How to connect a service to the ELIXIR AAI

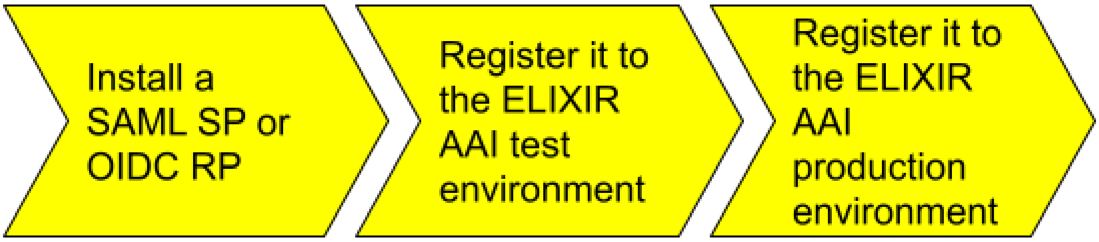
ELIXIR AAI task

!!! ATTENTION - NOT MAINTAINED !!!

ELIXIR AAI has been migrated into the LifeScience AAI. This document is relevant only to the ELIXIR AAI, thus not maintained and has become out of date.

The new version of the document is available at
Instructions - How to connect a service to the Life Science AAI.

Service integration process


Install a SAML SP or OIDC RP
Register it to the ELIXIR AAI test environment
Register it to the ELIXIR AAI production environment

Step 1: Install a SAML SP or OIDC RP

ELIXIR AAI supports currently two technical protocols that you can choose from:

- SAML 2.0. You need to install a SAML 2.0 Service Provider (SAML SP) software and integrate it into your application.
- OpenID Connect. You need to install an OpenID Connect Relying Party (OIDC RP) software and integrate it into your application.

ELIXIR AAI task has organised training events on SAML SP and OIDC RP installation and integration and the training materials are available on-line. See details.

Step 2: Register the SP or RP to the Life Science AAI test environment

1. First register a personal LS ID (previously ELIXIR ID) for yourself, unless you already have one: Registration page.
2. Decide what attributes (user information) you will need in your SP/RP. A list of attributes the AAI can provide is available in this document.
3. Register your SP or RP in ELIXIR AAI's SP Registry: https://spreg.aai.elixir-czech.org/spreg/. Manual on the registration process is available at this link.
4. The ELIXIR AAI task checks the data and informs you that your service is registered to the LS test environment

- The LS test environment is a sandbox where you (or your colleague) can log in with your (their) personal LS ID to test your SP/RP.
- The LS test and production environments have the same endpoints for SPs/RPs (e.g. SAML SingleSignOnService Location, OIDC authorization_endpoint)
- You (or your colleague) need to first register to the LS TEST environment: https://signup.aai.lifescience-ri.eu/registrar/?vo=lifescience_test

5. For consistent user experience, LS Login has published design guidelines for the login page of the SP/RP. Consider adopting them in your SP/RP.
    - LS LOGIN LS REGISTER LS Login - design guidelines
    - If you decide to deploy a separate register button for new users to register an LS ID, the register button should link to the page: https://signup.aai.lifescience-ri.eu/fed/registrar/ with the following query string parameters:
        i. vo=target virtual organisation name (normally: lifescience)
        ii. group=group name (optional, if in place the user is presented also the group's application form)
        iii. targetnew=the group where the browser is redirected after the user is successfully registered
        iv. targetexisting=the URL to which the browser is redirected if the registration failed because the user is already registered to ELIXIR
        v. Example link (used in ELIXIR intranet): https://signup.aai.lifescience-ri.eu/fed/registrar/?vo=elixir&group=Community&targetexisting=https://www.elixir-europe.org/alreadyregistered&targetnew=https://www.elixir-europe.org/registration-successful
6. One of the claims/attributes LS Login manages is the list of the user's group memberships in ELIXIR. Decide if you want to ask ELIXIR AAI to enforce access to your service based on the user's group memberships.
    - The ELIXIR Proxy IdP will let the user access your service only if they are members of a group you indicate (or any of them if you indicate several)
    - If you have opted-in to this functionality but the user fails the group membership criteria, you can ask ELIXIR AAI to do one of the following:
      1. Just display "Permission denied"
      2. Display "Permission denied" and a link to the group's registration form (all of them, if there are several alternative groups)
      3. Display "Permission denied" and a link to a web page you decide
7. If you are registering a SAML2 SP:
    - Configure your SAML SP to consume the ELIXIR proxy IdP's SAML2 metadata file: https://login.elixir-czech.org/proxy/saml2/idp/metadata.php?output=xhtml
8. If you are registering an OIDC RP:
    - Follow the ELIXIR AAI OIDC deployment guide

Step 3: Register the SP or RP to the ELIXIR AAI production environment

1. Navigate to the SP registry provided by the ELIXIR AAI available at https://spreg.aai.elixir-czech.cz/spreg/
2. Open the detailed view of your service and click “transfer to production” button. You will need to specify by which ELIXIR Node is the service provided. If the service is not provided by an ELIXIR Node, uncheck the option “ I want to select responsible authorities”.
3. An approval request will be sent to the persons who will have to approve the transfer.
4. You will get notified by any changes via email.
5. After the transfer to production is approved, the ELIXIR AAI administrators will review your request.
6. Your service is transferred to the production environment.

   See full documentation of the procedure here.

Additional information on ELIXIR AAI

Generally, ELIXIR AAI supports connection of web-based services and non-web based services. ELIXIR AAI can provide authentication of the users as well as data needed for authorization.

Requirements and design

Common ELIXIR Service for Researcher Authentication and Authorisation (Full paper, F1000 Research, August 2018).

ELIXIR AAI Policies for Relying Parties

Eligibility to become a Relying Party

The following organisations can become Relying Parties for ELIXIR AAI and register a service (Relying Service) that consumes the authentication and authorisation services ELIXIR AAI provides:

- The ELIXIR Nodes and the Hub
- Other public and private organisations based on approval by the Heads of Nodes (HoN) Committee and the ELIXIR Director. The HoN Committee and ELIXIR Director can delegate their approval rights.

The Relying Services registered by Relying Parties must support research and collaboration in life sciences.

Protection of ELIXIR End Users’ personal data

- The Relying Party must follow laws, especially the data protection laws applicable in the country where the Relying Service is established, with regards to the End User’s personal data it receives from the ELIXIR AAI.
- To receive restricted user attributes, such as those retrieved from the user’s Home Organisation, the Relying Party must commit to GEANT Data protection Code of Conduct, version 1.0 or equivalent.

- If the Relying Party is outside the EU/EEA and the countries with adequate protection of personal data the Relying Party must take measures deemed appropriate by the European Commission, such as, to commit to the Contractual Clauses.

Liability

- The liability between an ELIXIR Node and the Hub is defined in section 12 of the ELIXIR Collaboration Agreement.

Group attributes information

ELIXIR AAI propagates information about users' group membership. This information is distributed in eduPersonEntitlement attribute.

- Entitlements contain full name of the group
  - e.g. elixir:groupName:subGroupName@elixir-europe.org
- Every group name has **@elixir-europe.org** scope.
- Only groups which are assigned to the resource in Perun will be propagated to the service provider.
- Service can receive assigned groups in the form of entitlements or it can receive just one entitlement which is assigned to those users who can access the resource.

Document history

Modified	Actor	Description
19.5.2017	Mikael Linden	Revamped the document
10.8.2017	Mikael Linden	Added a link to ELIXIR login - design guidelines
10.7.2018	Michal Prochazka	Added information about the automatic subscription to the elixir-aai-relying-services@elixir-europe.org mailing list
2.11.2018	Mikael Linden	Added that GEANT Code of Conduct not needed in ELIXIR test
16.11.2018	Mikael Linden	Added the new feature on access control enforcement based on a group membership
29.1.2020	Dominik F Bucik	Changed the whole registration procedure due to the introduction of the SP Registration APP
1.6.2020	Dominik F Bucik	Published the new registration procedure
12.4.2022	Dominik F. Bucik, Mikael Linden	Updated after LS Login migration