SA5 T1 Recommendations: eduGAIN Policy Changes

Authors: Nicole Harris, Brook Schofield, Rhys Smith

Table of Contents

1. Summary

As part of the GN4-1 Task on Trust and Identity Harmonisation (SA5 T1 project number reference) a review of the existing eduGAIN policy set has been completed. The purpose of the review was to update any processes that are currently not working or have been superseded within the policy set and to review how eduGAIN could become more technology agnostic.

The review has been socialized with various groups that have an interest in eduGAIN and was presented at the eduGAIN Town Hall meeting on 1 December 2015. eduGAIN Steering Group members are now asked to comment on and APPROVE the proposed changes.

2. Recommendations

The following is a summary of the proposed changes:

1. CHANGE the term “federation” within the document set to “federation operator” to more accurately reflect the nature of the agreement.
   Document changes required: **DECLARATION, CONSTITUTION.**
2. CHANGE the construct of the eduGAIN Executive Committee as follows: “The eduGAIN Executive comprises representatives from organisations that fund eduGAIN operations. The current executive is documented (on the eduGAIN website)”.
   Document changes required: **CONSTITUTION.**
3. CHANGE the construct of membership of the SG as follows: “Each Participant Federation should ensure that representatives can represent all technology profiles. Participant Federations may vote on all constitutional changes and new profiles but my only vote on changes to technical profiles they use.”
   Document changes required: **CONSTITUTION.**
4. REMOVE reference to the eduGAIN SG “appointing the Operational Team”.
   Document changes required: **CONSTITUTION.**
5. REMOVE all references to SAML within the Constitution and replace with “relevant technology profile”.
   Document changes required: **CONSTITUTION.**
6. Update the section on the Operational Team to describe relationship with existing SAML trust broker model (e.g. the MDS) and reference future trust brokers.
   Document changes required: **CONSTITUTION.**
7. ENSURE that the Federation Operational Practice Statement for the eduGAIN interfederation service (mentioned in Constitution) and MDS Aggregation Practice Statement [MAPS] (mentioned in existing Metadata Profile) currently referenced in policy are written by July 2016.
8. REMOVE the existing Attribute Profile as a normative document and instead provide a best practice guide for managing attributes that links to entity categories and work in REFEDS

on “meta” attributes.
Document changes required: **PROFILES**.

9. COMBINE the existing WebSSO profile and Metadata Profile into a single SAML Profile, taking care to acknowledge SAML1 issues.
Document changes required: **PROFILES**.

The SG and current Chair of the SG will be asked to how they would like to manage voting for these issues. For the eSG to agree to a revision of this Constitution requires an affirmative vote of at least two-thirds of current Participant Federations. A Simple Majority process can be used to vote on all other issues raised in this document.

3. Detailed Description of Change Requirements.

3.1 Federation “Operator”

The current eduGAIN Constitution defines a federation as “An association of organisations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions”. The Declaration asks “the federation” to commit to a series of statements and to sign the document. It is clear that the intention was not to ask the federation as whole to acknowledge and sign, and most federations do not in themselves exist as a legal entity so have no specific signing powers.

It has become common practice in other documentation to refer to the “Federation Operator” rather than a Federation when asking for commitments. It is recommended that the Declaration and the Constitution be updated to more accurately reflect reality and common practice.

3.2 eduGAIN Executive Committee

The current eduGAIN Constitution names the “GÉANT Exec” as the organization acting as the eduGAIN Executive Committee, but this project function no longer exists so eduGAIN effectively has no ability to sign-off changes at this level. This clearly needs to be rectified. The intention was to give Executive oversight to the organisation(s) funding eduGAIN as an appropriate governance model and not tie to a specific organisation.

It is recommended that no single organisation be named within the Constitution to avoid future issues with changing committee structures. It is also recommended that the document be phrased to allow additional funding partners to join an Executive Committee in the future.

It is recommended that the following word be used to reflect the needs of the eduGAIN Executive Committee: “The eduGAIN Executive comprises representatives from organisations that fund eduGAIN operations. The current executive is documented (on the eduGAIN website)”.

3.3. eduGAIN Steering Group

The current construct of the eduGAIN Steering Group has worked well and should not be changed, but some concern has been expressed about how the SG can effectively represent multiple profiles within eduGAIN that might require different skill sets. It is difficult to assess how this can be managed without real life experience of the way in which different profiles are likely to grow.

It is recommended that the following wording be used to reflect the relationship of the SG to various technology profiles: “Each Participant Federation should ensure that representatives can represent all technology profiles. Participant Federations may vote on all constitutional changes and new profiles but my only vote on changes to technical profiles they use.” This will allow participants to have a say on introducing new profiles into eduGAIN and reflect on the overall impact of the profile on the workings of eduGAIN, but will restrict votes to participants with an active interest once the profile is accepted.

The current eduGAIN Constitution refers to the SG as having responsibility for “appointing the Operational Team”. The SG has never had this right and the OT is appointed by the GN Project process. It is recommended that this reference be removed.

3.4 SAML in Constitution

When writing the eduGAIN Declaration and Constitution, the intention was to create a framework that was technology agnostic. Unfortunately via the many revisions some references to SAML appear in the Constitution (but not the Declaration). It is recommended that all current references to SAML be replaced with the term: “the relevant technology profile”.

3.5 eduGAIN Operational Team

The current eduGAIN constitution describes the Operational Team, but does not mention management of the current trust broker (MDS) in the list of functions. This does not present any specific issues with the current set-up where SAML-only management and the MDS are implied, but could cause issues further down the line when additional trust brokers are introduced. It is recommended that a phrase be added to this section calling out management of the trust broker.

An open issue for consideration is what might happen if a future profile wanted to implement an approach that led to multiple operational teams or different infrastructure management processes.

3.6 eduGAIN Practice Statements

In the current eduGAIN documentation, two eduGAIN Practice Statements are referenced: Federation Operational Practice Statement for the eduGAIN interfederation service (mentioned in Constitution) and MDS Aggregation Practice Statement [MAPS] (mentioned in existing Metadata

Profile). To the knowledge of the authors, these documents have never been written. It is now essential that these documents are created:

- As more and more federations join eduGAIN and publish entities more and more questions about process are being asked. These Statements should address some of the issues with process discussed at recent eduGAIN SG meetings: https://wiki.edugain.org/EduGAIN_SG-20150430 and https://wiki.edugain.org/EduGAIN_SG-2015Oct provide further background.
- As different technology profiles are introduced, it is important that the processes for operation via each profile be clearly addressed.

3.7 eduGAIN Profiles

The current eduGAIN profiles provide a range of guidance around use of SAML within eduGAIN. To support the introduction of further technology profiles and to tidy up existing practice, the following recommendations are made:

- The existing Attribute Profile should be REMOVED as a normative document, as it is not felt to be helpful as a guidance document. This should be replace with best practice advice on managing attributes. This should include references to the various Entity Categories and clear advice on how to manage scenarios where IdPs / federations provide different attribute sets. eduGAIN should work closely with REFEDS in creating this document.

- The existing Metadata Profile and WebSSO Profile should be combined into a single SAML Profile document for ease of management. The creation of this document would be a good opportunity to revisit the very limited set of MUST requirements and whether additional requirements for federations should be added.