Whitepaper: eduGAIN Futures WG recommendations

Version 0.1: consultation phase
22 June 2022

Contents

Introduction

eduGAIN was established in June 2011 and apart from some fundamental changes during the pilot phases prior to 2011, the operational model has remained relatively unchanged in the 11 years of operation [birthday]. The service has been very successful in achieving breadth of service with 75 member federations currently represented in the service and 8 candidates in the process of joining eduGAIN.

eduGAIN was designed as a lightweight, distributed and multi-lateral federated service. The idea of autonomy for each Identity Federation was built into the design of eduGAIN from the beginning, and eduGAIN did not intend to have any direct involvement in service operation at an entity level - the current eduGAIN Declaration states clearly that “In particular this declaration creates no rights of membership, nor of access to services, between Members of any federation” [declaration]. Technical requirements were designed to be lightweight in terms of the demands placed on the federation.

This process worked well for the initial cohort of eduGAIN federations but as the number of federations has grown, the “hands off” approach has come under deserved scrutiny. The following core issues have been raised on multiple occasions:

eduGAIN Problem Statements

1. With over 8000 entities included in eduGAIN, the number of different variables in the service experience between Identity Provider (IdP) and Service Provider (SP) has become extremely complex.
2. The inability to predict what information will be exchanged between IdP and SP makes it difficult for services to rely on eduGAIN interfederation to offer services.
3. The very different policies, processes and technical architecture (including security) adopted by Identity Federations in how they interact with eduGAIN causes confusion.
4. The different funding, staffing and service levels at Identity Federations makes the service offer variable across the eduGAIN environment.
5. Entities and / or Federation Operators are slow to change and match changing security, regulatory and policy requirements.
6. eduGAIN itself is slow to make decisions and necessary changes to its service model and other technological advances.
7. The mission and role and brand of eduGAIN is unclear, leading to different expectations.

The eduGAIN service teams and the eduGAIN Steering Group discussed these issues at length in various meetings and agreed that a wide ranging review of eduGAIN future service delivery was required and as such set up this Futures Working Group.

Timescales

It is envisaged that these changes will be introduced within a 3 year time frame. Some of the recommendations are already in progress and can be seen as “quick wins” whereas others will take time for both technological change and community adoption.

Radical Future Models

The proposals included in this report are conservative and close to the current service model for eduGAIN; no radical service change or future is considered. The proposals also assume that the business model for eduGAIN will remain the same and that eduGAIN will be predominantly funded via the GÉANT GN5 project and through GÉANT membership fees. This in itself introduces constraints around the changes that can be introduced.

It is recommended that eduGAIN leadership and the eduGAIN community use the development of the eduGAIN Strategy and future planning to challenge the existing service and business model and consider whether more radical changes should be introduced to ensure the service remains relevant and sustainable. Areas that may be considered in the future include:

- Challenge to core service approach: does the eduGAIN model serve the need of the community in the changing identity landscape or is the need for a distributed metadata service declining?
- Challenge to the business model: can a service continue to be effectively run and meet the needs of the community through the constraints of the project structure.

Overview of the Working Group

The eduGAIN Futures Working Group was established to help define a set of recommendations to improve the future service delivery of eduGAIN. The group was open to the following members:

- Any staff member of an eduGAIN Identity Federation.
- Members of the eduGAIN Service staff, including eduGAIN Security Team, Operational Team, Support Team and Secretariat.
- Recognised stakeholders from the wider eduGAIN community that are accepted by the group.

The group was promoted widely to eduGAIN stakeholder groups (REFEDS, FIM4L, FIM4R etc) to ensure representation from as many different stakeholders as possible.

Goals of the Working Group

The following goals were established for the Working Group:

1. To review the REFEDS Baseline Expectations document and make proposals for changes to eduGAIN to support the baseline [baseline].

2. To identify key issues with current eduGAIN service provision and make recommendations for improvements (e.g. support mechanisms for CoCo and R&S, lack of service offer to Service Providers, technology support for OIDC etc).
3. To review the governance model for eduGAIN and make recommendations for improvements.
4. To cross-reference proposals with other working groups and the eduGAIN service teams.

This report sets out the recommendations from the group in each of these areas. All notes and discussion from the working group meeting can be found on the working group wiki pages [futures-wiki].

Recommendations

Implementing baseline expectations - Goal 1

Recommendation 1.1	**Enforce the use of technical, management and security contacts for Federation Operators and implement regular testing for responsiveness of security and technical contacts**
Problem Statement	This addresses problem statement 6
Reference Material	This supports achieving [FO2] You publish contact information and respond in a timely fashion to operational issues
Supporting Evidence	Security challenge results: Out of 33 members that have published their security contacts, 30 answered the challenge. Security contact list 33/74 eduGAIN members
Impact	In case of an incident the newly formed eduGAIN CSIRT is not able to contact the missing eduGAIN members in a secure and trustworthy way

Recommendation 1.2	**Upgrade the eduGAIN technical infrastructure and policy process to allow eduGAIN to filter individual entities as appropriate**
Problem Statement	This addresses problem statement 5
Reference Material	This supports [FO1] You focus on trustworthiness of Federation as a primary objective and are transparent about such efforts
Supporting Evidence	The issue of whole federation streams being blocked due to issues with one entity has been raised by the community on many occasions

Impact	Individual entities have the potential to impact the service capability of other entities - which is not acceptable in a critical infrastructure environment. This recommendation should also consider the potential percentage of a federation feed that can show errors before the entire federation is considered unusable.

Recommendation 1.3	**Support the implementation of the eduGAIN CSIRT and develop robust security incident response practises in conjunction with Identity Federations**
Problem Statement	This addresses problem statement 3
Reference Material	This supports [FO4] You follow good practices to ensure authentic, accurate and interoperable metadata to enable secure and trustworthy federated transactions
Supporting Evidence	The REFEDS Survey tracks increasing interest among federations for security controls and an increased use of incident response plans The eduGAIN CSIRT has made good progress in establishing itself but there is still work to do in terms of understanding the remit of the team in any given security incident and the authority of the team in relation to individual eduGAIN members
Impact	The absence of coordinated incident response could damage the reputation and trust in eduGAIN

Recommendation 1.4	**Define clear guidance as to the required standard for "authentic, accurate and interoperable metadata" for eduGAIN - a review of the eduGAIN SAML Profile to make clear statements about what authentic, accurate and interoperable eduGAIN metadata should be.**
Problem Statement	This addresses problem statement 1
Reference Material	https://technical.edugain.org/documents
Supporting Evidence	Inability to offer SPs a guaranteed response from specific IdPs - experience of trying to connect is too varied.
Impact	Move towards improved interoperability between entities

Recommendation 1.5	**Create a roadmap to upgrade all entities to support Sirtfi, Privacy Requirements, and Assurance and make a formal part of the eduGAIN policy requirements. This should be a staged approach and where applicable (e.g. CoCo might not be used everywhere)**
Problem Statement	This addresses problem statement 5
Reference Material	[FO5] You implement and support frameworks that improve trustworthy and scalable use of Federation and promote their adoption by members and other participants
Supporting Evidence	Initiatives from Service Providers like NIH have pointed to a clear need for consistent standards in entities
Impact	Lack of adoption could lead to lack of access to services for users

Service model discussion - Goal 2

Recommendation 2.1	**Establish 3 consistent profiles to be met by Identity Providers with increasing levels of functionality (anon, pseudon, personalized)**
Problem Statement	This addresses problem statements 1 and 2
Reference Material	REFEDS Specifications: https://refeds.org/specifications
Supporting Evidence	We receive continued complaints from Service Providers that it is impossible to get consistent information from Identity Providers even for basic, low risk PII data exchange. Ensuring eduGAIN can guarantee this for specific sets of IdPs will improve service delivery
Impact	If eduGAIN cannot improve its service offer, SPs will look to alternative offers and platforms

Recommendation 2.2	**Have a consistent approach to how federations are expected to publish eduGAIN metadata upstream and downstream and manage federation metadata refresh**
Problem Statement	This addresses problem statement 3
Reference Material	Different approaches can be clearly seen in MET: https://met.refeds.org/
Supporting Evidence	Service Providers assume that all eduGAIN metadata is consumed by all participating members as evidenced by questions to the eduGAIN helpdesk
Impact	Users are unable to access services which they believe they should be able to access

Recommendation 2.3	**Create an eduGAIN strategy with clear mission statement. stakeholder engagement approach (e.g. with SeamlessAccess, eduTEAMS, REFEDS etc)**
Problem Statement	This addresses problem statement 7
Reference Material	No strategy exists so no reference available
Supporting Evidence	Confusion expressed by many stakeholder organisations
Impact	All stakeholders have different expectations of the service offer available from eduGAIN as this is not clearly articulated (e.g. what is eduGAIN's role in onboarding?, what is eduGAIN's role in compliance and monitoring etc)

Recommendation 2.4	**Improve the structure, communication and usage of the eduGAIN “check” tools**
Problem Statement	This addresses problem statement 5
Reference Material	https://technical.edugain.org/
Supporting Evidence	Lack of response to eduGAIN Support requests and confusion on how compliance is monitored in eduGAIN
Impact	Addressing the delivery and service level for these tools will increase usage and better support users in understanding their purpose

Recommendation 2.5	**Monitor emerging technologies and their interaction with eduGAIN / to ensure that changes in the identity landscape are effectively addressed and a roadmap for supporting new technologies can be created**
Problem Statement	This addresses problem statement 6
Reference Material	n/a
Supporting Evidence	Feedback from groups at meetings such as REFEDS, FIM4R, OIDF etc show that use cases and need for support for OIDC and non-web use cases may be more prevalent than is seen with eduGAIN discussions
Impact	Ensure better dialogue and reaction to requirements outside of the SAML space.

Governance discussion - Goal 3

Recommendation 3.1	**The eduGAIN governance model should be changed to introduce a geographically balanced elected Steering Group, with the current Steering Group changed to an (bi)annual assembly. Additional supporting advisory groups on policy and technical issues should be considered** **Non-member observers from representative groups could also be considered for the new Steering Group**
Problem Statement	This addresses problem statement 6

Reference Material	The eduGAIN Declaration and the eduGAIN Constitution would need to be revised and other policies should be looked at - e.g. dispute resolution
Supporting Evidence	This is supported by low participation numbers at eduGAIN Steering Group meetings and low traffic and response to queries on the eduGAIN mailing lists
Impact	This would have a wide-ranging political impact in terms of changing the terms of reference for eduGAIN but given the low participation in eduGAIN steering, the practical impact would be minimal for those federations not elected

Recommendation 3.2	**Improve consistency and reliability of data held about Identity Federations** **This should include implementation of the eduGAIN report tool, an annual audit process for Identity Federations and a review process when federation policies / people change**
Problem Statement	This addresses problem statement 3.
Reference Material	Outdated information held at: https://technical.edugain.org/ and other sources
Supporting Evidence	Service functionality has been impacted by out of date information and the trust model can be questioned when federations change policy with no review
Impact	Unreliable data on federation degrades the trust fabric

Recommendation 3.3	**Improve the joining process for new Identity Federations**
Problem Statement	This addresses problem statement 3
Reference Material	https://technical.edugain.org/ - joining
Supporting Evidence	Feedback from existing and pipeline federations have highlighted problems with the process
Impact	Federations have joined eduGAIN before they are technically ready and have not been able to properly participate. The joining process can be slow and unclear for participants

References

[baseline]	https://refeds.org/baseline-expectations
[birthday]	https://connect.geant.org/2021/04/21/edugain-at-10-the-star-at-the-heart-of-a-constellation.
[declaration]	https://technical.edugain.org/doc/eduGAIN-Declaration-v2bis-web.pdf
[futures-wiki]	https://wiki.geant.org/display/eduGAIN/eduGAIN+Futures+Working+Group+Charter
[technical]	https://technical.edugain.org/documents
[met]	https://met.refeds.org/