EOSC-Life: Building a digital space for the life sciences

D5.2 – Access and User Management System for Life Science – the implementation and usage report

WP5 – User management and access services
Lead Beneficiary: MU and Instruct
WP leader: Ludek Matyska (MU) and Callum Smith (Instruct-ERIC)
Contributing partner(s): BBMRI, INFRAFRONTIER, INSTRUCT, ABO, USMI, CSC, MU

Authors of this deliverable: **Slavek Licehammer, Mikael Linden, Callum Smith**

Contractual delivery date: **30 August 2020**
Actual delivery date: **23 February 2021**
H2020-INFRAEOSC-2018-2

Grant agreement no. 824087
Horizon 2020
Type of action: RIA

Table of Contents

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.

Executive Summary

This deliverable summarizes current status of implementing an access and user management system for the European life science research infrastructures. The Life Science AAI (Authentication and Authorisation Infrastructure) provides a way to coordinate how user identity and access is managed in research services and data in the (community-specific) federated infrastructure. The service is managed by the life sciences community and operated by the e-infrastructures, specifically GEANT and EGI.

The work package has followed the Life Science AAI blueprint (Deliverable D5.1) to implement the AAI service from technical, policy and legal perspective. The Life Science AAI is fully implemented and ready to enter the production phase; the actual service launch is waiting for the e-infrastructures to become linked third parties in the project, covering thus the remaining legal part of the whole deployment. The first two services relying on Life Science AAI have been integrated and first end users onboarded. After launching the service, the intention is to continue developing the service and supporting the adoption among the end users and relying services.

This deliverable describes the technical architecture of the Life Science AAI and explains how implementation and delivery of the service is coordinated between EOCS-Life and the e-infrastructures. The deliverable includes current progress on policy work, which is crucial for operations of the service. Current state of the service is described as well as processes developed as part of the operations, including processes for registration services or processes for helpdesk coordination between EOSC-Life and e-infrastructures. The deliverable also covers updates on the access management system ARIA, including the steps for integration with Life Science AAI.

Project Objectives

With this deliverable, the project has reached/this deliverable has contributed to the following objectives:

- To implement federated life science authentication and authorization infrastructure (AAI) and access proposal/control system supporting access through different user entry points, managing user life cycle and controlling and providing fine grained access control to the resources.

Detailed report on the deliverable

Background

The need to authenticate researchers and manage their access rights is common to many research infrastructures. Research infrastructures need to protect access to confidential information (such as samples from human patients or information about ongoing or proposed research projects) or expensive resources (such as sophisticated instruments or computing capacity). This requires sufficient information who the users are (identity proofing and user authentication), whom they are representing (affiliation with a home organisation) and what resources they can access (authorisation). These services are called an authentication and authorisation infrastructure (AAI). For more information on the AAI terms, concepts and paradigms, refer to section 1 of CORBEL D6.5 [CORB19].

Providing services for researcher authentication and authorisation fits well the research infrastructures' mission to support researchers' work. Research infrastructures are permanent entities facilitating research projects in collaboration with the research communities. They are well connected in their domain and able to understand the common needs of their user communities. On the other hand, AAI is not a core business for research infrastructures; encouraging collaboration in the research and education sector with other actors (such as e-infrastructures) who have a long history of developing the underlying AAI technologies and services.

As a result of the past CORBEL WP5 and AARC2 projects, EOSC-Life WP5 was chartered to define and implement Life Science AAI. In September 2019, deliverable D5.1 presented the blueprint of the Life Science AAI, including its technical and non-technical requirements. This deliverable describes the project progress towards implementing the blueprint and launching a Life Science AAI service.

Some BMS RIs have been operating their RI-wide AAI services for several years, including BBMRI-ERIC AAI and ELIXIR AAI. While those AAIs have been important for understanding the BMS community's needs on AAI, the eventual goal of Life Science AAI is to enable their migration to the Life Science AAI during the EOSC-Life project. Migration of the existing AAIs to Life Science AAI will be covered in the upcoming deliverable D5.3.

Description of Work

1. Life Science AAI Service Ecosystem

Life Science AAI is the common Authentication and Authorisation service portfolio for the research infrastructures participating in the EOSC-Life project and beyond. The Life Science AAI ecosystem covers not only the technical part but also policies and operations. The goal is to deliver a fully functional ecosystem which might be used by users from all around the world without any technical or legal barrier.

The ecosystem consists of services/components operated by biological and medical research infrastructures, services/components provided by e-infrastructures and possibly other parts provided by third parties. This chapter is describing the architecture, how the service ecosystem is coordinated and applicable policies.

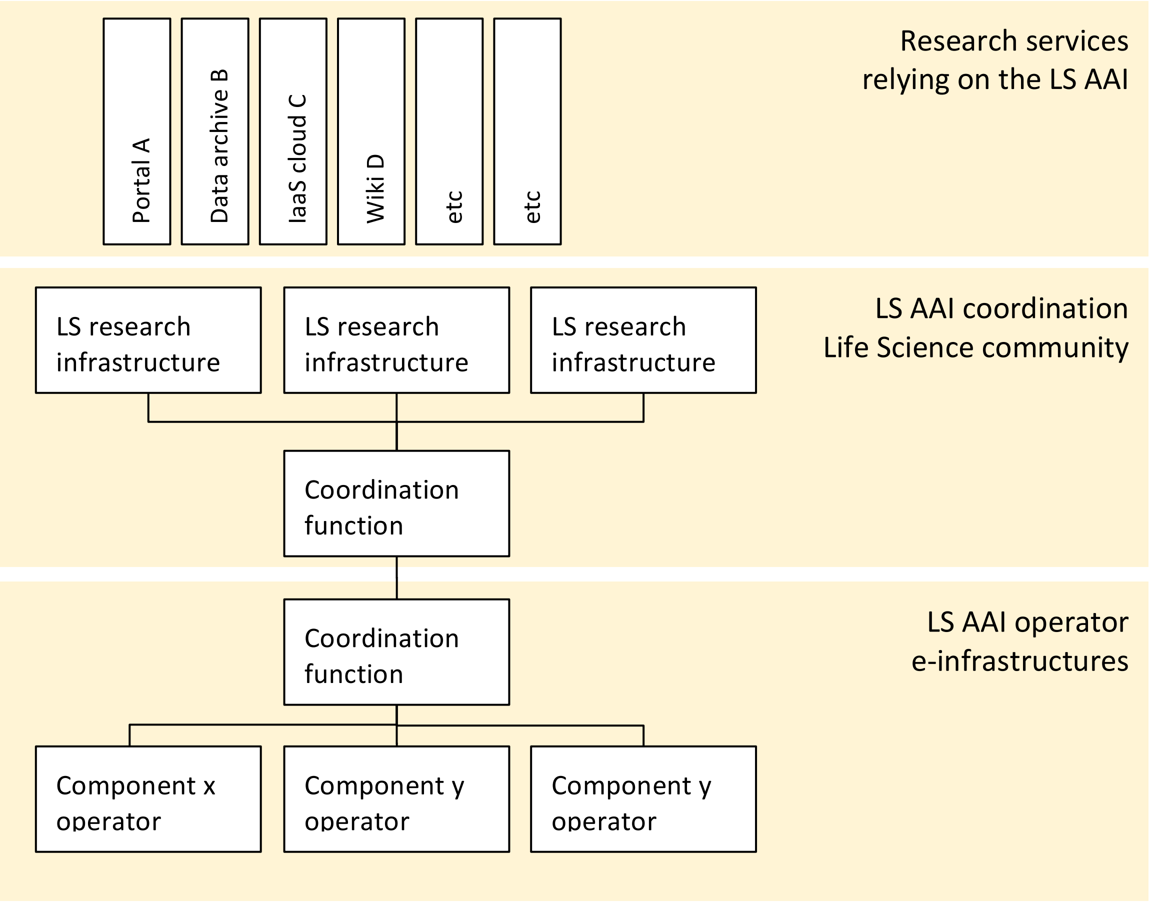
This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.

1.1 Service coordination

Life Science AAI is a service owned by the Life Science community, as represented by WP5 for the duration of the EOSC-Life project. In the adopted deployment model, e-infrastructures (EGI and GEANT) are operating the key technical components of the Life Science AAI.

The figure below outlines three layers

- Life Science AAI operators are the e-infrastructures running the technical components of the Life Science AAI.
- Life Science AAI coordination is the way for the Life Science community to organise the management and coordination of the Life Science AAI service.
- Services relying on the Life Science AAI are the customers of the Life Science AAI; the Life Science AAI exists to solve their needs on authentication and authorisation of the LS researchers. The services may be managed by the research infrastructures, organisations (such as universities or research institutes) affiliated with the research infrastructures, e-infrastructures or companies (such as commercial cloud providers). It is assumed that the relying services do not participate directly in the coordination of the Life Science AAI.


Portal A
Data archive B
IaaS cloud C
Wiki D
etc
etc
Research services relying on the LS AAI
LS research infrastructure
LS research infrastructure
LS research infrastructure
LS AAI coordination Life Science community
Coordination function
Coordination function
LS AAI operator e-infrastructures
Component x operator
Component y operator
Component y operator

The EOSC-Life WP5 has been the coordination function that drives the Life Science AAI related issues and discussion within the LS community and channels it to the Life Science AAI operators. In the similar way, the Life Science AAI operators have coordinated the operations of the Life

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.

Science AAI. Although informal communication is likely to take place in several channels, the formal dialogue (including potential agreements) between the Life Science AAI coordination and operation has been taking place between the two coordination functions.

The coordination has been taking place in two working groups:

- the technical deployment work has been coordinated by the Life Science AAI Technical working group
- the policy and legal framework for Life Science AAI has been coordinated by the Life Science AAI Policy working group

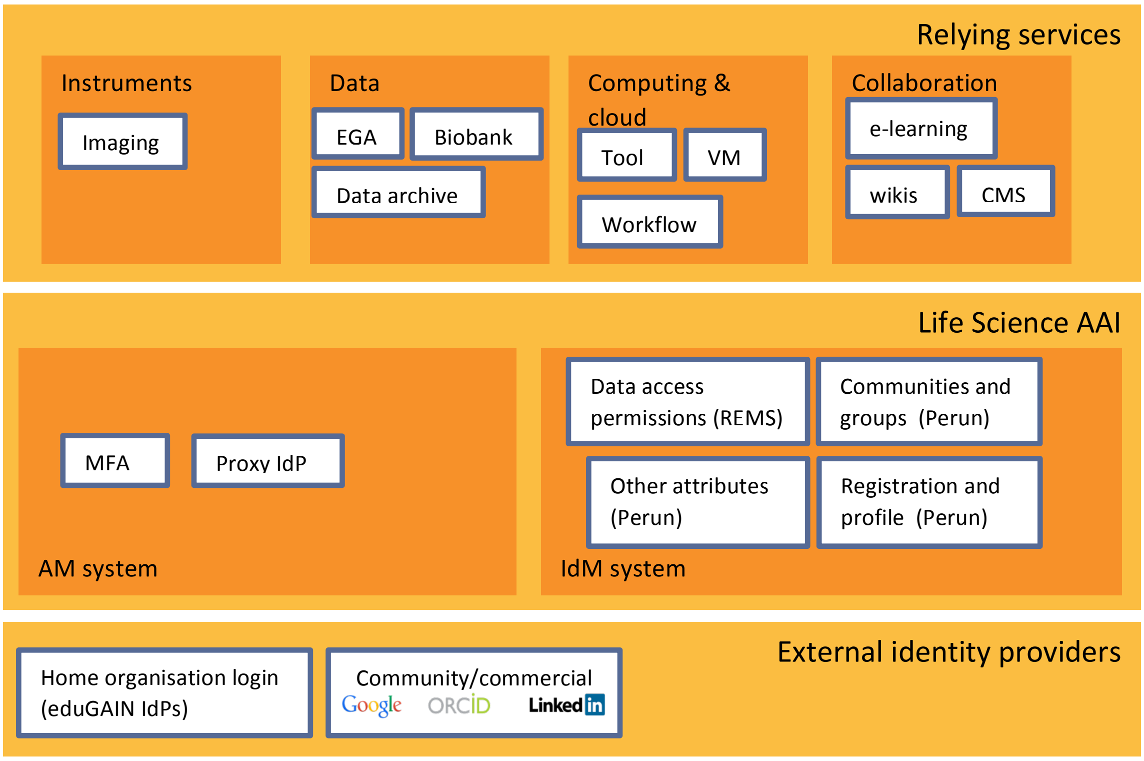
For the long-time sustainability of the Life Science AAI, it is necessary to identify the permanent entities that are responsible for organising the coordination functionality. However, presenting the long-term sustainable model for the Life Science AAI service is not in the scope of this deliverable.

1.2 Overall technical architecture

A proof of concept of an architecture for Life Science AAI was implemented during a pilot in collaboration with CORBEL WP5 and the AARC2 project in 2018. In September 2019, EOSC-Life WP5 delivered (Deliverable D5.1) an updated version of the technical requirements along with a new document describing the operational requirements and the available budget for the service. Even though the initial proof of concept architecture met most of the technical requirements, it became evident that the operational cost of the architecture would significantly exceed the available budget. Taking these into account, the e-infrastructures revisited the original architecture and produced a simplified, streamlined update focusing on delivering the required functional and operational requirements within the budget constraints of EOSC-Life. The technical architecture that has been deployed and is presented here is based on the streamlined model.

The diagram below illustrates the main components of Life Science AAI and its key integrations. A user logs in using an external identity provider, such as their home university or research institution logins (via the eduGAIN interfederation service operated by GEANT) or community or commercial alternatives (such as ORCID or Google). The Life Science AAI then gathers the authenticated user’s extra attributes from its internal sources and presents them to the services relying on Life Science AAI as illustrated in the upper part of the diagram. The relying services can be instruments (producing data for research purposes), data archives (managing data for secondary use), computing and cloud services (enabling researchers to compute on data) and various collaborative tools that support researchers’ interaction (such as, wikis, content management systems, mailing lists or e-learning environments).

This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 824087.



The internal architecture of Life Science AAI is composed from two main logical components: the identity management (IdM) system and the access management (AM) system. The key component of the access management is the IdP/SP Proxy component whose purpose is to handle user's authentication for the services connected to Life Science AAI. The proxy is an adapter between the external identity providers and the end services and in that role can do protocol and attribute translation when required by their specific needs. This opens a possibility for handling compatibility issues in a distributed environment where different actors have adopted heterogeneous technical approaches. The proxy is a critical component of the AAI because it handles all authentication transactions, therefore any outage of the proxy will have impact on all users.

Even though the main functionality of the proxy is mostly technical and therefore transparent for the users, the proxy is enhanced with other features realized as modules or separate components. The proxy can interrupt the user flow and interact with them. Typical use case is to redirect new users to registration, another example might be the check if the user is authorized to use the service which they are trying to access. If the user doesn't fulfil all conditions, the proxy can offer a solution in the form of immediate action (e.g. ask the user to commit to the necessary acceptable usage policy) or redirecting users to documentation or to a page where they can request access.

The proxy solely handles the whole authentication flow of the users; therefore, it is a logical place where stronger forms of authentication might be enforced. In some cases, the proxy can know if the stronger authentication method (e.g. multifactor authentication, MFA) was used by an upstream identity provider and react accordingly. For example, if the service which a user is trying

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.

to access requires strong authentication and it was not done by the external identity provider, the proxy can force users to perform multi-factor authentication provided by Life Science AAI. The proxy can even signal to the external identity provider that multifactor authentication is required, so the external identity provider can act accordingly.

The proxy is tightly integrated with the second main component which is the identity management system that manages all data related to the users and their identity, including their attributes. It also manages information required for authorization decisions, such as groups, roles or entitlements. The identity management system is designed to store data obtained from various sources. The primary sources are the users' external identity providers which may be authoritative sources for their role and affiliation in their home organisation. Using the APIs of the identity management system, data can be synchronized and stored also from other systems, such as REMS (Resource Entitlement Management System) and ARIA.

The identity management system provides a user interface where delegated managers can manage their users, organize them in groups and add access rights to them. Registration management is also available which enables managers to define registration flows to individual groups including user life cycle in the groups. Users without a manager role can access their own user profile to update their contact information, linked identities and other credentials (e.g. public keys for SSH secure shell access).

The identity management system is able to provision and deprovision user data or authorization rules to other services. This enables Life Science AAI to cater services where users don't sign in directly (e.g. management of mailing lists) or services which need to be notified promptly about user status changes even without direct users interactions (e.g. stopping cloud machines when the user is no longer authorized to use them).

In overall, the Life Science AAI architecture is designed to be modular. There are aforementioned two main logical components which act as a foundation for other components and integrations. The proxy handles anything related to user authentication flow, including connected external identity providers and the relying services. The identity management system can be used as a source or storage of data, or for an out-of-band integration.

The proxy is based on the SATOSA product and the identity management system on the Perun product. They both are operated by the e-infrastructures.

1.3 User registration and account linking

To start using Life Science AAI, a user needs to register a Life Science AAI and commit to the Life Science AAI Acceptable Usage Policy (AUP). Registration of a Life Science ID is open to anyone. The goal is to eliminate all barriers for users which might complicate usage of Life Science AAI. Users are encouraged to use their existing digital identities in the external identity providers to register a Life Science ID and authenticate it. Most academic users can use the digital identity provided by their home institution and made accessible through the academic identity federation eduGAIN. This is bringing comfort for users who don't need to manage another set of credentials, but can use the credentials which they are using on a daily basis in the home institution. That also covers typical problems with lost credentials and their recovery. Users can leverage the local support in their institution, which is more comfortable than any possible remote support by the

Life Science AAI operators. Moreover, if the home identity provider supports single sign-on, it will also cover authentication to Life Science AAI.

Alternative to using home institution identity providers is using community or commercial identity providers like ORCID, Google or LinkedIn. Those identity providers offer similar comfort like the academic ones and are available for the majority of users. As a last resort a Life Science Hostel identity provider will be provided, which enables users to create a new account with new credentials and use it as authentication to their Life Science ID. This solution might be suitable for users who cannot use other options or who prefer to have a local account only for Life Science AAI.

Utilizing an external identity provider requires to solve the possibility of one user having several options of external identity providers available. The Life Science AAI allows a user to link multiple external identities to a single Life Science ID. To link additional identity a user has to prove that they are able to authenticate with a new one as well as the one which is already linked. After the linking the user can use any of the linked identities to authenticate to their Life Science ID. Account linking might be automatically offered during registration of a new account when systems discover accounts with same or similar properties, for example an account using the same email address. In that case users can decide to only link a new identity instead of creating a new account.

Account linking is helping us with a situation when users are migrating from one institution to another which often means they will use the option to use the identity provider from the current institution, but they can use the one from the new institution. Using the same principle, users might link their personal social identity to have a backup way to access their Life Science ID in case they won't be able to use the primary authentication method. Last benefit of account linking is user comfort for users who are regularly using multiple authentication methods. Thanks to linked accounts users can choose any linked account to authenticate which will always lead to the same result.

1.4 Implementation progress

Implementation of Life Science AAI started in September 2019, after publication of deliverable D5.1. For the internal management and prioritisation of the implementation work, the features presented in D5.1 were distributed to three deployment phases called "bumps". Those formed the basis for monitoring the progress of the deployment.

The first "bump" had the theme "make it start" and covered the very necessary functionality; no viable Life Science AAI service can be offered without all of the features. It covered:

- deployment of key components, including the proxy identity provider (SATOSA) and the Identity Management service (Perun). (*)
- identity provider discovery service (for an end user to select their authentication provider) and its usability evaluation. (½)
- Proxy Identity Provider registration to eduGAIN (to enable end users log in with their home organisation identities) and selected commercial and community authentication providers (such as ORCID and Google). (*)
- flow for registering new users and populating their required attributes, including the user's approval of the Acceptable Usage Policy of Life Science AAI. (½)

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.

- flow for the registered users to link and unlink their Life Science ID to more identity providers. (½)
- endpoints (SAML 2.0 and OpenID Connect) to which the relying services can integrate to authenticate users and receive their attributes. (*)
- service to monitor the availability of the Life Science AAI components. (*)
- redundant setup, where the critical components of the Life Science AAI are run in at least two instances. (*)

The second "bump" had the theme "let relying parties and users in" and covered those features that build on top of the first bump and make it convenient for relying services and users to start using Life Science AAI. It covered:

- migration plan for ELIXIR AAI, BBMRI AAI and ARIA. (½)
- test environment where developers can test their service integration with Life Science AAI before exposing it to production use. (*)
- Hostel Identity Provider where those end users can create an account (with username and password) whose home organisation is not integrated to eduGAIN and who don't want to use the available community or commercial alternatives (like ORCID and Google) for login.
- automated tools and flows for relying service administrators to register and manage their services in Life Science AAI. (½)
- public statistics pages on the relying services registered to Life Science AAI and the number of logins by end users.

The third "bump" had the label "complete the functionality" and covered the rest of the features presented in deliverable D5.1; those features are not necessary for providing the basic service level of Life Science AAI and can be delivered later. It covered:

- service accounts that are needed when servers or machine accounts need to communicate with Life Science AAI or with each other.
- multi-factor authentication for relying services with higher security requirements and related framework to communicate achieved assurance levels to downstream services.
- manual management of affiliation information for users from those home organisations that cannot deliver the information programmatically (using the eduPersonAffiliation attribute delivered by the Identity Provider).
- other attributes relevant for relying services, such as home research infrastructure, home country, researcher status.
- delivery of permissions to access sensitive human data, following the emerging passport specification from the Global Alliance for Genomics and Health.
- active role selection, enabling a user with multiple roles (e.g. project memberships, affiliation) to select one for use in the current session.
- access control enforced in the proxy, enabling a relying service to request the Proxy Identity Provider to deny access for users who don't qualify to the access policy (e.g. group membership) configured for the relying service.
- credential translation, enabling an end user to receive an X.509 certificate if required for accessing a particular relying service. (*)
- complex protocol flows, such as the device code flow of OpenID Connect that enables e.g. Life Science AAI login with SSH Secure Shell
- service level reporting from e-infrastructures to the Life Science community

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.

The features presented with (*) were deployed and features with (½) were deployed partly in the end of January 2021.

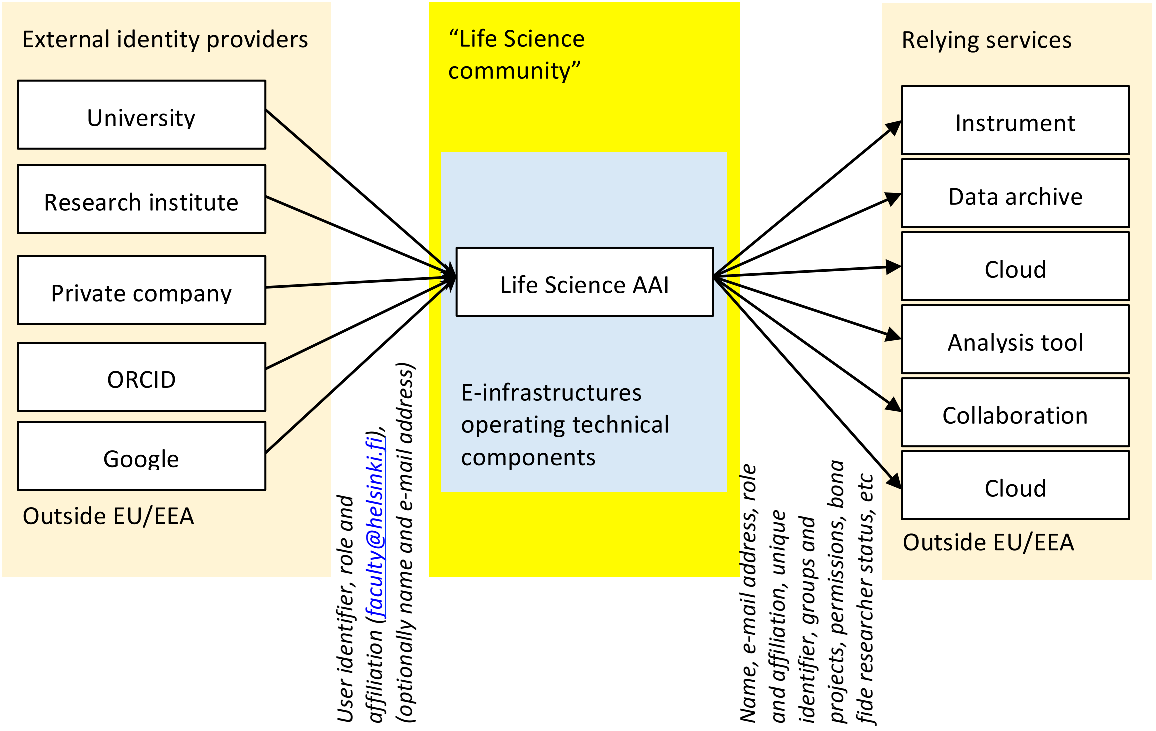
New requirements and clarifications to existing requirements are expected to be presented in the upcoming deliverable D5.3 which will be an update to the D5.1 “Access and User Management System for Life Science – The Blueprint”.

1.5 Life Science AAI Policy

This section gives a high level overview of the policy environment of Life Science AAI, including GDPR considerations, the contractual relations with external parties and the terms for the end users.

The Life Science AAI intends to be a permanent service with a sustainable governance and funding model that is developed later in the EOSC-Life project. This section does not cover the post-project model.

Overview and assumptions


External identity providers
University
Research institute
Private company
ORCID
Google
Outside EU/EEA
“Life Science community”
Life Science AAI
E-infrastructures operating technical components
Relying services
Instrument
Data archive
Cloud
Analysis tool
Collaboration
Cloud
Outside EU/EEA
User identifier, role and affiliation (faculty@helsinki.fi), (optionally name and e-mail address)
Name, e-mail address, role and affiliation, unique identifier, groups and projects, permissions, bona fide researcher status, etc

The diagram above gives a high-level view of the flow of information (personal data) that takes place when a researcher from an identity provider (such as, their home university) logs into a relying service via the Life Science AAI. The diagram highlights

- typical attributes that an identity provider may release to Life Science AAI and the Life Science AAI may release to a relying service.
- that some external identity providers and relying parties are established outside the European Economic Area.

This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 824087.

- that some components of the Life Science AAIs are operated by e-infrastructures as contractors of the Life Science community.

In the development of the policy, following assumptions related to the General Data Protection Regulation are made and will be further reflected to the approach in several policy documents:

- the external identity providers, Life Science Community and Relying parties (that manage the relying services) are all independent data controllers.
- during the project, Life Science Community is represented by Masaryk University who acts as the Life Science AAI data controller. For the post-project model the data controller may change.
- e-infrastructures (GEANT and EGI) are data processors, processing personal data on behalf of the Life Science community.
- all data released by Life Science AAI qualifies as personal data. No special categories of personal data are processed in Life Sciences AAI.
- the legal grounds of personal data processing is contract.

Virtual Organizations

Inside the Life Science AAI, research infrastructures and other communities may have their own smaller containers called “Virtual Organisations” (VO) that have their own pool of users and relying services not necessarily exposed to other VOs. A VO may

- introduce additional policies to users and relying services and impose its own approval criteria for them.
- manage extra user attributes that are not visible to other VOs.
- have nominated staff that have enhanced privileges to view and manage users and relying services in the VO.

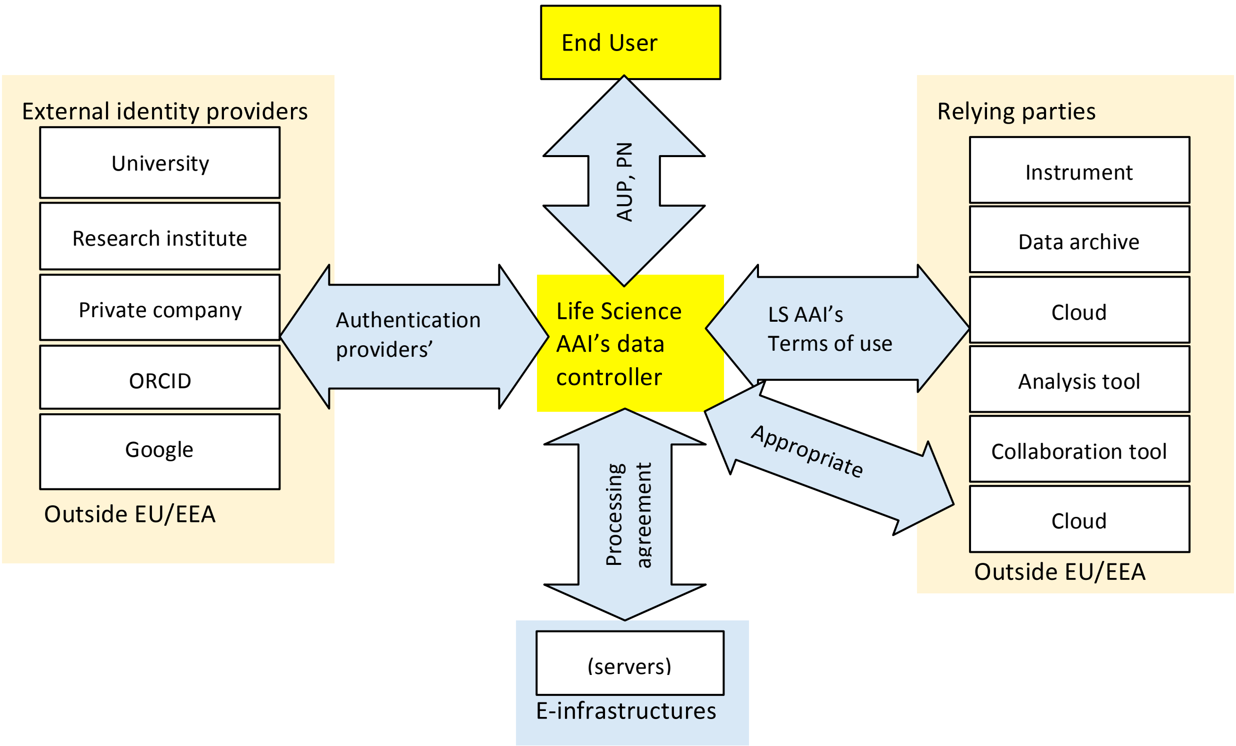
By default, all users and relying services belong to the catch-all VO “lifescience”. To avoid fragmentation and unnecessary obstacles for researchers consuming services from multiple research infrastructures, relying services are encouraged to make use of the catch-all VO to the extent possible.

The data controller of the Life Science AAI intends to be also the data controller of the VOs.

Contractual relations

This section highlights the contractual relationships the Life Science community (the Life Science AAI’s data controller) has with external parties and end users. The relationships are illustrated in the diagram and further described below.

This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 824087.



Life Science AAI's relation with end users are defined in the following policy documents:

- **The Acceptable Usage Policy** (AUP) for end users describes what Life Science AAI expects from an end user (don't share your credentials, don't do anything unlawful, etc). It also links to the Life Science AAI's privacy notice. (Appendix A.1)
- **The Privacy Notice** (PN) and **Cookie policy** for end users of Life Science AAI communicates to the end users in plain language what processing will be done on their personal data including the basis for the processing, their rights as data subjects, and GDPR contact points for their requests, complaints or enquiries. (Appendix A.2)

Life Science AAI's relation with other entities are described in the following contractual documents

- external identity providers' **Terms of use** cover the conditions under which the identity providers let Life Science AAI authenticate researchers against them and receive some of their attributes. These terms are typically set by the identity providers and cannot be negotiated (therefore they are not further discussed in this document). They normally exclude liability and cover requirements on data protection. Some terms (e.g. GEANT Data protection Code of Conduct and REFEDS Research and Scholarship) influence also the relying services of the Life Science AAI.
- Life Science AAI's **Terms of use for the relying parties** covers the obligations and rights between the Life Science AAI and the relying parties, including at least Life Science AAI's liability for service malfunction and poor quality and relying parties' data protection obligations. (Appendix A.3)

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.

- some relying services of Life Science AAI may be established outside EU/EEA and countries with adequate data protection. GDPR expects Life Science community has in place **appropriate safeguards** for those transfers of personal data (e.g. EC model contracts)
- e-infrastructures (GEANT, EGI) are assumed to operate the technical core components of the Life Science AAI on behalf of the Life Science community. The e-infrastructures are data processors for the Life Science community and the Life Science AAI data controller will have a **data processing agreement** with them.

Furthermore, Life Science AAI has some common policies which are applicable to several actors:

Who does the policy apply to Policy	Relying Parties	Virtual Organisations	Life Science AAI controller (and operator)
Service Operations security policy	X	X	X
Incident response procedures	X		X
Policy for processing personal data	X	X	X
Membership management policy		X	

- **service operations security policy** introduces the baseline expectations for operational information security that all need to comply with. (Appendix A.4)
- **incident response procedures** introduces step by step instructions for the security contact of the Life Science AAI and relying service in case of an information security incident. (Appendix A.5)
- **policy for processing personal data** defines the principles that must be followed in processing an end user's personal data. (Appendix A.6)
- **membership management policy** defines the obligations of the research infrastructures or other communities who choose to introduce and manage a VO of their own. (Appendix A.7)

Related policy work

Several components of the Life Science AAI policy are based on the Policy Development Kit (PDK)[1] prepared and published by the AARC project. To make the policy fit the needs of the Life Science community, some key adjustments are listed below

- redesigning the "infrastructure" concept. In the PDK, infrastructure covers not just the AAI but also "the IT hardware, software, networks, data, facilities, processes and any other elements that together are required to develop, test, deliver, monitor, control or support services" which are, in turn, defined as "components fulfilling a need of the users, such as computing, storage, networking or software systems." This wide definition of infrastructure goes beyond the mandate of the Life Science AAI which focuses only on the AAI service.
- Following from the narrower definition of the AAI service, also the Top level policy was dropped from the set of policies. As the Life Science AAI service is owned (initially) by

[1] https://aarc-project.eu/policies/policy-development-kit/

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.

Masaryk University, a document defining Masaryk University's internal managerial responsibilities was not found relevant.

1.6 User Experience Analysis

When building the AAI for the life sciences community it is essential that we meet the expectations of our users with the mechanisms by which they login. While the power of a multi-federated authentication platform is very useful for service operators and for authorization attributes and identity vetting, the average user 'simply wants to log in'. As such a frictionless authentication flow is essential for the success of the platform. An extensive user experience analysis has been performed building on the work done in the REFEDS community regarding proposed interfaces for authentication.

We began by identifying the key objectives of Life Science AAI and what we aim to achieve through the use of Life Science AAI. It was also key for us to define what the user communities that Life Science AAI will serve look like and identify some 'personas' that represent those user groups. We also assessed the existing interface that was available for the ELIXIR AAI page as a starting point of how the Life Science AAI may look when it moves to production and identified key problems and objectives to improve it. Competitor analysis was also performed using some of the key authentication technologies that people are used to using day to day. We assessed ORCID, Microsoft 365, Google, LinkedIn, OneLogin and Facebook. This was driven by a strong belief that whilst the platform is research focussed, users should not have to re-learn new mechanisms for authenticating to these tools that they already know through their experience of other tools they are likely to use day to day.

Problem

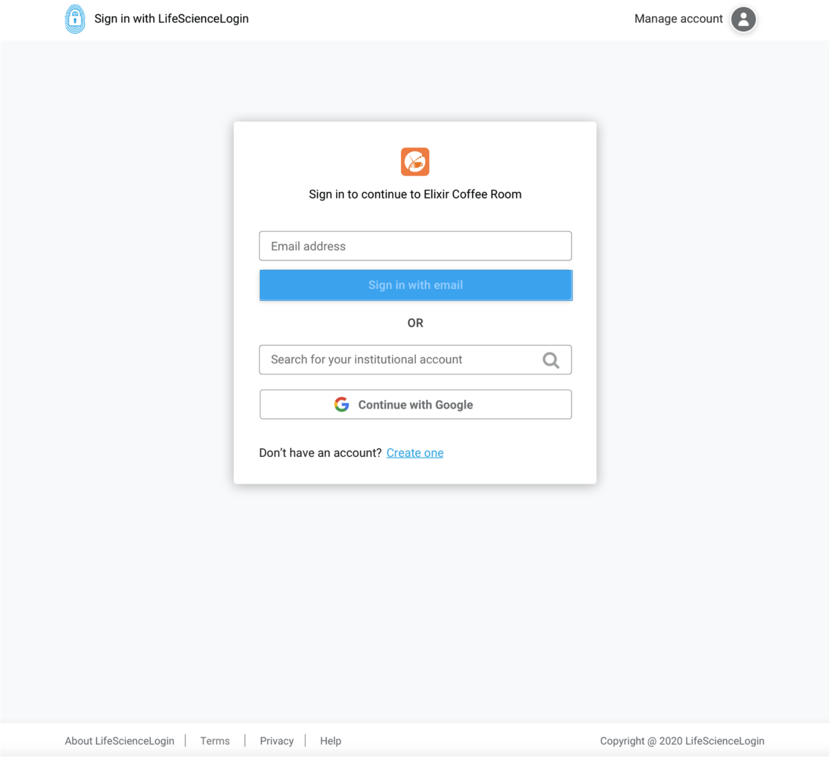
- Users are given too many login options (on login page)
- People have multiple institution login accounts along with social accounts, having to log in to various services with different accounts

Objectives

- Drive adoption of institutional logins for identity vetting purposes
- Streamline onboarding, offboarding and general usability
- Simplify login page and consolidate multiple login options
- Create a trusted brand that scientists and students will adopt

User stories are a method of capturing things that a user may want to do when using a piece of software. We identified the user stories for all of the aspects of login for Life Science AAI which were aligned to one or more of the personas. From these user stories, objectives and existing UIs for ELIXIR AAI we were able to produce a number of wireframe prototypes for a new login system. This prototype focused on users entering an email address as the primary step and being guided through the authentication workflows as a result.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.


Sign in with LifeScienceLogin
Manage account
Email address
Sign in with email
OR
Search for your institutional account
Continue with Google
About LifeScienceLogin | Terms | Privacy | Help
Copyright @ 2020 LifeScienceLogin

Sign in to continue to Elixir Coffee Room

Don't have an account? Create one

The image above is an early prototype of the authentication workflow that still features the social login on the home page. These screens were formed into a click-through prototype and then a number of users were invited to perform a user test. We used a tool called Lookback to perform these user tests. The user was given a scenario based around the user stories identified earlier in the process and key tasks to perform relating to the authentication flows. Lookback software allows us to record both the user's face and voice along with their browser window as they are going through the tasks. Users are encouraged to talk through their experience as they use the prototype and feedback any comments about the process as they go through it. From this we can identify common pain-points with quantitative analysis of the results and ensure that we are not shifting the design based on individual preference.

Having performed the user test we further iterated on the UIs which are now pending implementation. The email-lookup feature requires additional work performed to allow us to align a user's email address with an organisation in a simple way. We will be building a new UI theme to sit on top of the existing Life Science AAI platform to enable this new workflow without affecting the components providing the service.

2. Life Science AAI Operations

Technical operation of the key components of Life Science AAI components is handled by e-infrastructures, who are operating them and also improving them and enabling new functionality in the context of the technical requirements specification of Life Science AAI. Operations covers also the Life Science AAI helpdesk, documentation and processes which are designed based on the capabilities of the technical solutions provided by e-infrastructures.

To support the operational aspects the Life Science login web page[2] was created to aggregate all information for users. Currently it contains a description of the service, including a list of benefits which it offers, design instruction for using the login and register buttons of Life Science AAI and the acceptable usage policy. For the future this page will contain all relevant information for users, for example the user documentation will be available there.

2.1 Current status

Life science AAI is currently available only for members of EOSC-Life project. On a technical level it is prepared to be made available for all users, but there are some details pending in the policy and contractual area which have to be resolved before the AAI will be made public.

The operations with internal users has so far verified the feasibility of the technical solution as well as accompanied processes, including user and service registrations communications using the support channels. Life Science AAI is built on components whose capabilities were proven in deployments in other projects. Also, the architecture is similar to those successfully used in other projects. Thanks to this, it has been confirmed that a quite similar solution with the same components is already operated for thousands for users. Therefore, we are not expecting any issues when Life Science AAI will be made available for all interested users.

2.2 New releases and acceptance environment

The Life Science AAI has two identical environments - the production and the acceptance environment. The production environment is the main one, accessible to end users and where all services will be integrated. The acceptance environment is an exact copy of the production one, but it is hidden from common users. Its purpose is to test new features and configuration changes before it will impact users.

The acceptance environment is especially useful for testing changes in Life Science AAI which will have an impact on user flows in the system or on the user experience in general. It gives an option to test new upgrades thoroughly and assess their impact on users. It also makes it easier to mitigate such impact, for example, to update user documentation or notify users about upcoming changes.

Individual Life Science AAI components can be usually tested even without the acceptance environment but sometimes it is not possible to test complete functionality unless all components are in place. The acceptance environment can be also used for verifying that a new feature behaves as it was intended and there has been no misunderstanding in their requirement.

Therefore, all changes in the components, regardless if they are new features or just maintenance updates, will be deployed on the acceptance environment first. Only after acceptance by the life science representatives, the change will be deployed in the production environment and made available for all users.

[2] https://lifescience-ri.eu/ls-login/

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.

2.3 Test environment for new relying services

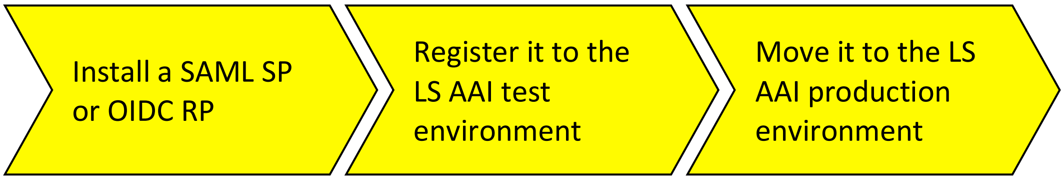
Also, the developers of the relying services want to make sure their service integration to Life Science AAI is fully tested before exposing the service to the end users. Even though the process for registering a new relying service (see the next section) is straightforward, there is some configuration on the service side which might be more complex. For this reason there is a test environment for the new relying services where all services are registered first and only after the service integration is verified it will be moved to production and made available to the users.

The test environment for relying services is an isolated area within the production environment of Life Science AAI. The acceptance environment described above is not used for testing new relying services because the acceptance environment is for testing and verifying new functionality for the whole Life Science AAI itself. The new relying services need to connect to the stable (production) environment where they can be tested by their developers.

The test environment for relying services is behaving exactly the same as the production one. The only difference is that the users who can log into the service are limited to those who have opted in for the service test environment. This setting guarantees that the service developer is able to test the integration themselves or with any other users if there is a need to. Moving the service from the test to the production environment is done exclusively on the Life Science AAI side, without any change on the relying service or its configuration. Therefore, if the service integration was properly tested in the test environment, there is a guarantee it will work in the production environment as well.

2.4 Process for registering a relying service

Each relying service which wants to use Life Science AAI for authentication and authorization must be registered at first. During the registration process, the new relying services are first exposed to the test environment described above. The process is further described below.


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

Before starting the service registration process, the service owner has to make sure the service's Acceptable Usage Policy (AUP) is not in conflict with the Life Science AAI's AUP that all end users accept when they register their Life Science ID. The service owner can extend the Life Science AAI's AUP with service specific extra terms but those cannot conflict with it. The service owner is also responsible for presenting the service specific extra terms to an end user.

Step 1: Install a SAML SP or OIDC RP

The developer of the relying service is responsible for installing and configuring the necessary software to integrate to the Life Science AAI. Life Science AAI supports currently two technical protocols that a service owner can choose from:

- Security Assertion Mark-up Language 2.0 (SAML 2.0), using a SAML Service Provider (SP) software
- OpenID Connect (OIDC), using OIDC Relying Party (RP) software

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.

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

The Life Science AAI test environment is a sandbox where the relying service developer can test their service's integration to Life Science AAI without exposing the service to common end users.

1. The service developer has to have a Life Science ID or register it for themselves.
2. The service developer has to decide what user attributes (user information) will be needed for the SP/RP.
3. The service developer has to register the SP or RP in Life Science AAI using the SP Registry page[3]
4. The Life Science AAI operator checks the data and informs the service developer that the service is registered to the Life Science AAI test environment.
5. For a consistent user experience, the Life Science AAI has published design guidelines for the login page of the SP/RP that the service developer is encouraged to adopt.
6. The service developer needs to decide if Life Science AAI should enforce access to the service based on the user's membership in a particular group, the user having sufficient level of assurance, or any other attribute.
7. The service developer should configure their
    - SAML SP to consume the Life Science AAI proxy IdP's SAML2 metadata file[4]
    - OIDC RP to point the OIDC well-known configuration endpoint[5]

Step 3: Move the SP/RP from Life Science AAI test to Life Science AAI production environment

When the service developer has tested their service sufficiently in the test environment, they need to contact the Life Science AAI support desk and ask to move the service to the production environment.

2.5 Process for onboarding new identity providers

All external identity providers (IdP) compatible with SAML2, OIDC or OAuth2 protocols can be technically integrated to the Life Science AAI. Currently there are two kinds of IdPs integrated: Academic identity providers which are available via the research and education identity federation eduGAIN, and commercial or community identity providers like Google and ORCID.

Commercial and community IdPs can be easily onboarded because the project has decided to support only a few of them, making it possible to test them completely. With eduGAIN, the situation is more complicated. The project wants to integrate all IdPs from eduGAIN to offer the option to use home organisation IdP for as many users as possible. However, there are thousands of IdPs in the eduGAIN and, therefore, it is not possible to verify the integration will work for all of them. The verification is complicated by the fact that normally a valid account in the IdP is needed to do it, but the accounts are usually available only for users from the institution which operates the IdP. Therefore, there is no technical option to fully automate such verification process and scale it on all eduGAIN IdPs.

[3] https://webapp.aai.lifescience-ri.eu/sp_request
[4] https://mdx.aai.lifescience-ri.eu/entities/https%3A%2F%2Fproxy.aai.lifescience-ri.eu%2Fmetadata%2Fbackend.xml
[5] https://proxy.aai.lifescience-ri.eu/.well-known/openid-configuration

The Life Science AAI has adopted an onboarding process where all eduGAIN IdP are initially integrated in the technical level but not exposed to be available for the users. During the sign-in process the users are presented with the list of only those IdPs who have been demonstrated to work. The users have also an option to try to sign-in using another IdP which has not been demonstrated to work, with a warning that the sign-in might fail. If the user manages to successfully sign-in with such an IdP, the onboarding process will be completed on the background which results in the IdP being fully enabled. For the future an additional process will be added which will cancel the onboarding of an IdP where problems have been detected.

2.6 Helpdesk

Helpdesk processes are crucial for smooth operations of Life Science AAI, because users need to authenticate to services and any interruption is preventing them from doing their work. Moreover, due to the distributed nature of the environment and usage of identity federations some of the workflows might be complex and inexperienced users might have problems to navigate through. Even though there is an ongoing work to enhance the user experience, there will always be users who need help to solve their issues.

Apart from end users, the helpdesk has to support also the technical part of the AAI, like connecting new services, changes in the service integration, questions about technical aspects of the AAI and so on. Last aspect of the helpdesk is to handle any questions and requests related to the AAI, which might be both technical and non-technical.

Based on the requirements above it is clear that the helpdesk must be able to represent the LS community as well as e-infrastructures responsible for technical implementation of Life Science AAI. It was agreed the helpdesk will be structured in three layers. Layer 1 support (L1) will handle initial contact with requestor, gather relevant information and offer basic advices (e.g. provide documentation). L2 will handle advanced problems which doesn't require technical expertise. L3 is for technical issues which require technical debugging or fixing problems on the service side.

For L1 helpdesk is crucial to know the users and their requirements. Therefore, L1 will be handled by the life sciences community. The L3 is strictly technical, so it has to be handled by the operators of the individual components. Currently, e-infrastructures are the only one who are operating such components, but for the future, there is expectation of specialized services operated by the life science community, which will mean L3 support even for those.

Level 2 helpdesk can be handled by either the life science community or the e-infrastructures. The initial proposal from e-infrastructures contained L2 operated by them, but during the implementation and pilot run of Life Science AAI was discovered that both L1 and L2 can be handled by a single team, which might even speed up resolution of requests. Therefore, both approaches to L2 are currently being discussed and the final decision will come in near future.

2.7 Documentation

Documentation is tightly related to helpdesk processes. Both L1 and L2 helpdesks need technical documentation to be able to navigate users and help with their problems. The technical documentation is provided by the e-infrastructures who are developing, configuring and operating individual components of Life Science AAI. Based on that the documentation for end users and use-facing services operators will be created by the L1 helpdesk. This will be within the

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.

competency of the L1 helpdesk, because it should take into account specifics of the Life Science AAI users and terminology they are accustomed to use.

The process was established within the Technical working group, which describes how the technical documentation is created by e-infrastructures, discussed within the Technical WG and then passed to the L1 helpdesk team. The helpdesk team will consequently process the technical documentation and create and publish user-facing documentation and manuals on the LS login web page[6].

3. ARIA access management for EOSC-Life RIs

ARIA access management is used across a number of research infrastructures on the ESFRI road map and TNA projects. It is primarily developed by Instruct-ERIC. In CORBEL ARIA was used as a platform for exploring opportunities to identify cross-RI use cases and automating parts of the access management. In order to further the goals of cross-RI applications it was clear that ARIA needed additional enhancements to existing functionality. We have also extended ARIA to better manage independent calls which was utilised in the open calls of EOSC-Life.

3.1 ARIA Development enhancements to meet RI use cases

Extending ARIA to meet existing use cases across the RIs that utilise it for management functions is essential for both the operations of RIs and for identifying opportunities to share experience on management and implementation of calls, access and delivery of access (whether to data or physical infrastructure). In this tranche of work we focussed on extending our calls management to integrate our powerful automated peer review system from the access management side of the application. We also looked at visits management and performed an extensive user experience review and implemented a significant uplift in terms of new functionality to allow facilities to better report on visit progress. A new authentication system has just been launched for ARIA that will allow the service to be completely forward compatible with Life Science AAI and take advantage of modern authentication technologies.

Integrated review of calls management

Automated review is a significant feature with ARIA and has been essential to the platform since its inception. There are two mechanisms by which users can submit an application/proposal to ARIA, one of them is through the access management system, that has a whole management package around visits, and delivery of access. The second mechanism is calls, which is a much more streamlined mechanism of application management which has much simpler post-award management and reporting. It became clear that whilst the two mechanisms are valuable to be distinct methods of managing applications that the automated peer review would be very valuable to call management in addition to access.

Peer review of applications in calls has been implemented identically to the feature set in access management. At either call creation or by editing the call at a later point the call administrator can define two pools of users named “moderators” and “reviewers”.

[6] https://lifescience-ri.eu/ls-login/

This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 824087.

An application can only have one moderator assigned to it. The role of the moderator is to take a decision about the proposal, choosing to approve or reject it. They can do this at any point after they are assigned to the proposal by a call administrator. This role is used in many different ways by different call administrators, sometimes this is a representative of a review panel, sometimes they are part of the review team for the access, or alternatively this role is assumed by a call administrator. Once they are assigned to the proposal they are invited, via email, to assign a number of reviewers to the application. Once the minimum number of reviewers have completed their review the moderator is informed that the application is eligible to be actioned. When they action the proposal, they can either choose to approve or reject it. Each call can have completely independently configured forms for both review and moderation.

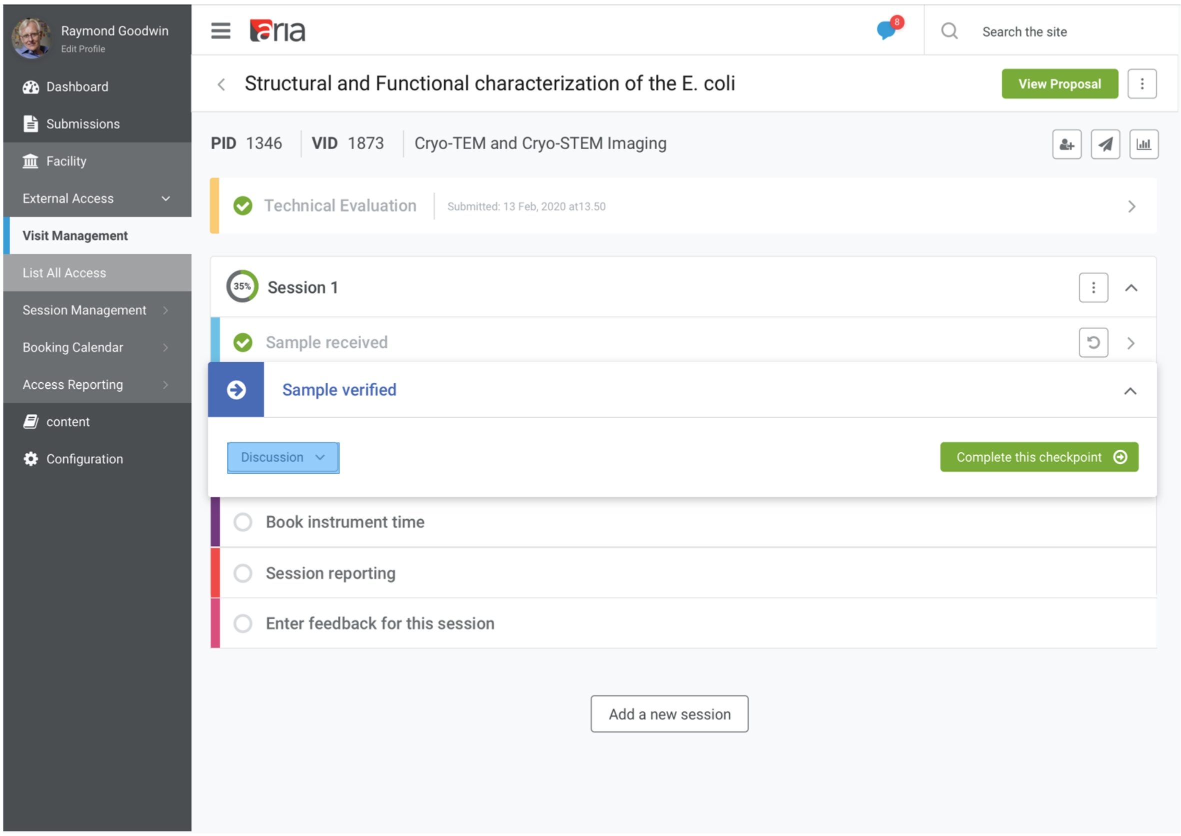
Reviewers, when they are assigned to review an application, are informed via email with a simple one-click link which will (after login) take them directly to a page with all the information they need to review. On this page they are given the review scoring form, the application detail and any guidelines they may need to complete the review. Should the application be actioned before their review is completed, they will be informed that their review is no longer required. If they are not able to review for any reason, then there is a link for them to indicate this in the initial email they receive. If this causes the total number of available reviewers below the minimum threshold for the call, then the moderator will be informed to add another review to the team.

Visit management improvements

As part of the tracking delivery of access visits management is the name given to the system in ARIA where facilities can detail information about the progress of the access. The term ‘visit’ has become somewhat a misnomer as this system is capable of tracking access whether physical, remote or indeed digital access to the service/technology. Utilising this visit management, the facility can keep the user clearly up to date with exactly the progress of their project and report metrics regarding the access to the infrastructure. A long-standing feature of visits management has been integrated scheduling for physical access and configurable ‘steps’ for remote access. It was clear through discussions with facilities and access-providers that these were not all encompassing. As such we began a project to enhance the visits management to better track the delivery of access and give facilities more tools for enhancing their own management of projects.

To start we performed an extensive user experience review of the current toolset to understand the missing requirements in the software. From this it was clear that a number of gaps lie in the current separation of the handling of ‘physical’ and ‘remote’ access. While ARIA created a distinction with how these visits were managed, the reality is that facilities may require a mixture of both. Physical access may require a number of “steps” to be completed before scheduling of an instrument can take place. Additionally, a remote access may still need to be scheduled on an instrument as part of delivering the access. We proposed a new unified access workflow that would allow for remote and physical accesses to have separately configured workflows with ‘checkpoints’ (an evolution of the previous ‘steps’ mechanism for the remote access) having the capacity for custom checkpoints with integrated functionality (such as instrument scheduling/booking).

We also identified, with the help of EU-OpenScreen, some gaps in the current visit tracking features and planned to add two new features for these checkpointed workflows. Now there is a ‘notebook’ feature where the facility and the access users can add information, files and other data to the checkpoints on an access. This has become a key feature as more access has gone remote in the COVID-19 situation. The other feature was worked in collaboration with University of Leeds, one of the access providers within the Instruct-ERIC RI and EU-OpenScreen again to capture some financial information around the delivery of access.



Having identified all of the core user stories and use cases for the visits management upgrade we built wireframe prototypes of the new procedures. Armed with these prototypes we contacted a number of key stakeholders identified within the user storying process to do some user tests and iterate on the wireframes based on feedback. After this we resulted with the visit-view that is shown above.

Once we had all the prototypes in place, we began work on upgrading the backend functionality to incorporate the new features and implemented the new UI. This new UI and features were presented at the ARIA workshop that was held in February 2020 jointly with CORBEL, iNEXT-Discovery and Instruct-ULTRA and had a total of 40 participants. The changes were released for general consumption in April of 2020.

Upgrading ARIA authentication and authorisation in preparation to adopt Life Science AAI

As ARIA grows, it became clear that we can not continue to use SAML2 as our primary authentication technology. SAML2 is largely a stateful authentication mechanism which relies heavily on browser sessions to maintain state between different page loads. It also relies on the web server responding to the request to also maintain a session of the user’s information to perform a successful authentication. ARIA now has multiple services that make up the whole application, so delegating tasks to those services with SAML2 in an authenticated way is impossible without complex state management. As such we have implemented an OpenID Connect authentication mechanism for all of the services inside the ARIA application.

The existing user database of ARIA is large at over 10,000 users. Migrating to Life Science AAI is a complex issue, further compounded by the nature of the users that make up this database. For the most part ARIA users are wet-lab scientists who are not experts in data tools or computation. As a result authentication must be completely seamless and easy for these users and not introduce additional hurdles to the process. Migrating the user database cannot be done automatically for a number of reasons, both technical and procedural. As such we need ARIA to be in a position to take advantage of a multi-stage migration process that allows the users to grow confidence in the Life Science AAI service.

The stages we proposed were Implementation, Migration and Adoption. In the first phase users can opt-in to login via Life Science AAI through an option on the ARIA login interface. Secondly, in the Migration phase, the Life Science AAI login will be prominently featured as the main mechanism to login, with other options still available, but less prevalent. The final Adoption phase will be a complete utilisation of Life Science AAI with all existing mechanisms to login disabled.

To ensure that we can support all three phases properly we have separated our identity and access management service out of the ARIA-core software. We have set up a Keycloak authentication service to provide the IAM platform for ARIA and built a custom adapter to allow users to migrate to this new authentication technology without any form of interruption or change to their logins. Passwords are fully migrated on their first login to the platform and no action is required from the user outside of accepting additional terms and conditions for the identity platform.

3.2 Implementation of ARIA to support EOSC-Life Calls

ARIA has been used in EOSC-Life for open calls in the three work packages WP9 (training), WP1 (data sets), and WP3 (open calls). The implementations for each of these calls was slightly different and tailored to the needs of that specific call.

WP9 training call utilised the ARIA calls management software as tracking of delivery of access was not relevant for the call. We implemented a custom theme for ARIA based on the EOSC-Life website and branding toolkit. This is essential for any setup of ARIA as the user must not feel lost when they arrive at the application system. We also worked with the team in WP9 to ensure all the correct questions and configurable options were implemented correctly. The automated review system discussed in 4.1.1. of this report was not ready for the time of this call, so review and reports were handled manually for this call.

WP1 internal call again utilised the same ARIA calls management software however now with the new developments that allow the automation of the peer review for these applications. No additional templating was required as the style from the WP9 template was generic enough to fit this use-case nicely.

WP3 open call was slightly more complex in review procedure so it was decided to use the access management system for this call. Slight modifications to the existing template were implemented to add the “contact the experts” buttons to the process and to include an EOSC-Life call dashboard where applicants could see all currently open EOSC-Life open calls, and past and

This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 824087.

present applications in one place. More information on the processes implemented for this call can be found in D3.1 of the EOSC-Life project [EOSC20].

3.3 Implementation of ARIA to support EOSC-Life Research Infrastructures

As part of widening access to the ARIA access management software we have been working with individual research infrastructures within EOSC-Life to set up their processes in ARIA. At the time of the deliverable, we have implemented the following:

Infrastructure	**Project**	**Implementation**
MIRRI	IS_MIRRI 21	DPA signed Contract agreed Integrated template Access route(s) configured Open for access
EMBRC	EMBRC (RI)	DPA signed Contract signed
EU-OpenScreen	EU-OpenScreen DRIVE	DPA signed Contract agreed Integrated template Access route(s) configured Open for access

Next steps

The main effort is now focused on moving Life Science AAI in production, meaning making it available for all users and all services. It is expected that might shift the priorities for the improvements of the service and it also might bring some new requirements which will be considered in the upcoming deliverable D5.3 on the upgrade of the Access and User Management System for Life Science Blueprint. It will also increase demands on the operations aspects of the service, which might lead to changes in existing processes (e.g. helpdesk processes) or even require developing new processes.

Connecting additional services may bring new technical challenges. However, components used in Life Science AAI are also used in other projects which have very similar architecture to Life Science AAI, therefore the project is not expecting problems on a technical level. There might be a peak in the number of services requesting registration when the service will be launched, which might bring additional workload on helpdesk. There is a possibility to organize a training for registering services to Life Science AAI which will have the services owners with the registration process and technical integration of their services.

Through our experience in CORBEL, we have identified the need to have easy to adopt GDPR templates to help establish access offerings that span across multiple research infrastructures. As

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.

part of delivering on Objective 1 of WP5 we will be looking at building a policy toolkit to help infrastructures produce these necessary GDPR arrangements to establish these calls. This work will underpin the multi-RI access applications project within ARIA to enable these to be configured quickly and easily.

For the credibility of the Life Science AAI service, it is necessary to make sure the service has a sustainable long-term funding and governance model. During the remaining project, the focus of the policy development work will shift towards defining the post-project service model that ensures the relying services feel confident to rely on Life Science AAI also in the long run.

References

AARC19 AARC2 project. Blue-print architecture. https://aarc-project.eu/architecture/

CORB19 Linden, M., Boiten, J., Courtot, M., Holub, P., van de Geijn, G., ; van Enckevort, D., Lappalainen, I., Nyrönen, T., Parkinson, H., Reihs, R., Senf, A., Spalding, D., Swedlow, J., Swertz, M., Törnroos, J., Kankaanpää, P., van Iperen, E. CORBEL Prototype implementation of distributed automated data access request, review and authorization and delivery systems. June, 2019. http://doi.org/10.5281/zenodo.3238496

EOSC20 Haley, N., Leitner, F., Bischof, J., Audergon, P. EOSC-Life Publication of generic guidelines for the organization of topic-specific Open Calls. September, 2020. https://zenodo.org/record/4048442

Abbreviations

AAI	Authentication and Authorisation Infrastructure
API	Application Programming Interface
ARIA	Access to Research Infrastructure Administration
BMS	Biological and Medical Sciences
GA4GH	Global Alliance for Genomics and Health
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
ID	Identifier

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.

IdP	Identity Provider
LS	Life Sciences
OIDC	OpenID Connect
RI	Research Infrastructure
SAML	Security Assertion Mark-up Language
SP	Service Provider
UI	User Interface
UX	User Experience
WP	Work Package

Delivery and schedule

The delivery is delayed: Yes

D5.2 has been delayed from August 2020 to February 2021 for the following reason: The Life Science AAI deployment was delayed. This was mostly due to delays in preparations of the policy and contractual aspects of the LS AAI.

Adjustments

Adjustments made:

None

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 824087.

Appendices

Appendix A. Life Science AAI policies

A.1. Acceptable Usage Policy

A.2. Privacy Notice

A.3. Terms of Use for Relying Parties

A.4. Service Operations security policy

A.5. Incident Response Procedures

A.6. Policy for processing personal data

A.7. Membership management policy (pre-final draft)

LS LOGIN

Acceptable Usage Policy and Conditions of Use

for users authenticating themselves using Life Science Login

This procedure is effective from <insert date>.

This Acceptable Use Policy and Conditions of Use (“AUP”) defines the rules and conditions that govern your access to and use of the resources and services (including transmission, processing, and storage of data) available to Life Science Login users. This includes the services relying on Life Science Login to authenticate their user and to make authorization decisions. These relying services are provided for the purpose of research and collaboration in life sciences. LifeScience Login and all the relying services are further denoted as “Services”.

This AUP is based on the WISE AUP 1.0[1] model and governs your use of Life Science Login to access the relying services. The AUP also acts as a baseline for your use of the relying services themselves, and these services may further extend the AUP with their own additional terms.

1. You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show consideration towards other users including by not causing harm to the Services; you have an obligation to collaborate in the resolution of issues arising from your use of the Services.
2. You shall only use the Services for lawful purposes and not breach, attempt to breach, nor circumvent administrative or security controls.
3. You shall respect intellectual property and confidentiality agreements.
4. You shall protect your access credentials (e.g., passwords, private keys or multi-factor tokens); no intentional sharing is permitted.
5. You shall keep your registered information correct and up to date.
6. You shall promptly report known or suspected security breaches, credential compromise, or misuse to the security contact stated below; and report any compromised credentials to the relevant issuing authorities.
7. Reliance on the Services shall only be to the extent specified by any applicable service level agreements listed below. Use without such agreements is at your own risk.
8. Your personal data will be processed in accordance with the privacy statements referenced below.
9. Your use of the Services may be restricted or suspended, for administrative, operational, or security reasons, without prior notice and without compensation.
10. If you violate these rules, you may be liable for the consequences, which may include your account being suspended and a report being made to your home organization or to law enforcement.

The administrative contact for this AUP is: admin@aai.lifescience-ri.eu

[1] This AUP is based on WISE SCI Baseline AUP 1.0.1 (25 Feb 2019) which is the work of the Members of the WISE Community SCI Working Group (CC-BY-NC-SA 4.0).

The security contact for this AUP is: security@aai.lifescience-ri.eu
The privacy statements (e.g., Privacy Notices) are located at: TBD[i]
LS-AAI is provided on a best-effort basis and provides no service level agreement.

[i] Link to the public listing of LS AAI relying services (where the privacy notice links are listed).

LS LOGIN

Privacy Notice for Life Science Login

This policy is effective from <insert date>.

Name of the Service	Life Science Login (“LS Login” in short)
Description of the Service	Life Science Login carries out the authentication of users and manages and delivers their access rights and other relevant personal data to the services relying on it.
Data controller	Masaryk University
Data controller’s data protection officer (if applicable)	poverenec@muni.cz
Jurisdiction and supervisory authority	CZ Czech Republic, The office for personal data protection[1]
Personal data processed	LS Login gathers contact and identifying information, such as: name, email address, membership in the groups you are affiliated to, external identifiers provided by your identity providers (e.g., unique identifier, affiliation). LS Login also gathers permissions and other information that defines user’s authorization to access services.
Purpose of the processing of personal data	LS Login processes your personal data to identify and authenticate you as a user of the services, and to manage your access rights and other personal data for the services. Processing of this kind of personal data is necessary for the performance of the contract between you and Life Science Login (provision of authentication and authorization infrastructure (AAI) services). The log files produced by the LS Login components will be used only for administrative, operational, accounting, monitoring and security purposes. Personal data of this kind are processed based on legitimate interest of the LS Login provider.

[1] https://www.uoou.cz/en/

Other Sources / Attribution / Acknowledgements: The research leading to these results has received funding from the European Community’s Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Template derived from the GÉANT Data Protection Code of Conduct version 2, used under CC BY-NC-SA 4.0.

Third parties to whom personal data is disclosed	LS Login will release your personal data to the services you are using. LS Login service may use third party services (personal data processors) for the LS Login service operation. Current list of the processors is: - GEANT[2] - EGI.eu[3] The logged information may be disclosed to other authorised participants via secured mechanisms, only for the same purposes and only as far as necessary to provide the services, usually done as a part of security and operational incident handling.
How to access, rectify and delete the personal data and object to its processing	Go to the page https://perun.aai.lifescience-ri.eu/profile/ or contact the Data Protection Officer above. To rectify the data released by your Home Organisation, contact your Home Organisation's IT helpdesk.
Data retention	Your personal data is deleted on request or if you have not used/logged in to LS Login service for 24 months. The operational logs and related information are kept independently in order to guarantee the security of the infrastructure and its optimization.
Data Protection Code of Conduct	Conduct for Service Providers[4], a common standard for the research and higher education sector to protect your privacy.

[2] https://www.geant.org/

[3] https://www.egi.eu/

[4] http://www.geant.net/uri/dataprotection-code-of-conduct/v1

Other Sources / Attribution / Acknowledgements: The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Template derived from the GÉANT Data Protection Code of Conduct version 2, used under CC BY-NC-SA 4.0.

Terms of use for Relying Parties (Service Providers)

These terms are effective from <insert date>.

You are reading this because You wish to rely on the Life Science Authentication and Authorisation Infrastructure ("LS AAI") and its LS Login service for user authentication and authorisation in your Service. These Terms of Use govern Your use of the LS AAI. By using LS AAI You accept that Your use of LS AAI will be subject to these Terms. These Terms will be binding and enforceable on You as contractual obligations. If You do not accept these Terms, then You must not use LS AAI.

Compliance with applicable legislation
You are obliged to ensure that You hold all necessary licenses, permits and rights and that You comply with any and all applicable laws in connection with the use of LS AAI.

Compliance with LS AAI policies
You are obliged to ensure that you recognise and comply with the following LS AAI policies and procedures:

- Service Operations security policy
- Incident response procedures
- Policy for processing personal data

Users' compliance
All users of the LS AAI are subjected to the Acceptable Use Policy.

Liability
Your use of LS AAI is entirely at your own risk. Nothing in these Terms of use creates any liability on the part of LS AAI.

Other agreements
If You have a direct agreement with LS AAI Service Owner, that agreement shall take precedence over these Terms. In any other case, the provisions of these Terms shall take precedence.

Governing law and jurisdiction
These Terms and any dispute or claim arising out of or in connection with them or their subject matter or formation (including non-contractual disputes or claims) shall be governed by and

construed in accordance with the legislation of the Czech Republic. The courts of the Czech Republic will have exclusive jurisdiction over any such dispute or claim.

Eligibility

You confirm that you are a duly authorised representative of Your organisation for approving these Terms of Use as a contractual obligation for Your organisation.

Definition of terms used in this and referenced documents

LS AAI Life Science Authentication and Authorisation Infrastructure, a service operated by the LS AAI service owner and potentially uses the brand LS Login for the Users.

LS AAI Service Owner. The LS AAI data controller. Masaryk University for the duration of EOSC-Life project or its post-project successor.

Service *(also: Relying Service)* A service that relies at least partly on the LS AAI for authenticating its users and managing their access rights.

Service Provider *(also: Relying Party)* An entity responsible for the management, deployment, operation and security of a *Service.*

User An individual authorised to access and use *Services.*

Virtual Organisation A group of *users*, organised with a common purpose, and jointly granted access to one or more Services. It may act as the interface between individual *Users* and *Services*.

Participant A Service Provider, the LS AAI service owner or a Virtual Organisation.

Security Contact *A group or individual responsible for operational security of the LS AAI or a Service.*

Service Operations Security Policy

This is the Service operations security policy for Life Science Authentication and Authorization Infrastructure (LS AAI) and the Services relying on it.

This policy is effective from <insert date>.

By running a Service, you agree to the conditions laid down in this document and other referenced documents, which may be subject to revision.

1. You shall provide and maintain accurate contact information, including at least one Security Contact who shall support Sirtfi [R1] on behalf of the Service.
2. You are held responsible for the safe and secure operation of the Service. Any information you provide regarding the suitability and properties of the Service should be accurate and maintained. The Service shall not be detrimental to the LS AAI nor to any of its Participants.
3. You should follow IT security best practices including pro-actively applying updates or configuration changes related to security. You shall respond appropriately, and within the specified time period, on receipt of security notices from the LS AAI or any of its Participants. You must support the Sirtfi Framework [R1] on behalf of your Service.
4. You shall document your processing of personal data in a Privacy Statement that is displayed to the User and whose link is made available to the LS AAI.
    a. You shall apply due diligence in maintaining the confidentiality of user credentials and of any data you hold where there is a reasonable expectation of privacy.
    b. You shall collect and retain auditing information in compliance with policies and procedures [R2], and must assist the LS AAI in security incident response.
    c. You shall use logged information, including personal data, only for administrative, operational, accounting, monitoring and security purposes. You shall apply due diligence in maintaining the confidentiality of logged information.
5. Provisioning of Services is at your own risk. Any software provided by the LS AAI is provided on an as-is basis, and subject to its own license conditions. There is no guarantee that any procedure applied by the LS AAI is correct or sufficient for any particular purpose. The LS AAI and other Participants are not liable for any loss or damage in connection with your participation in the LS AAI.
6. You may control access to your Service for administrative, operational and security purposes and shall inform the affected users where appropriate.
7. Your Service's connection to the LS AAI may be controlled for administrative, operational and security purposes if you fail to comply with these conditions.

Upon retirement of a Service, the obligations specified in clauses 1, 4 and 5 shall not lapse for the retention period of 6 months agreed with the Infrastructure.

[R1] https://refeds.org/sirtfi
[R2] https://docs.google.com/document/d/1rK2mBBNFYibuuejk63D5UCgIJjVd7jO3wdLThD2OHkQ/edit#

Incident Response Procedure

This procedure applies for any suspected or confirmed security breach with a potential impact on the LS AAI or on other Participants.

This procedure is effective from <insert date>.

The procedure builds on the function of the LS AAI Security Contact.

Security Incident Response Procedure for Service Providers

1. Aim at containing the security incident to avoid further propagation whilst aiming at carefully preserving evidence and logs. Record all actions taken, along with accurate timestamps.
2. Report the security incident to the LS AAI Security Contact point within one local working day of the initial discovery or notification of the security incident.
3. In collaboration with the Security Incident Response Coordinator (identified by the LS AAI Security Contact):
    a. Collect and strive to identify indicators of compromise (IoCs)
    b. Share incident status reports and IoCs with all affected participants (a “heads-up” and subsequent updates as needed), in the LS AAI and federation via their security contact (and, if needed, in other federations and with any external trusted entity involved)
4. Announce suspension of service (if applicable) in accordance with LS AAI, federation and interfederation practices. Public announcements should not contain details other than “Security operations in progress”, unless agreed otherwise with the LS AAI Security Contact point.
5. Perform appropriate investigation, system and network analysis and adequate forensics, and strive to understand the exact cause of the security incident, as well as its full extent. Identifying the cause of security incidents is essential to prevent them from reoccurring. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected participants.
6. Share additional status updates and IoCs as often as necessary to keep all affected participants up-to-date with the security incident and enable them to investigate and take action should new information appear.
7. Respond to requests for assistance from other participants involved in the security incident within one working day and investigate new IoCs being shared.
8. Take corrective action, restore access to service (if applicable) and legitimate user access.

9. In collaboration with the Security Incident Response Coordinator, produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labelled TLP AMBER or higher.
10. Update documentation and procedures as necessary.

Roles and responsibilities of the LS AAI security contact

The Security Contact coordinates the operational security capabilities of the LS AAI, including the enabling of compliance with the Sirtfi framework. The Security Contact may, in consultation with the LS AAI Service Owner and other appropriate entities, require actions by Participants as are deemed necessary to protect the LS AAI from or contain the spread of IT security incidents. The Security Contact is responsible for establishing and periodically testing a communications flow for use in security incidents.

Security Incident Response Procedure for the LS AAI Security Contact

1. Assist Participants in performing appropriate investigation, system and network analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. The time and effort need to be commensurate with the scale of the problem and with the potential damage and risks faced by affected participants.
2. Report the security incident to their federation security contact point within one local working day of the initial discovery or notification of the security incident.
3. Coordinate the security incident resolution process and communication with affected Participants until the security incident is resolved:
    a. Collect and strive to identify indicators of compromise (IoCs) from all involved entities
    b. Share incident status reports and IoCs with all affected Participants (a “heads-up” and subsequent updates as needed), in the LS AAI and federation via their security contact (and, if needed, in other federations and with any external trusted entity involved). If other federations are affected, the eduGAIN security contact point must be notified, even if affected participants in all other federations have been contacted directly.
4. Ensure suspension of service (if applicable) is announced in accordance with LS AAI, federation and interfederation practices.
5. Share additional status updates and IoCs as often as necessary to keep all affected participants up-to-date with the security incident and enable them to investigate and take action should new information appear.
6. Assist and advise participants in taking corrective action or restoring access to service (if applicable) and legitimate user access.
7. Produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labelled TLP AMBER or higher.
8. Update documentation and procedures as necessary.

Policy on the Processing of Personal Data of the LS AAI service

This policy is effective from <insert date>.

INTRODUCTION

This policy ensures that data collected as a result of the use of the LS AAI and Services is processed fairly and lawfully by Participants. Some of this data, for example that relating to user registration, monitoring and accounting contains “personal data” as defined by the European Union (EU) [GDPR]. The collection and processing of personal data is subject to restrictions aimed at protecting the privacy of individuals.

DEFINITIONS

In addition to the definitions in the Terms of Use for Service Providers document:
Personal Data - Any information relating to an identified or identifiable natural person [GDPR].
Processing (Processed) - Any operation or set of operations, including collection and storage, which is performed upon Personal Data [GDPR].
End User – An individual who by virtue of their membership of a recognised research community is authorized to use LS AAI services.

SCOPE

This policy covers Personal Data that is Processed as a prerequisite for or as a result of an End User’s use of LS AAI and Services. Examples of such Personal Data include registration information, credential identifiers and usage, accounting, security and monitoring records.
This policy does not cover Personal Data relating to third parties included in datasets provided by the End User or the research community to which they belong as part of their research activity. Examples of such data are medical datasets which may contain Personal Data.

POLICY

Participants:

1. Declare that they have read, understood, and will abide by the Principles of Personal Data Processing as set out below.
2. Declare their acknowledgement that failure to abide by these Principles may result in exclusion from the LS AAI, and that if such failure is thought to be the result of an unlawful act or results in unlawful information disclosure, they may be reported to the relevant legal authorities.

PRINCIPLES OF PERSONAL DATA PROCESSING

I. The End User whose Personal Data is being Processed shall be treated fairly and in an open and transparent manner.

II. Personal Data of End Users (hereinafter “Personal Data”) shall be Processed only for those administrative, operational, accounting, monitoring and security purposes that are necessary for the safe and reliable operation of LS AAI and Services, without prejudice to the End Users’ rights under the relevant laws.

III. Processing of Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are Processed.

IV. Personal Data shall be accurate and, where necessary, kept up to date. Where Personal Data are found to be inaccurate or incomplete, having regard to the purposes for which they are Processed, they shall be rectified or purged.

V. Personal Data Processed for the purposes listed under paragraph II above shall not be kept for longer than the period defined in a relevant LS AAI or Service policy governing the type of Personal Data record being Processed (e.g. registration, monitoring or accounting) and by default shall be anonymised or purged after a period of 24 months.

VI. Appropriate technical and organisational measures shall be taken against unauthorised disclosure or Processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data. As a minimum, Participants shall:

   A. Restrict access to stored Personal Data under their control to appropriate authorised individuals;

   B. Transmit Personal Data by network or other means in a manner to prevent disclosure to unauthorised individuals;

   C. Not disclose Personal Data unless in accordance with these Principles of Personal Data Processing;

   D. Publish to the LS AAI a single contact point to which End Users or other Participants can report suspected breaches of this policy;

   E. Respond to suspected breaches of this Policy promptly and effectively and take the appropriate action where a breach is found to have occurred;

   F. Perform periodic audits of compliance to this Policy and make available the results of such audits to other Participants upon their request.

   G. Ensure each Service interface provided for the End User must provide, in a visible and accessible way, a Privacy Policy containing the following elements:

      1. Name and contact details of the Data Controller Processing Personal Data;
      2. Description of Personal Data being Processed;
      3. Purpose or purposes of Processing of Personal Data;
      4. Explanation of the rights of the End User to:

         a) Obtain a copy of their Personal Data being stored by the Data Controller without undue delay;

b) Request that any Personal Data relating to them which is shown to be incomplete or inaccurate be rectified;

c) Request that on compelling legitimate grounds Processing of their Personal Data should cease;

d) Other rights compelled by the GDPR.

5. The contact details of the Data Controller to which the End User should direct requests in relation to their rights above;
6. Retention period of the Personal Data Processed.

H. Personal Data may only be transferred to or otherwise shared with individuals or organisations where the recipient:

1. has agreed to be bound by this Policy and the set of common LS AAI policies, or
2. is part of a recognised Computer Incident Response Team framework and as part of an incident investigation to prevent active or suspected misuse of Infrastructure services, or
3. presents an appropriately enforced legal request.

GEANT DATA PROTECTION CODE OF CONDUCT

If the LS AAI or Service receives personal data that is released under the condition that its recipient protects the data according to GEANT Data protection Code of Conduct, the recipient commits to follow the aforementioned code for that data.

Membership Management Policy

A template to be instantiated and adopted by each Virtual Organization using the LS AAI as its tool to manage membership

Pre-final Draft

This policy is effective from <insert date>.

INTRODUCTION

This policy is designed to establish trust between a Community and other Communities, Infrastructures, and the R&E federations.

This Policy applies to the Community Manager and other designated Community management personnel. It places requirements on Communities regarding eligibility, obligations and rights of their Users, and it governs their relationships with all Services and Infrastructures with which they have a usage agreement. The Community management personnel must ensure awareness and acceptance, by the Community and its Users, of the responsibilities documented in this Policy.

DEFINITIONS

A Community is a set of one or more groups of persons (Users), organised with a common purpose, with a Community Management willing to take responsibility for all sub-groups, jointly granted access to one or more Infrastructures. It may serve as an entity which acts as the interface between the individual Users and Services. In general, the members of the Community will not need to separately negotiate access with Service Providers or Infrastructures (hereafter jointly called Infrastructures).

Examples of Communities include, but are not limited to: User groups, Virtual Organisations, Research Communities, Research Infrastructures, Virtual Research Communities, Projects, Communities authorised to use particular portals or gateways, and geographically organised communities.

Life Science Login has a “LifeScience” community and may have additional Communities.

INDIVIDUAL USERS

The Community must define an Acceptable Use Policy (AUP) [ref]. The AUP must be shown to all persons joining the Community. Acceptance of the AUP by Community members who act as responsible persons towards the Services must be an explicit action, must be recorded, and must be a prerequisite for registration in the Community. The AUP must address at least the following areas:

- The aims and purposes, and the basis of membership of the Community
- Acceptable use

- Non-acceptable use
- Maintenance of user registration data
- Protection and use of credentials
- Data protection and privacy

The Community may rely on an Infrastructure AUP to address one or more of these requirements, provided that acceptance of such an Infrastructure AUP, in addition to the Community AUP, by the User is a prerequisite for registration. The Community AUP must not be in conflict with the referenced Infrastructure AUPs.

The data protection and privacy section of the AUP must address the relationship with the Infrastructure policies on the Processing of Personal Data, Security Traceability and Logging, and Service Operations Security.

Community procedures must ensure that the User is informed of and explicitly consents to material changes to the AUP, including those that arise out of new collaborative partnerships [ref], as soon as is feasible.

Hosts, Services and/or Robots (automated processes acting on behalf of the Community or a User) may be registered as members of the Community. In the case of such registrations, the Registration Data must include the personal details of the individual requesting registration who must assume, as a User, ongoing responsibility for the registered entity, and may be subject to additional policy requirements of the Infrastructure.

All Users are deemed to be acting in a professional capacity when interacting with or using Services or Infrastructure Resources assigned to the Community.

COMMUNITY MANAGER AND OTHER ROLES

The Community must define a Community Manager role and assign this role to two or more individuals. The Community Manager is responsible for meeting the requirements of this Policy and those of the applicable Policies of the Services and Infrastructures, and for implementing the necessary procedures and operational requirements [ref].

The Community Manager does not necessarily have to be a member of the Community. The role may be performed by any individual so designated by the Community, including Infrastructure personnel.

The Community Manager must implement procedures that ensure the accuracy of individual user registration data for all Community members who act as responsible persons towards the Infrastructure. The contact information must be verified both at initial collection (registration) and on an ongoing basis (through periodic renewal or review) [ref] and only stored and processed in compliance with applicable Data Protection legislation.

Other Community roles, such as additional management personnel and security contacts must be defined and assigned to individuals as specified in the Community Operations Security Policy [ref] or as required by the Infrastructure.

COMMUNITY

Aims and Purposes

As described above, the Community must define, in its AUP, its collective aims and purposes, i.e., the research or scholarship goals of the Community. In order to allow Infrastructures to make decisions on resource allocation [ref], the Community should make this definition available to them, and subsequently inform them of any material changes therein [ref].

Membership

The Community Manager is responsible for the Community Membership life cycle process of its Users [ref]. This responsibility may be devolved to designated personnel in the Community or in the Infrastructure, and their trusted agents (such as Institute Representatives or Resource Centre Managers), hereafter collectively called Sponsors.

The Community procedures must

- unambiguously name the individuals who take responsibility for the validity of the Registration Data provided [ref],
- ensure there is a way of contacting the User identified as responsible for an action while using Infrastructure services as a member of the Community [ref], and
- identify those with the authority to exercise control over the rights of its members to use the Infrastructure Resources assigned to the Community.

The Community must be aware that inappropriate actions by an individual member of the Community may adversely affect the ability of other members of the Community to use an Infrastructure [ref].

Membership Life Cycle: Registration

Membership Registration is the process by which an applicant joins the Community and becomes a Member. Registration Data must be collected at the time of Registration, verified and stored in compliance with the Data Protection and Privacy Policy [ref]. Reasonable efforts must be spent to validate the data.

The applicant must agree to abide by the AUP of the Community, and agree to use Resources of the Infrastructures exclusively for the Aims and Purposes of the Community.

Membership Life Cycle: Assignment of Attributes

Assignment of attributes (such as group membership, entitlements, or roles) shall be the responsibility of the Community Manager or of designated person(s) responsible for the management of such attributes.

Attribute management may be subject to an assurance profile agreed upon between the Community and the Infrastructures. Attributes shall be assigned only for as long as they are applicable.

Membership Life Cycle: Renewal

Membership Renewal is the process by which a User remains a member eligible to use Infrastructure Resources assigned to the Community. Membership Renewal procedures must make a reasonable effort to

- ensure that accurate Registration Data is maintained [RC4,RC5] for all eligible Users
- confirm continued eligibility of the User to use Infrastructure Resources assigned to the Community
- confirm continued eligibility of the User to any attributes
- ensure the reaffirmation of acceptance of the AUP of the Community

The maximum time span between Registration and Renewal, and between Renewals, for all Community members who act as responsible persons towards the Infrastructure, shall be one year. The User shall be able to correct and amend their Registration Data at any time.

Membership Life Cycle: Suspension

The Suspension of Community membership is the temporary revocation of full or partial rights and of any attributes. Suspension is done by or on behalf of the Community Manager.

A User should be suspended when the Community Manager is presented with reasonable evidence that the member's identity or credentials have been used, with or without the user's consent, in breach of relevant Policies.

Suspension can be requested by

- the Community Manager, the Sponsor of the User, those responsible for the assignment of attributes, or the User
- Security Officer(s) or designated operational staff of the Infrastructure
- Resource Centres participating in the Infrastructure

The Community Manager must cooperate fully with the investigation and resolution of security incidents reported by the Security Officer(s) of any Infrastructure [ref], including acting on any requests for suspension without delay.

Unless it is considered detrimental to the investigation and resolution of a security incident, the Community Manager should contact the User that was or is about to be suspended. The Community may define a dispute resolution process by which a User can challenge a Suspension.

User's rights shall not be reinstated unless the Community Manager has sent timely prior notification to all those who requested Suspension.

Membership Life Cycle: Termination

The Termination of Community membership is the removal of a member from the Community. Following Termination, the former member is no longer eligible to use Infrastructure Resources assigned to the Community and the Community must no longer assert membership or attributes for the former member.

In absence of overriding reasons, a request by the User for removal must be honoured.

The events that shall trigger re-evaluation of the User's membership of the Community include:

- a request by the Sponsor,
- failure to complete a membership Renewal process within the allotted time,
- end of collaboration between the User and the Community,
- end of collaboration between the User's Sponsor and the Community, if applicable,
- end of collaboration between the User and his/her Sponsor, if applicable.

PROTECTION AND PROCESSING OF PERSONAL DATA

The Community must have policies and procedures addressing the protection of the privacy of individual Users with regard to the processing of their personal data collected as a result of their membership in the Community and of their access to resources provided by any Infrastructure. These policies must be made available in a visible and easily accessible way and Users must explicitly acknowledge acceptance of these policies [ref] (through the AUP and registration process).

The Community must inform the User (through the AUP and registration process) of the policies on the processing of Personal Data of those providers with which it has entered into agreements and that can access the User's Personal Data [ref].

The Policy on the processing of Personal Data of the Community [ref] shall address at least the items in A.5 section 7 of the Template Policy on the Processing of Personal Data of the AARC

Recommendations and template policies for the processing of personal data [Ref], as amended from time to time.

It is recommended that any personal data stored by the Community is time-stamped in order to determine when it is appropriate to remove data that is no longer necessary for audit, traceability or any legal requirements.

AUDIT AND TRACEABILITY REQUIREMENTS

The Community must record and maintain an audit log of all membership lifecycle transactions. This audit log must be kept for a minimum period consistent with the Traceability and Logging Policies of all Infrastructures that provide resources to the Community. Audit logs containing personal registration data must not be retained beyond the maximum period allowed by the Policy on the processing of Personal Data of the Community (e.g. for as long as a member is registered and entitled to use resources and one year after this data is no longer associated with such an active membership or attribute assignment).

Events that must be logged include every request for:

- Membership,
- assignment of or change to a member's attributes,
- membership renewal,
- membership suspension,
- membership termination or re-evaluation.

Each logged event should record the date and time, the originator, the details of the event, and whether or not it was approved. The identity of the person granting or refusing the request should be recorded, including any verification steps involved and other people consulted, such as Sponsors.

REGISTRY AND REGISTRATION DATA

The Community must operate, or have operated on its behalf, a Registry that contains the membership data of the Community. This registry must be operated in a secure and trustworthy manner and in compliance with the security requirements of the Community and of the Infrastructures [OS1] in terms of authentication, authorisation, access control, physical and network security, security vulnerability handling and security incident handling. The Registry must also be operated in a manner compliant with REFEDS Sirtfi version 1 [Ref] [OS3].

The Registry must store at least:

- Registration data, including personal data of the User
- attributes assigned to members

The Registration data for a User comprises verified information on at least:

- family name(s)
- given name(s)
- the employing organisation name and address
- any applicable Sponsor identity
- a professional email address
- unique and non-reassigned identifier(s) of the User and the source of authority of each identifier

and is recommended to contain:

- professional contact telephone number so as to inform the User promptly during the investigation of security incidents and of lifecycle events
- other contact information, as voluntarily provided and maintained by the User.

The types of information recorded must be listed in the Policy on the processing of Personal Data of the Community.