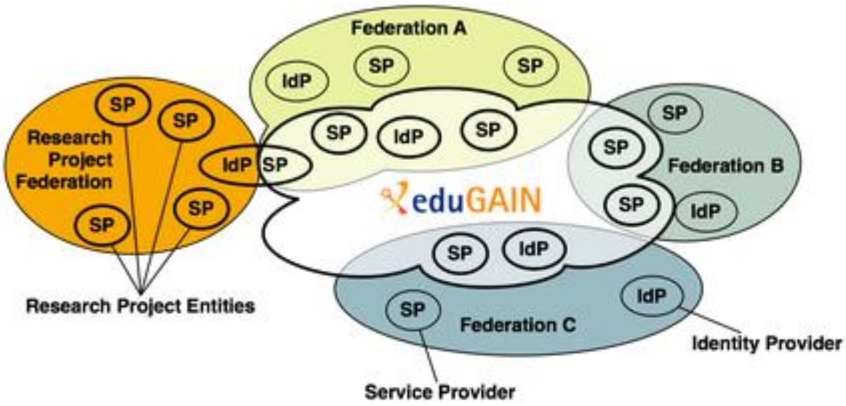
SA5 T5 recognised several options that Large Projects can choose from in order to integrate to eduGAIN as shown in Figure 2.8.



Option A: All SPs of a research project join eduGAIN via existing federations



Option B: Research project operates own federation and joins eduGAIN



Option C: Research project operates a single SP (as hub) which joins eduGAIN via an existing federation

C.1 Using (SAML) IdP Proxy/Hub
C.2 Using (Web) Proxy

Figure 2.8: Approaches for Large Projects to eduGAIN integration

There are advantages and disadvantages for Large Projects in each of these options recognised by Task 5. Projects they are working with are presented in the document Options for Joining eduGAIN [JoiningOptions]. FaaS could offer Large Project services that would ease the adoption of eduGAIN: these possibilities are discussed in Section 3.3.

3 Opportunities to address the needs of the FaaS Target Groups

Based on a Market Analysis for FaaS target groups which was presented in the previous Section, general approaches on how to assist them in using federation technologies can be deduced. In this Section, all opportunities will be analysed. Although not all of them can be realised under GN3plus framework or timeframe, this summary can be helpful for other GN3plus tasks or can serve as planning for GN4. For this iteration of FaaS services development, we are focusing on the WebSSO federation services because eduroam is implemented in nearly all GN3plus partner NRENs and there is larger need for support to WebSSO federations.

3.1 Opportunities to address NRENs needs

3.1.1 Addressing the lack of manpower issues by lowering barrier of technology implementation

Helping NRENs in deploying the technical components needed for Federation would cut the manpower needed for building and operating a Federation. In this way, the lack in manpower, which is one of the most evident issues NRENs are having, would be addressed. Results presented in Figure 2.1 show that:

- One NREN chose and is operating a Hub&Spoke central login federation. As this NREN is already operating a central Login service, there is no business case for FaaS services.
- Three NRENs chose a full mesh federation architecture. This federation architecture leaves the responsibility of maintaining authentication servers to institutions, while the federation operator is designated for metadata management and optionally a central discovery service. FaaS could ease the burden of NRENs operating those central services.
- Two NRENs have not yet decided which architecture to choose. These NRENs probably do not have the technical skills and/or manpower to build a federation and would benefit the most from an easy-fix solution.

Before analysing possible ways of supporting NRENs, it is important to make clear which federation matters remain the responsibility of NRENs and cannot be supported by FaaS. NRENs would be offered FaaS services which are easing the technological barriers, but they would still be responsible for all other federation matters which include:

- Management of a federation policy.
- Dealing with new IdPs and SPs joining the federation (auditing, approving, registering etc.).
- Support and communications with their IdPs and SPs.

Based on the analysis outlined above, there are several ways to support NRENs; these are described below.

- For NRENs that decided to start a Full Mesh Federation, FaaS could offer a **central Resource Registry tool**. At this point of time, these NRENs are serving a small number of institutions so metadata can be managed manually, but having a web-based tool to manage information about SP and IdP entities that participate in the federation is the right way to properly manage a production Federation. This Resource Registry tool can have features like:
    - Self-service registration of SP and IdP participating in the federation.
    - SP can express which attribute it requires and/or desires.
    - SP can declare which IdPs it accepts.
    - IdP can declare which attributes it is releasing.
    - Generation and maintaining of federation metadata.
    - Signing of federation metadata.
    - Generation of attribute release polies for Shibboleth IdPs.
    - Generation of information about federation.
- For NRENs that decided for Full Mesh federation, FaaS could offer a **central Discovery Service** which could be used by SPs for a faster bootstrap on federating their services. Central Discovery Service feeds from the federation metadata and a SP only has to point to it. The Discovery Service can also be implemented in such a way that it is possible to embed it on the SP page, avoiding redirection and thereby offering a more consistent and transparent look-and-feel for the user.
- For NRENs that have not chosen an architecture for a federation and need an easy-fix solution, FaaS could **offer a Hub&Spoke federation**. In the case that an NREN would still prefer a Full Mesh architecture, they could revert to services FaaS is offering for such federations described previously. The drawback of the Hub&Spoke architecture is the introduction of a central point of failure. There are two types of Hub&Spoke architectures: with distributed and with centralised login. Using Hub&Spoke with distributed login architecture introduces a central point of failure, while institutions still have to operate Identity Provider. Where NRENs institutions operate their own Identity Provider, it is expected that they would rather choose Full Mesh federation.

If FaaS offered Hub&Spoke federation with centralised login**,** NRENs institutions would not have to deploy a new authentication infrastructure and in this way they could quickly and easily join the federation. Centralised login could authenticate users directly against the institution's Identity management system. Another possibility would be to use Radius backend authentication that would authenticate against a Radius server which institutions already use for eduroam. However, there are the following serious concerns about a Hub&Spoke federation with centralised login:

- Protection of personal data; when logging in. Users are entering their home institution's credentials in centralised login operated by GÉANT and probably hosted out of their country. Because of the need for personal data protection, we can anticipate that NRENs could have issues with accepting such solution.

- Compatibility with Identity management system. It is difficult to foresee all types of Identity management systems that institutions could have in place. There is the risk that a solution offered by FaaS could either be very generic (and therefore difficult to maintain), or too constrained (so that not all institutions can be supported).
- Compatibility among Radius servers. Properly implemented, the Radius protocol is capable for performing both authentication and transfer of user attributes. However, the Task does not have expertise with all Radius server platforms and there is uncertainty about their support for the transfer of user attributes.

3.1.2 Addressing the lack of SPs issue

As shown in the Market Analysis, the most significant issue hindering deployment of Federation is lack of SPs with AAI requirements that would drive the deployment and acceptance of Federation. NRENs expect to get highly professional SPs from eduGAIN, but there is no such list of SPs available through eduGAIN and it is uncertain if eduGAIN can soon meet these NRENs expectations. There are several ways in which FaaS could help NRENs in dealing with finding SPs.

- Help NRENs to understanding which SPs would promote the adoption of Federation. Each federation has a group of SPs which were driving the adoption of Federation by institutions and users. In general, it is unlikely to have one “killer” SP which is serving all users. It would be useful to gather the **list of top SPs from existing federations** so NRENs could shortlist SPs that could serve their Federation.
- As stated in the market analysis, NRENs have very few existing services that have demand for WebSSO inter-institutional access and they often don’t know if their institutions have such services either. Running a new service on their own or purchasing a service just to boost the federation is not a realistic option either. On the other hand NRENs could easily make use of free cloud services such as Google aps for education and Microsoft 365. But, there are classic questions like: privacy of user data -- Where is the user data stored (is it in EU or non-EU territory)? What is the sustainability of that free service (what if they start charging)? -- and so on. The services the FaaS could offer is to **suggest a pool of SPs** which NRENs could use as drivers for building the federation. The FaaS task does not have the resources to run or broker SPs, but conveniently another GN3plus task can help here.

The SA7 T3 Cloud Brokerage and Vendor Management Task aims at providing NRENs with a well-balanced portfolio of cloud services. The goal of this task is to acquire and manage the delivery of services from providers to the pan-European GÉANT community. These parties can be commercial vendors as well as NRENs and other research and education communities. The Task strives for an attractive, well-balanced portfolio of cloud services. This task gathers the NRENs' national brokerage activities into a focused effort towards service providers, to secure agreements on behalf of the GÉANT community: to negotiate and secure the best possible terms and to assist NRENs and their customers to obtain access to these services.

SA7 T3 is focusing their work into four groups of cloud services which are depicted in work packages[4] :

- **Collaboration suites**. Focuses on the collaboration suites offered by Google and Microsoft: Google Apps and Microsoft Office 365 which are the starting points for introducing cloud services for most NRENs. To prevent a situation where each NREN has to negotiate a deal and maintain this agreement on their own, SA7 will try to put in place a central framework agreement (utilising the size of the total NREN community and the work already done and in place at several NRENs) for both Google Apps as well as Microsoft Office 365. NRENs can use this framework agreement (template) to sign the actual contract with either Google or Microsoft at a national level.
- **File storage and synchronisation services**. File storage and synchronisation services offered to Universities and/or individual users (Box-like, remote backup, remote storage, etc.) are probably the most attractive cloud services for users and thus for NRENs. A catalogue of offered services (from commercial vendors and/or other NRENs acting as service providers) will be made and the framework agreement (template) will be prepared for potential NREN users. Starting points include:
    - NORDUnet agreement with Box Inc. (scale up towards other NRENs).
    - File storage requirements list from SURFnet.
    - Interest in ownCloud from several NRENs (together with TERENA).

- **Realtime communication, web conferencing services**. Some of the NRENs are already using such services (Adobe Connect Pro, Cisco WebEx, BigBlueButton, etc.) but have difficulties to negotiating the best prices from the vendors. SA7 will contact vendors and try to negotiate a deal (utilising the size of the total NREN community) and produce a central framework agreement for web conferencing services that come from commercial vendors. Moreover, SA7 will explore the possibility that one (or more) NRENs establish a service based on Open Source (free, like BigBlueButton) software that could be used by other NRENs with substantial savings compared to commercial vendors.
- **Infrastructure as a Service**. Exploring the possibility of using a commercial solution, especially one from another NREN cloud infrastructure, or to expand an NREN's own private cloud solutions in a hybrid cloud model. When possible, the framework agreement toward infrastructure cloud providers will be offered to NRENs. The catalogue of all provided services and framework agreements will be produced and offered to NRENs for their consideration. Starting points include:
    - Microsoft Azure (several NRENs are already in contact with the vendor; there is a need to focus these efforts).
    - GRNET Okeaons.
    - GreenQloud (the deal between GreenQloud and SURFnet could be scaled up).

The SA7 T3 cloud service portfolio includes a range of services which would have a large user base and could serve as a booster for the NRENs federation. Enabling easy access to those services for NRENs would solve their issues with searching for SPs. SA7 T4 is facilitating technical integration and

[4] The description of these work packages is taken from the GÉANT Intranet planning of SA7 T3

implementation work in order to connect these services to the IT infrastructure of the NREN community, the networks and AAI middleware.

3.1.3 Addressing the lack of knowledge issues

Data presented in Figure 2.2 show that NRENs do not have knowledge issues about understanding and deploying technical infrastructure and with writing the policy document. However, when asked about support that FaaS can offer them, results in Table 2.2 show that NRENs were keen to gain more knowledge.

When the GN3plus project started, such a comprehensive knowledge base did not exist, but recently, eduGAIN Wiki pages (http://wiki.edugain.org) have been constructed with the aim of providing technical instructions and recommendations how to make use of eduGAIN. According to the available description of wiki purpose and the outline at the moment of writing of this document, the wiki will provide guidelines, pointers to external pages and configuration samples. The work of generating a policy framework for Federation policy had already started in the GN3 project.

Since a knowledge base is already being established, there is no need for FaaS to duplicate these efforts.

3.2 Opportunities to address the needs of Institutions

Based on the Market Analysis, Institutions, face two barriers: deployment of Identity Management Systems and deployment of authentication infrastructure. In both cases Institutions are lacking in knowledge and in manpower. These issues are addressed below.

3.2.1 Addressing the lack of knowledge issues for IdM

Providing guidelines and best practice documents for IdM deployment, procedures and maintenance would be a good approach to lowering the knowledge barrier. However, those guidelines could heavily depend on the local circumstances at the Institution and available technologies. Thus, there is a high risk that such guidelines are too generic or too specific to be of practical use.

3.2.2 Addressing the lack of manpower issue for IdM by lowering the barrier of technology implementation

The way to help Institutions to implement IdM would be to offer them a Virtual Machine “**solution in a box” that contains easy to set up IdM solution**. These VMs could be hosted at the institutional site. The other option would be for FaaS to offer to host these VMs in a cloud. However, given the fact that they would be used to store sensitive personal data, there is high probability that institutions would insist on retaining control of it, so there is a risk that this option would be unsuccessful. It should be remembered that there are no means to address the institution’s problem of lack of manpower to manage user identities, as this is a task they must handle internally.

3.2.3 Addressing the lack of knowledge issues for authentication infrastructure

Providing guidelines and best practice documents for authentication infrastructure deployment would be good approach to lowering the knowledge barrier. However, those guidelines could depend heavily on the technical requirements set up by the federation operator. Thus, there is a risk that such guidelines are too generic or too specific to be of practical use.

3.2.4 Addressing the lack of manpower issues for authentication infrastructure by lowering the barrier of technology implementation

Another way to help institutions in implementation of authentication infrastructure would be to offer them **a hosted IdP solution.** There is high probability that this service would be interesting for smaller institutions and institutions that don’t have enough IT staff to run AAI on their own. For example, this service is offered by GARR (the Italian NREN) on a national level and in CANARIE (the Canadian NREN). However, the following concerns question the feasibility of this solution in FaaS scenario (as with the Hub&Spoke solution described in Section 3.1):

- Protection of personal data. When logging in, users are entering their home institution’s credentials in the IdP operated by GÉANT and probably hosted from outside their country. Because of data protection of personal data, we can anticipate that Institutions could have issues with accepting such a solution and this relationship should be regulated with appropriate agreements;
- Compatibility with Identity management system. It is difficult to foresee all types of institutions Identity management systems in place. As consequence there is the risk that the solution FaaS offered could either be too generic and difficult to maintain, or so constrained that it would fail to gain institutional support.

3.3 Opportunities to address the needs of Large Projects

As stated in Market Analysis, SA5 T5, the Enabling Users Task, is closely collaborating with several Large Projects in order to address the challenges they are facing. This collaboration should be in general fruitful for Large Projects as one of the outputs will be to adopt and disseminate Federation current best-practice solutions.

SA5 T5 analysed possible ways for Large Projects to reveal their SPs and IdP through eduGAIN. Based on these models, we can consider if there is a business case for FaaS services.

- **Option A** – All SPs are joining eduGAIN via existing federations. This approach is the most straightforward option as it reuses existing infrastructures, guides and processes. SA5 T5 considered this the most reasonable option for most use-cases. In the case of adding services to an existing federation, there is no business case for FaaS services as the resources of existing federations are being reused.
- **Option B** – The research project operates its own federation and joins eduGAIN. From FaaS's point-of-view this is the same as NREN federation use case, where there is greater number of SPs and none or couple of IdPs. In this case, Large Projects could use some of the services FaaS is offering for NRENs.
- **Option C** – The research project operates a single SP as hub which joins eduGAIN via an existing federation. In this option, Large Projects deploy a central hub which needs to be customised for Large Project requirements. Because it is hard to make a generic hub that could easily be adapted to different Large Projects, there is no business case for FaaS services in this scenario.

4 Evaluation of possible services offered by FaaS Pilot Service

In the previous Section, all possible scenarios of supporting FaaS target group were analysed. For some of these scenarios it was recognised that they are already covered by other GN3plus tasks and activities and because it is not reasonable to duplicate work they are not considered further. In this Section the rest of the scenarios of services that FaaS could offer are analysed with respect to the feasibility of their implementation in the FaaS Pilot Service. In particular, it is important to consider the:

- Achievability of the chosen solution given that the timeframe for implementation and to starting the Pilot service is five months, until 1. April 2014.
- Increase the benefits of the chosen solution while minimising the risk that the solution is not of much use to many customers.
- Sustainability of the chosen solution given that several interviewees stated that it might be difficult to pay for FaaS. In particular this means that the chosen solution must have low maintenance costs.

4.1 FaaS services to support NRENs

There are several options that FaaS can offer to support NRENs that are not already in the field of work of other GN3plus activities:

Options **1a** and **1b** for NRENs who want to build their own federation in the traditional way and which includes the Resource Registry and the Central Discovery services. This solution can be used by the Full Mesh federations but might be also interesting for the Hub&Spoke federations for managing the metadata for the interfederation business. There are several Resource Registry tools suitable for NREN needs. Choosing one of them and generalising it for use by different federation operators should be possible in the available time. There are also several Discovery Service tools available which would be candidates for implementation. This solution is also lowering the technical barrier for participating in the eduGAIN because it offers easier manipulation of interfederation metadata to the federation operator and supports opting-in federation entities to participate in eduGAIN. Easier access to eduGAIN means easier access to services that would otherwise have to be provided by a cooperative SP. At the start of building a federation it is likely that NRENs will focus on the technical implementation first and leave the writing of Policy documents for later. It is also reasonable that they want to do learn the technology and run a pilot of the federation before deciding if they want to invest into making federation their production service. This leads to a “chicken and egg” problem because without a formalised Policy, the federation cannot join eduGAIN. The solution is for the NREN federation to trial eduGAIN test metadata which offers links to several SPs.

- Option **1c** provides a quick start of the federation where NRENs institutions do not need to learn and deploy a new authentication infrastructure in order to run an IdP. Again, it is stressed that there is high risk that Institutions might reject this solution because of personal data protection issues. NRENs would need to have trust in FaaS for correctly managing this issue, and Institutions would need to have trust in NRENs. Of course, suitable agreements would need to be in place to legally regulate this “trust”. Without further investigation of the Institutions associated with particular NRENs it is not possible to predict their opinion.

- Option **2a** allows NRENs to learn which SPs would be candidates for the federation. The list of favoured SPs could be constructed by FaaS in collaboration with REFEDS by inviting federation operators to share their experiences of SPs.

In the timeframe of five months, FaaS can implement only one of the first three options (**1a**, **1b** or **1c**) outlined above. Because of risk that the option 1c would not be approved it was decided to implement the first option. Option **2a** is easy to accomplish in the time, so it was decided to proceed with this also.

4.2 FaaS services to support Institutions

Based on the analysis presented in Section 3.2 one of the ways to support institutions would be to provide them with the knowledge base. However, these instructions might be considered either too generic or too specific to be of practical or immediate use, so the Task decided not to pursue for this for FaaS.

The second possibility is to offer a hosted IdP service, which would allow institutions to be offered hosted AAI. Reservations to this approach are described in Section 3.2 and address the same trust issues as with running Hub&Spoke federations discussed in Section 3. In addition, there are the following concerns:

- It is difficult to predict the manpower resource needed to maintain this solution because of the uncertainty over the exact number of institutions and how many of them would subscribe.
- The institutions would probably need a guarantee of sustainability before subscribing.
- Without NREN providing a federation, institutions cannot federate their IdP.

In the GN3plus timeframe, it is difficult for FaaS to develop and provide both services for NRENs described in the previous Section and the hosted IdP solution. Because of the concerns outlined above, the Task decided that FaaS should begin by supporting NRENs and defer supporting institutions through the hosting of IdP as a proposal for the further development of FaaS services.

4.3 FaaS services to support Large Projects

The analysis in Section 3.3 shows that SA5 T7 (Enabling Users) is driving the support for the AAI needs of Large Projects. In the case that a Large Project decides to run a federation on their own, then FaaS services for NRENs running a federation would be appropriate.

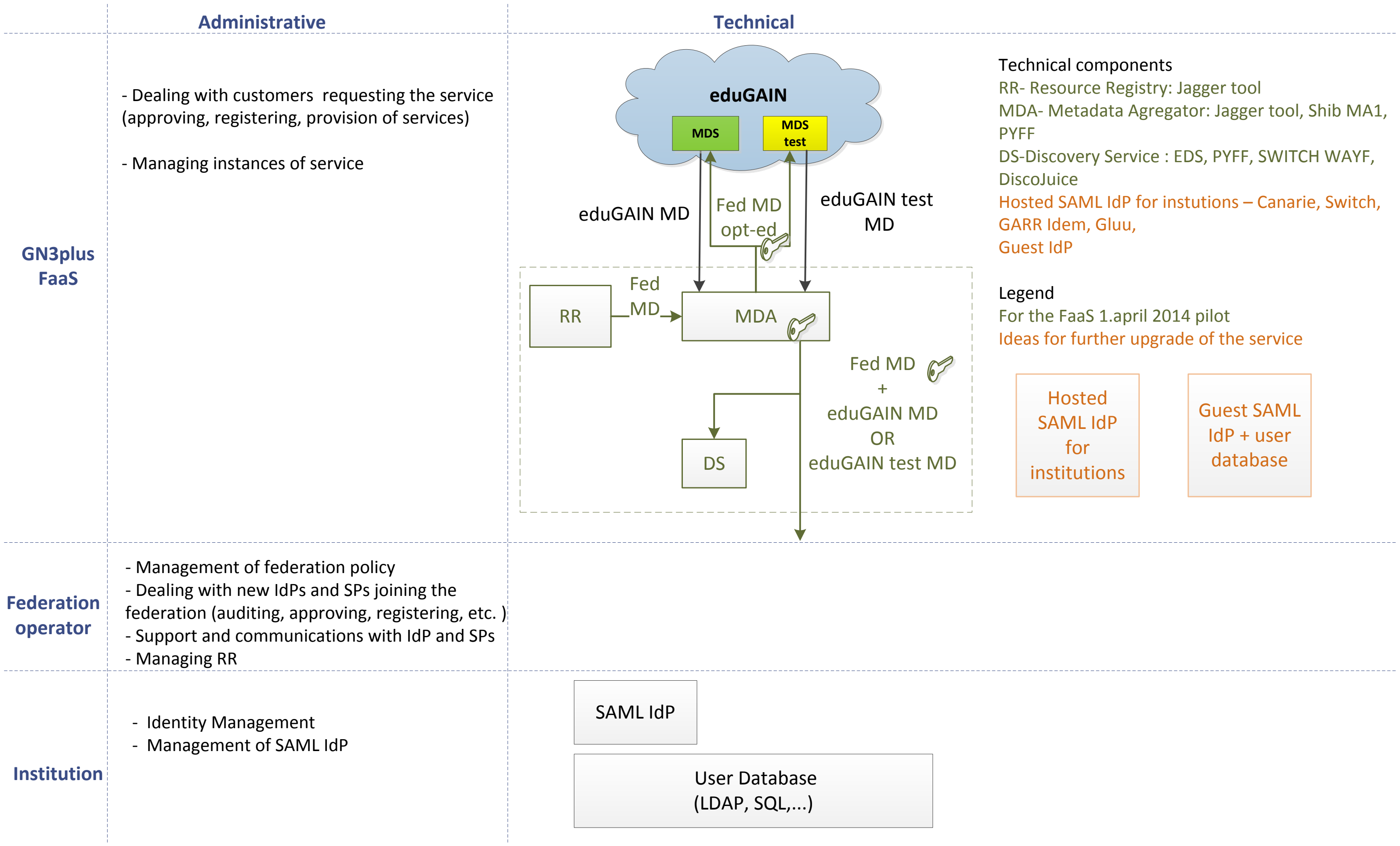
5 FaaS Pilot Service definition

FaaS Pilot will provide Resource Registry and Discovery Service to Federation operators.

The FaaS Pilot architecture is shown in Figure 5.1 and shows the administrative and technical responsibilities of GN3plus FaaS, the Federation operator and the Institution. Note the range of responsibilities that are staying in the hands of Federation operators and Institutions.

The figure contains the technical elements for the FaaS Pilot service which are due to be implemented by 1. April 2014 (outlined in green). Arrows show metadata flows and the signing of metadata in respect of eduGAIN and the federation. The Metadata Aggregator is presented separately as it can be implemented as a part of the Resource Registry or as an individual tool. For the technical components of the FaaS solution, there are several tools available and they are also listed in the figure. The next task of FaaS is to evaluate each of them and choose the ones which are the best fit for the FaaS service.

Figure 5.1 also contains technical components (outlined in red) that are suggestions for a future development of FaaS. As suggested in Section 4.2, hosting IdP would be the way to encourage more institutions to participate in the federation. Hosting of the Guest IdP could be a precursor to offering an IdP-hosted solution for a large number of institutions. Guest IdP would be operated by the federation operator and provide an AAI account for users whose institutions do not operate an IdP.



- Dealing with customers requesting the service (approving, registering, provision of services)

- Managing instances of service

Technical components
RR- Resource Registry: Jagger tool
MDA- Metadata Agregator: Jagger tool, Shib MA1, PYFF
DS-Discovery Service : EDS, PYFF, SWITCH WAYF, DiscoJuice
Hosted SAML IdP for instutions – Canarie, Switch, GARR Idem, Gluu,
Guest IdP

Legend
For the FaaS 1.april 2014 pilot
Ideas for further upgrade of the service

- Management of federation policy
- Dealing with new IdPs and SPs joining the federation (auditing, approving, registering, etc.)
- Support and communications with IdP and SPs
- Managing RR

- Identity Management
- Management of SAML IdP

Figure 5.1: FaaS Pilot Service Architecture

Appendix A Market Analysis Statistics

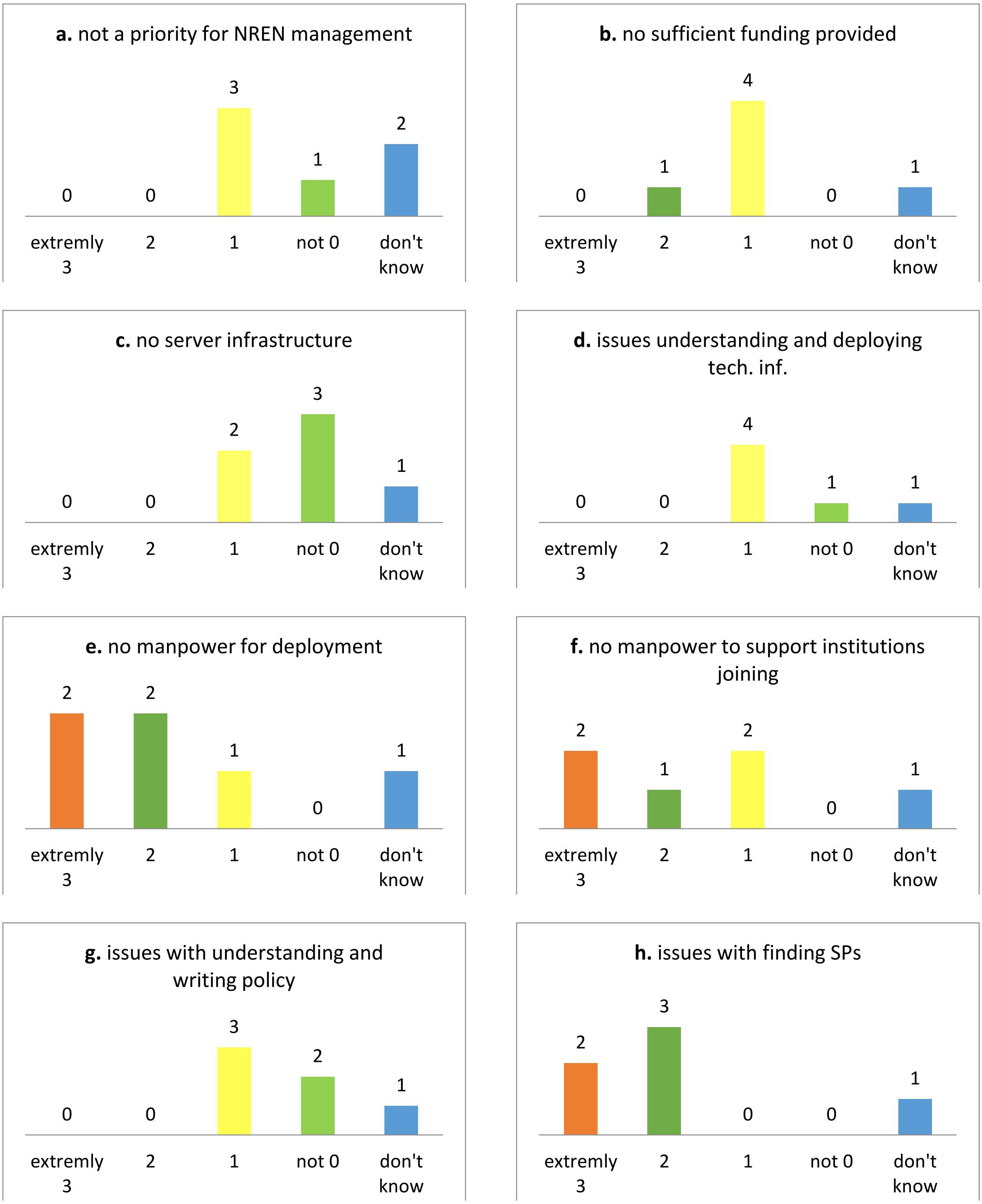


Figure A.1: Relevance of problems NRENs have with deploying WebSSO Federation

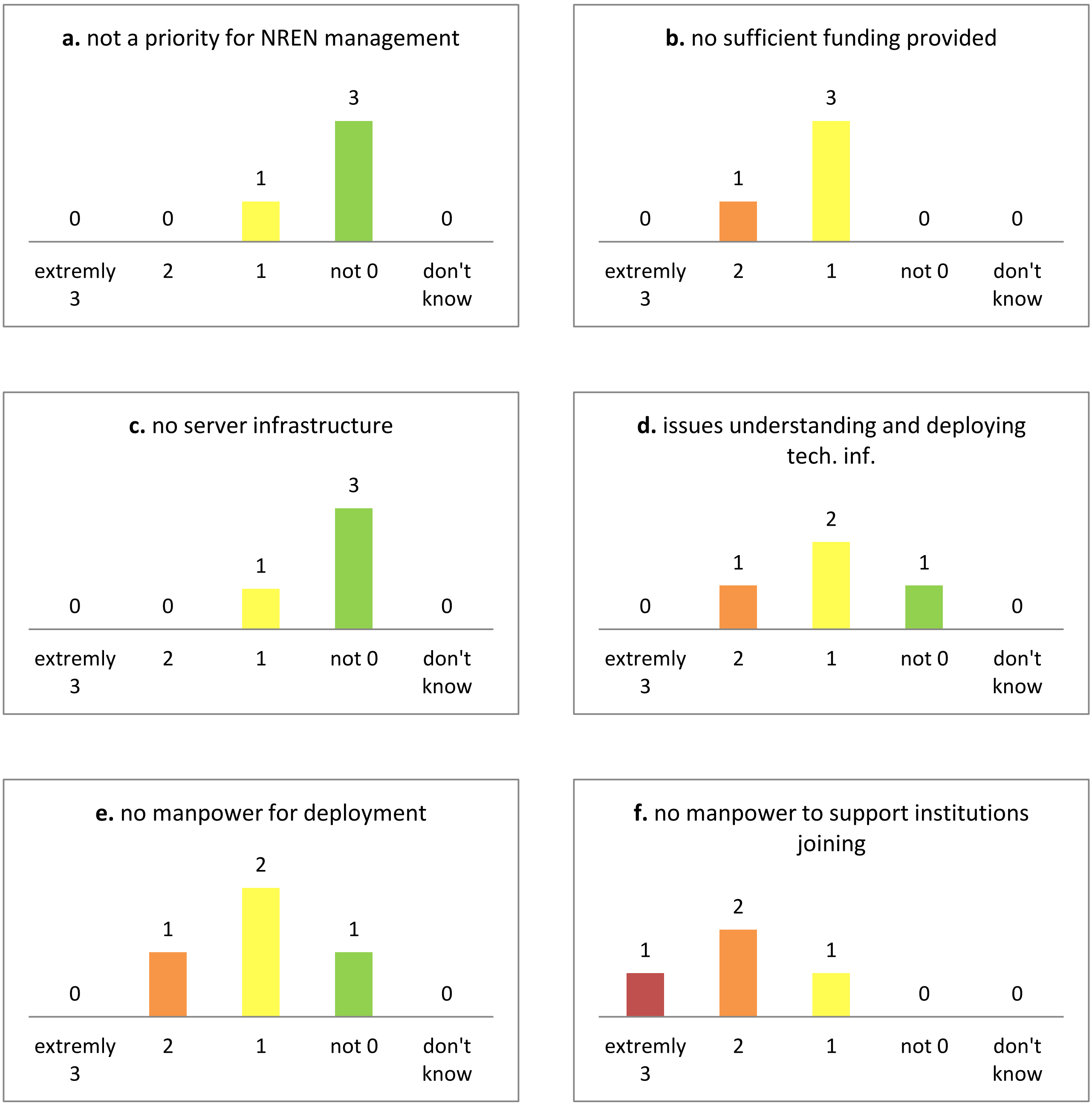


Figure A.2: Relevance of problems NRENs have deploying eduroam

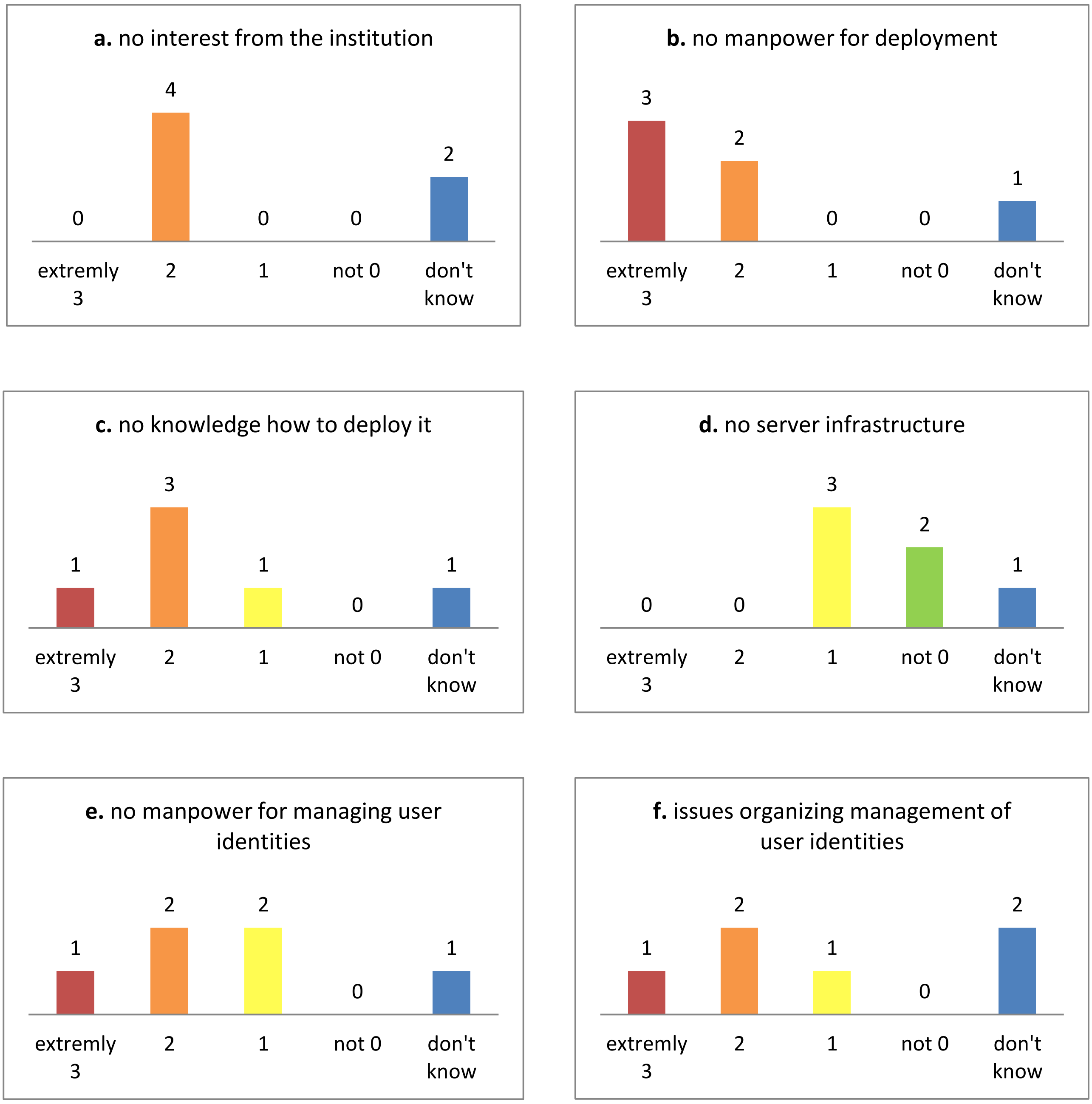


Figure A.3: Relevance of problems institutions have deploying Identity management system and maintaining user identities

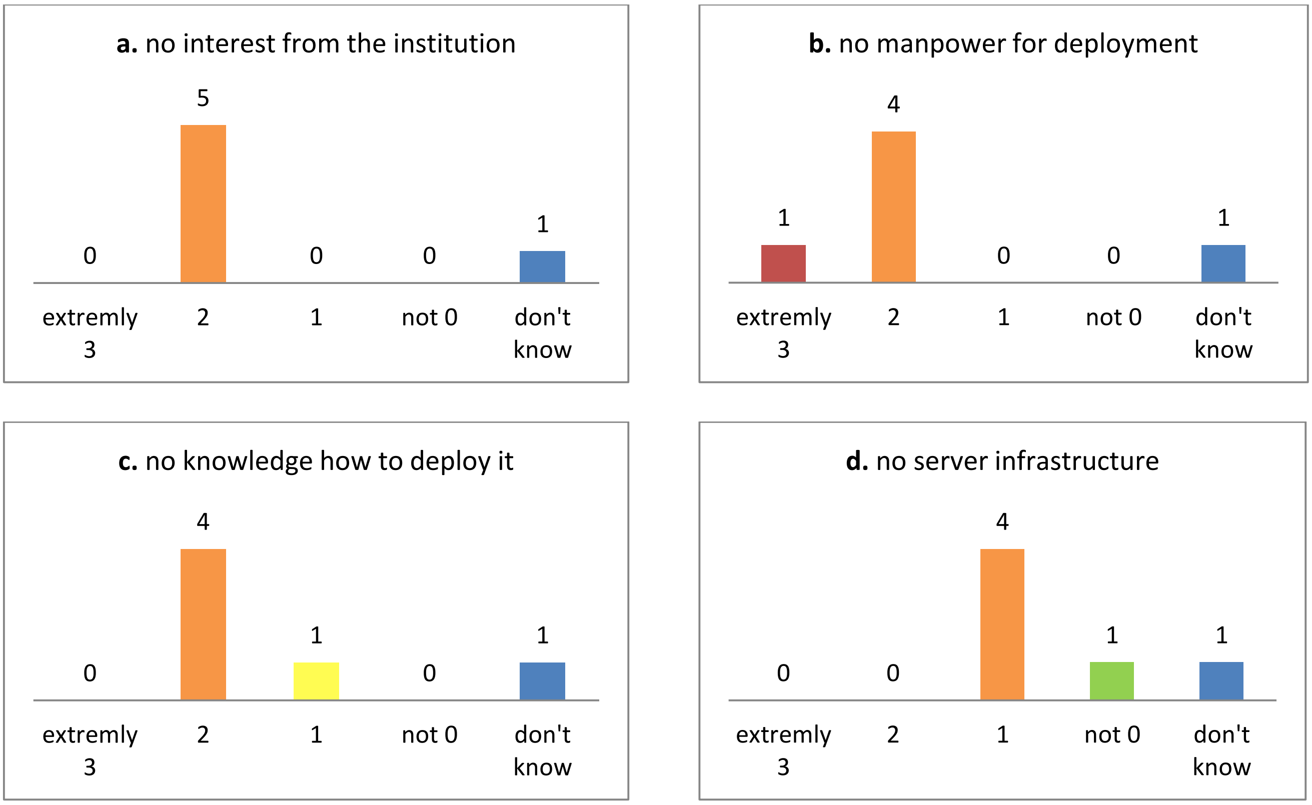


Figure A.4: Relevance of problems institutions have or potentially would have in adopting the WebSSO federation

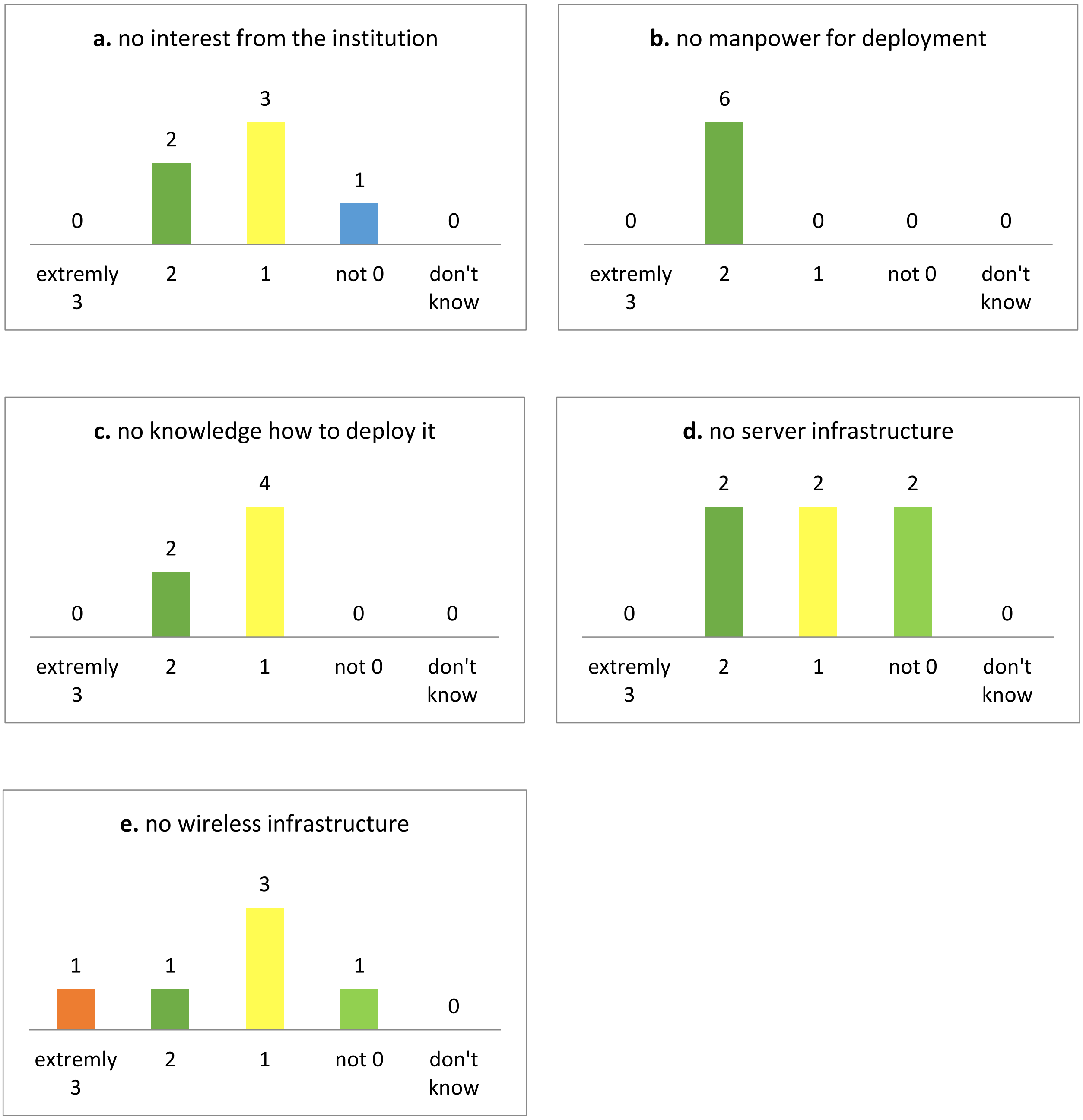


Figure A.5: Relevance of problems institutions have or potentially would have on adopting the eduroam federation

References

[Compendium] TERENA 2012 compendium
http://www.terena.org/activities/compendium/2012/pdf/TER-C12-final-web.pdf

[DataProtection] Data Protection Code of Conduct
https://refeds.terena.org/index.php/Data_protection_coc

[eduGAINjoining] Options for Joining eduGAIN. GN3plus Document Code: GN3PLUS13-642-16

[FIMpaper] FIM Paper
https://cdsweb.cern.ch/record/1442597

[FIMresponse] REFEDS and eduGAIN groups response to the FIM paper.
https://refeds.terena.org/images/4/4d/AnalysisFIM4RDocument1-0.pdf

[UseCases] Enabling Users use-cases
https://intranet.geant.net/SA5 T5/SitePages/AAIforUserCommunities.asp

Glossary

AAI	Authentication and Authorisation Infrastructure
eduGAIN	The eduGAIN service allows Authentication and Authorisation Infrastructures to interact, enabling the sharing of data between federations and providing an interconnection framework to applications willing to provide their services, content or resources to multiple federations.
eduroam	An international roaming service for users in research and higher education
EIFL	Electronic Information for Libraries, see www.eifl.net
EuroCAMP	European Campus Architecture Middleware Planning, see http://www.terena.org/activities/eurocamp/
FaaS	Federation-as-a-Service.
Federation	Identity federation. An association of organisations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions.
IdM	Identity Management systems.
IdP	Identity Provider. A server acting in an Identity Provider role as defined in SAML 2.0 specifications, cf. [SAMLOverview] SAML Security Assertion Markup Language, http://www.oasis-open.org/committees/security
Moonshot	A Janet (UK NREN) project with the aim of streamlining access services and simplify authentication across distributed computing grids.
NREN	National Research and Education Network.
REFEDS	Research and Education Federations, Europe, a Trust Federation, see https://refeds.org
SAML	Security Assertion Markup Language, see https://refeds.org/europe_map.html
SP	Service Provider. Service Provider. A server acting in a Service Provider role as defined in SAML 2.0 specifications, cf. [SAMLOverview].
VPN	Virtual Private Network.
WebSSO	Web Single Sign-On.