[ARCHIVED] Service Provider Simplified Registration to eduGAIN

WARNING The procedure described below is not active anymore. Please refer to How_to_Join_eduGAIN_as_Service_Provider for information on Service Provider registration to member federation.

Relevant Links

- Wiki page with process instructions: https://wiki.edugain.org/How_to_Join_eduGAIN_as_Service_Provider
- Agreement with UK Access Management Federation

Metadata Processing Instructions/Checklist

This checklist describes what happens if an SP operator submits metadata during the Easy SP Registration workflow using the UK Access Management Federation as federation of last resort.

Process Overview

The process starts for the Support team with a registration request that by an SP administrator on the web page How to Join as Service Provider, to the mailing list simplified-registration@lists.geant.org and from there to support@edugain.org. From this point on the goal of the Support team should:

1. Check the submitted metadata and contact details using the below
2. Enquire SP admin about missing/ aspects of request if needed
3. Forward the validated metadata to the UK Access Helpdesk (service@ukfederation.org.uk) via email with the template Email in Appendix A1 to include it in their federation metadata and . It that at this point the SP administrator already completed applied already for membership in the UK Access Management Federation as described in Step 2 of the Step-by-Step guide. that the Service Provider and fully functional.

To process a registration request, the Service Levels described in Appendix A2 apply as agreed with the UK Access Management Federation.

Checks

When receiving a new SP registration including contact details and metadata as in the form on the Step-by-Step guide, the following checks should:

Legit Registration Check

- Check if registration is real and plausible.
  - If registration is likely to be from a (SPAM) bot, ignore it
  - If it is unclear whether the registration is real, ask back

Manual Checks

- Check if `s name is valid using the domain name of the contact email address to check whether there a web page for that domain name (appending www. to name). If page or company name don’t match or are obscure in another way, ask the contact why there is a mismatch.
- Check whether does already exists in (using MET: http://met.refeds.org/) If it already exists, inform the contact that his SP in via federation XY. Therefore, no additional registration of this SP . (This step could also and built into the metadata submission form in case there would be many SP registrations)
- Check that the submitter owns the email address they entered by sending a verification email can later on

Metadata Checks

The goal of these checks are to ensure that submitted metadata is valid and to ensure that it also contains all the required elements plus ideally the optional elements from the Metadata Profile

- Use validation tool to ensure that metadata is well-formed and valid according to the used SAML2 schemas. using all SAML2-related /schemas listed in Appendix A3. One could use the SAML tools provided here (https://code.geant.net/stash/users/switch.haemmerle/repos/saml-tools /browse/xml-validation) or use for example , an Java-based XML manipulation tool , an Java, an Java
- Open the service’s URL (e.g. using the URL used in one of the ) to open the service’s web page and check if the service is running and providing more or less what the service’s name and description imply
- See if the service has the REFEDS Research & Scholarship (R&S) entity category set.
  - If the category is set, leave it up to the UKAMF helpdesk to validate if the requirements are met the category is set met the category is set are met
  - If the category is not set, judge yourself using the criteria (section 4) of the category is not set the category is not set the category is not set
- https://refeds.org /category/research-and-scholarship if the R&S entity category would be applicable for this SP. If so, change metadata to include this. be applicable be applicable
ToDos and Future developments for Registration Form

This section contains ToDo’s and future improvements. The latter are features to implement only if there is a need or request for them.

ToDos

- JavaScript-Captcha to prevent bots submitting form

Future improvements

- Add samlmetajs to check SAML metadata and show a warning in case of invalid metadata but still allow submission of the form.

Appendix

A1. Mail template to forward registration after successful check

Mail to: service@ukfederation.org.uk

Subject: New eduGAIN registration for

Body:

Dear UK Access Management service desk

The eduGAIN Support team has received a request to register the following service as eduGAIN service via the UK Access Management federation. We have done some preliminary precheck of the SAML2 metadata and kindly ask you to guide the contact person (details provided below) through your registration process. Please keep support@edugain.org also in the loop.

Contact details:

<insert contact details here>

Metadata:

(is attached to mail)

Best regards

eduGAIN Support Team

A2. SLA and Metrics

The following Service Level Agreement (SLA) and Metrics were agreed with the UK Federation: The following Service Level Agreement is applicable during the pilot:

- Availability of service infrastructure (metadata aggregate MDA and the Central Discovery Service CDS): target is 99.5% (excluding service-affecting maintenance, which is capped at 0.5%)
- Response time of all email enquiries (time till an automated ticket number is issued): target is 4 hours
- Response time of all email enquiries till a reply is sent: 2 working days
- Membership applications processing time once all required information has been received: target is 5 working days (due to the fact that membership application from some SPs might be complicated)
- Time till registered UK Access Management Federation SPs are recorded in the UK Access Management Federation and eduGAIN: target is 2 working days During the pilot data for the above metrics should be collected to evaluate and tune the SLA if necessary.

A3. Schema/Namespace to check against

- http://www.w3.org/2000/09/xmldsig#
- http://www.w3.org/2001/10/xml-exc-c14n#
- http://www.w3.org/2001/XMLSchema-instance
- urn:oasis:names:tc:SAML:2.0:metadata
- urn:mace:shibboleth:metadata:1.0
- urn:oasis:names:tc:SAML:metadata:mrpi
- urn:oasis:names:tc:SAML:metadata:rpi
- urn:oasis:names:tc:SAML:metadata:ui