ELIXIR AAI task force

Requirements on ELIXIR AAI

Mikael.linden@csc.fi/19.2.2015

This document presents the requirements on the ELIXIR AAI (Authentication and Authorisation Infrastructure), the identity and access management infrastructure that ELIXIR provides to the ELIXIR services (called Relying Parties).

These requirements are based on the ELIXIR AAI Use case analysis. This document, in turn, will be used as the basis for the ELIXIR AAI design document.

The ELIXIR AAI is expected to be deployed gradually, as part of the proposed EXCELERATE EC project.

# ELIXIR identity

Any natural person can become an ELIXIR user by registering an ELIXIR identity. The user may need to commit to certain baseline terms of use when registering the ELIXIR identity. The exact content of the terms will be developed later.

An ELIXIR identity is uniquely identified by an ELIXIR identifier. The Relying Parties are expected to use the ELIXIR identifier as the primary unique identifier of the user, although the Relying Parties may receive also other user identifiers and attributes.

**ELIXIR identifier syntax**

The ELIXIR identifier’s format has two parts:

* The first part (syntax derived from Linux accounts[[1]](#footnote-1)) begins with a lower case letter or an underscore, followed by lower case letters, digits, underscores, or dashes. They can end with a dollar sign. In regular expression terms: [a-z\_][a-z0-9\_-]\*[$]?
* Second part which is a fixed string “@elixir-europe.org”

**Special identifiers**

The ELIXIR identifiers beginning with underscore are dedicated to special purposes. ELIXIR identifier “\_test@elixir-europe.org” is a test account reserved for testing the proper functioning of the ELIXIR AAI and the Relying Parties must not authorize it to access any valuable resources.

**Examples**

* bobs@elixir-europe.org
* 123abc@elixir-europe.org
* mikael\_linden@elixir-europe.org
* \_test@elixir-europe.org

**Cardinalities, changes and reassignment of identifiers**

The ELIXIR identifier represents a single natural person. It cannot represent a group of persons or a person that is currently acting in a specific role (e.g. a position like “on-duty operations manager” that circulates among a pool of persons).

A single person can have several ELIXIR identifiers. While this is not desirable and probably confusing especially for the person him/herself, there is no practical means to enforce a stricter policy.

The ELIXIR identifier cannot change i.e. be replaced by another identifier belonging to the same person. The initial choice of the identifier is expected to take this into account (e.g. not use family name if the person wants to change it due to marriage/divorce). The ELIXIR identifier does not change if the person changes his/her affiliation.

The ELIXIR identifier cannot be re-assigned i.e. revoked and subsequently assigned to another person.

**Current affiliation(s) attribute of an ELIXIR user**

The current affiliation attribute is a multivalued attribute that indicates the organization(s) (called a home organization, such as a research institution or private company) the end user is currently affiliated with and the type of the affiliation. A user can have several home organisations at the same time, if he/she for example works or studies in several organisations in parallel. The Relying Parties who need to close access rights on an affiliation change can monitor changes in the attribute.

The syntax and semantic of the attribute follows the eduPersonScopedAffiliation attribute defined in eduPerson schema (version 201310[[2]](#footnote-2)). Following values are recommended for use to the left of the “@” sign:

|  |  |
| --- | --- |
| Faculty | The person is a researcher or teacher in his/her home organization. The exact interpretation is left to the home organization, but the intention is that the primary focus of the person in his/her home organization is in research and education. |
| Member | "Member" is intended to include faculty, staff, student, and other persons with a full set of basic privileges that go with membership in the home organisation, as defined in eduPerson. In contrast to “faculty”, among other things, this covers positions with managerial and service focus, such as service management or IT support. |
| Affiliate | The "affiliate" value for eduPersonAffiliation indicates that the holder has some definable affiliation to the university NOT captured by any of faculty, staff, student, employee, alum and/or member. |

In other words, if a person has “faculty” affiliation with a certain organization, he/she has also the “member” affiliation. However, that does not apply in a reverse order. Furthermore, those persons who do not qualify to member have an affiliation of “affiliate”.

Examples

* faculty@helsinki.fi
* member@ebi.ac.uk

To become a holder of the **faculty or member attribute values** in ELIXIR AAI, the user must either

* Perform federated login to ELIXIR AAI using his/her home organisation’s credentials, during which the home organization releases the related eduPersonAffiliation or eduPersonScopedAffiliation attribute, or
* Be assigned that identifier by his/her home organisation’s ELIXIR coordinator

To become a holder of the **affiliate attribute value**, the user must either

* Use either of the two alternatives above, or
* Demonstrate he/she controls an e-mail address that belongs to the home organisation

The freshness of the attribute values is guaranteed by asking him/her to refresh the value every 12 months using the procedure described above.

There must be a mechanism to revoke a person’s affiliation immediately if needed.

The operations of ELIXIR AAI must have a support process to help ELIXIR users who change their affiliation. The support process must help the user at least to associate her/his new institutional identifier to his/her existing ELIXIR identity.

**Other attributes**

Following external identifiers can be associated to the ELIXIR identity

* Federated identifier, such as the eduPersonPrincipalName attribute
* Social media identity (e.g. Google, LinkedIn)
* ORCID identifier

The federated identifiers must be recorded by asking the user to log in to ELIXIR using the identifier.

Some attributes can be self-managed by the user him/herself in a web-based self-service UI, such as

* Name (unless the user has registered for step-up authentication, see below)
* Preferred language
* timezone

Changing some attributes has restrictions, such as

* e-mail address (the user needs to demonstrate ownership of the address by a handshake protocol)
* home organization type

**Logging and history**

For accountability and incident response purposes, the ELIXIR AAI must store adequate log information on the use of the ELIXIR identities.

ELIXIR AAI must store adequate history of each ELIXIR identity, including the previous affiliations the user has had.

**Technical interfaces for Relying Parties**

The ELIXIR AAI must provide following technical interfaces for the Relying Parties

* LDAP directory for querying user attributes
* SAML Identity Provider which is able to deliver the necessary attributes to the Relying Party in the Authentication Response message

# AUTHENTICATION

**Supported authentication providers**

Each ELIXIR identity has one or several associated authentication providers:

* Identity Providers managed by the researchers’ home organisations to which ELIXIR AAI connects via the eduGAIN interfederation service or otherwise. Researchers can use their home organization managed authentication credentials to log in (SAML 2.0 technology)
* Identity Providers managed by common social media providers, such as Google, Linkedin or ORCID. ELIXIR users can register a social identity to log in to ELIXIR (typically, OAuth2 technology)
* ELIXIR account that is an ELIXIR managed authentication service. The user can use his/her ELIXIR identifier and an associated password to log in

To qualify as an authentication provider, the eduGAIN Identity providers must

* Provide sufficient Level of Assurance (LoA). The LoA floor comprises of:
	+ The accounts must belong to individual users
	+ The home organisations must have a standard identity proofing mechanism for end users when they receive their login credentials
	+ The home organisations must close departing end users’ accounts or remove their eduPersonAffiliation/eduPersonScopedAffiliation values
* Be willing to release attributes to ELIXIR AAI. ELIXIR AAI commits to the GEANT Data protection Code of Conduct.

**Account linking**

An end user can link several external authentication providers to his/her ELIXIR identity, and use them mixed when accessing the ELIXIR services. The Relying Party is always expected to use the user’s ELIXIR identifier as the primary user identifier.

To link a new authentication provider to his/her ELIXIR identity, an end user first logs in to ELIXIR AAI using his/her existing authentication provider and performs a subsequent log in using the new authentication provider. The ELIXIR AAI must provider a web-based self-service management UI for this.

To help existing Relying Parties to migrate to ELIXIR AAI, a Relying Party can receive not just the authenticated user’s ELIXIR identifier but also the external identifier that was used to authenticate him/her. For example, when a user with the ELIXIR identifier bobs@elixir-europe.org logs in via eduGAIN, the Relying party receives two identifiers:

* ELIXIR identifier: bobs@elixir-europe.org
* External identifier: bsmith@universityx.org (eduPersonPrincipalName, indicating the home organization identity that Bob used for login)

**Step-up authentication**

Initially, all external authentication providers and the ELIXIR accounts are assumed to provide a basic LoA for both the initial proof of identity and login. The situation can be later re-evaluated as well-established external LoA frameworks and providers become available.

ELIXIR AAI deploys a service for step-up authentication, which covers both strong (face-to-face) identity proofing of an ELIXIR identity and strong (two factor) authentication at the login time.

Strong identity proofing is deployed by asking each home organisation’s ELIXIR coordinator to deploy practices for face-to-face identity proofing, supported by the technical infrastructure provided by ELIXIR AAI. Strong authentication is provided by registering a second authentication factor for the user during the face-to-face identity proofing. Initially, following second factor authentication mechanisms are suggested:

* SMS-OTP (one-time password delivered to the user’s registered cell phone number),
* a smartphone application (e.b. Tiqr, <http://tiqr.org/>) and
* a hardware token generating one-time passwords, (e.g. Yubikey, a token emulating a keyboard).

The exact registration workflow for identity proofing depends on the authentication mechanism used. This example illustrates the idea:

1. A user logs in to ELIXIR AAI (using weak authentication)
2. The user clicks “associate a strong authentication means to my ELIXIR identity”
3. The user performs strong authentication to ELIXIR AAI with his/her authentication token
4. ELIXIR AAI gives the user an activation code
5. The user goes to his/her home organisation’s ELIXIR coordinator and presents face-to-face the activation code and his/her government photo ID
6. The ELIXIR coordinator uses his/her own strong authentication means to log in to ELIXIR AAI, verifies the user’s ELIXIR identity and the photo ID and enters the user’s activation code to the system
7. The user can start to use the step-up authentication service

A Relying Party can request step-up authentication for an ELIXIR user, and ELIXIR AAI delivers if it is available for the user. Following ELIXIR services are expected to require step-up authentication:

* Access to sensitive human data in biobanks and European Genome-Phenome Archive (EGA)
* Cloud management (a project representative launches a VM for his/her project)
* etc

**Technical Interfaces for Relying Parties**

ELIXIR AAI provides following interfaces to the Relying Parties

* SAML WebSSO Authentication request protocol
* OpenID Connect?
* X.509 credential translation (TO BE DEFINED)

# GROUPS AND ROLES

ELIXIR AAI has a service for managing ELIXIR users’ group memberships and roles in the groups they belong to. Management of groups is done in a web interface.

Each user can belong to one or several groups. This is represented by the user having a “member” role in the group. A group member can have also arbitrary additional roles in the group, such as “secretary” or “chair”.

Each group has one or several owners (members with a special role “owner”). The creator of a group becomes the initial owner of the group. The group owner is able to

* delegate group ownership to other members
* manage the group’s properties (such as name)
* invite group members (requires confirmation by the invited user)
* add group members (no confirmation needed by the invited user)
* remove group members
* assign and delete additional attributes (roles) for users in the group

The group owner needs to periodically confirm that the group is still active.

In the future, ELIXIR group management service can be integrated to external group management systems (e.g. VOOT or SCIM technology)

# BONA FIDE SERVICE

As described in section 1, any natural person is eligible to have an ELIXIR identity. On the other hand, use case analysis has demonstrated a need for certain “ELIXIR community membership” or “bona fide life science researcher” status which would qualify the user to some basic services. Those services cannot be made fully public (i.e. anyone with an ELIXIR identity) but, on the other hand, the administrational overhead for accessing the services is wanted to be kept in the minimum.

What exactly is required for receiving a status as a bona fide life science researcher is out of scope for this document. However, it is assumed to have the following components

* The candidate must commit to a certain community code
* The community must approve the bona fide status for the candidate

In ELIXIR AAI, “bona fide life science researchers” is a special group (see the previous section) with the following properties:

* The group has a shared ownership. Each ELIXIR organization has one person with the group owner role. That person can invite, add or remove persons from the group
* Additionally, an alternative way to receive bona fide status is that five existing ELIXIR users with the bona fide status vouch for the candidate
* else/what (the user has a publication in well-established life science magazine? Can this workflow be automated e.g. via ORCID API?)

The bona fide status is a property of a person and is not affected by his/her affiliation changes. However, the bona fide status expires over time and needs to be refreshed every \_\_\_\_ years. The refresh procedure is similar to the initial procedure for receiving bona fide status.

ELIXIR AAI must store sufficient history and audit trail for a person’s bona fide status.

# Dataset entitlement management

ELIXIR AAI has a workflow service dedicated for the management of the ELIXIR users’ access rights to resources, especially to sensitive datasets. The user applies for access rights to the datasets by filling in and submitting an electronic application with the necessary attachments. The application is then circulated to the individual or body (such as a Data Access Committee) evaluating the applications and approving or rejecting them or returning them for amendments. If approved, the members of the application receive access rights to the datasets applied.

The service has the necessary functionality for reporting and audit trail of the entitlements granted.

The entitlement service has interfaces for

* Importing dataset’s metadata from the data archive’s metadata catalogue for automated provisioning of the related application circulation workflows
* Launching a data access application from an external source, such as the portal of the data archive
* Exporting the entitlements to an external system for access rights enforcement

# ACCESS CONTROL LAYER

ELIXIR AAI defines a distributed interface for delivering access rights from the system component where they are granted and archived (Policy Decision Point, PDP) to the system component that enforces the access control (Policy Enforcement Point, PEP). A typical use scenario for the access control layer is the management of the access rights to sensitive datasets that are replicated to several data centers (PEP) but whose access rights are still granted centrally (PDP).

A pull model (PEPs query the PDP on demand) is assumed for the access control layer, in order to enable quick revocation of access rights in all PEPs.

Any particular technology is to be decided between the PDP and PEPs.

1. <http://paulgorman.org/technical/presentations/linux_username_conventions.pdf> [↑](#footnote-ref-1)
2. http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201310.html#eduPersonScopedAffiliation [↑](#footnote-ref-2)