Addressing e-Research Requirements

Date: 6 March 2012

Authors: Licia Florio (TERENA), Nicole Harris (JISC Advance), Christoph Witzig (SWITCH), Mikael Linden (CSC), Ajay Daryanani (RedIRIS), Ann Harding (SWITCH), Lukas Haemmerle (SWITCH).

Version: 0.7

Status: DRAFT

Abstract

Various e-Research projects and infrastructures driven by the interest in using Federated Identity Management (FIM) technologies, produced in 2012 a paper called 'Federated Identity Management (FIM) for Research Collaborations' [1]. The paper, hereafter referred to as FIM paper, provides requirements for the usage of federated access from various e-Research communities, identifies issues towards the wider adoptions of FIM technologies and identifies some pilot studies. These pilot studies are meant to explore the requirements on federated identity management services in more detail and will report on the results. However more pilots should be identified as a joint effort between the Identity Federation community (i.e., national identity federations, eduGAIN [2] and REFEDS [3]) and the e-Research communities.

This document has been prepared by REFEDS and eduGAIN groups in response to the FIM paper. The aim of this document is to analyse the requirements and the issues identified in the FIM paper with the purpose to define a roadmap to address them. This document also wishes to shade some lights on some aspects of Federated Identity Management that may have led to misunderstandings.

It is evident that to progress the work in this area funding is needed; although this paper does not intend to address the funding issue, suggestions with regards to the funding will be provided where possible.

For the work to be successful it is essential that both Identity Federations/eduGAIN and e-Research communities engage in a joint collaboration from which both parties can gain mutual benefits.

1. Introduction

In 2011 representatives of different e-Research projects, driven by the need to support dynamic and cross-boundary user collaboration, started to discuss federated identity management. Part of the discussion was meant to evaluate whether federated identity management could be a viable solution for their users.

These discussion culminated into a the FIM paper that describes the requirements from the various groups, presents some specific use-cases and highlights challenges to the widespread uptake of federated Identity management technologies in the e-Research community.

The FIM paper presents a set of requirements from the e-Research community in relation to Federated Identity Management. Although issues have been identified, the paper also stresses a general interest in using Federated Identity Management to support e-Research projects and infrastructures.

This offers an opportunity and a challenge for identity federation (IDF) operators, represented by REFEDS, as well as for eduGAIN to work together with the e-Research community to enable access to cross-boundary services.

Support for cross-boundary services (also known as inter-federation) will inevitably require some enhancement and changes to the current identity federations, will involve policies and trust frameworks to be adjusted to fit community requirements and legal aspects.

2. Approach

This paper tries, on behalf of REFEDS and eduGAIN groups, to address three main aspects:

1. Identify requirements and challenges highlighted in the FIM document and begin to provide an answer to them (see section 4). Whilst the eduGAIN team will focus on specifying and implementing pilots mostly based on existing solutions, REFEDS with the support of the Identity and Trust Research Activity that will be part of GN3plus and the FIM group can look at different horizons.
2. Describe the challenges identified in the FIM paper and address them (see section 5);
3. Identity use-cases together with the e-Research communities: these should be prioritiesed as short- or long term efforts to help with resource allocation and planning.

It is important to note that these document does not offer answers or solutions to all problems identified in the FIM4R paper, but it is just a first step to that goal. It is expected that the FIM4R community to engage and help propose alternative solutions to complete the picture.

3. Stakeholders

The work proposed in this document involves multiple stakeholders, each of which can, and must play an important role in order for the challenges identified by the FIM paper to be addressed.

REFEDS has evolved into a global community which reaches out not only to identity federations in Europe, US and Asia-Pacific but also to some big research collaborations. It would therefore be desirable to use REFEDS as the vehicle to build the community, to report on the progresses and to receive feedback. REFEDS could particularly help with policies, attribute harmonisation and the use of level of assurance.

The GÉANT project [4] gathers most of the NRENs in Europe. Although the core mission of GÉANT is the network provisioning, GÉANT also runs service like eduGAIN, the infrastructure to enable trustworthy exchange of information for authentication and authorisation purposes among the GÉANT partners and other cooperating parties.

To ensure that funding and commitment is available via GÉANT (and its follow-on project called GN3plus) during the 2013-2015[1] period, plans have been made for eduGAIN to engage more dynamically and more proactively with e-Research projects on pilots,.

Various e-Research projects and infrastructures, such as CLARIN [5], ELIXIR [6] and others have already the necessary organisational support to engage with eduGAIN and REFEDS to work towards the same goals.

Lastly but definitely not the least the FIM community and those involved in the preparation of the FIM paper are one of, if not *the* main stakeholder. As many of the groups and communities that are represented by the FIM paper are not actively involved, neither in REFEDS nor in GÉANT, REFEDS and eduGAIN should ensure that liaisons are established among these three groups.

4. Priority List of Functional Requirements

The list below which has been discussed with some of the authors of the FIM4R paper shows the prioritised functional requirements to indicate the relative urgency by which these requirements are needed.

- **User friendliness (high).** The attitude of end-users towards FIM tools has changed. Single-Sign On is assumed to be the basis of interaction with the suite of digital services. The tools that support the FIM framework should be simple and intuitive and integrate with the many other IT tools used in daily life. Ease of use will be particularly important since many researchers only access the ICT systems concerned infrequently or on a part-time basis. Support for citizen scientists and researchers without formal association to research laboratories or universities is essential.

  See chap 4.5 for proposals on how to address this specific point. As a general note a way forward could be to associate low-assurance identities for citizen scientists and higher-assurance identities for university researchers.

- **Browser & non-browser federated access (high).** The wide-range of applications in use in the various communities includes many which do not have a simple web-browser front-end. Non-browser based interfaces are essential to support machine-machine interactions in secured workflows.

[1] This work will be carried out as part of GN3plus project, the follow up of the current GN3 project.

There is an important aspect both for e-Researchers and for Identity Federations.
See chapter 5.1 for a more in depth analysis.

- **Multiple technologies with translators including dynamic issue of credentials (medium).** No single technology can meet the need of all communities. Translators between one type and another will be required to allow credentials from one community to be used on other services and this translation will often need to be dynamic.

  Some work in this space has already been done, i.e. SWITCH SLCS, TERENA TCS, GEMBus STS etc.
  It would be worth collecting all the effort to understand their strengths and weaknesses and to describe the use-cases these systems address.

- **Implementations based on open standards and sustainable with compatible licenses (high).** These are essential for interoperability and sustainability.

  All identity federations infrastructures are built on standard technologies. This remains one of the cornerstone of the RE community.

- **Different Levels of Assurance with provenance (high)**. A single Level of Assurance in the quality of authentication cannot meet the need of all communities. Credentials issued under different levels will need to include the provenance of the level under which it was issued.

  There is a need for both identity federations and e-Research communities to develop and deploy a common LoA profile. See chap 5.5 for more about this point. This is however a very difficult area and although it is considered a high priority, it is a long term problem.

- **Authorisation under community and/or facility control (high)**. The assignment of attributes to individual users within a given community for use in authorisation decisions needs to be managed by that community. Externally managed federated IdPs cannot fulfill this role.

  See more in chap 5.4.

- **Attributes must be able to cross national borders(high).** Many of the research use cases require user attributes (in many cases including the need to release personal information to identify users) from an IdP in one country to be used by an SP in another country. Data protection considerations must allow this to happen.

  The GEANT Code of Conduct is addressing precisely this point. See chap 5.2 for more discussion.

- **Bridging communities (medium).** FIM is important and will be even more important in many research fields, commercial sections and social groupings. Therefore, bridging between the various communities is a central issue with an efficient mapping of the respective attributes. Here, again user friendliness

is an issue with the goal of maximum transparency and with requiring minimum actions by the users of these systems.

See chapter 5.4 and 5.6 for discussion on the attribute space.

- **Well defined semantically harmonised attributes(medium)**. For interoperable authorisation across many service providers it is necessary for the names and possible values of attributes to be well understood and standardised. This may be very difficult to achieve between different research communities but convergence is important.
  This point overlaps with the two previous one, but it is listed here for completeness.
  See chapter 5.4 and 5.6 for discussion on the attribute space.

- **Flexible and scalable IdP attribute release policy(medium)**. Different communities and indeed SPs within a community are likely to require a different set of attributes from the IdPs. The IdP policy related to the release of user attributes and the negotiation mechanism needs to be able to provide this flexibility. Bi-lateral negotiations between all SPs and all IdPs is not a scalable solution.
  This aspect also related to the way attributes will need to be aggregated from different sources of authority including federated IdPs and community-based attribute authorities.

5. Proposals to Address Requirements and Barriers to FIM Usage

This chapter discusses some of the challenges identified as preventing the wider adoption of FIM technologies. For some of them there is already consensus on how they can be addressed, for others a longer term approach is proposed.

A more extensive list of requirements is reported in Annex I.

5.1 Federated access for web and non-web applications

Even though Web browsers provide a de-facto interface to the majority of Internet services, many applications are either not web-based or are more effectively used through a native application. The need to extend federated access technologies beyond web is therefore an important problem.

The lack of widely deployed standards for federated identity for non-web applications has been a long standing issue. However things have improved somewhat and there are now a few technologies that look promising:

(i) Moonshot [7]

(ii) OAuth [8]

(iii) OpenID Connect [9] although this technology has not been sufficiently tested and it is not widely adopted yet.

(iv) SAML ECP (Enhanced Client or Proxy) Profile [10]

(v) Others (to be added)

A Moonshot pilot led by JANET is due to start by the end of 2013[2], whilst the SAML ECP Profile has been successfully used for some use-cases. However, there is not enough experience yet to understand which technology would work better for which use-case.

Proposal: It would be interesting to analyse in more details the technologies listed above and provide a summary about their strengths and challenges. Small pilots could also be identified.

Who: Part of this work could be carried out as part of the Joint Research Activity "Identity&Trust" in GN3plus. TF-EMC2 [11], FIM community and REFEDS could be used as vehicles to discuss the progresses and get feedback. The GN3plus Service Activity will report on the results on the Moonshot pilot and on which use-cases addressed.

Timeline: This is a mid term work. Some results could be available early 2014.

5.2 IdPs not always releasing attributes

Service Providers in the identity federations for higher education and research are reporting problems in receiving necessary users' attributes from their home organisations (IdPs).

This problem is due to different reasons, such as national data protection laws not being federation-friendly, the combination of bilateral ways to manage attributes difficulties and poor technical tools, the difficulty for technical people to deal with legal documents and the fear to compromise users' privacy, and/or SPs in some cases asking per-service specific attributes. In many cases IdPs may not have the effort or skills to configure the IdP to release ad-hoc attributes[3].

In many cases Identity Federations provide guidelines on which attributes should be released; however even then some IdPs prefer to take a conservative approach that leads to no attributes (or to very limited attributes) to be released.

The **Data protection Code of Conduct** (CoC)[4], developed together by eduGAIN and REFEDS, describes an approach to meet the requirements of the EU Data Protection Directive in federated identity management. The Data protection Code of Conduct defines behavioural rules for Service Providers which want to receive user attributes from the Identity Providers managed by the Home Organisations. It is expected that Home Organisations are more willing to release attributes to Service Providers who manifest conformance to the Data protection Code of Conduct.

The CoC can help, if adopted by all federations. However dissemination is needed to (i) train SPs to request only necessary attributes and (ii) to explain IdPs how to safely release attributes.

At the time of writing some pilots are on-going between some Identity Federations and some e-Research communities (i.e., CLARIN) to test the Code of Conduct. The results of these pilots will help shape any future work.

The usage of Research & Scholarship Entity Attributes or more in general of Entity Attributes recently discussed on the REFEDS list could also offer a way forward. The idea is to categorise services to simplify the configuration of identity providers; in this

---

[2] In addition to the JANET pilot, a similarly scoped pilot is planned as part of GN3plus.

[3] See more about this at: https://refeds.terena.org/index.php/Managing_Data_Protection_Risks_Using_the_Code_of_Conduct

[4] https://refeds.terena.org/index.php/Data_protection_coc

way IdPs can agree to release the pre-defined set of attributes that are listed in a specific category.

At the time of writing InCommon is testing this approach with the introduction of the "**Research and Scholarship Category**" that applies to service providers that support research and scholarly activities such as virtual organizations and campus-based collaboration services.

If widely accepted, this approach could make it easier to release attributes.

Proposal: Could REFEDS/eduGAIN prepare a basic package explaining the basic data protection issues and the CoC? This package could then be customised by different federations and made available online.

Who: REFEDS/eduGAIN/e-Research projects.

Timeline: TBA

Proposal 2: Gather information on the usage of Entity Categories from InCommon and other federations that are using/testing it and discuss the possibility of scaling Entity Categories on a more global level.

Who: REFEDS.

Timeline: Summer 2013

5.3 IdPs for guest users

As indicated in the AAA Study[5] [13] and previously reported in the TERENA Compendium and by the REFEDS group, the number of federated access infrastructures in the research and education community has been growing constantly since 2005. To date, the majority of the NRENs in Europe offer (directly or via a third party) federated access for their users. However, the level of deployment, the participation of institutions and the amount of services available via different federations vary significantly from country to country. For instance, not all research institutions, libraries and community datacentres are connected to national federations.

Identity Federations particularly cater for users affiliated with an institution. Users without an affiliation (for example, because their home organisation has not joined an IDF) or users affiliated with multiple institutions or 'nomadic users' (i.e., persons who move from one institution to another), cannot be easily supported by IDFs at this point in time. The 'nomadic users' pose an interesting challenge to the Identity Federations, particularly when they tend to be identified with researchers; for instance, access to the researchers' publications or researchers' data may become unavailable to the owners when they move to another institution.

There are views that guest IdPS could ease the deployment of federated access. Although this solution can be rather appealing and there are in fact some Identity Federations that offer guest IdPs, there are still concerns on the scale of the guest IdPs on how should operate them, on the costs to operate them and on the longer term sustainability of the guest IdPs. Typical questions are "Who should operate them? Should that be offered by each Identity Federation? By the collaboration communities? By a third party, like TERENA, EGI, etc., ? There are some views that propose the research collaboration to take the responsibility to operate the guest IdPs, although this would have clear implications on the budget.

[5] The AAA Study was led by TERENA and carried out by a consortium that also involved libraries. The final version of the AAA Study Report can be found

For some use-cases, social accounts (such as Google accounts or Facebook login) could be used, so long as these providers are accepted by the services. For other use-cases, a more in depth discussion is needed to understand what level of trust is needed during the verification process (see also section 5.5).

One of the limitations with the usage of social IdPs, for instance, is that it is not possible to affiliate a user with an organisation (e.g. his university that does not have yet an AAI). Whilst this may not be an issue for some use-cases (i.e. it is sufficient to uniquely identify individual researchers even if they change employer/institute), it would not solve the other set of use-cases where a user is allowed to access some resources because of his/her affiliation. The former set of use-cases could also be solved by using ORCID or ISNI identifiers.

Proposal: Create a discussion group that involves some e-Research projects, some Identity Federations representatives and the specific GN3plus groups to define the use-cases that could be addressed by social identity providers, ORCID and ISNI. If third parties trusted attribute providers were available they could then provide the additional attributes needed by for instance e-Research services.

Who: To be identified e-Research groups (via FIM), GN3plus dedicated groups and selected Identity Federations (via REFEDS).

Timeline: Mid term work (some results to be expected in 2014)?

5.4 Fine grained Authz and attribute authorities that handle attributes for specific communities

As emerged during the VAMP Workshop[6] held in September 2012, there is general consensus that the model to manage attributes, where all attributes are provided by the users' IdP, is not scalable. A better model would be to enable research communities or more in general third parties to maintain specific and additional information about the users.

There seems to be general consensus in a model where the e-Research communities administrate the attributes that are specific to their work, whilst the university IDP only administrate the attributes that are managed best by them.

However, adding a third entity to the current identity federation model has implications on the trust model, typical questions are "How do you trust an attribute provider?", "Who operates them?" and "What is the flow to retrieve attributes?". Clearly both the technical model to implement external attribute authorities and the implication on the trust model need to be addressed.

It is also worth noting that any new model to be successful cannot require significant changes on the Identity Federations, as these are production systems and the introduction of new elements is not trivial. On the other hand, a model where the 'burden' falls entirely on the SPs will not be successful either, as SPs seem to have already problems with federated access.

Proposal 1: Can we identify some possible models to use external attributes providers?

Proposal 2: Upon completion of proposal 1, can we select a model and test it with a research project and a couple of federations first?

---

[6] http://www.terena.org/activities/vamp/ws1/

Who: Concerning proposal 1 plans have been already made to explore this space in TF-EMC2 and GN3plus. Some work could start before April 2013 (expected starting time for GN3plus).

Concerning proposal 2, volunteers could be recruited via REFEDS and the FIM community. eduGAIN is certainly a candidate to support any recommended model.

Timeline: This work will not start before summer 2013.

5.5 Support for different LoAs

Whenever Identity Federations and e-Research communities engage in discussion related to the support of LoA, most of the times these discussions end without a clear way forward. If on one side the need of LoA is acknowledged by both parties, on the other side it seems hard to identify specific actions.

In principle the underlying technologies upon which identity federations are built, would support the introduction of different LoAs, although there is no standardised way among different federations to express that an institution has performed additional verifications on the users' identity.

However identity federations operators seem to be reluctant to support different LoAs if this is only useful to a small number of users. This is due the fact that supporting different LoAs has implications on the operational costs.

REFEDS has tried to watch this space for a while. Beside the limited resources available, REFEDS failed to identify a real killer use-case. There have been also some exercises to map current federation policies to existing LoA profiles. However, the two main profiles (InCommon and Kantara IAF) do not seem to properly address the main RE international use-cases. Equally the e-Research community should be able to properly document their requirements and possibly define their own profile.

Proposal1: Identify a group of researchers and federations and work together to define requirements. This is a very slippery soil, so this is expected to be a long term effort. Engage in a discussion with LifeScience to gather their LoA requirements.

Proposal2: Explore ways to implement workflows to handle higher LoAs, using third parties trusted by IdPs as well as the IdPs. Trusted third parties could vet identities and assert LoAs for research community specifically.

Who: To start exploring this space it could be sufficient to have one e-Research group and one Identity Federation.

Proposal3: Would make sense to conduct a policy mapping exercise between the IGTF policy and Kantara IAF (NIST 800-63 based)?

Proposal4: Document the risk/value calculation for identities for a few pilot projects including a few based on the IGTF policy and some that are not "GRID"-based. Possible outcome is a set of common valuation criteria for e-science projects.

Timeline: Long term (2-3 years?)

5.6 Attributes Harmonisation

Although this is not an issue that has strongly emerged in the FIM paper, it is worth to mention it here as it has been discussed several times also in the context of Identity federations and e-Research communities.

There have been lengthy discussions on how to harmonise attributes. More specifically on: c

- What attributes the IdPs populate for their end users? (e.g. what is the attribute to express a person's name?)
- Are the IdPs actually willing to release the attributes (see section 5.2 on attribute release)?
- What expectations are there for the attribute values? (e.g. Is the attribute for a researcher's email address populated by the institutional email address or can it be populated by a Gmail or Hotmail address?)
- What semantics and vocabularies are used? (e.g. how to express "this person is a researcher in good standing"?)

Although, reality seems to show that global harmonisation of attributes is not a feasible goal in the short term, there have been successful attempt to harmonise individual attributes. See for instance the proposal made by Andrew Cormack on eduPersonScopedAffilitiation (ePSA). Another rather successful attempt to harmonise attributes for inter-operability use-cases was provided by SCHAC, the SCHema for ACademia [14].

One of the recommendations from the AAA Study, was to aim for well-defined semantic of attributes within a community and to define mapping mechanisms among various groups. However, although this proposal is less ambitious than the global harmonisation, it is nonetheless very challenging, particularly concerning the vocabulary and the mechanism to coordinate this among various communities.

The Kantara Initiative [15] has started a new working group called "Attributes in motion[7]" with the aim to create a set of best practice documents around:

- The handling of attributes by Identity Providers, Relying Parties, and Service Providers
- The definition and proposed use for contexts
- The definition, best use, requirements and criteria of an Attribute Broker

It may be worth monitoring the progresses in this space.

Proposal: Let's start by assuming that there should be a difference between NREN AAI attributes and research community attributes and that both these attributes are needed.

Could the e-research communities identify use-cases for pan-European attributes? Or per research community ?

Proposal 2: The research communities should get the mean to administrate their own attributes which should then be aggregated by the SP. It would be worth exploring this model via small pilots. Are there pilots running about this?

Who: A couple of Identity Federations and research collaboration.

Timeline: Mid term work (some resulted to be expected early 2014).

6. Addressing Perceived Risks Using FIM

The FIM paper identifies a number of risk related to the usage of FIM; the table below summarises the most important points.

This paper tries to provide an answer to most of these issues.

Issues	Comment
Increase of phishing attack, due to the WAYF redirect	The REFEDS group will provide a page summary to detail why this is not a real issue. It will be included in the next version of this paper. We could also publish it as a REFEDS blog post.
Trust model in IdF: can SPs misuse attributes obtained from IdPs?	It is important to note that in the current Identity Federation set up, the misuse of attributes is already covered by law, see the data protection laws and particularly the eduGAIN the Code of Conduct. It would be good however to describe how Identity Federations would deal with complaints or misuse. We proposed to link this with the topic below.
Incident response in federated environments	To date the number of incidents reported by the Identity Federations is incredibly low. Most of the federations have already efficient help-desk supports and most of the issues are solved at national level. However it may be worth discussing the creation of a list (maybe as part of REFEDS) for federation operators to share warnings. There has been some work both in the EGI community and in eduroam, which may be relevant. Both have been presented at TF-CSIRT meetings: eduroam: https://community.ja.net/blogs/regulatory-developments/article/dealing-misuse-eduroam EGI: http://www.terena.org/activities/tf-csirt/meeting36/smutnicki-egi-csirt.pdf **Proposal**: discuss this on the REFEDS

	list for comments. **Proposal**: Document Identity Federation procedures to deal with incidents
Easy integration and good deployment for Service Providers	Well-known problem, sadly no solution at the moment. REFEDS is looking at guidelines to help improve deployment on service providers side.
Credential revocation in case of compromised credentials	More documentation on the workflow used to address this issue should be provided. **Proposal**: Discuss this topic with the REFEDS group and seek feedback from them.

7. Addressing the Recommendations from the FIM4R Report

A. Risk Analysis

The FIM4R paper recommends that "A pragmatic risk analysis of the use of identity federation from the point of view of a research infrastructure provider will be necessary to reassure the security officers at participating sites".

In response to this, this paper proposes the research community to own and manage their own risk register and to define procedures to perform such a risk analysis. REFEDS should support this process and could possibly feed into the assessment of the register on a regular basis.

B. Pilot Studies

The FIM4R recommendation about this point is "The progress of the pilot projects should be coordinated with the experts who belong to operational national and international identity federations a) to leverage their technical expertise with other service providers and b)create a "science-neutral" collaboration round for technology transfer".

Could a proposal be defined to ensure that the results of the pilots are well documented and shared between both the e-Research communities and REFEDS?

It is important to note that GN3plus offers a good opportunity to address some of the use-cases that can be selected jointly by the FIM and REFEDS/eduGAIN groups. Some federations (i.e., CSC) are already working on pilots with some e-Research initiatives.

Obviously REFEDS would be supportive of this.

C. Separation of Authorization and Authentication

The FIM4R paper recommendation on this point states "The need for an external attribute authority managed by the research community implies a formal separation of the authentication performed by the IdP and the authorization performed on behalf of the SP".

The FIM4R paper has this as a recommendation to technology providers. However it would be important to look at real and good examples (VOMS?, REMS?) of how such an attribute authority could be managed. An example of this is the SWITCHtoolbox (VO solution), which implements a third party attribute authority where (research) groups manage the group membership (and potentially other attributes) themselves. There might other similar solutions that could be analysed.

There is also a lot of work to be done on shared definition of what is meant by attribute authorities/providers.

D. Credentials revocation

The FIM4R recommendation on this point states “The credentials issued by the IdP to the user or the SP should be revocable in case they are discovered compromised”.

Identity Federations already offer this feature and offer advice and guidance on how this works.

E. Attribute delegation to the research community

The FIM4R recommendation states “Many of use cases identified by the research communities call for personal information to be aggregated with community defined attributes in order to grant access to digital resources and services. Compared to existing use cases, this aggregation means that an external attribute authority (typically managed by the research community itself) is needed in addition to the IdP and SP”.

C and E are effectively the same, please refer to C .

F. Levels of Security

The FIM4R recommendation about this states ” A one size fits all model for levels of security supported for a given FIM system will not scale into the future. … More work is required on the standardisation efforts for levels of assurance and communication and enforcement of LoA”.

See chapter 4.5 for proposals about this.

8. Identifying Pilots

A preliminary list of possible pilots to be discussed with the FIM community at large and with the specific e-Research groups in more details, is appended below. Clearly each of the proposed pilots needs to be specified in more detail.

1. Arts and humanities i.e., CLARIN, DARIAH, CESSDA and possibly others
2. See Dave Kelsey presentations in June in Nijmegen [16]
3. Central service to issue X.509 certs; IdPs could interface with this service via a credential translation (see TCS etc)
4. IdPs used for the HEP community to be accredited by IGTF; these IdPs would then be ‘qualified’ to perform more rigorous vetting and hence to offer higher LoA ;
5. The ELIXIR pilot mentioned in FIM paper. A presentation about the results is expected during the FIM meeting in March.
6. LIGO [17] may be interested in engaging in a pilot

7. EUDAT [18]?
8. Any others?

ANNEX I

This table below lists the requirements and barriers issues that were identified in the FIM paper.

Community	Requirements	Barriers	Comments
HEP	1. High level of trust	ID Fed do not support this due to a lack of use-cases	This requirement seems to refer to the high level of trust for authentication, but it should be confirmed. Identity Federations could support stronger authentication if there were use-cases that would require it. However the additional costs to implement more extensive vetting procedures should also be assessed in relation to the benefits achieved. Should we work and identify use-cases?
	2. Fine grained authZ	ID Fed support this	It is probably an issue for e-Research people but IDFs don't/can't necessarily solve the issue for e-Research people. e-Research people may need to deploy and operate an VOMS/AP/attribute aggregation service for their own community. A discussion should take place on whether e-Research groups want IDFs to take a role here, or someone else (such as EUDAT).
	3. Credential translation service	There are already working examples see SLCS, TCS etc.	There are some examples that address some use-cases. EUDAT is also working on additional translation services. **Proposal**: it would be useful to have a discussion with the FIM community to understand how far such systems should go. Maybe a better dissemination to explain what is already available may be useful.
	4. Provide support for "homeless'	During the AAA workshop[8] held in Brussels in July 2012, it was agreed	How do we ensure this is done by all federations? Should REFEDS (or somebody

	users	to recommend ID Fed to offer a guest IdP for 'nomadic' users	else) offer a guest IdP as a service? Could we rely on social IDs for low level assurance? Some people believe that the quality of the vetting procedures for a guest IdP would not be high enough and in any case not higher than what is currently offered by social Identity Providers. Therefore it would more cost-effective to use social Identity Providers. The dependence on using solutions based on social Identity Providers should be examined carefully. For example, the social providers could alter they APIs, their service model, etc., without notice. An important limitation in using social Identity Providers is the impossibility to affiliate a user with an organisation. However while a guest IdP would be able to authenticate users, a third party should provide additional attributes for these users.
	5. Easy to use solution (the FIM paper proposes OpenId-enabled access for portals, wiki etc)	Although OpenID or any other equivalent account could be used for some use-cases they would not solve the problem related to handle ad-hoc attributes as required by some international collaboration.	Short term issue? **Proposal**: Explain (maybe in a blog) OpenID is strength and weaknesses in relation to identity federations. The documentation produced by SWITCH (http://www.switch.ch/aai/support/faq/SWITCHaai_and_OpenID.html) could be a good starting point.
Photonics	1. Confidentiality	This came out as a strong requirement from this community (see page 4-9 FIM document).	Is this a requirement for their service? Is there a believe that identity federations cannot offer confidentiality?
	2. Unique identifier for their users to access different	This seems to be a recurrent requirement. The Umbrella project is already offering	Is this anything we should look at? I think there is a NIH problem here. As far as I understand the Umbrella concept and LIGO in the US, they are very similar –

	facilities	support for this community.	one central IdP, which could be federated (i.e. registered as an SP to IDFs).
Arts& Humanities	1. Authentication issues for a user wanting to access resources distributed over several archives	The main problems for this community are due to the fact that: 1. Not all institutions belong to a national federation. 2. Even when users belong to an institution that is part of a federation the release of attributes can still be problematic. Many IdPs in fact do not expose user-attributes even if the national IDF requires them to do so.	Guest IdPs could offer a short term solution to this problem, assuming the whoever runs a guest IdP could recover the operational costs. Clearly a better a more scalable solution but longer term would be that ESFRIs, EC, national agencies, provide funding to expand IDFs towards 100% coverage
	2. Attributes not released by the IdP despite the ID Fed mandate them	Could we try and ensure that at least ePPN (or any other) is released by all IdPs in a ID Fed?	How realistically can we achieve this? Can we offer fall-back solutions for when the IdPs do not release attributes? There are several issues here: 1) not all IDFs populate the same attributes (eduGAIN solution: there is a list of RECOMMENDED attributes for eduGAIN IdPs) 2) Attributes are populated, but they are not released due to data protection concerns. Hopefully Data Protection CoC solves this issue. See more about this in section 4.2.
	3. General SP Problem: one of the	Problem with the federation policies	Long term problem. REFEDS is working to provide a federation policy 'template' and

	main issues relates to the ID Fed opt-in policies (each IdP have to request to connect to an SP).	and the laws.	recommendations on what should be included or not in a federation policy. However this will not solve all the problems, but it is a step forward. The Data Protection CoC has good chances to solve this issue. REFEDS could try and put some more pressure on federations themselves to look at how they operate and make real commitments to standardising / improving things for SPs.
	4. Lack of standardised way for distributing SPs metadata	This is due to the lack of harmonisation among different federations. Both eduGAIN and PEER[9] could work to improve this aspect.	Short term issue? A pilot built on the PEER [18] software is expected to start in 2013. It would be good to ensure the participation of some of e-Research SPs. If all federations and all IdPs participated in eduGAIN, then each SP would have to register only with one federation and be exposed to the other federations via eduGAIN. Currently, CLARIN has registered SPs to DFN-AAI, SURFnet and Haka, and of course their metadata management is different, which has made CLARIN unhappy.
	5. Attribute Harmonisation	This is a well-known problem, but sadly not one that can be solved in the short term if at all.	Long term. It's hard to enforce changes to attributes. We may try and improve things within a community (as recommended by the AAA Study), but there are doubts on how much it can be achieved. **Proposal**: have a discussion on this topic involving different groups.

References

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

[2] eduGAIN
http://edugain.org/

[3] REFEDS
https://refeds.org

[4] GÉANT project
http://www.geant.net/pages/home.aspx

[5] CLARIN
https://www.clarin.eu/

[6] ELIXIR
http://www.elixir-europe.org/

[7] Moonshot
https://www.ja.net/products-services/janet-futures/moonshot

[8] OAuth
http:// http://oauth.net/2/

[9] OpenID Connect
http://openid.net/connect/

[10] ECP (Enhanced Client or Proxy) Profile
https://wiki.oasis-open.org/security/SAML2EnhancedClientProfile

[11] TF-EMC2
http://www.terena.org/activities/tf-emc2/

[12] Entity Categories

https://spaces.internet2.edu/display/InCCollaborate/Research+and+Scholarship+Category
http://wiki.swamid.se/display/SWAMID/Entity+Categories
macedir.org/draft-macedir-entity-category-00.html

[13] AAA Study

https://confluence.terena.org/display/aaastudy/AAA+Study+Home+Page

[14] SCHAC:
http://www.terena.org/activities/tf-emc2/schac.html

[15] Kantara Initiave
http://kantarainitiative.org/

[16] D. Kelsey's presentation:
http://www.clarin.eu/system/files/kelsey22jun12.pptx

[17] LIGO
http://www.ligo.caltech.edu/

[18] EUDAT
http://www.eudat.eu/

[19] PEER
https://refeds.terena.org/index.php/PEER