15-04-2016

GN4-1 White Paper: Service Aspects of Assurance

Work Package/Activity:	09/SA5
Task Item:	Task 1
Dissemination Level:	PU (Public)
Lead Partner:	GÉANT Association
Document Code:	GN4-1-16-32949f
Authors:	Daniela Pöhn (DFN/LRZ), Tangui Coulouarn (DTU), Nicole Harris (GÉANT)
Co-authors:	Mikael Linden (CSC), Lukas Hämmerle (SWITCH), Wolfgang Pempe (DFN)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

Contents

1 Introduction 1

2 Federations 1

2.1 Preliminary work 1

2.2 Questionnaire 2

3 Identity Providers 1

3.1 Questionnaire and Findings 1

3.1.1 Questionnaire 1

3.2 Findings 2

3.3 Possible Costs 5

3.4 Further Input 5

4 Minimum Requirements 6

5 Potential Solutions 7

References 9

Glossary 9

Figure 3.1: Proportion of IdPs that use a vetting process 2

Figure 3.2: Proportion of IdPs that document their vetting process 2

Figure 3.3: Proportion of IdPs using two-factor authentication 3

Figure 3.4: IdPs times to update eduPersonAffiliation value 3

Figure 3.5: Proportion of IdPs documenting all processes 4

Figure 3.6: Proportion of IdPs that would like to have an assurance service provided by GÉANT/their NREN, based on cost scenario 4

1 Introduction

In the research and education environment, Federated Identity Management (FIM) facilitates access to diverse resources on the part of students and researchers. Using FIM, universities can send user information to service operators in the form of attributes. This makes life easier for users as it means they only need to identify themselves once at their home organisation, which acts as the Identity Provider (IdP). FIM also helps the owners of resources – i.e. the Service Providers (SPs) - to manage access and usage. Historically, before GÉANT established the eduGAIN interfederation, FIM had been developed mainly in national contexts.

Meanwhile, some research communities also built up their own environments in parallel, and while many have at least partly joined eduGAIN, there are still open issues regarding identity management. These issues are addressed in the FIM4R paper, which was written by various research communities' representatives [FIM4R]. One such issue that is of particular importance is the extent to which the identity of a user has to be verified. This may include, depending on the standard, identification of the user, authentication, and update of user information, as well as other aspects. The amount of confidence that can be placed in these features is known as assurance, and is traditionally defined by assignation of a Level of Assurance (LoA). Some research communities tend to have higher requirements than federations in terms of LoA.

The community is also becoming increasingly aware that a strictly hierarchical approach to assurance may not be the best approach to meeting its requirements. Traditional "levels" of assurance are presented hierarchically, with each increase seen as being an improvement on the level below. However it is rare for any given infrastructure or community to need the exact set of requirements defined within any one of those levels, while they may actually prefer to select requirements from different levels. This can lead to unnecessary requirements being placed on organisations simply because they are included in the same level as their desired requirements. A better approach may be simply to refer to assurance profiles that are scoped against the specific needs of each community, allowing them to be more effectively tailored to their actual needs. These assurance profiles may overlap in terms of hierarchical notions of strength and leave out certain sections of traditional profiles altogether. This approach is in line with the discussions of the Vectors of Trust (VoT) group within the IETF [VoTWG].

Although the FIM4R paper was written in 2013, the issue of assurance remains open to this day. Some federations, e.g., InCommon (USA) and SWAMID (Sweden), have made attempts to roll out assurance profiles, which however have not produced definitive results. In order to help IdPs within eduGAIN as well as research communities, GÉANT and the Authentication and Authorisation for Research and Collaboration (AARC) project are approaching the issue from two different angles. GÉANT is addressing the aspects relating to federations and IdPs with the objective of reducing their costs, while AARC is looking at the question from the research communities' and the SPs' perspective. These two approaches, which are complementary, are presented in this White Paper. The document addresses the service aspects of Levels of Assurance, outlining the findings of the surveys carried out of the federations and IdPs, as well as the results of internal dialogues with the IdPs. These results are then compared with the insights provided by AARC [MNA3.1], to draw up 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 given 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 requirements related to the IdPs. These requirements may be defined either as a part of policies or as assurance profiles/levels.

In the sections below, the preliminary assessment work carried out is first described, followed by a summary of the results of the questionnaire submitted to federation operators.

2.1 Preliminary Work

The federation landscape in terms of assurance appears to be quite diverse. Federations differ in the way they assist IdPs: some such as Haka (Finland) and SURFnet (Netherlands) offer a self-assessment tool to measure the maturity of IdPs; many others only define minimum requirements. As public organisations, the IdPs of the Danish federation WAYF are required to comply with IT security rules (ISO 27001) and be audited.

The various definitions of assurance also differ. The German federation DFN-AAI established its own LoA with two classes, Basic and Advanced, focusing on three different aspects (registration and original identification, update of information, and authentication) [DFNAAI]. InCommon, the US federation, adapted the NIST Special Publication 800-63 [NISTSP80063], calling the two lowest levels Bronze and Silver. The Swedish federation SWAMID has started to roll out assurance based on the Kantara Identity Assurance Framework (IAF) that introduces Assurance Levels (ALs). SWAMID AL1 is a subset of Kantara IAF AL1 [SWAMID].

The implementation of assurance seems in general problematic. In Germany, although requirements are low, they still prove too high for many IdPs, resulting in a simplification of requirements on the part of federation operators. In the US, even though a formal LoA was introduced, five IdPs managed to obtain the Bronze certification and only one IdP received the Silver. The Swedish federation had more success while introducing the Kantara AL2 for eduID.se. Nevertheless, the cost for the introduction was significant, at between €20-50 per account just for eduID.

Even relatively small countries such as Switzerland have hundreds of thousands of accounts within the SWITCHaai federation. Consequently, IdPs also have costs and need manpower to reach a higher LoA, so assurance as a default feature would do away with the value proposition of federated identity for many such organisations.

A common problem that exists in today's R&E federation landscape is that it is difficult to quantify the specific degree of 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]. There is however no consistent mapping of these expectations. This

problem is recognised by the community and parallel efforts to better describe and document the baseline practices of federations is underway with the preparation of a proposed Metadata Registration Practice Template [eduGAIN Wiki] for eduGAIN participants. Improved 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 submitted to the operators of five federations: Haka, DFN-AAI, SWAMID, InCommon, and WAYF. The survey was carried out to gain an overview of current practices and estimate the costs for higher assurance.

Responses to 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, but do not enforce it strictly. Furthermore, the Identity Management Practice Statement is often written in the national language, which means it cannot be understood by most international SPs. Documentation is required in most cases, but again this is not enforced. Audits are carried out in few federations, and these are mostly self-audits or pairwise audits.

Federation operators generally do not know of any IdPs that would like to increase their assurance standing beyond the baseline of the federation, as most already tend to struggle with the current requirements. If the general assurance requirements were to be increased, the federation operators estimate that high costs would be incurred by IdPs. The high burden on SPs for handling multiple assurance profiles in terms of knowledge and changing technical installations to support multi-assurance policies was also noted.

The Interoperable Global Trust Federation (IGTF) was also asked for its perspective on this issue. The IGTF is an organisation that operates to define common policies and guidelines that help establish interoperable, global trust relations between SPs and IdPs within a Grid Community. However, the IGTF has no contracts in place with IdPs, although it can enforce sanctions for those IdPs that fail to comply with its requirements. The IGTF mandates that IdPs must provide both an Identity Management Practice Statement and Documentation. It also requires them to carry out peer-audits to assess each other's compliance with the policies. IGTF has also introduced a lower LoA, which may have led to confusion in some instances.

3 Identity Providers

Universities and research institutions that are responsible for running an Identity Provider (IdP) for their staff and students were surveyed. IdPs are typically connected to a user directory that contains the users' attributes. While federations adhere to certain standards and policies, IdPs demonstrate varying levels of maturity. A questionnaire was first sent out to the IdPs to establish their average and minimum standards.

3.1 Questionnaire and Findings

The areas covered by the questionnaire and the findings of the survey are set out below.

3.1.1 Questionnaire

The questionnaire was sent to French, US and German IdPs, as well as to the GÉANT IdP. One of the surveyed IdPs is member of the ϕEDUrus (Russia), Kalmar (Nordic Countries), SIR (Spain), UK federation (UK), InCommon, IDEM (Italy), Tuakiri, AAF (Australia), Surfconext (Netherlands), eduGAIN, and SAFIRE (South Africa) federations, whereas one other does not belong to any federation. In terms of manpower, one IdP has a small to medium amount, and five have a small amount. Their number of users also varies:

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

The survey questions covered 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.

To obtain more information about costs, which is a complex question as many aspects need to considered and different departments are involved, IdPs were asked to select one of the following answers:

- 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

The questionnaire helped to explore the current status of IdPs within eduGAIN. Apart from one, 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 Figure 3.1.

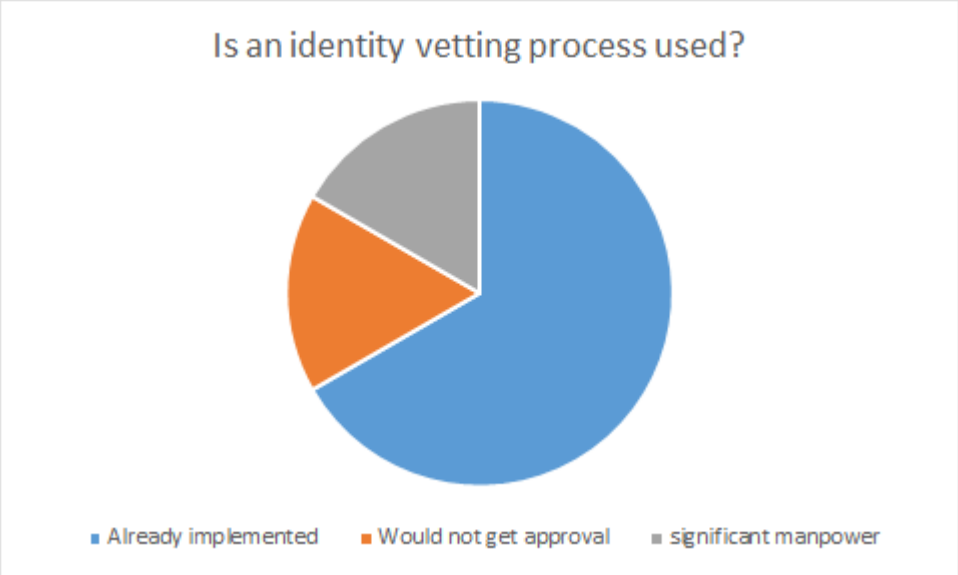

Figure 3.1: Proportion of IdPs that use a vetting process

However, although they may have a vetting process in place, not all IdPs document it. Half of the IdPs document the process, while two IdPs could implement with a small amount of manpower. Another IdP stated implementing this would generate a significant need for manpower.

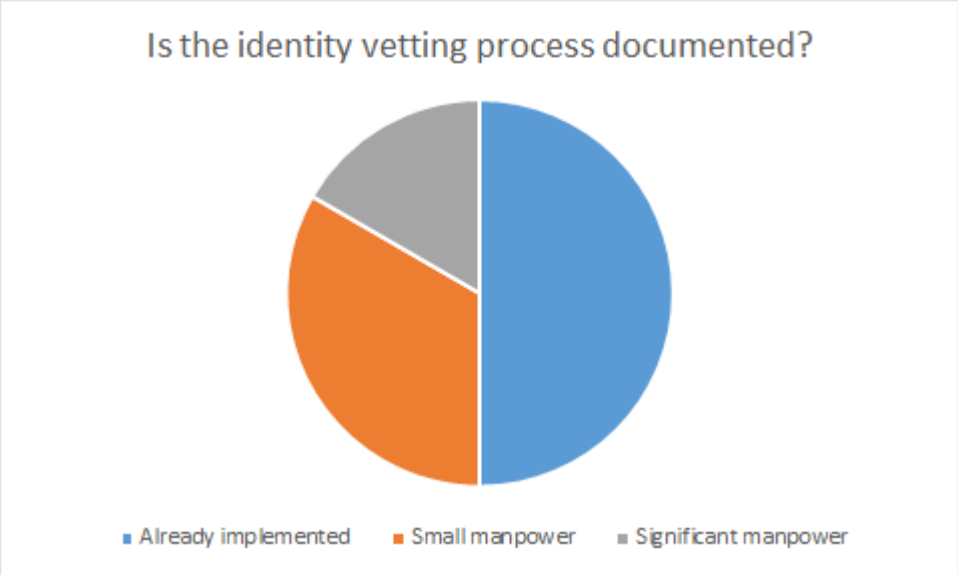

Figure 3.2: Proportion of IdPs that document their vetting process

All but one of the interviewed IdPs require certain criteria for passwords. None have second-factor authentication in place, which in most cases would require either too much manpower or high-cost changes to be implemented.

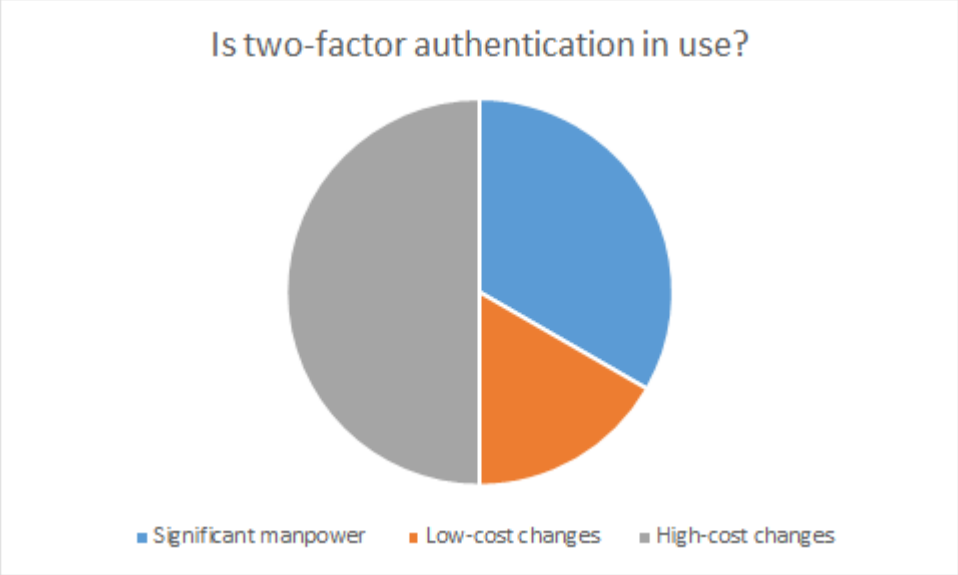

Figure 3.3: Proportion of IdPs using two-factor authentication

If a user leaves, the time period required to close an account and update the eduPersonAffiliation attribute varies between different IdPs. These time periods (less than 2 weeks, less than 6 months, and more than or equal to 6 months) are more or less evenly distributed across IdPs.

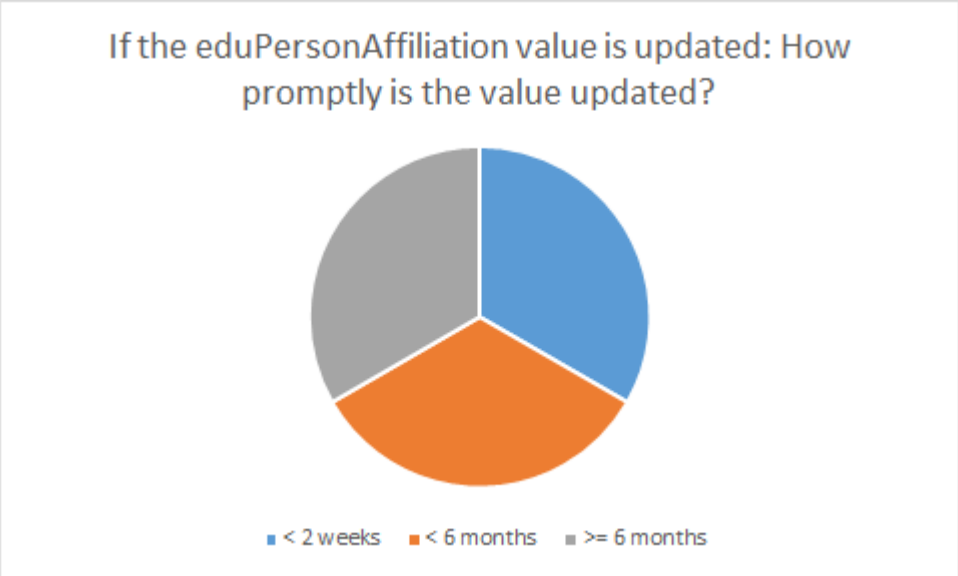

Figure 3.4: IdPs times to update eduPersonAffiliation value

While two of the IdPs document all processes, others would need small to significant manpower increases to implement this.

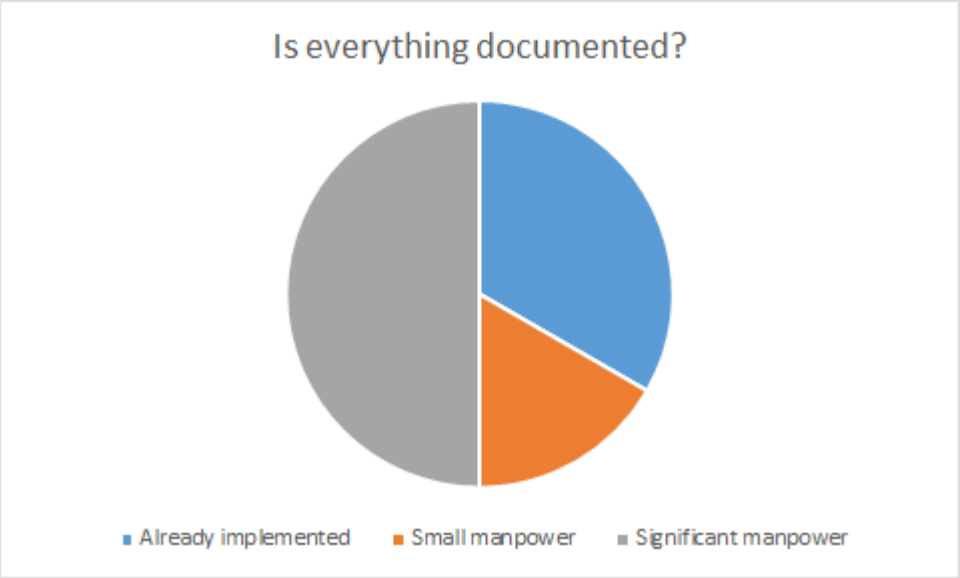

Figure 3.5: Proportion of IdPs documenting all processes

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

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

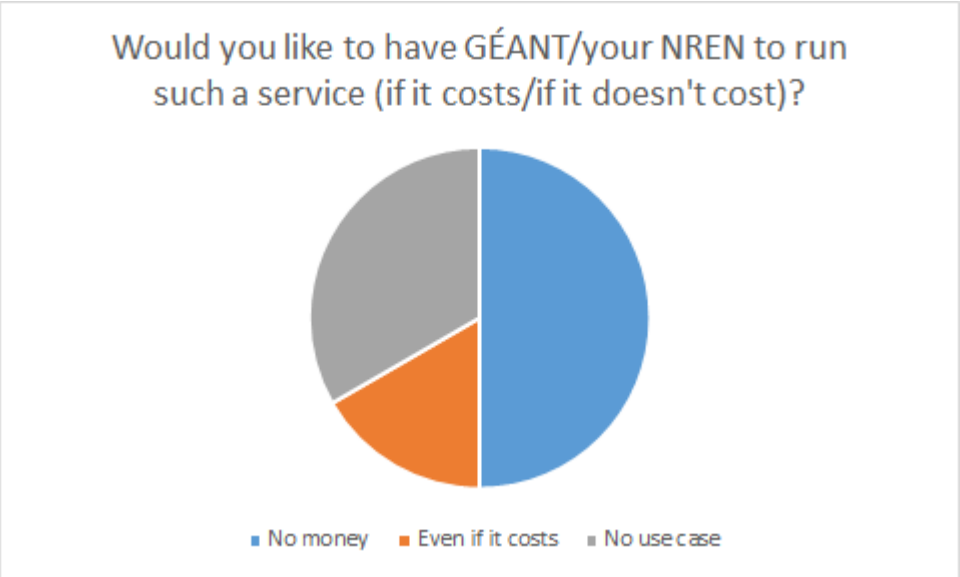

Figure 3.6: Proportion of IdPs that would like to have an assurance service provided by GÉANT/their NREN, based on cost scenario

In addition to the NREN federations, IGTF, which has a higher maturity level compared to the IdPs that responded to the questionnaire, was also interviewed. IGTF's identity vetting process is documented

and identifiers are not reassigned. Its IdPs are peer-reviewed and are required to issue public documents, such as the Identity Management Practice Statement. Its time frame for updating user data can be up to 400 days.

3.2 Possible Costs

The results of the questionnaire show that some aspects/requirements can be achieved without much manpower or incurring high costs, including unique identifiers and persistent, non-reassigned identifiers.

An identity vetting process is generally in place, but not always documented. Documenting the process could be achieved with a small amount of manpower and is therefore feasible.

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

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

3.3 Further Input

Further input was received from IdPs in Germany and the USA. In Germany and other countries, IdPs often do not have enough funding to implement second-factor authentication, as this is not assigned a high enough priority in university management. Some even fail in terms of attribute quality. These problems have to be solved before a higher level of assurance is set.

Various IdP operators in the US federation InCommon described the problems they encounter. Tom Barton from the University of Chicago pointed out their difficulties in finding a suitable auditor, which took them about a year. Nick Roy explained that at Iowa the estimated costs for achieving the Silver qualification were around USD 2 million and 2 000 hours of staff time. These issues highlight the problems with current LoAs. Attaining a 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 to this white paper are as follows:

- *Is your institution interested in implementing either Bronze or Silver?*
  Half yes answers, half no answers.
- *Are you aware of any SPs that require Bronze or Silver?*
  1 yes answer.
- *Does your institution have any users that need access to SPs requiring Bronze or Silver?*
  2 yes answers.
- *Are there services your institution would like to use, but cannot because your IdP lacks a required assurance profile?*
  Only no answers.

- *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 (most).
  - 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 answers, half no answers
- *Interested in an InCommon Multi-Factor Authentication Assurance Profile?*
  Mostly yes answers, 1 no answer. Others: don't know
- *Other assurance profiles?*
  Mostly no answers for R&S, trustmarks, NIST and research collaborations
- *Thoughts?*
  - difficulties getting 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 inter-comparisons with international federations.

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

4 Minimum Requirements

The AARC project [MNA3.1] 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, carried out a survey among research communities. Through guided interviews, they identified a proposed assurance baseline, which is the minimum standard for research communities. The aspects addressed are the following:

- Individual accounts (i.e. no shared accounts).
- Persistent, non-reassigned 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 improvement can be identified:

- **Non re-assigned identifiers:** although persistent identifiers (such as 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 it takes to change user data is 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 set guidelines, a template should be designed, which then can be used for the self-assessment.
- **Incident response:** Security Incident Response Trust Framework for Federated Identity (SIRTFI), but only as a later step, since SIRTFI, as well as the related minimum assurance requirements have only recently been introduced. SIRTFI is a REFEDS working group to enable the coordination and enhancement of security incident response as an assurance profile across federated organisations [SIRTFI].

From the further input analysed, especially from InCommon, it emerges that for higher levels pairwise audits are preferable external audits.

5 Potential Solutions

From the analysis set out above, the following recommendations on assurance were 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 a self-assessment template / tool with the best recommended being 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 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.

A GÉANT Assurance Profile should comprise a combination of 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 these, the following recommendation can be made:

- **Recommendation 5:** 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 web tool described above.

- **Recommendation 6:** Implement second-factor authentication. GÉANT could offer this as a service or procure a Duo-type solution for the community.

Online verification of the user's identity could be part of the second-factor authentication. In the 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. As such, the following recommendations directed at federation operators are made:

- **Recommendation 7:** 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 attaining the manpower and funding to reach these goals.

- **Recommendation 8:** eduGAIN should work to ensure that all federation operators subscribe to a Metadata Registration Practice Statement that complies with the recommended standard template.

References

[DFNAAI]	https://www.aai.dfn.de/en/der-dienst/degrees-of-reliance/
[eduGAIN]	www.edugain.org
[eduGAIN_Wiki]	https://wiki.edugain.org/Main_Page
[FIM4R]	Daan Broeder et al.: Federated Identity Management for Research Collaborations. http://cds.cern.ch/record/1442597/files/CERN-OPEN-2012-006.pdf?version=2
[InCommon]	http://www.incommon.org/docs/assurance/IAP.pdf
[MNA3.1]	AARC project: Milestone MNA3.1 - Recommendations on minimal assurance level relevant for low-risk research use cases
[NISTSP80063]	http://csrc.nist.gov/publications/PubsSPs.html#800-63-Rev1
[SIRTFI]	https://wiki.refeds.org/display/GROUPS/SIRTFI
[SWAMID]	https://www.sunet.se/swamid/policy/
[VoTWG]	https://www.ietf.org/mailman/listinfo/vot.

Glossary

AARC	Authentication and Authorisation for Research and Collaboration
FIM	Federated Identity Management
IdP	Identity Provider
IGTF	Interoperable Global Trust Federation
LoA	Level of Assurance
REFEDS	the Research and Education FEDerations group
SIRTFI	Security Incident Response Trust Framework for Federated Identity
SP	Service Provider
VoT	Vectors of Trust
VoTWG	Vectors of Trust Working Group