Guidelines
How services can participate in eduGAIN

Co-financed by the Connecting Europe Facility of the European Union

Table of contents

1 Executive Summary

This document provides information on how service providers can enable federated access to users and institutions in several countries via eduGAIN. The document is structured as follows:

- An introduction to explain how services can enable federated access
- A section to describe the work done in MyAcademicID to enable federated access for student mobility services via eduGAIN. This information is based on the Blueprint Architecture defined in Milestone MS1.1 (please see MyAcademicID website).
- And another section that describes the generic flow for a SAML service to become available in eduGAIN. The information is based on the content in the eduGAIN wiki. For more information about eduGAIN please refer to the eduGAIN website.

2 Introduction

Services that offer resources to the research and education sector and wish to enable federated access can benefit from eduGAIN. eduGAIN is an infrastructure that enables participating national research and education identity federations in more than 50 countries to share services among each other. This allows users that belong to an institution that is a member of one of the federations in eduGAIN to authenticate to all services available in eduGAIN using the credentials provided by their own institution. Users can therefore use one set of credentials to access different services; services can reduce their administrative burden to allow access to users in different regions.

Examples of services that are offered via eduGAIN are:

- Wikis and other collaborative platforms;
- e-journal content providers (i.e. publishers)
- cloud service providers

Generally, a service becomes available in eduGAIN by joining one eduGAIN member federation, which will expose the service to all other federations and their users. In this way a service only needs to join one federation to reach to a wider international audience rather than having to join multiple ones; this minimizes the technical and contractual work on the service provider side.

It is important to note that (unless provisions are made by the federations) a service is expected to support SAML2.0 protocol. Chapter 4 describes the relevant steps for a service to be integrated in eduGAIN as a **SAML Service Provider**. Following the instructions provided in this document, a service provider will be able to deploy a SAML2.0 compliant Service Provider and publish it in a national federation and via that in eduGAIN. Please note that this document is aimed at services that can support web-based authentication; if this is not case other provisions need to be taken.

Over the last years, to better address the needs of research collaborations and to facilitate service providers to enable federated access, the adoption of an IdP/SP proxy has gained a lot of traction. This model has been championed by the AARC project that has defined an architectural model as well as a number of policy and technical guidelines to ensure harmonised deployment of authentication and authorisation infrastructures that wish to deploy an IdP/SP proxy. The IdP/SP proxy is connected to eduGAIN via a national federation, in which it acts as a service provider. This proxy generally connects

other services, for which it acts as an identity provider. The security aspects of such a proxy are regulated by the Snctfi framework.

The IdP/SP proxy offers a single point of connection to service providers and takes the responsibility for providing the connection to eduGAIN, removing the need for each service to individually join a federation. The usage of an IdP/SP proxy makes it easier to enable federated access to services that support other protocols than SAML such as OIDC, OAuth2, etc. This feature is particularly useful for a virtual community that needs to manage different type of services in a more dynamic and agile manner. This is the approach taken within MyAcademicID, where different type of services are being federated.

3 Enabling Federated Access for Student Mobility Services

In MyAcademicID project a set of representative services that are used for enabling student mobility was identified. These services include:

- the Erasmus Dashboard;
- the Erasmus Mobile App;
- Online Learning Agreement (OLA);
- and the PhD Hub

Although it was not included in the list of services in the MyAcademicID project, during the workshops we recognised the additional value that the integration of the European Student Card (ESC) portal would bring. Thus, the ESC Portal is also included in the list of services for which federated access would be beneficial.

These services have some common characteristics, but also important differences. The Erasmus Dashboard, the Online Learning Agreement, the PhD Hub and the ESC Portal, are web-based applications, which offer personalised services to users. In the case of the Erasmus Dashboard, students are identified in the system, which is accessible to higher education staff that manage the student mobilities. The other services are directly accessible by the students. In all cases, the users, being students or higher education staff, need to authenticate themselves in order to access those services and at the same time the services need to know which institution the user is coming from. The Erasmus Mobile App has very similar requirements as the previous set of services, but it is a mobile application.

In order to enable federated access to the mobile app and the web-based services, we are going to leverage the pool of identities provided by eduGAIN. This will allow (a) users to authenticate at their home institutions and (b) services to receive information about the users' affiliation and contact information from the home institutions. The services are going to be connected through a multi-protocol SP Proxy (Service Provider Proxy) provided by GÉANT, which allows the services to use the OpenID Connect protocol in order to authenticate users in eduGAIN, which uses the SAML protocol.

In addition, the MyAcademicID project aims to also leverage eIDs via eIDAS to allows users to authenticate to Student Mobility Services with their eID.

To support the heterogenous services described above and given the fact that these services are currently not federated (thus they are not part of any federation) it was agreed to use a multi-proxy architecture, which is depicted in the picture below.

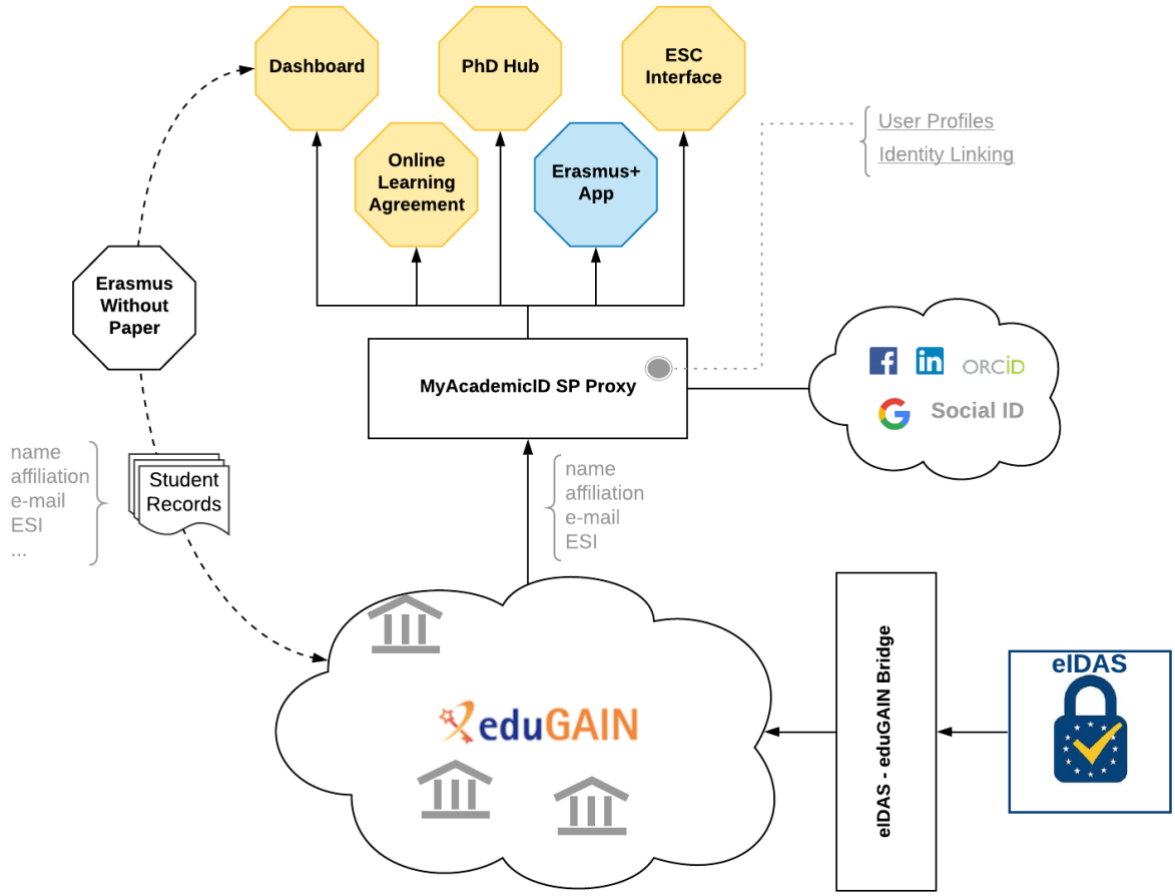


Figure 1: MyAcademicID Blueprint architecture (see the MyAcademicID website for more details)

3.1 The SP Proxy

The Service Provider (SP) Proxy is operated by GÉANT and is connected to eduGAIN as a service provider. Such a proxy offers the follows benefits:

- It allows to use the existing authentication stack of the services (both SAML and OpenID Connect are possible);
- Instead of having to connect the services to eduGAIN individually, they will connect to the GEANT SP Proxy; this makes things easier for the services;
- Handling the discovery of thousands Identity Providers and their metadata can be complex. This capability will be provided by the GEANT SP Proxy, so the services do not have to adapt to the multi-federation, multi-identity-provider environment of eduGAIN.
- Currently, these service use Google authentication to authenticate users. The GEANT SP Proxy can be configured as an Identity Hub with Account Linking capabilities. Again, these are

capabilities that will be provided by the GEANT SP proxy to all the connected Erasmus services, without having to modify anything on the service side.

3.2 The eduGAIN-eIDAS Bridge

The eduGAIN-eIDAS bridge is a SAML-to-SAML protocol proxy that acts as a bridge between the eIDAS Network and the Identity Federations in eduGAIN. In eduGAIN the proxy appears as an Identity Provider, while in the eIDAS Network, the proxy appears as an eIDAS Service node. This proxy is currently connected to the Swedish eIDAS test environment. Student Mobility services will not directly connect to this proxy.

3.3 How Student Mobility Services can Connect to the SP Proxy

Below is the list of information required for each service that will connect to the SP proxy.

Name of the Organization Offering the Service	
URL of the organisations website	
Name of the Service	
Link to the landing page of the service	
A brief description of the service	
Admin contact	
Security contact	
Technical contact	
Link to the privacy policy	
Link to the acceptable usage policy / Terms of Service	
Link to the SP logo	
GEANT CoCov1 compliance	[ ] Yes [ ] No
Research & Scholarship compliance	[ ] Yes [ ] No
SAML2 Support	[ ] Yes [ ] No
Link to the SAML metadata of the SP (if the service supports SAML)	
OIDC support	[ ] Yes

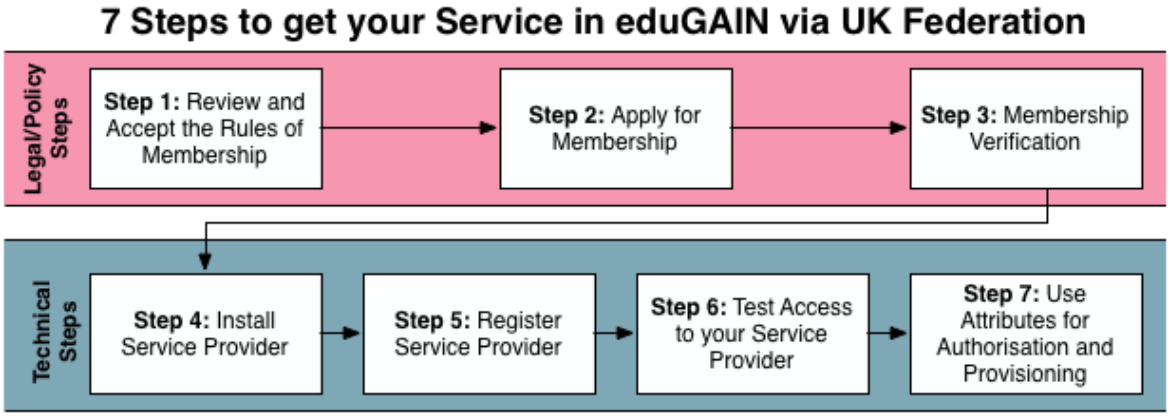
	[ ] No
OIDC Redirect URI (if the service supports OIDC)	
Authentication Method (if the service supports OIDC)	[ ] client_secret_basic [ ] client_secret_post
Attributes required	[ ] Persistent Identifier [ ] First name and last name [ ] e-mail address [ ] Affiliation [ ] ORCID

Table 1: List of information expected from a service that connects to the SP proxy

4 Joining eduGAIN via a National Federation as a SAML Service Provider

This chapter describes in detail how a service can participate as a SAML Service Provider in eduGAIN by joining a Research and Education Federation; please note that a service can decide to join any federation (if the federation policy allows for that).

There are basically two parts in this process: A legal (steps 1-3) and a technical part (step 4-7). The diagram below provides a brief overview, followed by more detailed instructions.



4.1 Step-by-Step Guide

Step 1: Review and Accept the Rules of Membership

Before becoming a member in a federation (and thus also in eduGAIN), a Service Provider needs to review and accept that federation policy. This document basically lists the service rights and duties within the federation.

Step 2: Apply for Membership

In this step, the organisation that operates the service formally requests to join a federation and involves an agreement to be signed. The application is usually in writing and contains information on the organisation and on the person authorised to sign the relevant documents.

Step 3: Membership Verification

In this step the federation verifies all the information provided by the applicant service is correct. This is a very important step in order to process your registration request, so please make sure that the contact details are correct and that the delegated persons are notified about the required actions in advance.

Step 4: Install Service Provider

Now that the registration application is under way, you might want to install and configure a Service Provider implementation, compatible with the SAML 2.0 specification. The two most popular implementations are:

- Shibboleth Service Provider, which is implemented and maintained by the Shibboleth Consortium. It's the most common and popular SAML implementation in eduGAIN and it also includes most features relevant for eduGAIN. Therefore, this is generally the recommended SAML implementation to use. It works very well with Apache and IIS as web server. It requires root access because it requires the mod_shib web server module.
- SimpleSAMLphp, which is implemented and maintained by Uninett. This PHP implementation of SAML is recommended only if PHP is already used. It does not require root access but to make use of federated login requires code changes in a PHP application.

Please read section 4.2 (Installation & Configuration), which contains detailed instructions for the installation and necessary configuration of a Service Provider, using one of the aforementioned implementations. Also make sure that, once installed, the Service Provider is tested using the SAML implementations sanity checks (e.g. for Shibboleth running "shibd -t" on linux) to ensure that the software was correctly installed. Ideally, the Service Provider is also tested against a SAML2 Identity Provider to ensure that it was configured correctly.

Note: It is not recommended to try creating an own SAML implementation. SAML is a very complex standard and trying to come up with something on your own, most certainly will cause interoperability issues. Generally, eduGAIN's Web SSO profile requires a SAML Service Provider to support the SAML2int profile.

Step 5: Register Service Provider

Once the Service Provider software is installed, configured (see section 4.2) and working, the next step is to register the Service Provider with the federation.

This process is federation specific, so it is out of scope for this document. However the eduGAIN wiki provides an example based on UK Federation.

The submitted information will be validated against a predefined set of rules upon submission. It can take from a few hours up to a few days until your SP's metadata is published in eduGAIN.

Upon successful publication your service contact point will be notified and the Service Provider will be available as a service the federation and in eduGAIN.

Step 6: Test Access to your Service Provider

After your Service Provider is registered, you are then welcome to test the functionality (i.e. federated login) yourselves. Unless you have an account at an eduGAIN Identity Provider, you can use the eduGAIN Access Check Service, available in https://access-check.edugain.org This service allows you to test federated login to your own service using a few predefined test identities.

What you should check is if your Service Provider receives the attributes it requests.

Step 7: Use Attributes for Authorization and Provisioning

Once the attributes are available at the SP, they can be used for Access Control or they can be used within your web application. How to do that is for example described on the Shibboleth Access Control example in the Shibboleth wiki.

Attributes are typically also used to provision an account in web applications (i.e. create a user record in the database). To use attributes within a web application protected by Shibboleth, simply read them from the web server environment (where you also would read the REMOTE_USER variable from).

SP Metadata

To register the Service Provider (SP) with a federation, one typically has to provide its SAML2 metadata to the federation operator. If you don't have metadata about your SP yet, you might need to generate/compose it first. Shibboleth can generate SAML2 metadata about itself, just try accessing https://your.host.org/Shibboleth.sso/Metadata

SimpleSAML PHP has a similar feature. Just open the URL https://your.host.org/simplesaml/module.php/saml/sp/metadata.php/default-sp

In both cases, metadata only contains technical information. You should enrich metadata with the non-technical information (e.g. technical contact, name, description) following this example.

Please refer to the eduGAIN wiki for further details on this step

Annex – More Information on Federated Access

Federated access enables a service provider to rely on the authentication of users performed by the home institutions (Identity Providers) of the users; this means that a service only needs to manage the authorisation aspects and does not need to maintain and manage users' credentials. eduGAIN makes it possible to scale federated access globally.

A comprehensive overview of material to explain the foundation of federated access and SAML identity federations is available on the AARC website (AARC Federations 101).

A short 4 minute movie on interfederation and eduGAIN is also available "How to benefit from interfederating through eduGAIN".

To see and try federated login in action, you might want to have a look at SWITCH's AAI Demo.