Best Current Practices Guide for Joining eduGAIN as a Federation

Introduction

This page contains information for federations that wish to join eduGAIN. This guide therefore is primarily aimed at operators of academic identity federations, in particular the technical staff members of a federation operator.

This page is structured in distinct steps that are aligned with the eduGAIN joining process. It assists federations to produce all the required information for each step in order to streamline the process for both the joining federations as well as the eduGAIN Operations Team. In addition this page provides best practices, recommendations and implementation options that have proven to work well for other eduGAIN member federations.

Prerequisites

Before actually starting the joining procedure, please ensure that the following prerequisites are given.

Check Requirements

Please read and understand the requirements that your federation meet to join eduGAIN. The requirements are summarized below:

Participant Federations MUST:

- Primarily serve the interests of the education and research sector.
- Provide a point of contact for their Members for dealing with technical issues.
- Provide processes for handling complaints and incidents involving their Members.
- Have a published Metadata registration practice statement.
- Follow the eduGAIN SAML 2.0 Metadata Profile if it decides to exchange the metadata of Entities via eduGAIN (“upstream metadata”).

If you are unsure whether your federation meets these requirements or if you need more information about the requirements, please contact edugain@geant.org.

Opt-In vs Opt-out

Before joining eduGAIN you might want to consider how the entities (Identity and Service Providers) in your federation can join eduGAIN. Adding all of them to eduGAIN might not be reasonable as some of them are certainly used only locally (e.g. federated services used only by users of a single university) and therefore do not have to be part of eduGAIN.

There are basically two choices how entities can be added to eduGAIN from a federation's point of view:

Opt-In

In this model each Service Provider (SP) and Identity Provider (IdP) of a federation has to do something to get included in eduGAIN. Depending on your federation, this might include:

Organisations first have to sign a special interfederation/eduGAIN policy document. This might be necessary because your existing federation policy does not yet cover the case where your SPs and IdPs would be interfederated, thus communicate with SPs and IdPs from other federations abroad.

SPs and IdPs have to apply configuration changes. This can include:

- Loading an additional/different metadata file that contains metadata for the other eduGAIN entities
- Adapting the attribute release policies (IdPs) and attribute mappings (SPs) to also support the international attributes recommended by eduGAIN (link to recomme)
- For SPs: Maybe using a different Discovery Service that also shows the eduGAIN IdPs
- SPs and IdPs might have to tick a checkbox or send an email to the federation operator to make them expose the entities metadata in the eduGAIN metadata upstream (local federation's metadata which then is included in eduGAIN metadata).
- Run a check (especially IdPs, e.g. https://attribute-viewer.aai.switch.ch/interfederation-test/) to ensure that they are ready for and conforming with eduGAIN

The advantage of opt-in is that only those entities are exposed that are really to interoperate with other entities from other federations. For some entities, it might not make sense to be part of eduGAIN. Examples of such entities are

- SPs that require a license (a bilateral agreement with each Home Organisation) or are otherwise scoped to a closed, national community
- SPs that provide a service only in the local language
- SPs that have attribute requirements that are incompatible with the international attribute practices (for instance, the SP consumes eduPersonAffiliation="staff" for granting access to the service, and the semantics of that attribute are heterogenous, as shown in the REFEDS ePSA paper)
- SPs that have Level of Assurance requirements which eduGAIN cannot fulfill

Such entities might not want to opt-in, therefore they don't have to take any steps.

The disadvantage is that opt-in does not scale very well for many entities and it generally takes longer because SP and IdP administrators actively have to do/change something in order to join eduGAIN, which could take years. To motivate entities to get eduGAIN-enabled needs also quite some marketing efforts to make them aware of eduGAIN and to highlight the advantages of taking this step. Especially the latter point is difficult because for the people running an Identity Provider the advantages of becoming interfederation-enabled is less obvious. The IdP administrators sometimes rather see the risks (data privacy, personal data of users sent to services abroad/in another federation) and additional work than the advantages that their users (especially researchers) benefit from.

Opt-Out

Compared to the opt-in model, your SP and IdP administrators in the opt-out model don't have to do anything specifically (legal or technical) to be exposed to eduGAIN. Typically this only works if the federation policy already allows the federation operator to use this model when becoming an eduGAIN member federation.

To use this model, there are a few conditions that have to be met before taking this step:

- The federation policy should allow the federation operator to add entities to eduGAIN and/or to integrate eduGAIN entities in the local federation's metadata
- All entities load and regularly/automatically update metadata provided by the federation operator. This allows the federation operator to just include all eduGAIN metadata to make the local entities also communicate with eduGAIN entities. Entities that opt-out, then have to load a different set of metadata, which only includes entities of the local federation.
- The attributes used in that federation ideally are a super-set of those attributes recommended to support in eduGAIN. Having IdPs support additional attributes usually takes a long time.

If Opt-out is also chosen for SPs, you also have to be aware that your central Discovery Service might have to be adapted to also show eduGAIN Identity Providers.

The advantage of this model is that it saves work for everybody involved. The federation operator because he can accelerate the eduGAIN-adoption considerably without much marketing efforts (the federation participants should though be clearly informed about this step and its consequences). The administrators of affected entities generally don't have to do much. What they can and in some cases should do is:

- SP administrators should revise their access control policies
- SP administrators might consider using a different (better scalable) Discovery Service or restrict the IdPs that are shown in the Discovery Service to those whose users actually should be allowed access to the service
- IdP administrators should revise the attribute release policies and ideally add rules to release attribute based on the GÉANT Data Protection Code of Conduct and REFEDS Research & Scholarship entity categories.

The disadvantage of this approach is that the federation operator needs initially to do more work to carefully plan this move. What happens otherwise is that entities are exposed to eduGAIN which are not really ready for eduGAIN. Be it that they don't load/update metadata containing other eduGAIN entities, be it that their access control rules are too wide, be it that attribute release is not configured well and thus users cannot really access eduGAIN services. All of these cases deteriorate not only usability and reputation of eduGAIN but also that of the local federation. Therefore, this should be avoided if possible.

Before applying the opt-out model, it is recommended to leave administrators of the affected entities several weeks time to opt-out before their entity is published to eduGAIN. It also might make sense from a federation operator's point of view to remind some entities specifically to consider an opt-out. This is especially true for SPs that are used internally only or for IdPs whose users are very unlikely to access eduGAIN services.

What kind of federations have adopted opt-in or opt-out?

An overview of which federation has chose which model is available on the Metadata Upstream/Downstream page. Practice has shown that federations who have a comprehensive and protective local policy framework in place tend to be inclined to take an opt-in model, because

- the local policy introduces data protection requirements for SPs registered to the federation and the Home Organisations assume all SPs are following those. In an opt-out model the IdPs would be exposed to a lot of SPs who are not.
- the local policy framework introduces requirements on Level of Assurance and attribute semantics and population for Home Organisations registered to the federation and the SPs assume all IdPs are following those. In an opt-out model the SPs would be exposed to a lot of IdPs who are not.
- the local federation policy has a clause that the federation operator must ensure that all Home Organisations and SPs (present in the federation metadata) are committed to the local federation policy.

There are also federations that do not have comprehensive local policy and focus mainly on the technical infrastructure (reliable SAML2 metadata exchange and delivery). For them, adopting an opt-out model is more straightforward.

Recommendation: IdP Opt-Out, SP Opt-In

In the recent years, more and more federations (e.g in Sweden, France, Italy) have decided to move from an opt-in model to an opt-out model. The opt-out model can be implemented for IdPs only or both, IdPs and SPs. For operators of eduGAIN services it is important that many organisations and their users can log in via eduGAIN. Having many Identity Providers in eduGAIN is therefore preferable. On the other hand, only services should be accessible via eduGAIN that also are configured properly to be accessed via eduGAIN. Therefore, a good choice is to use the opt-out model for IdPs and an opt-in model for SPs.

Also have a look at the section *eduGAIN Upstream metadata* on how to best handle eduGAIN upstream and downstream metadata that is affected by the opt-in or opt-out choice.

"*RENATER has good experience with this hybrid model (IdP Opt-out, SP Opt-in). It really makes sense for SPs to decide to join eduGAIN and anyway they need to use a different discovery service for eduGAIN and that's the most visible part of the eduGAIN participation iceberg. Doing Opt-out for IdPs really makes sense because Virtual Organisations (VO) are expected to become the lion share of eduGAIN SPs and VO members represent only a small number of person per institution; it would be hard for VOs to convince one institution to join eduGAIN.*"

-- Olivier Salaün from RENATER, the federation operator for France

Read the eduGAIN Policy

Federations willing to join eduGAIN should read, understand and accept the eduGAIN Policy documents. The eduGAIN policy consists mainly of two documents:

- eduGAIN Constitution
- eduGAIN Declaration

On the eduGAIN Resources page there are four further optional profile documents available. Even though they are optional, it is strongly recommended to implement these profiles because they improve the interoperability with other eduGAIN entities. This reduces the number of problems and thus benefits you and the users of your federation. The profiles are summarised below:

eduGAIN Metadata Profile

The eduGAIN metadata profile defines rules for SAML metadata producers that plan to submit their metadata to the eduGAIN Metadata Service (MDS) for aggregation. It is based on the OASIS SAML V2.0 Metadata Interoperability Profile Version 1.0 and intends to facilitate scalable SAML interoperability between eduGAIN participants.

eduGAIN Attribute Profile

This is the recommended profile for end users' attributes exchanged throughout the eduGAIN service. This profile covers only the Web Single Sign-On scenario.

eduGAIN SAML 2.0 WebSSO Profile

This optional profile defines the SAML 2.0 Web Single Sign-on Protocol Profile for the eduGAIN Service. It currently is a pointer to the SAML2int (link http://saml2int.org/) profile as this is the only allowed SAML 2.0 profile to be used in eduGAIN. SAML2int is a SAML 2.0 Interoperability Deployment Profile that defines a minimum set of bindings and rules that needs to be followed by entities participating in eduGAIN with regards to which bindings should be used, which parts of the SAML messages should be signed or encrypted and how, etc.

GÉANT Data Protection Code of Conduct

The Data protection Code of Conduct describes an approach to meet the requirements of the EU Data Protection Directive in federated identity management. The Data protection Code of Conduct defines behavioral rules for Service Providers which want to receive user attributes from the Identity Providers managed by the Home Organisations. It is expected that Home Organisations are more willing to release attributes to Service Providers who manifest conformance to the Data protection Code of Conduct.

Local Federation participants

Federations willing to join eduGAIN should already have at least one (1) participating entity Identity Provider and this should be reflected in the federation's metadata.

Establish a secure communications channel

All email sent to the eduGAIN Operations Team for registration purposes and future updates must be signed with a personal certificate. Only certificates from CAs listed in TACAR service are accepted.

If you cannot get such a certificate to send signed emails or if your personal certificate is issued from a CA not listed in the TACAR service, please contact the eduGAIN Operations Team in order to establish a different secure communications channel.

Joining Steps

Registration of interest in joining eduGAIN

General

The first steps towards joining eduGAIN is to register the Federation's interest in joining by communicating this to the eduGAIN Operations Team.

Contact Details

Contact details (email address, full name) for eduGAIN related matters. Please keep in mind that the assigned contacts should be available for comments and information for the whole duration of the process to join eduGAIN.

Federation Action List

Send an email message to edugain@geant.net stating the interest to join eduGAIN and containing the contact details defined above.

Expected Outcome

The eduGAIN Operations Team receives the registration of interest from the federation and works with the responsible person defined in the contact details sent in order to establish a secure communications channel.

Note:

In general, it is strongly recommended that the federation operator during the joining process and afterwards reacts quickly on email requests from the eduGAIN operations team or other eduGAIN members. Federations that don't react in a timely manner on questions regarding their federation, are considered less trustworthy because in case of a security incident or another eduGAIN-realted problem, a quick reaction is essential.

Sign the eduGAIN Policy Framework Policy Declaration

General

The joining federation needs to read, understand and accept the Policy Declaration document for the eduGAIN Policy Framework.

Requirements

The Policy Declaration document for the eduGAIN Policy Framework (available on the eduGAIN documents page).

Federation Action List

A person who is authorized to represent the federation should sign the printed document and send it to the postal address of the eduGAIN Operations Team:

```
eduGAIN c/o GÉANT
Level 6
Hoekenrode 3
1012BR Amsterdam
The Netherlands
```

A scanned version of the signed declaration should be sent via signed email to the following address edugain@geant.net.

Expected Outcome

eduGAIN Operations Team receives the signed Policy Declaration document from the joining Federation.

Provide the necessary Federation information

General

Now that the secure communication channel has been established between the eduGAIN Operations Team and the joining Federation, the rest of the necessary information should be exchanged.

Being an eduGAIN member federation on a technical level mostly means exchanging SAML2 metadata with eduGAIN. There are basically two metadata files exchanged between a federation operator and eduGAIN.

eduGAIN Upstream metadata

The upstream metadata contains all entities (IdPs and SPs) of a member federation that should be included in eduGAIN metadata. The upstream metadata is provided by the federation operator for consumption by the eduGAIN Metadata Distribution Service (MDS).

Most federations don't publish all their entities in eduGAIN metadata. This might have legal and technical reasons (see sections about opt-in vs opt-out). Even if a federation chooses the opt-out model described above, this means that not all entities of that federation will be part of eduGAIN. Therefore, there will almost always be a separate metadata file that is aggregated by eduGAIN MDS. This file does not have to be public on your web page, but it certainly will be public on the eduGAIN technical page.

The eduGAIN Metadata Profile contains useful information what should be published about entities that you add to eduGAIN. It is strongly advised that all recommendations ("SHOULD") are implemented. Many problems and issues around eduGAIN stem from the fact that the recommendations are not implemented. E.g. ensure for example that all Service Providers from your federation publish which attributes they request. Otherwise, they most probably won't get any, which causes login problems for end users.

eduGAIN Downstream metadata

The eduGAIN Downstream metadata contains all entities in eduGAIN. It is generated and published by the eduGAIN Metadata Distribution Service (MDS), see https://technical.edugain.org/metadata for details.

The downstream metadata is needed because you federation's entities that are part of eduGAIN should also consume metadata about other eduGAIN entities. Therefore, you as federator operator should provide your entities with that downstream metadata. It is strongly recommended to provide an own version of eduGAIN metadata to your local entities and not directly make them consume from MDS. Consuming eduGAIN metadata directly from MDS is considered bad practice for several reasons. MDS was not built to serve metadata to potentially thousands of entities. Also, you as federation operator lose the ability to filter out eduGAIN entities that for example are not compliant with your federation policy. Furthermore, this might result in conflicts because your entities might load metadata for other eduGAIN entities of your federation twice (once via MDS and once via your local federation's metadata).

Providing a separate eduGAIN metadata file has also the advantage that you can also split metadata in two files, one for your SPs and one for your IdPs. Given that eduGAIN metadata has grown quite large, this mitigates scalability issues. Federations are advised to remove their local federation's SAML entities from the eduGAIN downstream metadata in order to avoid having duplicate entity listings.

Some federations choose to integrate eduGAIN metadata directly in their federation metadata or create two metadata streams: one containing local entities only and one containing local+eduGAIN entities. This is especially the case for federations that choose the opt-out model.

For federations that choose the opt-in model, an alternative is to provide separate metadata files containing entities of the local federation and eduGAIN entities.

Information on how to republish the eduGAIN downstream metadata can be found in Republish eduGAIN Metadata.

Metadata Signing Certificate

eduGAIN collects the metadata of all the participating federations, re-signs and publishes the aggregated metadata for the interfederation so that it can be consumed by all the participating Federations. In order to be able to validate the integrity and authenticity of the Federation's metadata, the eduGAIN Operations Team needs to receive the certificate with which the Federation signs it's locally aggregated metadata.

Governance Information

eduGAIN is governed by the eduGAIN Steering Group (see eduGAIN governance). Each federation should assign one delegate and at least one deputy to participate in the eduGAIN Steering Group (eSG). The eSG decides for example if a new federation is accepted as eduGAIN member or not. Therefore, there role of a delegate serves an important purpose.

Federation Online Presence

Each Federation should have an online presence with information regarding the federation structure, the participating entities, etc. It should also define an English Metadata Registration practice statement for the federation. This document must describe rules and procedures used for registering entities which get exposed to eduGAIN. Finally the policy of the Federation should be made available. The relevant documents for the existing federations, which are available here , can be consulted when authoring the Federation Policy and the Metadata Registration practice statement. The templates from REFEDS also provide an excellent starting point for your federation's Policy and Metadata Registration Practice Statement

Requirements

- The URL where the Federation publishes its metadata.
- The signing certificate with which Federation metadata is signed.
- The full names and email addresses of the delegate and the deputy delegate of the Federation.
- The URL pointing to the website (English version, if available) of the Federation.
- The URL pointing to the English version of Metadata Registration practice statement for the federation.
- The URL pointing to the English version of the Federation's policy.

Federation Action List

Compose the information of the items described in the requirements section above and send them via signed email to the eduGAIN Operations Team

Expected Outcome

eduGAIN Operations team checks the provided information. They verify that the Federation's locally aggregated metadata are syntactically correct, that the provided URLs are valid and correspond to the required information. A reply is sent to the joining Federation indicating whether the information provided is correct and sufficient and requesting modifications or updates if necessary.

Finalization of the joining process

Once the joining Federation has successfully completed all the steps indicated above and eduGAIN Operations Team has received the required information, a final approval is required by the eduGAIN Steering Group (eSG). The current procedure is that five members of the eSG are chosen to examine the application of the new candidate federation.
The members are selected alphabetically cycling through the list of existing members. In particular they will inspect metadata, the web page, the federation policy, the metadata practice statement and other aspects of your federation. They then will send recommendations and questions to the eSG mailing list. They also might ask for more information. As mentioned, it helps if you reply to questions quickly as this demonstrates that you as a federation operator are likely to also be responsive in case of security incidents or other eduGAIN-related emergency situations.

Finally, the eSG will vote on the application. If the vote is successful, the eduGAIN Operations Team adds the newly joined Federation to the Metadata Distribution Service (MDS) production service and updates the eduGAIN participant list.

Finally an email notification is sent to the federation announcing the successful completion of the joining process.

Post Joining

When the federation has successfully joined eduGAIN

Disseminate information regarding eduGAIN

You can perform the following steps to make your community aware of eduGAIN

- Write guides for your SPs and IdPs on how to make use of eduGAIN and publish them on your federation's website. See for example the following guides:
  - SWITCH: https://www.switch.ch/aai/support/documents/interfederation/
  - RENATER: https://services.renater.fr/federation/docs/fiches/edugain
- Organize events, trainings for your community.
- Create mailing lists when eduGAIN related issues will be discussed.

Stay updated

You can perform the following steps to stay updated with the latest discussions/events:

- Your federation's deputy and delegate should register to the eduGAIN steering group mailing list
- Your federation's deputy and delegate and possibly other key members of the operations team should register to the following mailing lists:
  - edugain-discuss@lists.geant.org
  - refeds@lists.refeds.org
  - fog@lists.refeds.org