How to offer a service in eduGAIN

This page provides a general high-level overview of the steps that are necessary for a service operator to enable his service for eduGAIN.

A more concrete guide with step-by-step instructions is provided by the page How to Join eduGAIN as Service Provider.

What does it mean to operate an eduGAIN service

Operating an eduGAIN service means that a service can outsource user identity management and password management to the user’s home organisation (e.g. university) that does this for their users. To make federated login via eduGAIN work, the service has to add support for the SAML protocol that sends the user to his home organisation for authentication and then redirects him back to the service together with some user attributes. Most services rely on the very popular Shibboleth Service Provider to initiate and perform the whole SAML login process so that the service itself has to only declare where a SAML session should be enforced (e.g. on directory /auth/login or when user clicks on a certain link) and then has to consume the user attributes provided by the SAML Service Provider in a reasonable way.

Instead of having users register first with your service by completing a registration form, a service can just force them to log in via federated/eduGAIN login and it then typically gets some information about the user (unique identifier, name, email, organisation, affiliation), which can be used to auto-provision an account in the service application if that is needed. One of the most important aspects that changes for the service: There are no username and password available anymore for the user.

In brief, offering a service as eduGAIN service has the following advantages:

- No need to deal with user password management anymore as this is done by the users' home organisation
- Account provisioning on the service can be automated based on the user's attribute
- Users from more than 40 countries and more than 3000 academic and research organisations can potentially access your service.
- The service of course still can fully control who can access the service implementing some access control based on the user's attributes

There are also a few disadvantages:

- The application does not get the user's username and password anymore. The username can be substituted with an attribute (unique identifier, email) sometimes.
- The service has to integrate and operated an additional component that does all the SAML protocol work
- If attributes are released to a particular service or not is controlled by the Identity Provider (e.g. university) of the user. It is not guaranteed that all attributes a service requests are released by the Identity Provider.

Requirements

The service to be enabled for federated login via eduGAIN should meet the following requirements:

- **Web-based**: The service should be a web application. Even though non-web profiles like the SAML ECP profile could be used in eduGAIN too, most Identity Providers in current identity federations (including) eduGAIN support web-based applications only.
- **SAML Interoperable**: It is assumed that the service can be protected by a SAML Service Provider like Shibboleth or Simple SAML PHP. For many popular web applications there are plugins, modules or documentation available that explains how to achieve this. Just google for the product and "saml" or "shibboleth".

General Procedure

A. Service Registration

Because eduGAIN is not a confederation (federation of federations) but an interfederation service (provides connectivity between certain entities of different federations), it contains a subset of all services in federations that joined eduGAIN. This means that in order to enable a service for eduGAIN, that service has to become part of an existing identity federation, which joined eduGAIN. This is depicted in the following graphic:
If the service is already registered in an identity federation that is part of eduGAIN, proceed to B.

If the service is not already registered in an identity federation, register it with an existing Identity Federation that is already an eduGAIN member federation. If the organisation in whose name the service is registered is not yet member of that federation, it might be necessary to join that federations first. The processes to join a federation depends from federation to federation but it will most likely involve the organisation signing some kind of a service agreement.

**B. Adapt Application to Support SAML-based Login**

If the service already makes use of SAML for authentication, proceed to C. If not, continue with:

1. Install a SAML Service Provider like Shibboleth or SimpleSAML PHP to protect the service.
2. Adapt the application to use the SAML attributes in order to authenticate users and use their attributes (like mail, display name, unique identifier, etc.)
3. Implement access control rules or some kind of group management if authorization is needed.

**C. eduGAIN Opt-In**

Most federations participating in eduGAIN expose only those entities to eduGAIN that opted-in for eduGAIN. The process to opt-in for eduGAIN depends from federations to federation. Some federations just require the service operator to tick a checkbox on the federation's management interface, others will require a signed document from the service operator or his organisation.

In most federations it is also necessary to adapt the configuration of the Service Provider in order to opt-in. Often this involves configuring another source of SAML2 metadata, which then contains the eduGAIN entities.

Please consult the documentation of the federation that the service is registered with in order to find out if and how the service can be opted-in for eduGAIN support.

**D. Support the GÉANT Dataprotection Code of Conduct**

The GÉANT Dataprotection Code of Conduct a self-declaration stating that the operator of the service will follow the data protection principles mentioned in the Code of Conduct. For services operated in EU/EAA and Switzerland it is strongly recommended to support the Code of Conduct because it increases the chance that Identity Provider will release all or more of the requested attributes to the service. The Code of Conduct increases the trust that an Identity Provider can have in that service when it comes to provide it with data about the user who wants to access the service.

**E. Use a Discovery Service that supports Interfederation**

When a service can be accessed by users from multiple organisations from multiple federations, it must be ensured that the user during the login process can find and select the organisation he wants to authenticate at. This process is called Identity Provider Discovery. There are multiple open-source implementations (Shibboleth Discovery Service, SWITCHwayf) that allow to operate an own Discovery Service. Alternatively, there are also hosted solutions (Disco Juice) that could be used instead.

Some SAML implementations like SimpleSAML PHP already include a Discovery Service that will automatically display all Identity Providers whose users might access the service.

One particular aspect to handle specifically is the case where users need to access the service who are affiliated with an organisation that:

- Is not yet part of eduGAIN
- Cannot become part of eduGAIN

In such cases, one solution might be to add a special Identity Provider that serves as a "Home for the Homeless" users. Such Identity Provider are operated by multiple federations. Often they allow user self-registration only by verifying an email address. There are however also solutions that allow an operator of a service to specifically create accounts for users that are eligible/verified to get access to the service.

**F. Adapt attribute mapping and attributes Used**

If the service already was operated within a particular federation before its target user group was extended to also include eduGAIN users, it might be necessary to review and adapt the attributes that the service (or its Service Provider) is able to consume and use for authentication and authorization. The attribute names and values used in some federations might be slightly different to the ones used in other federations.

**G. Adapt Access Control Rules**

After reviewing the attributes that are supported by the service and its Service Provider, it might also be necessary to check if the access control rules still work. This is in particular the case for applications that perform access control based on certain attributes and their values.
H. Test Interfederation Access

Testing access to a service via eduGAIN will often require a user from another federation to access the service. This is because most federations don’t allow test accounts.

How to start?

The above high level topics that are relevant for adding a service to eduGAIN are described in greater detail and extended by step-by-step instructions on the page How to Join eduGAIN as Service Provider.

Special Cases

For research groups that are likely to operate many services and potentially in different countries and federations, we recommend reading the document Options-for-Joining-eduGAIN.pdf (PDF) that illustrates the different options that apply in such cases.