The GN4 project has been undertaking a review of the current SAML documentation used in the eduGAIN policy set and is proposing a revision of a single SAML profile to replace the existing eduGAIN Metadata Profile. It is further proposed that the eduGAIN WebSSO Profile and Attribute Profile will be removed from the eduGAIN policy set and form part of a set of best current practice documentation, which will form stage three of the policy review process.

This is part of a wider review of the full eduGAIN policy set as described on the GÉANT wiki.

The eduGAIN SG will have final approval rights for the document. The following documents are available for this review:

- Proposed eduGAIN SAML profile
- Supporting paper on the process (also copied below). Please note this also contains a set of QUESTIONS you might wish to reflect on.

You can respond to this consultation directly by filling in the table below, commenting on the eduGAIN SG list or sending your comments to nicole.harris@ geant.org.

This consultation is now closed.

<table>
<thead>
<tr>
<th>#</th>
<th>Reference</th>
<th>Comment</th>
<th>Proposer</th>
<th>Actions</th>
</tr>
</thead>
</table>
| 1 | Metadata Signing | In order to assure metadata integrity and originality, each federation aggregate MUST be signed as specified in [Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0]. This signature made with the key matching the one supplied to the eduGAIN OT is the only element on which trust is based. In particular the eduGAIN aggregator does not use trust that might be derived from an https endpoint details.

Metadata signature verification is done against the public key alone. If the public key for the channel is supplied in the form of an X.509 certificate, other aspects of the certificate such as its expiry date do not form part of signature verification. This is in accordance with the SAML metadata interoperability profile. In particular an expired certificate will still be used for the verification purpose. | Tomasz W | Adopt this proposal |
| 2 | Metadata Signing | Include the following:

- The signature was made using an explicit ID reference, not an empty reference. - The signature reference refers to the document element. - The signature's digest algorithm is at least as strong as SHA-256. Specifically, MD5 and SHA-1 are not permitted as digest algorithms. - The signature's signature method is RSA with an associated digest at least as strong as SHA-256. Specifically, MD5 and SHA-1 are not permitted as digest algorithms. - The signature's transforms contain only permissible values: -- Enveloped signature -- Exclusive canonicalisation with or without comments | Tomasz W | Adopt this proposal |
| 3 | Terms (Entity) | Replace exchanged by published in the following sentence:

"In this document, an Entity refers to an entity’s metadata that a Participant Federation has exchanged through eduGAIN." | Thomas L | Adopt this proposal |
| 4 | Terms (Home Organisation) | Replace: “The organisation with which the end users are affiliated.” with: “The organisation with which an end user is affiliated.” | Thomas L | Adopt this proposal |
| 5 | Terms (eduGAIN Policy Framework) | Typo: SAML Profil -> SAML Profile | Thomas L | Adopt this proposal |
| 6 | Terms (SAML V2.0) | Replace: “Security Markup Language” with “Security Assertion Markup Language” | Thomas L | Adopt this proposal |
| 7 | Terms (SAML Metadata) | Sort this term before SAML Metadata Producer. | Thomas L | Adopt this proposal |
| 8 | Terms (SAML Metadata) | This requirement should not be hidden in the Terms, but move to ‘3 Metadata Production’:

"Valid SAML Metadata MUST meet the requirements defined in the SAML Metadata Specification [SAMLMeta] including [SAMLMetaErrata]." | Thomas L | Adopt this proposal |
<p>| 9 | Terms (Metadata Registration Practice Statement (MRPS)) | Drop the second sentence “Every eduGAIN Member Federation must publish an MRPS.”. This requirement is already included in 2 Metadata Registration on line 60. | Thomas L | Adopt this proposal |
| 10 | line 65 | The reference for [REFEDS-MDRPS] is missing. | Thomas L | Adopt this proposal |</p>
<table>
<thead>
<tr>
<th>Line</th>
<th>Text</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>line 84</td>
<td>The reference for [SAMLCore] is missing.</td>
</tr>
<tr>
<td>12</td>
<td>line 88</td>
<td>The reference for [MDRPI] is missing.</td>
</tr>
<tr>
<td>13</td>
<td>line 90</td>
<td>The reference for [MDUI] is missing.</td>
</tr>
<tr>
<td>14</td>
<td>line 103-104</td>
<td>Drop &quot;other values in the service's native languages for the elements where appropriate.&quot; since it is already mentioned on lines 127-128.</td>
</tr>
<tr>
<td>15</td>
<td>A general remark</td>
<td>The current eduGAIN policy is supposed to be technology agnostic, from which it follows that the requirement for the presentation of the federation policy at the moment of joining may be fairly lax. At the moment of enabling a given profile, we should probably require additional documents like a profile-specific part of the federation policy, this should perhaps be mentioned as a required document in the SAML profile?</td>
</tr>
<tr>
<td>16</td>
<td>Metadata registration</td>
<td>I find this somewhat misleading. Other sections of the document refer mostly to how the federation aggregate is produced, signed etc. This section mentions the internal document of a federation which describes how the entities make their way to the federation itself. While I fully support the need to have the registration statement requirement, I would see this particular as an element of something bigger. I would suggest that this section speaks about elements that need to be registered with the OT and which are now mentioned in several places, like the signing key, the registrationAuthority value, the metadata location. This section should state that this information needs to be passed to the OT in a trust preserving way. I would not however specify what this means, this might be specified in the Operations document.</td>
</tr>
<tr>
<td>17</td>
<td>General questions</td>
<td>1. The aim of this profile seems to be to improve interop among entities in different federations by means of defining common practices by fed ops and edugain ops. Interop issues can sometimes result from different filtering policies implemented by different federations when they consume edugain metadata. Examples include federation-specific standards for end point scheme (HTTP vs HTTPS) and minimum key length (1024 vs 2048+). Is this profile the right place at which to define edugain-wide standards for such things? If so, is this the right time to consider doing so in these two instances? 2. Members of federations are advised by their federations' operators to check the signature of their federation metadata to verify its authenticity and integrity. Does eduGain do likewise in the process of aggregating member federations' metadata for redistribution? If not, should it, and if it does not but should, is this profile the right place in which to address that requirement?</td>
</tr>
<tr>
<td>18</td>
<td>Line 111</td>
<td>line 111 change SHOULD to MUST</td>
</tr>
<tr>
<td>19</td>
<td>Key rollover</td>
<td>Chris/CAF: No additions specific to key rollover but a request for improved operational state information on the technical.edugain.org website. No specifics to key rollover but it would be useful to have a way to render a time difference for publishing time on the eduGAIN OT website. Many federations exhibit latency on republishing stemming from operational practices and offline signing techniques. It would be helpful to know in a dashboard fashion the following:  - Last update of mds.edugain.org  - And per federation last known update of eduGAIN data and time difference since MDS publishing. This will go a long way in managing expectations of when to expect data to circulate beyond '24-48hrs'. I suggest a simple table view of flag and age difference from MDS so we may know how far we all drift from each other republishing data from the eduGAIN MDS 'creation date'. While this could exist in the 'twisty list' for each federation, one visual dashboard page of observed latency would be more helpful in this regard.</td>
</tr>
</tbody>
</table>
Scopes

regex scopes should be permitted and eduGAIN should ensure scopes do not collide when accepting aggregates from Members (see longer notes)

There are few legitimate uses of regexp scopes that even UKf accepts. IMO it’s a SHOULD. One should have no worries about the entity being silently discarded somewhere if it violates a SHOULD.

Actually the Scope element is only a subset of the issue of using internet domain names in metadata.

Domain names are significant (in terms of security):
* entityIDs
* endpoint URLs
* scopes

I’d suggest to include a more generic section about using domain names in metadata, and include the special requirement of Scope’s not being a regexp here.

ECP and logout

They MAY exist and should be strongly encouraged with ‘SHOULD’. ‘MUST’ would be very hard to do but having ‘SHOULD’ will keep parity to these features across multiple technologies like OIDC and moonshot. See below for more on this.

BGP recommendations

- Recommended attributes and mapping across the given attribute profiles
- Vocabulary
- Unique identifier practices
- Entity categories (or mapping within given technology profile to exhibit it)
- Consistent application of scope within the technology profiles
- Security characteristics such as position on logout

Metadata Production

The profile pulls in MetaIOP in the section on "Metadata Production": "Whatever is specified as a MUST in the SAML V2.0 Metadata Interoperability Profile should also be considered as REQUIRED within this eduGAIN Metadata Profile." But that’s a rather tall order, because MetaIOP also days (lines 271-273): "Any <md:RoleDescriptor> element (or any derived element or type) appearing in the metadata instance MUST conform to this profile’s requirements." But certain implementations are simply incapable or satisfying MetaIOP, such as MS-ADFS in some versions), e.g. with use of expired keys, or the issue with one key not being able to be part of two EntityDescriptors, etc. So by joining eduGAIN as a Metadata Producer all now MUST support MetaIOP (which is of course a good thing, as that’s the basis for our trust model), but that would actually prevent MS-ADFS and other lesser implementations from participating. (I.e., they wouldn’t be allowed into a federation’s upstream feed.)

References

References should be sorted alphabetically. Glossary could be further trimmed (but sometimes expanded for brevity, e.g. define “Metadata” to mean SAML 2.0 Metadata and only use “Metadata” in the rest of the doc, should save dozens of instances of “SAML Metadata”).

Table of contents: Add

All entity information provided to eduGAIN is considered public information

Proposal: remove requirement/recommendation (and the matching check in the eduGAIN validator) for the

Proposal: remove requirement for the element "eduid:OrganisationURL" to have values in English (xml:lang="en")

Proposal: remove information on <mdrpi:PublicationPath>
I vaguely remember a discussion about dropping the requirement of providing Organization elements in English. I don't remember the outcome, nor I fully understand the sentence `<md:Organization>` with values in English other values in the service's native languages for the elements where appropriate." I feel to miss a conjunction between "English" and "other values".

Kristof B  
slight adjustment made to clarify. See above for more detailed info on previous discussion

Instead of the sentence about validUntil, I'd recommend the following amended paragraph: "A validUntil attribute with a value not later than 2304 hours (28 days) after creationInstant. Under normal operation conditions the validUntil attribute SHOULD refer to a time not earlier than 72 hours (3 days) after creationInstant." (G ->3!)

Kristof B  
Adopted

If present, MDUI MUST meet the following criteria - add logo on publicly accessible site.

from eduGAIN support chat.  
Adopted

Federations MUST provide their members with trustworthy SAML Metadata about eduGAIN Entities, signed with their own signing key.

Peter S

Add a table that includes the namespace prefixes as per: http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop-cs-01.html#1_1__Notation

Peter S

Specify this is upstream metadata. Would need to define upstream metadata or word in such a way to make clear.

Peter S

remove these lines

Peter S

Change to: "the eduGAIN MDS conforms to the rules for Metadata Consumer and Metadata Producers as stated in MetaIOP."

Add a reference to MAPS.

Peter S

Clarify that this is SAML metadata producers.

Peter S

**eduGAIN SAML Profile Review - the Long Read**

**Purpose**

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

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

**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.
- Removing 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.

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).

Aim Two:

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

- 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.pdf.

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


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 Current Best 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.

Aim Three:

To support aim three, a specific Current Best 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 timeliness.
- References to SAML2Int.
A document agreeing an approach for adding items to the BCP 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)

**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 additional 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?