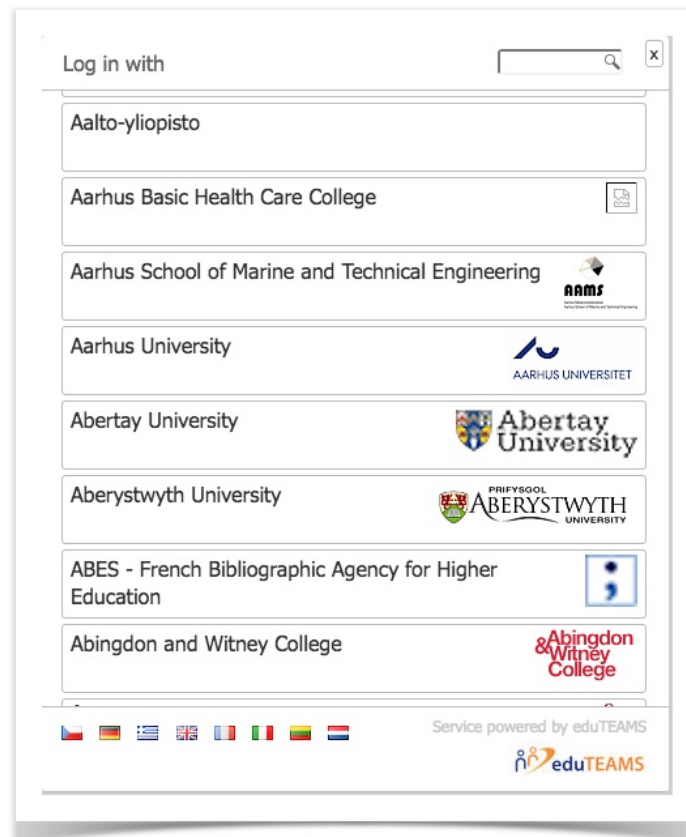


12-04-2019

eduTEAMS Discovery Service Feedback Report



Grant Agreement No.: 85672
Work Package: WP 5
Task Item: Task 2
Nature of Deliverable: Report
Dissemination Level: CO (Confidential)
Lead Partner: SWITCH
Document ID: Discovery Service, WAYF, SAML
Authors: Lukas Hämmerle (SWITCH)

© GÉANT Association on behalf of the GN4-3 project.

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Table of Contents

1	Introduction	2
2	Survey	4
3	Responses	6
4	Conclusion	11
	References	11
	Glossary	12

1 Introduction

This report gives an overview about the feedback received by the users of the eduTEAMS Discovery Service [ETDS]. The eduTEAMS Discovery Service is a service that was deployed in the GÉANT 4 phase 2 project [GN] by the JRA3 Task 2 (“eduGAIN Service Development: e-Research and Service Providers”). The prospect service aims at providing a generic purpose Identity Provider (IdP) discovery service that can be used by all SAML Service Providers (SP) in eduGAIN that support the SAML2 Discovery Service protocol [IDPDS]. The need to offer such a service was identified by a “Market Analysis for Virtual Organisation Platform as a Service” [VOPaaS] conducted with the help of several research communities during the GÉANT 4 phase 1 project. The market analysis was the basis to create the GÉANT eduTEAMS service bundle [ET], which consists of a bundle of services that help research and other communities to make better use of eduGAIN.

1.1 Service History

The eduTEAMS Discovery Service was created in 2018 after an evaluation of several SAML Discovery Service implementations. Eventually the decision was taken to rely on the CESNET Discovery Service [CDS] as a basis and ask CESNET to operate the service on behalf of GÉANT in the context of the eduTEAMS service bundle. The key points in favor of the CESNET Discovery Service were:

- It can be used as central discovery service but also as embedded discovery service
- It is easy for an SP to embed the discovery service via a JavaScript
- It had been operated reliably and stable in production for years
- It supported some of the state of the art interface elements
- It supported multiple languages
- It was designed in a very privacy preserving way because the operator of the service will not know which IdP/organisation a user selects
- It provides a very innovative (per SP configurable) IdP filtering mechanism to display only a subset of all IdPs in the list of organisations
- It was offered by CESNET to be operated on their already highly-available infrastructure

CESNET had already reliably operated this discovery service for their own eduID.cz federation for several years. Therefore, the eduTEAMS Discovery Service could be deployed with only a few modifications as separate instance operated on the same highly-available infrastructure as the eduID.cz discovery service. Once deployed, a few user interface improvements and extensions requested by the eduTEAMS product owner were implemented over the next few months.

The service was then officially announced in December 2017 via the eduGAIN Discuss mailing list¹ and again in June 2018 at the TNC 2018 conference in a lightning talk². Thus, efforts to advertise the service have been very limited because strategy changes of the eduTEAMS service resulted in some key stake holders suggesting to separate the discovery service from the eduTEAMS bundle. This would consequently imply renaming and move the discovery service, which is easier with a smaller user base. Despite little marketing efforts over the months an increasing number of SAML Service Providers started to rely on the eduTEAMS Discovery Service.

1.2 Strategic Reevaluation

With the start of the GÉANT 4 phase 3 project the topic of Identity Provider discovery needs to be reviewed again because it was decided not to include a discovery service in the production eduTEAMS service bundle and because the results of the RA21 initiative [RA21] is likely to change the IdP

¹ <https://lists.geant.org/sympa/arc/edugain-discuss/2017-12/msg00008.html>

² <https://tnc18.geant.org/core/presentation/216>

discovery landscape. RA21 aims at revolutionizing the IdP discovery process introducing a new architecture that could compete with or extend the current eduTEAMS Discovery Service.

To get some data on the usage and the satisfaction of those SP operators that have already started using the eduTEAMS Discovery Service, a survey was conducted. The following chapters describe the survey and its findings in detail.

2 Survey

The survey's aim is to get some first-hand feedback that could help decide where to focus efforts in the IdP discovery topic. The number of Service Providers that had made use of the eduTEAMS Discovery Service was rather small since its announcement.

2.1 Target Audience

To conduct the survey all Service Provider entityIDs were collected from the logs between August 2018 and March 2019. Only services with at least 20 SAML Discovery Service requests were considered. The resulting entityIDs of services that were invited to provide feedback are:

Requests	SP / entityID
15152	eduroam Visitor Access (eVA) SURFnet https://eduroamvisitoraccess.org/simplesaml/module.php/saml/sp/metadata.php/edugain-sp
5163	Clarivate Analytics SP (Web of Knowledge & EndNote Web) https://sp.tshhosting.com/shibboleth
4511	IRMA attributes https://privacybydesign.foundation/simplesamlphp/module.php/saml/sp/metadata.php/surfnet
438	SAFIRE Test Service Provider https://testsp.safire.ac.za/Shibboleth.sso/Metadata
205	eduTEAMS Membership Management Service https://registry.eduteams.org/shibboleth

145	LHCONE Development Grafana Dashboard https://grafanadevel.lsd.fkit.edu/sp
121	Haka Attribute Test Service https://rr.funet.fi/attribute-test
51	LIGO Scientific Collaboration Proxy https://saml-proxy.ligo.org/sp
22	eduTEAMS HEXAA Membership Management Service https://eduteams.hexaa.eu/shibboleth

Table 1: Services ordered by IdP Discovery Requests from August 2018 - March 2019

Some of the above services were no longer in eduGAIN at the time when the survey was conducted.

To contact the service operators via e-mail, the technical and/or support contact from the SPs were extracted from eduGAIN metadata via the eduGAIN Entities Database [EED]. In case of the service 'Clarivate Analytics SP' the operators of the SURFconext federation were contacted instead of the actual service operators because this service provides a list of Discovery Service to end users depending from which federation they are from. In case of Dutch users, it was SURFconext that provided Clarivate the Discovery Service URL of the eduTEAMS Discovery Service.

2.2 Questions

The service contacts were asked via e-mail (sent by the author on March 28th 2019) to provide a statements on the following questions:

- A. How did you get aware of discovery.eduteams.org?
- B. Why did you start using it and not another discovery service?
- C. Are you and are the users of your service happy with the eduTEAMS Discovery Service?
- D. Do you plan to continue using it, maybe also for other services?
- E. Do you have non-eduGAIN services for which you also would like to use the eduTEAMS Discovery Service if it supported non-eduGAIN IdPs?
- F. Which features do you particularly like about it?
- G. What could make the service even better for you?
- H. Are there any other comments you have for the developers/operators?

3 Responses

Within a week 7 out of 9 recipients responded via e-mail (77% response rate). Another reminder was sent to the remaining 2 service operators after a week. As the survey questions were sent in text form in a personalized e-mail messages to the (technical) service contacts, the responses sometimes did not address all of the survey questions but still provide valuable inputs to get the SP operators perspective on the discovery service.

Find below the responses, which were slightly redacted (removed salutation/signature, corrected spelling errors, added missing text for better understanding in square brackets):

Service: **LIGO Scientific Collaboration Proxy**

Responder: Paul Hopkins <paul.hopkins@astro.cf.ac.uk>

Response:

I have been using the eduTEAMS Discovery Service with a SAML Proxy that I have been piloting as part of the AARC2 project.

A. How did you get aware of discovery.eduteams.org?

Niels van Dijk [former eduTEAMS product owner], who is also part of the AARC2 project, suggested I could use it.

B. Why did you start using it and not another discovery service?

I have also set-up a Discovery service which will eventually know about both the eduGAIN and LIGO entities, but when my proxy was published in eduGAIN this was not ready so I used the eduTEAMS service.

C. Are you and are the users of your service happy with the eduTEAMS Discovery Service?

Yes, but it has only been used in testing by myself.

D. Do you plan to continue using it, maybe also for other services?

There is no plan to continue to use it. I actually switched away from it a couple of weeks ago.

E. Do you have non-eduGAIN services for which you also would like to use the eduTEAM Discovery Service if it supported non-eduGAIN IdPs?

We do have non eduGAIN services which would use both eduGAIN and non eduGAIN IdPs, but that is why we are developing a SAML proxy.

F. Which features do you particularly like about it?

[No response]

G. What could make the service even better for you?

[No response]

H. Are there any other comments you have for the developers/operators?

Thanks for reaching out to us, I appreciate that it provides a useful service to us, and others.

Service: LHCONE Development Grafana Dashboard

Responder: Andreas Petzold (SCC) <andreas.petzold@kit.edu>

Response:

A. How did you get aware of discovery.eduteams.org?

I was looking for a ready to use discovery service and was reading existing documentation of DFN-AAI and GÉANT. On the GÉANT web pages I found discovery.eduteams.org.

B. Why did you start using it and not another discovery service?

Very easy to use and absolutely no work for integration.

C. Are you and are the users of your service happy with the eduTEAMS Discovery Service?

Yes!

D. Do you plan to continue using it, maybe also for other services?

Indeed, I'm planning to use it also for a new production service.

E. Do you have non-eduGAIN services for which you also would like to use the eduTEAM Discovery Service if it supported non-eduGAIN IdPs?

Not yet, but it would be great to have the possibility, if we should ever have the need.

F. Which features do you particularly like about it?

Ease of integration into the local service.

G. What could make the service even better for you?

[No response]

H. Are there any other comments you have for the developers/operators?

[No response]

Service: Clarivate Analytics SP (Web of Knowledge & EndNote Web) and IRMA attributes

Responder: Joost van Dijk <joost.vandijk@surfnet.nl>

Response:

Error! No text of specified style in document.

Document ID: Discovery Service, WAYF, SAML

“Clarivate Analytics, Web of Knowledge & EndNote Web is a service from <http://ukfederation.org.uk> that I am not familiar with.

I see that their login page lists several federations, and redirects to these federations’ discovery services.

SURFconext doesn’t have a Discovery Service currently, we are a hub & spoke federation and use a discovery service on our proxy instead.

Maybe Clarivate has its login page configured with federations and corresponding discovery services, and uses discovery.eduteams.org as a fallback for federations without a discovery service ?

I guess it is best to contact their Technical Support at science.ShibbolethSupport@Clarivate.com to find out.

As an additional note: I have known of the eduTEAMS Discovery Service since TNC18 from the lightning talk by Jan Chvojka. We have actually used it for our IRMA SP (Privacy by Design Foundation) as we were having trouble with DiscoJuice.”

Comment: We did contact Clarivate Support as well but have not received a reply from them.

Service: **Haka Attribute Test Service**

Responder: Timo Mustonen <timo.mustonen@csc.fi>

Response:

“I cannot remember how did we find discovery.eduteams.org, it has been used with our attribute-test quite a while now. This solution was available, did the tricks we wanted it to do, and so far there has not been any need to look for replacement for it. I cannot recall any complains, so I would say users are happy with the current solution. We haven’t any plans or a need to abandon discovery.eduteams.org as a discovery service solution for our attribute-test.”

Service: **eduTEAMS HEXAA Membership Management Service**

Responder: Mihály Héder <mihaly.heder@sztaki.mta.hu>

Response:

A. *How did you get aware of discovery.eduteams.org?*

Because we operate an eduTEAMS service it was obvious to rely on the eduTEAMS Discovery Service for IdP discovery .

B. *Why did you start using it and not another discovery service?*

It was faster and had better UX [user interface] than the stock pyff-disco at the time

C. *Are you and are the users of your service happy with the eduTEAMS Discovery Service?*

Yes, very, no issues at all

D. Do you plan to continue using it, maybe also for other services?

Yes and yes, if there is a new eduGAIN SP we deploy we will use it

E. Do you have non-eduGAIN services for which you also would like to use the eduTEAM Discovery Service if it supported non-eduGAIN IdPs?

Yes, absolutely, we have SPs that need local federation IdPs that are non-eduGAIN IdPs and this prevents us from using the eduTEAMS discovery service.

F. Which features do you particularly like about it?

To be frank, mostly that I don't need to configure anything

G. What could make the service even better for you?

[Support for] non-eduGAIN IdPs

H- Are there any other comments you have for the developers/operators?

I have not seen a single downtime, congratulations to the operators!

Service: **eduroam Visitor Access (eVA) | SURFnet**

Responder: Paul Dekkers <paul.dekkers@surfnet.nl>

Response:

"I can already share how I heard about eduTEAMS; I was complaining to our SURFconext admins they didn't provide me with a nice WAYF for eduGAIN, and I think it was Niels [van Dijk] that brought it up. Before, I was using something in SimpleSAMLphp with DiscoJuice."

Service: **SAFIRE Test Service Provider**

Responder: Guy Halse <guy@tenet.ac.za>

Response:

A. How did you get aware of discovery.eduteams.org?

One of the REFEDS or eduGAIN mailing lists, I can't recall which.

B. Why did you start using it and not another discovery service?

As its name suggests, testsp.safire.ac.za is our test service provider (a bit like SWITCH's AAI Attribute Viewer). We also occasionally use it to demonstrate different modes of discovery, and so it supports both central and local discovery.

We were using DiscoJuice as an example of local, embedded in-browser discovery. However that's had repeated problems with its CDN, and the project seems to be abandoned. So I started looking for an alternative.

C. Are you and are the users of your service happy with the eduTEAMS Discovery Service?

Yes :-)

D. Do you plan to continue using it, maybe also for other services?

[No response]

E. Do you have non-eduGAIN services for which you also would like to use the eduTEAM Discovery Service if it supported non-eduGAIN IdPs?

Yes

F. Which features do you particularly like about it?

The RA21-ish idea of offering previously used accounts.

G. What could make the service even better for you?

A callback or similar to allow for IdPs to prioritized; geolocation. Basically a way to make IdPs that make more sense to users of the service percolate towards the top of the list.

Adopting more RA21 ideas seems to be sensible.

H. Are there any other comments you have for the developers/operators?

Please be cogniscent of and document the Content-Security-Policy requirements :)

4 Conclusion

Analyzing the responses above the following statements can be made:

- SP operators are generally quite satisfied with the function and the operation of the eduTEAMS Discovery Service (e.g. reflected in responses to question C.). 4 survey participants expressed a positive and 3 a neutral/rather-positive opinion of the service. There is no negative feedback in the responses received.
- SP operators appreciate that there is a generic-purpose discovery service available in eduGAIN, especially if an SP's local federation does not operate a Discovery Service also listing eduGAIN IdPs. 3 of 4 service operators (who explicitly responded to question D.) consider continue using the discovery service and also intend to use it for additional SPs.
- Ease-of use, speed and stability of the eduTEAMS Discovery Service were positively mentioned.
- 3 SP operators chose the eduTEAMS Discovery Service [DS] because DiscoJuice no longer has been available.
- The IdP filter (one of the key features of the CESNET Discovery Service) was not mentioned as advantage. Most probably this feature is not known very well even though it is a key differentiator compared to other SAML Discovery Service implementations.
- A wish and need was expressed to make the Discovery Service also support non-eduGAIN IdPs by 2 of 4 survey participants who explicitly responded to question E.
- Feature requests mentioned (in questions G and H) are: Documentation of Content Security Policy requirements, support for non-eduGAIN IdPs, allow SP to prioritize certain IdPs in the list of IdPs, order IdPs by geolocation information

References

[CDS] CESNET Discovery Service, <https://www.eduid.cz/en/tech/wayf>

- [DS] DiscoJuice - The user friendly IdP Discovery Service, <http://discojuice.org/>
- [EED] eduGAIN Entities Database, <https://technical.edugain.org/entities>
- [ET] eduTEAMS Service, <https://eduteams.org>
- [ETDS] eduTEAMS Discovery Service, <https://discovery.eduteams.org/>
- [GN] GÉANT project, https://www.geant.org/Projects/GEANT_Project_GN4
- [IDPDS] SAML DS Specification “Identity Provider Discovery Service Protocol and Profile”, <http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf>
- [RA21] RA21: Resource Access for the 21st Century, <https://ra21.org/>
- [VOPaaS] Deliverable D9.2 Market Analysis for Virtual Organisation Platform as a Service (VOPaaS), http://www.geant.org/Projects/GEANT_Project_GN4-1/deliverables/D9-2_Market-Analysis-for-Virtual-Organisation-Platform-as-a-Service.pdf

Glossary

DS	Discovery Service
IdP	Identity Provider
SAML	Security Assertion Markup Language
SP	Service Provider