17-07-2017

eduGAIN SAML Profile Review

Document history

Revision No.	Description of change	Author	Date of change
1.0	Document drafted	Nicole Harris	17-07-2017

Table of Contents

1 Purpose

The purpose of the eduGAIN SAML profile review has several aims:

- To update the eduGAIN SAML documentation in line with the new eduGAIN constitution and the move to a technology agnostic framework.
- To re-evaulate the need for specific eduGAIN profiles for SAML considering the changing environment since last review.
- To reposition elements of the eduGAIN policy framework as best practice documentation to support the evolving framework.

2 General requirements

When the eduGAIN Policy Framework was written, the SAML profiles documentation considered and called-out several existing SAML profiles created by OASIS. Instead of simply referencing these profiles as requirements for eduGAIN participants, a decision was taken to develop specific requirements for eduGAIN. This reflects the fact that eduGAIN is an interfederation operational environment and needs to focus on the drivers and requirements to make **service operation as effective as possible** for participants. This may differ from other profiles that are driven by more idealistic implementation goals or focus on deployment at the campus level.

With this general aim in mind, the updates for this profile have focused on the following approaches:

- Making as many requirements MUST instead of SHOULD, or removing them from the profile. There is a general misunderstanding or bad implementation of SHOULD requirements and the incentive to implement, and if requirements exist for operational reasons then MUST is a better position.
- Removing requirements that cannot easily be monitored by the eduGAIN OT.
- Moving elements that might be considered “gold standard” rather than operational to best practice requirements.
- Ensuring that all wording is aimed at requirements for Federation Operators rather than requirements for entities – eduGAIN should not dictate entity behaviour but do that through Fed Ops.
- Reviewing the changing SAML profile documentation to reflect on new things that should be brought into the eduGAIN environment.

With this focus, it is important that the eduGAIN SAML profile is closely associated with the eduGAIN Operational Practice Statement and for this document to be published at the same time as the new SAML profile.

3 Aim One

To support aim one, the following changes have been introduced to the documentation:

- One single SAML profile covering all requirements for SAML eduGAIN participants.
- Restructuring the document to reflect the different stages of metadata production, management and publication.
- Strengthened many requirements from SHOULD to MUST. Some remain SHOULD as deemed it would have significant service impact to move to MUST. Federations should be clear on what SHOULD means in this context though and be pushed for implementation.
- Added requirement for Metadata Registration Practice Statement and requirements around scopes (some still to be resolved).
- Introduced some elements that are already operationally required by eduGAIN.
- Removing some elements that cannot be monitored and are general best practice issues (e.g. role based emails).

4 Aim Two

As part of the initial review of eduGAIN, the following profiles were reviewed and are referenced in the eduGAIN policy:

- Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.
- Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.
- SAML V2.0 Metadata Interoperability Profile Version 1.0: http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop-cs-01.pdf.
- SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0: http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/saml-metadata-rpi-v1.0.pdf.
- SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/sstc-saml-metadata-ui-v1.0.pdf.

The following document is included in the eduGAIN Metadata Profile references but is not referenced in any requirement in the main document:

- SAML Version 2.0 Errata 05: http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf.

This should be properly referenced in the documentation with a clear indication if any errata affect eduGAIN recommendations. (outstanding action)

Since the eduGAIN SAML-related profiles were created in 2012 / 2013, there have been some changes to the environment for SAML profile support.

SAML2Int has moved to a new home at Kantara and a working group within InCommon has committed to updating the specification, which will resolve the current known issues with version 0.2. As SAML2Int is a deployment profile predominantly focused on guidance for entities, this will be moved to the Best Current Practice section of the eduGAIN website in the future structure and will not form part of the policy set.

As a companion to SAML2Int, Kantara released the SAML V2.0 Implementation Profile for Federation Interoperability in 2016. This is not intended to define a fix set of behaviours for a given environment, which the eduGAIN profile does intend to do, but the broader set of interoperability features referenced should be reviewed in light of the eduGAIN interoperability requirements. Areas where the Kantara Implementation Profile significantly expands requirements that may be relevant to eduGAIN are keyroller and algorithm support.

Other profiles introduced since the eduGAIN profile was developed are:

- SAML V2.0 Enhanced Client or Proxy Profile Version 2.0: http://docs.oasis-open.org/security/saml/Post2.0/saml-ecp/v2.0/cs01/saml-ecp-v2.0-cs01.pdf.
- SAML V2.0 Asynchronous Single Logout Profile Extension Version 1.0: http://docs.oasis-open.org/security/saml/Post2.0/saml-async-slo/v1.0/cs01/saml-async-slo-v1.0-cs01.pdf.

At this stage it is not seen as necessary to include or expand on any of the requirements In the ECP and Logout profiles in the eduGAIN Policy Framework.

5 Aim Three

To support aim three, a specific Best Current Practice area will be created on the eduGAIN website. This will set out a series of best practice approaches to be agreed with the eduGAIN SG. This is likely to include:

- A best practice document on attribute management, referencing approaches such as R&S and CoCo.
- BCP references for R&S, CoCo, Sirtfi and MFA.
- Possible BCP references for the REFEDS assurance framework depending on timescales.
- References to SAML2Int.

A document agreeing an approach for adding items to the Best Current Practice page will also be agreed.

The eduGAIN WebSSO Profile and Attribute Profile will be removed from the eduGAIN policy set.

This work will happen as phase 3 of the eduGAIN policy review, following the Constitution update (complete) and the SAML profile review (this work item).

6 Questions for the consultation

- Please review the application of SHOULD and MUST to requirements. Would you like to move any in either direction, delete any of the current list or add any addition requirements. Should we maintain any SHOULD requirements at all?
- Would you like to add anything to the eduGAIN profile on keyrollover / algorithm support is the current text on signing requirements sufficient?
- Do you have any comments on the proposed addition of information on scopes to the eduGAIN policy (see existing comments on document).
- The issue with persistent / transient nameIDs is noted. The current preference is not to add any requirements to the eduGAIN policy set on these but work to see this updated in existing SAML profiles.
- Does eduGAIN need to take any specific stand on ECP or logout profiles?
- Are you happy with removing the eduGAIN WebSSO Profile and Attribute Profile from the policy set?