Service Aspects of Assurance

Authors:
Daniela Pöhn, Tangui Coulouarn, Nicole Harris
Co-authors:
Mikael Linden, Lukas Hämmerle, Wolfgang Pempe

Table of Contents

1. Introduction

In the research and education environment, Federated Identity Management (FIM) has been created in order to facilitate access to diverse resources used by students and researchers. By making use of FIM, the universities can send user information, so called attributes, to the operator of the service. This facilitates the life of users, who only identify themselves once at their home organisation - the Identity Provider (IdP). FIM also helps the owners of resources – called Service Providers (SP) - to manage access and usage. FIM has historically developed in national contexts, before GÉANT established the inter-federation eduGAIN.

In parallel, some research communities also built up their own environments. While many have, at least partly, joined eduGAIN, there are still open issues regarding identity management. These issues are addressed in the FIM4R paper [1], which was written by different representatives of research communities. One important issue is the extent to which the identity of a user has to be verified. This includes, depending on the standard, identification of the user, authentication, update of user information, and further aspects. The amount of confidence in these features is known as assurance, and is traditional details as a Level of Assurance (LoA). Some research communities tend to have higher requirements than federations.

The community is also becoming increasingly aware that a strictly hierarchical approach to assurance may not be the best approach to solving the requirements of the community. Traditional “levels” of assurance are presented hierarchically, with each increase seen as being an improvement on the level below. It is often unlikely that any given infrastructure or community needs the exact set of requirements within any one of those levels and may wish to actually pick and choose from different levels. This can lead to unnecessary requirements being placed on organisations simply because they are part of any given level. A better approach may be to refer simply to assurance profiles that are scoped against the specific needs of any given community, allowing the requirements to be more effectively scoped. These assurance profiles may overlap each other in terms of hierarchical notions of strength and leave out certain sections of traditional profiles altogether. This approach is inline with discussions by the Vectors of Trust (VoT) group within the IETF [2].

Although the FIM4R paper was written in 2013, the issue of assurance is still open. Some federations, e.g., InCommon (USA) and SWAMID (Sweden), have tried to roll out assurance profiles, but still struggle. In order to help IDPs within eduGAIN, but also research communities, GÉANT and Authentication and Authorisation for Research and Collaboration (AARC) address the issue from two different point of views. GÉANT thereby has the costs for IdPs as an objective. The complementarity between the two approaches is presented below.

About this document

The presented white paper addresses the service aspects of Level of Assurance. After describing the approach that was taken, the paper first presents the situation of federations. We then visualize the situation of IdPs, based on a survey and the results from internal dialogues with IdPs. These results are then compared with the insights given by AARC [3], which leads us to a set of recommendations.

2. Federations

National federations are collections of organisations operating SPs and IdPs and other relevant entities that agree to interoperate under a certain set of rules. In the research and education (R&E) environment, they are driven by a federation operator who provides processes and often tools to support the operation of the Identity federation. The most important task of federations is to establish trust between members/participants. Among other things, they define policies and also requirements concerning the IdPs. These requirements can be described assurance profiles or/and as policies.

First the preliminary work is explained, before the questionnaire to federation operators is described.

2.1 Preliminary work

The landscape of the federations in terms of assurance appears to be quite diverse.

Federations differ in the way they assist IdPs: some federations such as Haka (the Finnish federation) as well as SURFnet (Netherlands) offer a self-assessment tool to measure the maturity of IdPs; many other federations only define minimum requirements. The IdPs of the Danish federation WAYF have, as public organisations, to comply with rules regarding IT security (ISO 27001) and be audited.

The definition of assurance also differs. The German federation DFN-AAI established their own LoA with two classes, Basic and Advanced, focusing on three different aspects (registration and original identification, update of information, and authentication). InCommon, the federation of the US, adapted the NIST Special Publication 800-63, calling the two lowest levels Bronze and Silver. The Swedish federation SWAMID started to roll out assurance based on Kantara Identity Assurance Framework (IAF) that introduces Assurance Levels (ALs). SWAMID AL1 is a subset of Kantara IAF AL1.

The implementation of assurance seems problematic. In Germany, although the requirements are low, they were too high for many IdPs, resulting in a simplification of requirements. In the

US, even though a formal LoA was introduced, 5 IdPs managed to get Bronze and only one IdP received Silver. The Swedish federation explains that the only IdP that is Kantara approved is eduID (eduid.se with AL2), while all other IdPs try to get to the Swedish AL1. "If we would do it again or coach someone in doing it it would be less. The costs to get only eduID to Kantara AL2 was between 20-50k€," Valter Nordh explained. The IdPs have, at the same time, also costs and needed manpower to reach AL1.

A common problem that exists in today's R&E federation landscape is that it is difficult to quantify the specific assurance that is offered by federations. All federations provide a baseline of assurance through the practices articulated in their policies, operational practice guides and technical requirements for participants. Federations are also expected to reach standards through participation in initiatives such as eduGAIN [4]. There is however no consistent mapping of these expectations. This problem is recognised by the community and parallel efforts to better described and document the baseline practices of federations is underway with a proposed Metadata Registration Practice Template being prepared for eduGAIN participants. A better mapping of the baseline behaviour of federations will in turn inform a better understanding of the baseline expectations for IdPs.

2.2 Questionnaire

A questionnaire was given and filled out by operators of five federations, i.e., Haka, DFN-AAI, SWAMID, InCommon, and WAYF. The survey was carried out in order to get an overview of the current practice and try to estimate the costs for higher assurance.

The questionnaire revealed that most documents and processes are in place, but not enforced. The federations have contracts with IdPs and require an Identity Management Practice Statement, though do not strictly enforce it. Furthermore, the Identity Management Practice Statement is often in the mother tongue, so international SPs cannot read it. A documentation is in most cases required, but again not enforced. Audits are in a few federations done, mostly self-audits or pairwise audits.

Federation operators generally don't know any IdPs that would like to increase their assurance standing beyond the baseline of the federation, as they tend to struggle with the current requirements. Nevertheless, if the general assurance requirements would be increased, the federation operators estimate high costs for IdPs. An additional comment was the high burden for SPs to handle multiple assurance profiles in terms of knowledge and changing technical installations to support multi-assurance policies.

Additionally, Interoperable Global Trust Federation *(*IGTF) was asked about their point of view. The IGTF is an organization to establish common policies and guidelines that help establish interoperable, global trust relations between SPs and IdPs within Grid Community. IGTF has, in contrast, no contracts with IdPs in place. Nevertheless, sanctions are possible for IdPs not complying with the requirements. An Identity Management Practice Statement is not only required, but also enforced. Documentation is required, while peer-audits are used to investigate the compliance of IdPs. Also, different LoAs might lead to confusion, as experienced by introducing a lower LoA.

3. Identity Provider

The universities and research institutions interviewed are responsible for running an Identity Provider for their staff and students. The IdP typically is connected to a user directory that contains the user's attributes. While federations have certain standards and policies, the IdPs demonstrate different levels of maturity. In order to find out about the average and the minimum basis, a questionnaire was sent to different IdPs.

3.1 Questionnaire and Findings

In the following section, we first present the questionnaire and then the findings of the survey.

3.1.1 Questionnaire

The questionnaire for IdPs was sent to French, US and German IdPs as well as to the GÉANT IdP. One IdP is member in the federations фEDUrus (Russia), Kalmar (Nordic Countries), SIR (Spain), UKfederation (UK), InCommon, IDEM (Italy), Tuakiri, AAF (Australia), Surfconext (Netherlands), edugain, and SAFIRE (South Africa), whereas another IdP has no federation. While one IdP has small to medium amount of manpower, 5 stated they have small amount of manpower. The number of users differ as well:

- 4x < 50 000 users
- 1x < 10 000 users
- 1x < 100 users

The questions comprise the following areas:

1. Identity/account concept;
2. Registration and proof of identity;
3. Online authentication;
4. Freshness of user data;
5. Step-up authentication;
6. Provenance and level of assurance.

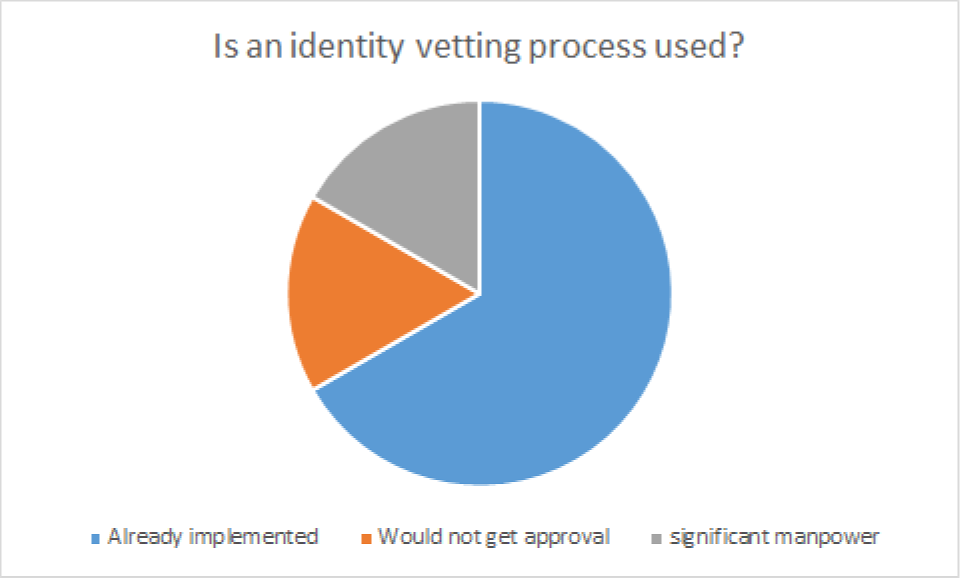
In order to get more information about the costs, a difficult question, as many aspects have to be regarded and people of different departments are involved, the answers could be:

- Already implemented.
- Could implement with small amount of manpower.

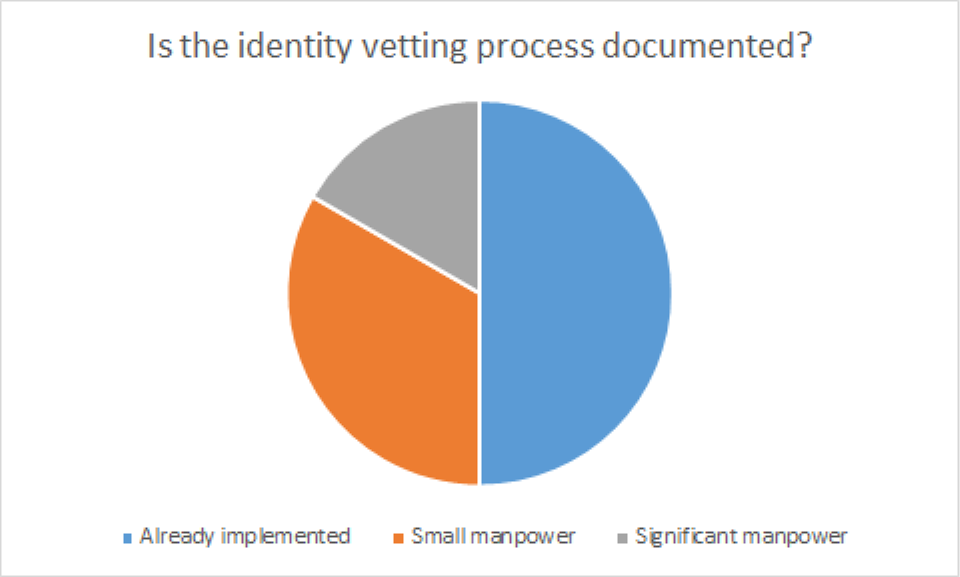
- Could implement with significant manpower.
- Could implement with low-cost system changes.
- Could implement with high-cost system changes.
- Would not get approval to make this change (please explain why).

3.1.2 Findings

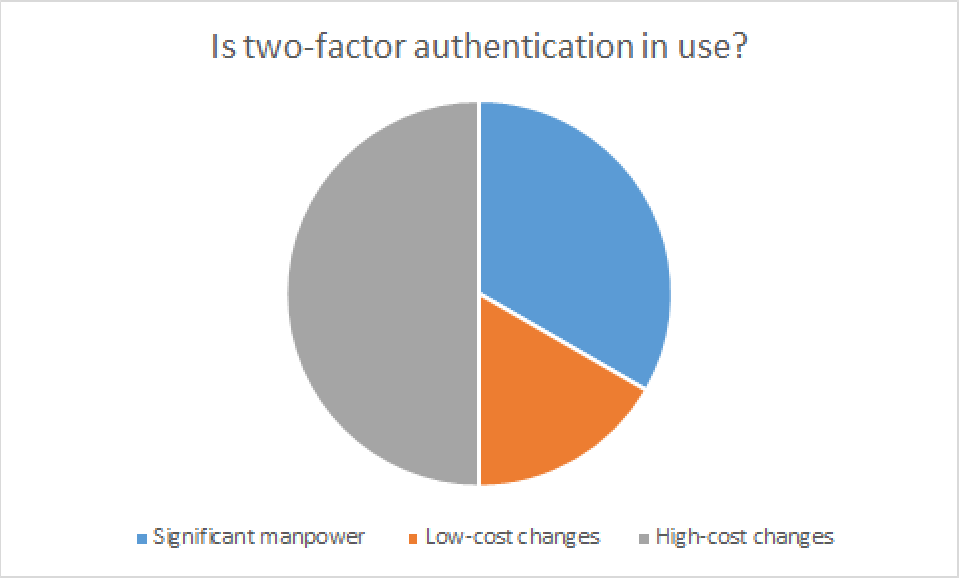
By asking IdPs this questionnaire, the current status of IdPs within eduGAIN was explored. Besides one IdP, all IdPs use individual accounts, which are persistent, **but can be re-assigned after a certain time**. Similarly, most IdPs have an identity vetting process, as shown in the Figure below.



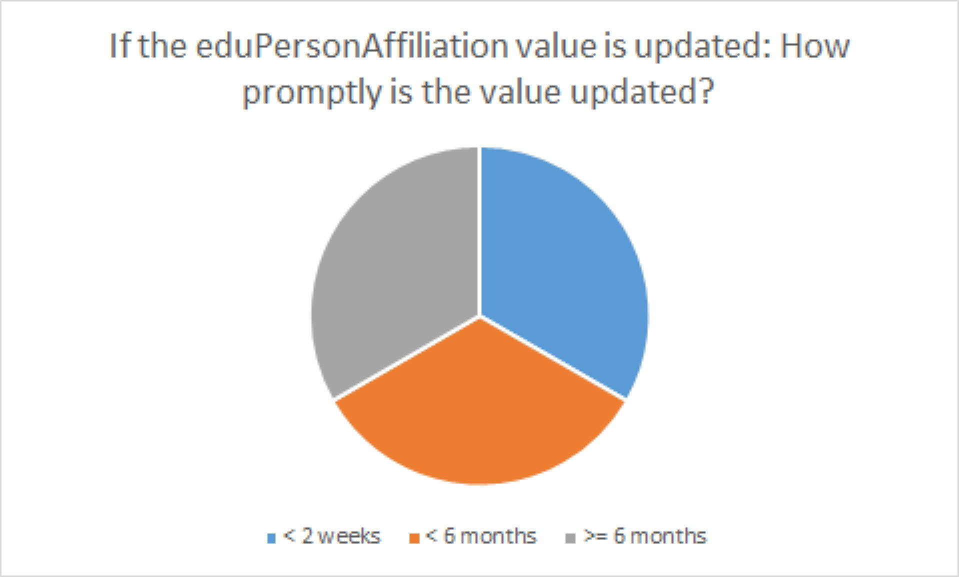
Although a vetting process is in place, not all IdPs document it. Half of the IdPs document the vetting process, while two IdPs could implement it with small manpower. Another IdP states it would lead to a significant manpower need.



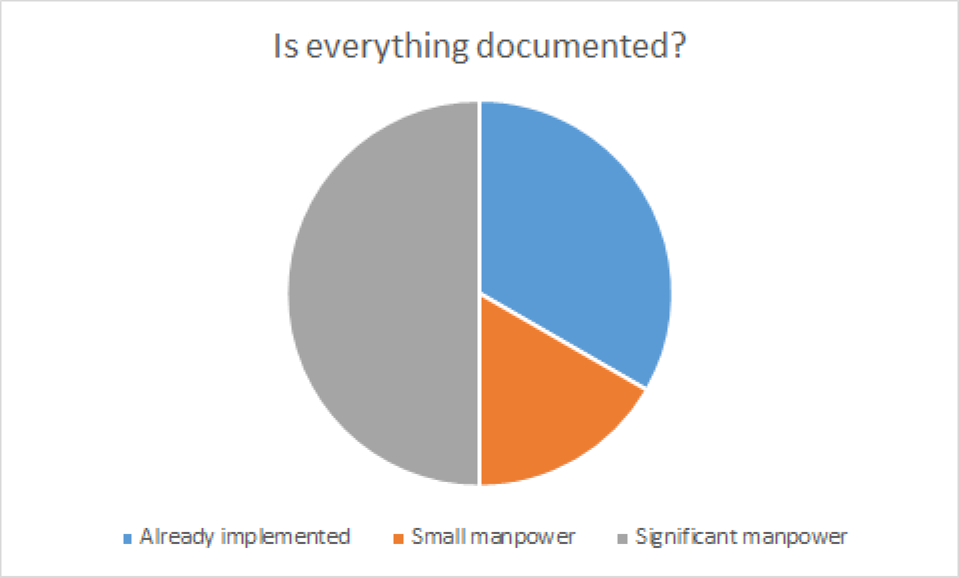
Besides at one IdP, all asked IdPs require certain qualities for passwords. None of the interviewed IdPs have second-factor authentication in place, which would lead in most cases either to significant manpower or high-cost changes.



If a user departs, the closing of an account and the update of the eduPersonAffiliation attribute is done within a different time period. The amount of time is evenly distributed between less than 2 weeks, less than 6 months, and more than or equals 6 months.

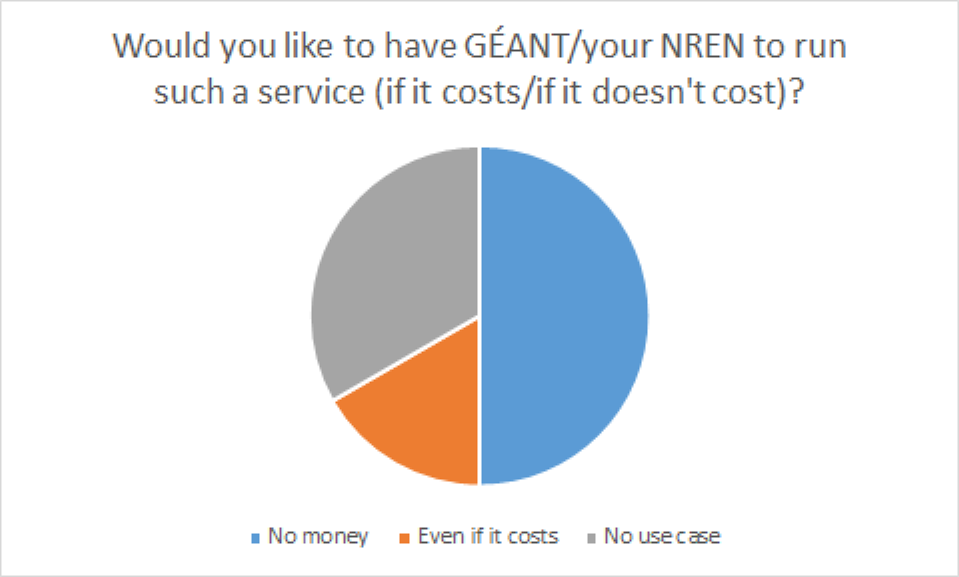


While two of the IdPs have all processes documented, other IdPs would need small up to significant manpower.



Similar results can be seen for the implementation of Incident Response Process and the usage of Identity Management Practice Statement. The results of the questionnaire show that most processes of IdPs are in place, but not enforced and not documented to the best level.

When asked about a step-up assurance service by GÉANT or their Home Federation, whatever the outline would be, most of the IdPs would like to use such a service. This also shows, that IdPs would like to have support, e.g., for introducing second-factor authentication.



Besides NREN federation, IGTF was also interviewed. They have a higher maturity level compared to the IdPs of the questionnaire. Identity vetting process is documented and identifiers are not reassigned. IdPs are peer-reviewed and have public documents, like the Identity Management Practice Statement. Only the time frame for updating user data can be up to 400 days.

Possible costs

The results of the questionnaire show, that several aspects/requirements can be achieved without much manpower or high costs:

- Unique identifiers;
- Persistent, non re-assigned identifiers.

The identity vetting process is generally carried out, while it is not always documented. The documentation of the vetting process could be done with small manpower and is, therefore, feasible.

Other aspects seem to be more expensive or time consuming. These are:

- Documentation of all processes;
- Promptly update of information;
- Second-factor authentication;
- Audit.

Further input

Further input was received from IdPs in Germany and the USA.

In Germany and other countries, IdPs often have not enough money to implement a second-factor authentication as it is not given a high enough priority in university management. Some even fail with the quality of the attributes. These problems have to be solved before a higher level of assurance is set.

In the US federation InCommon, different IdP operators explained their problems. Tom Barton from the University of Chicago described their problems finding a suitable auditor, which took them around one year. Nick Roy explained, that at Iowa the estimated costs were around USD 2 million and 2,000 hours of staff time in order to achieve Silver. This describes the problems with current LoA. Higher LoA normally requires an audit, which can be expensive and time consuming, especially when no auditor is recommended. Also the costs for second-factor or similar technology can be high.

Additionally, a survey was carried out by InCommon, asking different questions about their assurance programme. The main outcomes relevant for this white paper are as follows:

- *Is your institution interested in implementing either Bronze or Silver?*
  Half of the answers yes, half of them no.
- *Are you aware of any SPs that require Bronze or Silver?*
  1 yes.
- *Does your institution have any users that need access to SPs requiring Bronze or Silver?*
  2 yes.
- *Are there services your institution would like to use, but cannot because your IdP lacks a required assurance profile?*
  only no.
- *In what circumstances would it be valuable to your organization to be able to self-assert that your operation meets either of these specifications?*
  looking towards future needs (mostly).
  ease of obtaining the assurance level.
  chicken and egg problem.
  general security audit reporting.
  with external SPs.
- *What specific components do you value the most?*
  identity vetting: almost all;
  credential process: half,
  authentication technology/strength: almost all,
  attribute assurance: half

- *Are you aware of federated authentication contexts that require or that you think should require multi-factor authentication?*
  half yes, half no
- *Interested into an InCommon Multi-Factor Authentication Assurance Profile?*
  mostly yes, others I don't know, 1 no
- *Other assurance profiles?*
  mostly no, for R&S, trustmarks, NIST, research collaborations
- *Thoughts?*
  difficulties to get decision makers on board,
  multi-factor is excellent start,
  very few auditors understand or are qualified to verify the requirements for InCommon Assurance,
  big trust issues to overcome,
  interoperability and intercomparisons with international federations

Even though IdPs would like to improve, they currently don’t see the need for a higher LoA (“chicken and egg problem”). Nevertheless, some IdPs are interested multi-factor authentication. This is also the case in Germany and probably in many other federations.

4. Minimum requirements

The AARC project [3] concentrated on interviewing SPs and research communities to gain a greater understanding of the requirements from the perspective of the services. The team members, therefore, made a survey among research communities. By guided interviews, they identified a proposed assurance baseline, which is the minimum standard for research communities. The aspects are the following:

- Individual accounts (i.e. no shared accounts).
- Persistent, non re-assigned identifiers.
- Documented identity vetting, which is not necessarily face to face.
- Password authentication with some good practices.
- Departing user’s ePA changes promptly.
- Self-assessment of LoA supported with specific guidelines.
- Incident response in a later step.

Compared with the results from the questionnaire, the following areas for improvements can be seen:

- Non re-assigned identifiers: although persistent identifiers (like eduPersonPrincipalName) are used, many Identity Providers currently reassign them.
- Documented identity vetting: although IdPs have a vetting process in place, it is not always documented.

- Departing user’s ePA changes promptly: the time for changing user data lays between 2 weeks and 6 months. As closing accounts depends on internal processes and some universities have alumni accounts, the eduPerson(Scoped)Affiliation should be updated within 1 month.
- Self-assessment of assurance supported with specific guidelines: in order to have guidelines, a template needs to be designed, which then can be used for the self-assessment.
- Incident response: Security Incident Response Trust Framework for Federated Identity (SIRTIFI), but only at a later step, since SIRTIFI is new as well as the minimum requirements. SIRTIFI has the purpose to enable coordination of security incident response across federated organisations.

Compared with the further input, especially from InCommon, audits for a higher level should be pairwise and not with an external auditor.

5. Potential solutions

As the result of this analysis, the following recommendations for assurance can be derived:

- **Recommendation 1**: work with AARC to create and document a baseline assurance profile for IdPs, mapped to the requirements identified by AARC. Work on best practice in some areas (e.g. password authentication practice) is still required.
- **Recommendation 2**: create Self-assessment template / tool with best recommendation: this could be a GÉANT web tool, combined with SIRTFI and other monitoring/testing tools, including recommendations and best practices. This would help address documentation requirements from the AARC minimum set.
- **Recommendation 3**: address the status of quo of reassignment of identifiers by working with REFEDS to survey the problem space and possible solutions to this embedded practice by organisations. This may include changing general recommendations on identifiers in current common documentation.
- **Recommendation 4**: continue to work with REFEDS and AARC on maturing the SIRTFI approach to incident response.

Basically, the GÉANT Assurance Profile would be a combination of passed self-assessment, persistent identifiers, changing the affiliation promptly, and documentation. At a later step, SIRTFI could be added.

It might be the case, that some IdPs are required to have additional assurance practices in place for edge cases within the SP community. For them, the following recommendation can be made:

- **Recommendation 4**: Implement peer (pairwise) auditing of IdPs, which need to document their approach against the GÉANT assurance profile, in order to verify compliance with lower costs than external audits. The results of these audits can be displayed in the described web tool.
- **Recommendation 5:** Implement second-factor authentication: GÉANT could offer it as a service or procure Duo-type solution for community.

Online verification of the user's identity could be part of the second-factor authentication. In case of WebID, this would cost 350 Euros for the installation, 50 Euros monthly and 10 Euros per identification.

As previously mentioned in this document, the maturity of IdPs is closely related to the maturity of federations and the willingness of federations to help support and roll-out these concepts within their federations. As such, the following recommendations directed at federation operators are made:

- **Recommendation 5**: GÉANT should develop federation maturity reports aimed at managers, helping to improve the maturity of federations at a general level and to support the federations in achieving the manpower and funding to reach these goals.
- **Recommendation 6**: eduGAIN should work to ensure that all federation operators have a Metadata Registration Practice Statement that complies with the recommended standard template.

References

[1] Daan Broeder et al.: Federated Identity Management for Research Collaborations. http://cds.cern.ch/record/1442597/files/CERN-OPEN-2012-006.pdf?version=2 [Accessed: 16-11-2015].

[2] Vectors of Trust Working Group: https://www.ietf.org/mailman/listinfo/vot.

[3] AARC project: Milestone MNA3.1 - Recommendations on minimal assurance level relevant for low-risk research use cases.

[4] eduGAIN: www.edugain.org.