Coordinated Research Infrastructures Building Enduring Life-science services
- CORBEL -

Deliverable D5.2
Report on Common Access Framework Concept

Lead Beneficiary: Instruct and INFRAFRONTIER
WP leader: Susan Daenke (Instruct-ERIC), Michael Raess (INFRAFRONTIER)
Contributing partner(s): Instruct, EMBL, MDC, INFRAFRONTIER, CSC, BBMRI-ERIC

Contractual delivery date: 30 April 2019
Actual delivery date: 3 May 2019

Authors of this deliverable: Natalie Haley

Grant agreement no. 654248
Horizon 2020
H2020-INFRADEV-1-2014
Type of action: RIA

Content

Executive Summary

This deliverable presents the Common Access Framework developed within CORBEL work package 5 to manage seamless access to multiple research infrastructures within individual research projects. The ARIA (Access to Research Infrastructure Administration) access management software, developed in-house by Instruct-ERIC to manage their own user access, was adapted to meet the specifications of the CORBEL project and provide a pilot platform for accessing multiple biomedical science Research Infrastructures (RIs) in CORBEL. The platform was tested by scientists belonging to the different scientific communities with research questions at the boundaries of the different research infrastructures through the First CORBEL Open Call which from October 2016 – December 2016. Following the First Open Call, feedback was collected on all areas of infrastructure access through CORBEL, including the WP5 common access pilot platform in ARIA. WP5 used this feedback to improve the platform and, due to the scientific success of the First Open Call, a Second CORBEL Open Call was launched in March 2018 using the ARIA system with these improvements.

In addition to the ARIA platform which enables common access to physical infrastructure and expertise, WP5 worked on a pilot concept for a common authentication and authorisation tool, with the aim to establish an authentication and authorisation infrastructure (AAI) which meets the combined requirements of the biomedical science infrastructures, such that a scientist would be able to access resources with a single unified identity and single sign on. This work culminated in a pilot Life Science AAI, jointly with the AARC2 project where CORBEL WP5 provided the use cases and technical specifications required for the AAI and AARC2 e-infrastructures provided the AAI components and operated the pilot AAI. As a result of this work we plan to continue collaborative efforts with the e-infrastructures to bring into production a full Life Science AAI which will be supported by the EOSC-Life project starting in March 2019.

Project objectives

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

a) To establish an infrastructure platform that integrates ESFRI services for life sciences.

b) To build the framework for transnational open user access for the sustainable use of shared services.

c) To identify common processes amongst access models where standardisation might be achieved.

d) To implement specific standardised processes or methods in the access model, test their compatibility in the individual RIs and in the use cases and receive feedback from the users involved.

e) To investigate a framework for a coherent single access route to all research infrastructures through a shared access framework.

Detailed report on the deliverable

Background

The core aim of the CORBEL project is to facilitate harmonisation amongst biomedical research infrastructures to enable ground-breaking scientific discoveries which often occur at the intersection of different research fields. Within work package 5 (WP5) our aim is to develop a common access framework to harmonise user access to infrastructure services. This deliverable presents our achievements in this area. We begin by introducing the ARIA access management software developed and maintained by Instruct-ERIC. We detail the adaptations which were required to tailor ARIA to the needs of CORBEL for access to multiple research infrastructures. We then present a report of the use of ARIA in the First CORBEL Open Call (Leitner, Popp, & Vidal, 2018) for research projects led by WP4 using the adapted ARIA platform developed within WP5, and how lessons learnt from the First Open Call were used to improve the ARIA platform for the Second Open Call. Alongside the work on a common access management system, WP5 worked with the AARC2 project to commission a pilot authentication and authorisation infrastructure for common login and identity management for services across the Life Science research infrastructures. We present the Life Science AAI pilot and conclusions from the pilot formulated into an improved specification of the technical requirements. Finally, we look towards the sustainability of the ARIA platform for integrated access to multiple research infrastructures, and the common Life Science AAI in the future, both for the remainder of the CORBEL project and beyond.

Description of Work

In deliverable D5.1 “Report on existing user access models and regulatory access policies identifying common elements” (Daenke & Krishnan, 2017) we identified areas where harmonisation could be achieved across Life Science research infrastructures through a survey of the (10 at time of survey) research infrastructures participating in CORBEL on their access models and service provision. Results from this analysis suggested that functions performed by more than 7 RIs were candidates to be modelled into a common user access framework. From these functions we determined it would be beneficial to consolidate the processes of proposal submission, scientific peer review, technical and ethical evaluation, and service/technology/expertise management and tracking through development of the ARIA software suite. Virtual access (to computational software, tools and resources) was also highlighted in D5.1 as a key function particularly in the life science RIs and therefore CORBEL WP5 worked to define and pilot a new Authentication and Authorisation Infrastructure for the life sciences to control access to virtual and remote resources.

Access to Research Infrastructure Administration (ARIA) Software

ARIA is a suite of cloud software developed by Instruct-ERIC, originally designed to manage scientific peer review and research visits to structural biology facilities. ARIA services include access management (submission of research proposals, peer review, service/technology access visits, access reporting), community management (jobs, events, news, internal messaging, networks, forums, surveys, mailshots), facility management (booking calendars, user training record) and data management (API, document hosting).

For the purposes of the CORBEL project, the most relevant functionality is access management. The basic access workflow in ARIA is shown in Figure 1. The applicant constructs a planned access request by indicating which services/technologies they require access to. For each service/technology requested, a 'visit' is generated associated to the applicant's proposal. The visits can be ordered by the user and an 'access route' for each visit can be selected from those routes offering access to that service/technology. The applicant then fills in a proposal form specified by the access route(s) selected. The applicant finally nominates the proposal research team by selecting the Principal Investigator (PI) and collaborators. The applicant can go back and review all steps before submitting the proposal. An administrator checks the proposal for eligibility for the access route and selects a moderator for the proposal. The moderator's role is to oversee the proposal peer review. The moderator selects reviewers who are invited to complete a review form online. When sufficient reviews are completed the moderator is invited back to make the final decision on proposal acceptance or rejection informed by the reviews.

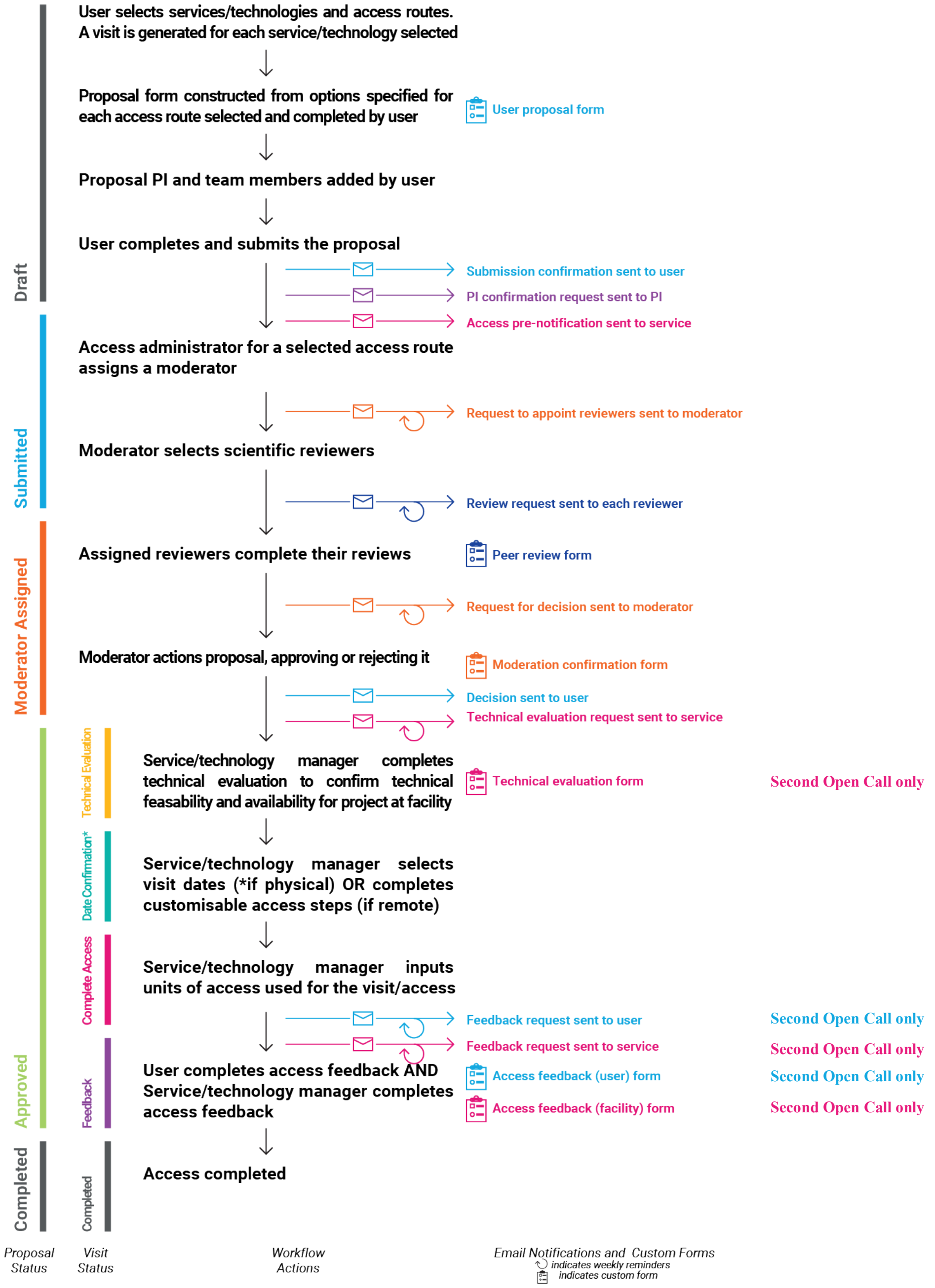

User selects services/technologies and access routes.
A visit is generated for each service/technology selected
Proposal form constructed from options specified for each access route selected and completed by user
User proposal form
Proposal PI and team members added by user
User completes and submits the proposal
Submission confirmation sent to user
PI confirmation request sent to PI
Access pre-notification sent to service
Draft
Access administrator for a selected access route assigns a moderator
Request to appoint reviewers sent to moderator
Moderator selects scientific reviewers
Submitted
Review request sent to each reviewer
Assigned reviewers complete their reviews
Peer review form
Request for decision sent to moderator
Moderator actions proposal, approving or rejecting it
Moderation confirmation form
Moderator Assigned
Decision sent to user
Technical evaluation request sent to service
Technical Evaluation
Service/technology manager completes technical evaluation to confirm technical feasability and availability for project at facility
Technical evaluation form
Second Open Call only
Date Confirmation*
Service/technology manager selects visit dates (*if physical) OR completes customisable access steps (if remote)
Complete Access
Service/technology manager inputs units of access used for the visit/access
Feedback request sent to user
Second Open Call only
Feedback request sent to service
Second Open Call only
Feedback
User completes access feedback AND Service/technology manager completes access feedback
Access feedback (user) form
Second Open Call only
Access feedback (facility) form
Second Open Call only
Approved
Completed
Completed
Access completed
Proposal Status
Visit Status
Workflow Actions
Email Notifications and Custom Forms
indicates weekly reminders
indicates custom form

Figure 1: ARIA proposal and visit workflow.

When the proposal is accepted, processes begin in parallel for all visits associated with the proposal. First the service/technology managers perform a technical evaluation of the proposed access to ensure technical feasibility of the work in their facility and to ensure that the facility has sufficient availability to provide the access. After technical evaluation has been completed, the steps differ depending on whether a physical visit or remote facility access has been requested. For physical access, the next step is for the service/technology manager to input the date of the access. In the case of remote access, this step is replaced with one or more configurable remote access steps. Then, when the access has been completed, units of access are input to record resources (e.g. time) used for the access. Finally, feedback questionnaires are sent to the applicant and the service/technology managers. When feedback is collected from all parties the visit is completed, and when all visits are complete, the proposal itself is completed.

To implement the access workflow, ARIA defines a number of classes. These are shown in Figure 2. There are specific connections between these classes, for example, a visit is to a single service/technology. A service technology is provided by one or more machines/methods, where each machine/method is hosted at a single centre (facility). Access routes available are determined on a service/technology level. CORBEL brings together multiple different research infrastructures, however there is not a class in ARIA for a 'research infrastructure'. A research infrastructure is a grouping of related services and resources for research in a particular field. It may be distributed across multiple facilities or single-site. Consequently, we defined research infrastructures in ARIA as a grouping or centres (which represent RI nodes/sites) providing certain service/technology types (which represent the thematic area of the RI).

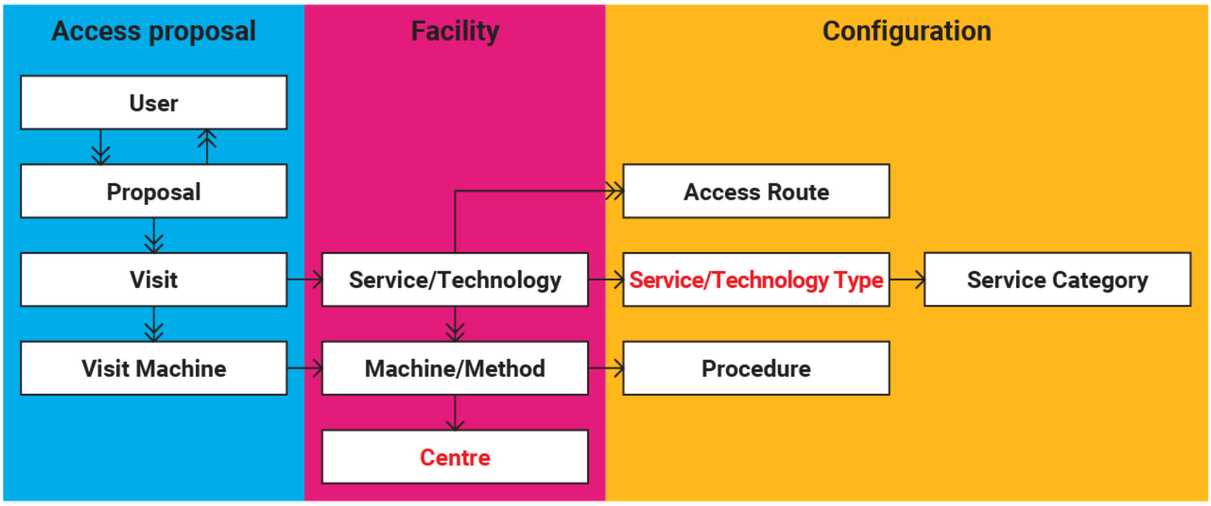


Figure 2: Classes in ARIA and their interconnections. Double-headed arrows indicate a one-to-many connection between two classes and single headed arrows indicate a one-to-one connection between classes. A "Research Infrastructure" is a grouping of Service/Technology Types and Centres (labelled in red).

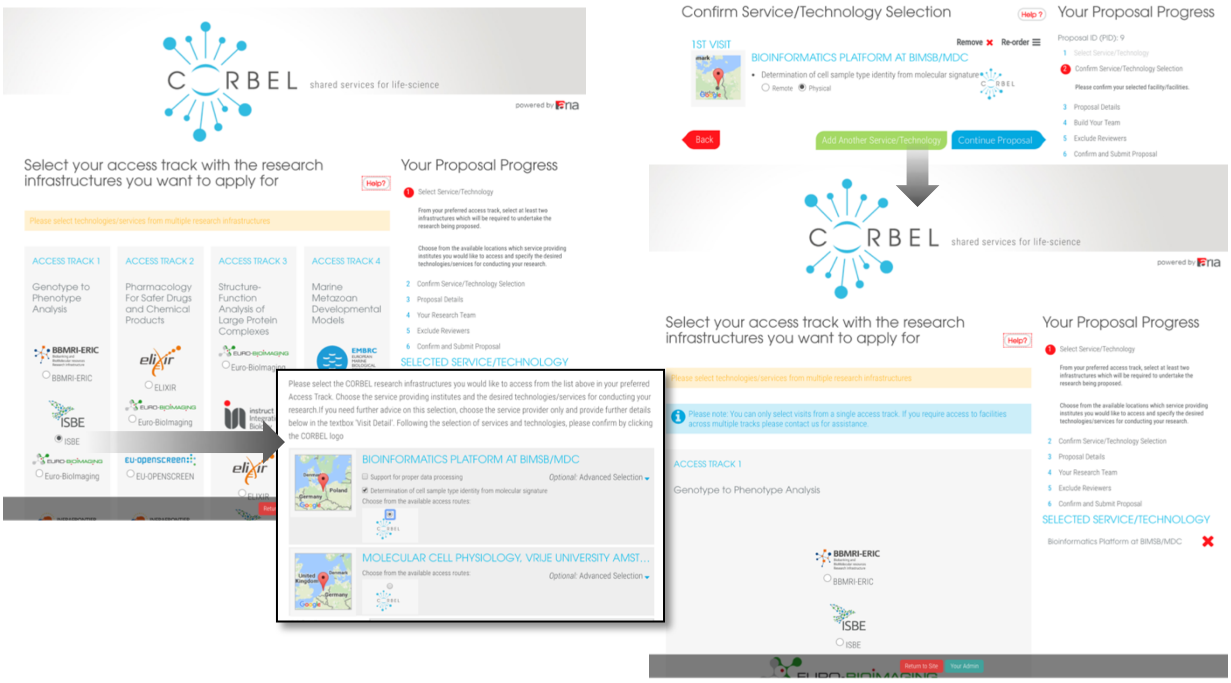
The user-facing part of the ARIA system is the proposal submission system, where users are able to create a proposal including the request of access visits (which may be either physical or remote[1]) to services/technologies; and the user dashboard, where users are able to track the status of proposals

[1] Within ARIA remote access is defined as either mail-in-sample or other access to a service/technology which does not require the scientist to make a physical visit to the infrastructure.

and resume work on draft proposals, edit their user profile, check their ARIA messages and contact administrators and facility about their proposals.

The back-end of ARIA, called the admin panel, is where the administrative functions are performed, and also where peer review and access/visit tracking and management is completed. Each of the objects in Figure 2 can be created, configured and customised in the ARIA admin panel.

Adaptations to ARIA for the First CORBEL Open Call for Research Projects



Select your access track with the research infrastructures you want to apply for

Please select technologies/services from multiple research infrastructures

Your Proposal Progress

1 Select Service/Technology

From your preferred access track, select at least two infrastructures which will be required to undertake the research being proposed.

Choose from the available locations which service providing institutes you would like to access and specify the desired technologies/services for conducting your research.

2 Confirm Service/Technology Selection

3 Proposal Details

4 Your Research Team

5 Exclude Reviewers

6 Confirm and Submit Proposal

SELECTED SERVICE/TECHNOLOGY

Please select the CORBEL research infrastructures you would like to access from the list above in your preferred Access Track. Choose the service providing institutes and the desired technologies/services for conducting your research.If you need further advice on this selection, choose the service provider only and provide further details below in the textbox 'Visit Detail'. Following the selection of services and technologies, please confirm by clicking the CORBEL logo

BIOINFORMATICS PLATFORM AT BIMSB/MDC

☐ Support for proper data processing

☑ Determination of cell sample type identity from molecular signature

Choose from the available access routes:

MOLECULAR CELL PHYSIOLOGY, VRIJE UNIVERSITY AMST...

Choose from the available access routes:

Confirm Service/Technology Selection

Your Proposal Progress

Proposal ID (PID): 9

1 Select Service/Technology

2 Confirm Service/Technology Selection

Please confirm your selected facility/facilities.

3 Proposal Details

4 Build Your Team

5 Exclude Reviewers

6 Confirm and Submit Proposal

1ST VISIT

BIOINFORMATICS PLATFORM AT BIMSB/MDC

- Determination of cell sample type identity from molecular signature

○ Remote ● Physical

Please note: You can only select visits from a single access track. If you require access to facilities across multiple tracks please contact us for assistance.

ACCESS TRACK 1

Genotype to Phenotype Analysis

SELECTED SERVICE/TECHNOLOGY

Bioinformatics Platform at BIMSB/MDC

CORBEL shared services for life-science
powered by aria
Help?
ACCESS TRACK 1
Genotype to Phenotype Analysis
ACCESS TRACK 2
Pharmacology For Safer Drugs and Chemical Products
ACCESS TRACK 3
Structure-Function Analysis of Large Protein Complexes
ACCESS TRACK 4
Marine Metazoan Developmental Models
BBMRI-ERIC
ISBE
Euro-BioImaging
ELIXIR
EU-OPENSCREEN
EMBRC
instruct
Optional: Advanced Selection
Remove
Re-order
Back
Add Another Service/Technology
Continue Proposal
Return to Site
Your Admin

Figure 3: Service/technology selection display for the CORBEL access tracks in the First CORBEL Open Call.

The CORBEL Open Call opened access to infrastructures to cover the 4 WP4 use cases: Genotype-to-phenotype analysis, Pharmacology for safer drugs and chemical products, Structure-function analysis of large protein complexes and Marine metazoan developmental models. Access tracks were implemented on the user-facing side with a completely custom technology selection page (Figure 3).

Each of the 22 service/technologies, from the 8 Research Infrastructures offered in the First Open Call, were configured within the ARIA software including the creation of 115 machines/methods to deliver the services. In some cases, a service would be provided by multiple machines/methods and in these cases the selection of machines could be performed by the user during the construction of their application. This was optional and not enforced at the time of the First Open Call.

Customised forms were implemented for the user proposal and for the review form. At the time of setting up the First Open Call the technical evaluation form was not customisable and was simply a free text field where the service/technology operators would describe in plain text their technical comments on the proposed work.

Initially access was limited to one access track. Once the CORBEL applicants had selected their first service/technology from one of the access tracks they would be 'locked-in' to only selecting services from that particular track. Although users needed to select access to services from multiple RIs to be eligible for the CORBEL Open Call, this was not initially enforced in the software therefore some ineligible applications to the First Open Call were received.

Outcome and feedback from the First CORBEL Open Call and adaptations to ARIA for the Second CORBEL Open Call

Two surveys were implemented using the survey functionality within the ARIA software suite to obtain feedback upon the application process. One survey was sent to the CORBEL end users, the other was sent to the CORBEL service providers. The surveys provided important feedback on the access model, and this feedback was used to perform improvements to the ARIA access management system, and to the access processes used in the CORBEL Open Calls. Responses to the service provider survey were received from 17 service providers spanning all 8 of the research infrastructures participating in the call (BBMRI, ELIXIR, EMBRC, EU-OPENSCREEN, Euro-BioImaging, INFRAFRONTIER, Instruct, ISBE). Responses to the user survey were received from 19 applicants. The questions asked in both surveys are included in deliverable D4.2 (Leitner, Popp, & Vidal, 2018). In most cases, questions in the user survey and the service provider survey were analogous e.g. service providers were asked “If applicants contacted you prior to their application, did you appreciate these discussions about prospective projects?” and “If applicants contacted you prior to their application, do you think it improved the quality of the applications?” whilst users were asked “You were invited to get in contact with your preferred service providers ahead of your application submission. Did you make use of this offer and do you think it affected the quality of your application?”. This allowed the comparison of specific aspects of the application process from the point of view of these different stakeholder groups.

Conclusions from survey and example steps taken to improve the access model

1. Contact with service providers
In the First Open Call approximately half of the users had been in contact with service providers in advance of their application. In cases where the user had been in contact with the service provider beforehand, both parties agreed that the interaction was helpful with no users or service providers stating that the communication was not helpful to the application/project. As a result of this feedback, for the Second Open Call, prior communication with the planned service providers was a prerequisite for the application. This was achieved by making users self-validate that they had been in touch with the service providers by clicking a checkbox before the application form could be submitted in ARIA. Service providers were then contacted by WP4 project managers to ensure that the user had been in contact prior to the application being sent to peer review. This demonstrated that despite the checkbox, some users had not been in contact with the service providers, so an additional field was added to the proposal form in ARIA to ask the users to provide the details of the person(s) they had been in contact with at each service provider.

2. Cross Access-Track projects
When asked about the grouping of services into access tracks, with both groups there were those who found the grouping helpful to define and focus a scientific target. Users tended to find this structuring into access tracks more helpful than service providers. There were however also those who found the access tracks narrowed their options in both stakeholder groups. This was also evident from the projects in the First Open Call where some projects requested services from multiple access tracks. To allow the users to be guided but not restricted by the access tracks, we introduced the ability for users to select their services, first from an access track, but then giving the option of selecting any of the CORBEL Open Call services through an additional expandable menu at the bottom of the page.

3. Suggestions for ARIA improvements

In the service provider survey, there was a free text field for comments on suggestions for improvements to the ARIA software. Suggestions made which have since been implemented are:

- Providing training and help material on how to use ARIA
- Saving a survey in progress
- Email notifications to service providers along the workflow
- Allowing the service providers to view proposals before scientific review in ARIA
- Allowing the service providers to view (anonymised) scientific reviews for proposals requesting access to their services

In addition to the feedback received from the two surveys, the WP4 project managers suggested many changes to improve the access system for the Second Open Call informed by their experience managing and facilitating the projects from the First Open Call. In response to their feedback, the following changes were made:

- Selection of a lead Research Infrastructure (from the list of selected research infrastructure) to spearhead the project. This is implemented in the proposal submission form where the applicant must suggest a lead RI, and during technical evaluation the service providers are asked if they agree with the choice of lead RI or would suggest an alternative.
- Users to select on a calendar an expected start and end date, and their current level of expertise for each visit to a service provider in the proposal submission form.

Introduction of bespoke training sessions for service providers (joint activity with WP9)

Support and training on ARIA is crucial in order for all users (end users, service providers, reviewers and project managers) to understand and get the most from the system and the features on offer. In December 2017 the ARIA help guides (Instruct-ERIC, 2017) were launched. These pages gave information on how to complete common tasks in ARIA and were organised by the role/type of user e.g. user applying for access, scientific reviewer, service provider, administrator. These pages have been disseminated within the CORBEL community in emails and presentations. They are also linked to from within the administration pages in ARIA. In the 16 months from their launch (12/12/2017) until (12/04/2019), the ARIA help-guides have 5802 page views (3611 unique).

In collaboration with WP9, WP5 presented a top-level overview of the ARIA suite as part of the CORBEL webinar series in January 2018. This webinar is also available for viewing online via the CORBEL website and YouTube channel (Sanderson, ARIA - Powering your access management from the cloud, 2018). In May 2018 WP5 produced two bespoke CORBEL training webinars in collaboration with both WP4 and WP9 tailored to the Second Open Call. One webinar was tailored to scientific reviewers and included a 10 minutes section on how to complete a scientific review in ARIA. The other webinar was tailored to service providers and contained a 20 minutes section explaining how to complete access visits in ARIA. Both webinars are available in full and abridged to contain only the ARIA sections (Sanderson, Using ARIA for CORBEL service providers, 2018) (Haley, 2018) on YouTube.

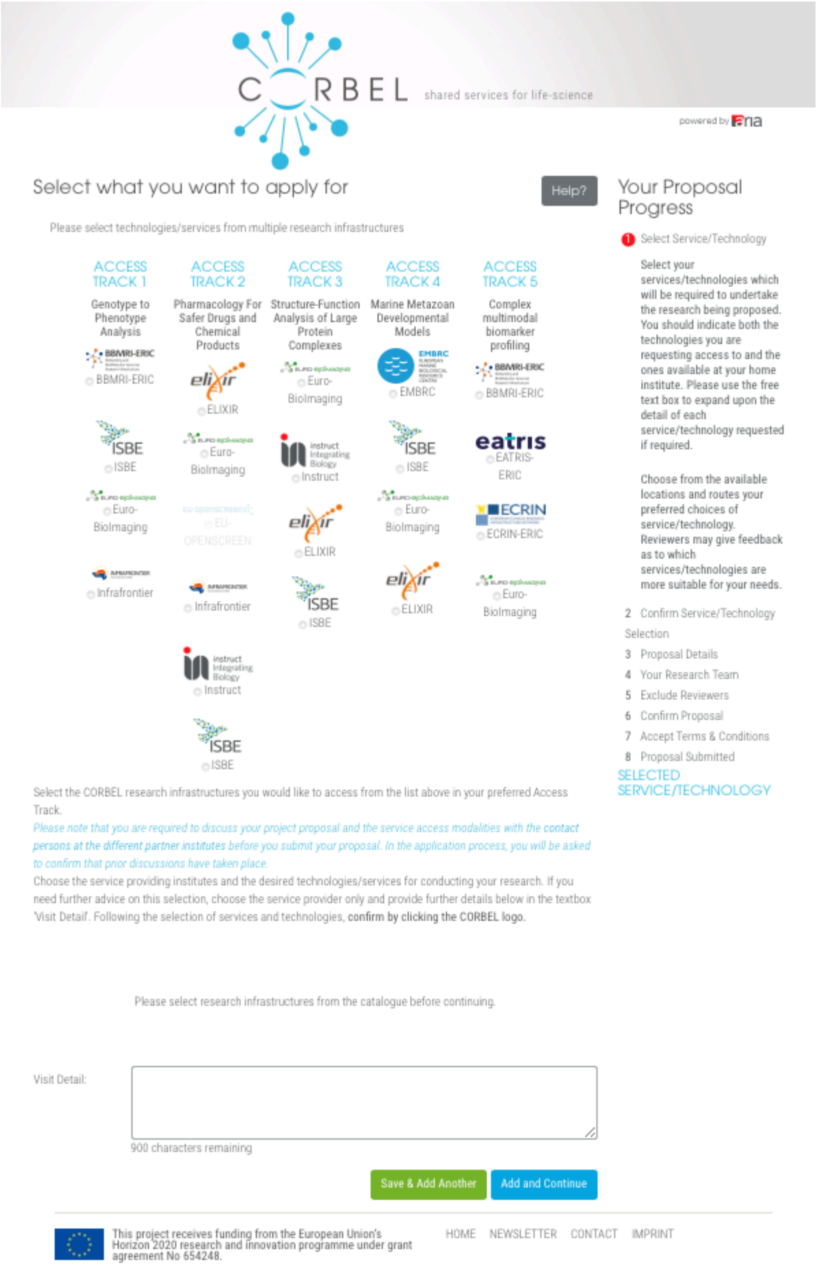
GDPR compliance changes

The General Data Protection Regulation EU 2016/679 came into force. The provisioning of user access necessarily involves the processing of personal data, and therefore action was required in order to bring the access management system used for CORBEL into compliance. Steps were taken to hide personal data of ARIA registrants which was previously displayed publicly on online profile page.

Users of the ARIA system are now required to specify an affiliation to one or more project / research infrastructure / academic organisation using the ARIA software system, or else state explicitly that they have no such affiliation. This is done in order to ensure that only the personal data of ARIA registrants involved in a particular project / research infrastructure / academic organisation (such as CORBEL) will be processed according to the legal bases for processing defined by that project / research infrastructure / academic organisation. 328 ARIA users are currently associated with CORBEL as a project (as of 17/04/19). This feature of project/RI selection at registration will be crucial as more infrastructures adopt ARIA software to manage their access as it provides a mechanism to identify which users 'belong' to which infrastructure.

New Access Track for WP3 use cases

In the Second Open Call, a new access track (Access track 5) was created to cover the use cases for direct medical application of life science RIs delivered by WP3 on the topic of "complex multimodal biomarker profiling". This involved two new research infrastructures in the Second Open Call, ECRIN and EATRIS, bringing the total number of RIs participating in the CORBEL Open Calls to 10. 7 New service/technologies and 22 new machines were added to ARIA to provide access track 5. There were also minor changes to the services offered in the original 4 access tracks including the addition of some services, and the removal of others no longer offered. For the Second Open Call there were a total of 30 services/technologies offered with 154 machines. The first application page for the Second Open Call is shown in Figure 4.



Select what you want to apply for

Please select technologies/services from multiple research infrastructures

ACCESS TRACK 1	ACCESS TRACK 2	ACCESS TRACK 3	ACCESS TRACK 4	ACCESS TRACK 5
Genotype to Phenotype Analysis	Pharmacology For Safer Drugs and Chemical Products	Structure-Function Analysis of Large Protein Complexes	Marine Metazoan Developmental Models	Complex multimodal biomarker profiling
○ BBMRI-ERIC	○ ELIXIR	○ Euro-BioImaging	○ EMBRC	○ BBMRI-ERIC
○ ISBE	○ Euro-BioImaging	○ Instruct	○ ISBE	○ EATRIS-ERIC
○ Euro-BioImaging	○ EU-OPENSCREEN	○ ELIXIR	○ Euro-BioImaging	○ ECRIN-ERIC
○ Infrafrontier	○ Infrafrontier	○ ISBE	○ ELIXIR	○ Euro-BioImaging
	○ Instruct			
	○ ISBE			

Select the CORBEL research infrastructures you would like to access from the list above in your preferred Access Track.

Please note that you are required to discuss your project proposal and the service access modalities with the contact persons at the different partner institutes before you submit your proposal. In the application process, you will be asked to confirm that prior discussions have taken place.

Choose the service providing institutes and the desired technologies/services for conducting your research. If you need further advice on this selection, choose the service provider only and provide further details below in the textbox 'Visit Detail'. Following the selection of services and technologies, **confirm by clicking the CORBEL logo.**

Please select research infrastructures from the catalogue before continuing.

Visit Detail:

900 characters remaining

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 654248.

Your Proposal Progress

1 Select Service/Technology

Select your services/technologies which will be required to undertake the research being proposed. You should indicate both the technologies you are requesting access to and the ones available at your home institute. Please use the free text box to expand upon the detail of each service/technology requested if required.

Choose from the available locations and routes your preferred choices of service/technology. Reviewers may give feedback as to which services/technologies are more suitable for your needs.

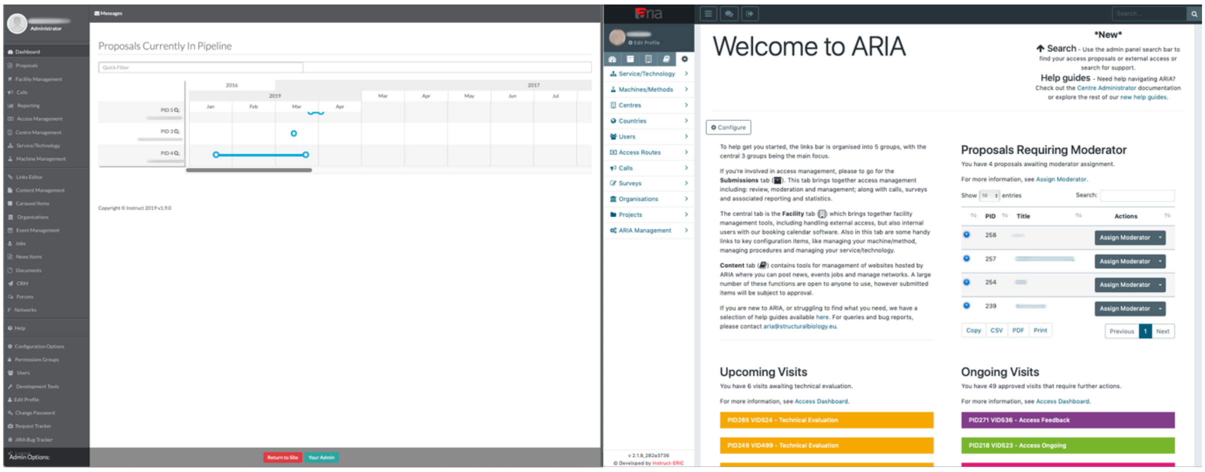
2 Confirm Service/Technology Selection
3 Proposal Details
4 Your Research Team
5 Exclude Reviewers
6 Confirm Proposal
7 Accept Terms & Conditions
8 Proposal Submitted

SELECTED SERVICE/TECHNOLOGY

Figure 4: First application page for the Second CORBEL Open Call showing new access track 5.

ARIA version 2

Between the close of applications for the First Open Call, and the opening of the Second Open Call, a new version of ARIA was released. This version change involved a total rewrite and restructure of the underlying code, and redesign of the admin panel interfaces to improve their organisation and make the administrative functions easier to use. The main menu sidebar of the admin panel in version 1 was a long list of functions and became difficult to navigate. To enhance navigability, this long list was subdivided into 5 tabs grouped by type of administrative function (see Figure 5). The first tab gives the administration panel dashboard. This page provides an orientation for the users when they first arrive into the admin pages. Following a subversion release of ARIA v2.1, this page was further extended to give a configurable role-based one-page view of actions pending in the ARIA system for the current user e.g. proposals which require moderation. Another critical enhancement was full support of responsive web design for the admin panel for both accessibility and mobile optimisation to allow for administrators to action proposals rapidly.



Proposals Currently In Pipeline

Copyright © Instruct 2019 v1.9.0

Welcome to ARIA

New

Search - Use the admin panel search bar to find your access proposals or external access or search for support.

Help guides - Need help navigating ARIA? Check out the Centre Administrator documentation or explore the rest of our new help guides.

To help get you started, the links bar is organised into 5 groups, with the central 3 groups being the main focus.

If you're involved in access management, please to go for the **Submissions** tab. This tab brings together access management including: review, moderation and management; along with calls, surveys and associated reporting and statistics.

The central tab is the **Facility** tab which brings together facility management tools, including handling external access, but also internal users with our booking calendar software. Also in this tab are some handy links to key configuration items, like managing your machine/method, managing procedures and managing your service/technology.

Content tab contains tools for management of websites hosted by ARIA where you can post news, events jobs and manage networks. A large number of these functions are open to anyone to use, however submitted items will be subject to approval.

If you are new to ARIA, or struggling to find what you need, we have a selection of help guides available here. For queries and bug reports, please contact aria@structuralbiology.eu.

Proposals Requiring Moderator

You have 4 proposals awaiting moderator assignment.

For more information, see Assign Moderator.

Show 10 entries Search:

	PID	Title	Actions
	258		Assign Moderator
	257		Assign Moderator
	254		Assign Moderator
	239		Assign Moderator

Upcoming Visits

You have 6 visits awaiting technical evaluation.

For more information, see Access Dashboard.

PID265 VID524 - Technical Evaluation

PID249 VID499 - Technical Evaluation

Ongoing Visits

You have 49 approved visits that require further actions.

For more information, see Access Dashboard.

PID271 VID536 - Access Feedback

PID218 VID523 - Access Ongoing

Figure 5: ARIA admin panel dashboard in version 1 (left) and version 2 (right). Extensive changes to the dashboard and to the admin panel navigation between the two versions separate groups of related actions into 5 tabs in version 2.

Functionally there were also enhancements to the proposal workflow introducing new functionality and customisability. Technical evaluation was extended to include a fully customisable input form specified per access route, to be filled in by the service operator which replaced the plain-text input from ARIA version 1. This was used in the Second Open Call to collect more precise technical information during the technical evaluation step such as maturity of project, technical ability of the applicant, combination of RIs, capacity of service/technology. Support for better management of visits was also added in version 2 to provide better management of remote access and also better representation of the access actually provided by the centre.

Life Science AAI Pilot

From the survey results in D5.1 (Daenke & Krishnan, 2017), we noted that the majority of life science RIs provide virtual access to computational services including data and software, methods are required to ensure that users of virtual services can be identified (via authentication) and can be given appropriate access rights and privileges (authorisation). This is done by an authorisation and authentication infrastructure or AAI. Here, there is a clear benefit if a user is able to authenticate and become authorised centrally to avoid placing the burden upon individual service providers to provide their own AAI, and to enhance the user experience as they can use a single account to access a wide range of services. Life Science research infrastructures participating in CORBEL collaborated to commission an authentication and authorisation infrastructure (AAI) for the Life Science community. The aim was to provide a common single-sign-on to be connected to all Life Science RI computational services. This was initiated through the gathering of technical requirements for such an infrastructure from members of the Life Science community. Use cases were collected from Life Science RIs and used to build an initial document of technical requirements for a Life Science AAI. The first version of this technical requirements specification (Linden, et al., 2018) was prepared by CORBEL WP5 to open a call for proposals to procure the Life Science AAI pilot as part of the AARC2 project pilots. AARC2 is the successor to the AARC project and aims to produce policies and best practices for AAIs, and to implement pilot AAIs for research community use cases. Partners of AARC2 span research infrastructures, e-infrastructures and national research and education networks (NRENs). The selected proposal for the Life Science AAI Pilot was put together jointly by three e-infrastructures

EGI, GÉANT and EUDAT, the AAI operators, and the resulting pilot ran from November 2017 – November 2018.

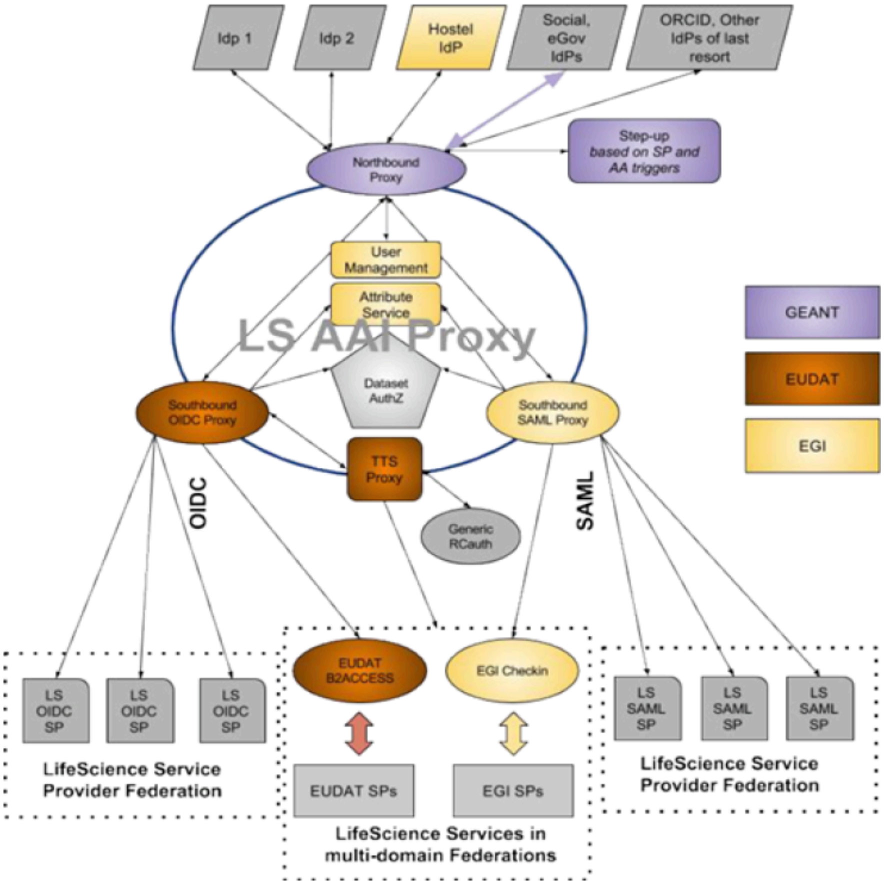


Figure 6: Life Science AAI Pilot Architecture provided jointly by e-infrastructures GÉANT, EGI and EUDAT. Colour code indicates the e-infrastructure providing that component.

The AAI operators constructed the pilot AAI based on the AARC blueprint architecture (AARC2, 2017) which is depicted diagrammatically in Figure 6. Three proxies make up the Life Science AAI, and each proxy is operated by a different e-infrastructure. Components in grey are either components from the life science community or third-party components to be connected to the Life Science AAI. The pilot itself was broken down into three phases detailed in Table 1.

Phase	Period	Description
1	December 2018 – January 2019	AAI operators performed the initial assembly of the AAI components, defined the required attributes and user registration protocol. At the end of phase 1 the results were demonstrated in a live demo.
2	February 2018 – May 2018	Identity providers (IDPs) and service providers (SPs) were integrated into the Life Science AAI constructed in Phase 2. These included IDPs (ARIA) and SPs (ARIA, ELIXIR Coffee room, Euro-BioImaging Portal) from the Life Science RIs
3	June 2018 – November 2018	Testing of the Life Science AAI was performed in phase 3 by the Life Science community. Weekly calls were held between representatives of the Life Science RIs participating in the pilot

	and AAI operators to discuss feedback from the testing process and refine the Life Science AAI based on feedback.

Table 1: Phases of the AARC2 Life Science AAI Pilot

Informed by the results of the pilot, in particular the testing performed by CORBEL WP5 in phase 3, the technical requirements specification was updated. Key additions to the technical requirements included the introduction of usability requirements to ensure adoption by the Life Science community, as all user interfaces must be simple and intuitive to use; capacity requirements to ensure that the AAI is sufficient to serve the demand of the Life Science community as it expands; and browser/OS compatibility requirements. The updated technical requirement specification will be used to inform the future of the Life Science AAI and is included in Appendix 1: Updated Technical Requirements for the Life Science AAI.

Next steps

Towards sustainability of the common access framework

The success of the Open Calls in CORBEL and the clear demand shown from applications to the Open Calls for combined access to research infrastructures, especially in some commonly requested combinations, demonstrates that a mechanism for future support of common RI access is highly desirable. Additionally, the technical accomplishments of the Life Science AAI pilot and the motivation of the life science research infrastructures to converge on a solution to better serve the needs of their user communities and reduce duplication of effort justifies continued effort to make a production Life Science AAI a reality.

WP4 also provided a view of how the service pipelines forged during the Open Calls and VIP projects might be sustained in deliverable D4.2 “Sustainable plan for user access to common RI services for 4 use case cross-ESFRI Life Science research infrastructure pipelines” (Leitner, Popp, & Vidal, 2018). In this deliverable WP4 make three recommendations for common service provision beyond CORBEL. They suggest as their first recommendation, a common access management system and web presence which highlights the importance of the sustainability of the ARIA software developed through WP5.

Sustainability of the common access framework will be discussed in more detail in deliverable D5.3 “Strategy for expanding application of common access model based on feedback from WP3 and WP4 pilots”, however we introduce in this deliverable some of the efforts which are being made towards the sustainability of both the ARIA system for access management to multiple research infrastructures and the common authentication and authorisation infrastructure.

Continuation of the Life Science AAI – From pilot to production

Whilst the Life Science AAI pilot was ongoing, discussions were being held between e-infrastructure representatives from EGI, EUDAT and GÉANT, and representatives from Life Science Research Infrastructures to discuss a production Life Science AAI, beyond the pilot. The move to a production-level service, including the transfer of users from existing RI AAIs (e.g. ARIA AAI, ELIXIR AAI) will be supported by EOSC-Life, a new Horizon 2020 project (grant agreement number 824087). Dedicated effort and resources are set aside in work package 5 of EOSC-Life for the procurement of AAI services. This work should cover the sustainability of the common AAI solution up to the end of the EOSC-Life project. During the EOSC-Life project, plans for future support and sustainability of the Life

Science AAI will be determined. EOSC-Life will build upon the results and work of CORBEL building and refining the technical requirements for a common AAI for the Life Sciences.

Future ARIA developments will ease ARIA adoption and support integration with non-ARIA systems

Work on the ARIA system will continue to improve the ARIA API to allow better integration with external software systems, such as the ability to identify users and synchronise proposals between software in place in different infrastructures. The trend towards developing ARIA to support more customisation for objects and workflows will continue, which should allow its use for a wider range of use cases generated by the research infrastructures who might wish to adopt it. Many research infrastructures, both from the Life Sciences and beyond, are in discussion with Instruct-ERIC regarding the adoption of ARIA. ARIA can be adopted as either a cloud-based service hosted by Instruct-ERIC, or as a locally hosted instance. In the latter case, work is ongoing to ensure that different locally hosted ARIA instances are able to interoperate (including management of IDs) so that proposals and information can be shared and synchronised between them.

References

AARC2. (2017). AARC Blueprint Architecture - AARC-BPA-2017. https://aarc-project.eu/architecture/.

Daenke, S., & Krishnan, N. (2017, March). CORBEL Report on existing user access models and regulatory access policies identifying common elements. 10.5281/zenodo.376187.

Haley, N. (2018). Using ARIA for CORBEL reviewers. https://youtu.be/d7e_pXui2Ec.

Instruct-ERIC. (2017). ARIA Help Guides. https://instruct-eric.eu/help/guides.

Leitner, F., Popp, C., & Vidal, M. (2018, December). CORBEL Sustainable plan for user access to common RI services for 4 use case cross-ESFRI BMS research infrastructure pipelines. 10.5281/zenodo.2222358.

Linden, M., Holub, P., Lappalainen, I., Matyska, L., Nyrönen, T., Procházka, M., et al. (2018). Common Authentication and Authorisation Service for Life Science Research. Trondheim: TERENA Networking Conference 2018 (TNC18), https://tnc18.geant.org/core/presentation/133.

Sanderson, F. (2018). ARIA - Powering your access management from the cloud. https://www.corbel-project.eu/webinars/aria-access-management.html.

Sanderson, F. (2018). Using ARIA for CORBEL service providers. https://youtu.be/arUJJNiGvc4.

Abbreviations

Abbreviation	Definition
AAI	Authorisation and Authentication Infrastructure
AARC2	Authentication and Authorisation for Research and Collaboration
API	Application Programming Interface
ARIA	Access to Research Infrastructure Administration
AUP	Acceptable Usage Policy
BBMRI	European research infrastructure for biobanking and biomolecular resources
BMS	Biological and Medical Sciences
EATRIS	European research infrastructure for translational medicine
ECRIN	European research infrastructure for clinical research
eduGAIN	Interfederation of research and education identity federations
EGI	European Grid Infrastructure
ELIXIR	European research infrastructure for life-science data
EMBRC	European research infrastructure for marine biology
EOSC	European Open Science Cloud
EOSC-Life	EOSC-Life, A cluster project from the life science research infrastructures expanding digital biology in Europe funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 824087
ESFRI	European Strategy Forum on Research Infrastructures
EU-OPENSCREEN	European research infrastructure for screening and medicinal chemistry
EUDAT	European data infrastructure
Euro-BioImaging	European research infrastructure for advanced biological imaging technologies
GDPR	General Data Protection Regulation
GÉANT	Pan-European network for research and education
ID	Identity
IdP	Identity Provider
IE	Internet Explorer
Infrafrontier	European research infrastructure for phenotyping and archiving of model mammalian genomes
Instruct	European research infrastructure for structural biology
ISBE	European research infrastructure for systems biology
LS	Life Science
MFA	Multi-Factor Authentication
NREN	National Research and Education Network
OAuth	Open Authorisation
OIDC	OpenID Connect
ORCID	Open Tresearcher and Contributor ID
OS	Operating System
PC	Personal Computer

RAF	REFEDS Assurance Framework
REFEDS	Research and Education Federations Group
REST	Representational State Transfer
RI	Research Infrastructure
SAML	Security Assertion Markup Language
SFA	Single-Factor Authentication
Sirtfi	Security Incident Response Trust Framework
SP	Service Provider
SSH	Secure Shell
VO	Virtual Organisation
WP	Work Package

Delivery and schedule

The delivery is delayed: No

Adjustments made

N/A

Appendices

Appendix 1: Updated Technical Requirements for the Life Science AAI March 2019

1. Introduction

1.1. This document

This document presents the requirements for a Life Science AAI, the common Authentication and Authorisation service portfolio for the research infrastructures participating in the EOSC-Life project and beyond. The document intends to serve the design and deployment of the Life Science AAI.

This document is prepared by the Work Package 5 of the CORBEL project together with the AARC2 project. The work is based on the use case gathering among the AAI experts of the participating research infrastructures and the Life Science AAI pilot in the AARC2 project.

This document describes the Life Science AAI requirements as understood by the contributing research infrastructures at the time of writing. Some requirements may change over time as the needs of the Life Science community evolve and as the contributors learn them better. This document tries to highlight the key factors relevant for the success of the Life Science AAI.

In addition to this Technical requirements specification, there are other documents that describe other aspects of the Life Science AAI, including

- Requirements on service levels
- Requirements on organisational and legal aspects, including data protection

1.2. Terms

AAI	Authentication and authorisation infrastructure. The services described in this document for the Life Science community.
Account	A user account in an authentication provider external to the Life Science AAI, such as the researcher's Home Organisation or a Commercial company.
Authentication provider	An organisation external to Life Science AAI that manages users' Accounts and authenticates them in the Life Science AAI.
Bona Fide researcher	A researcher in good standing. An extra user attribute issued and managed by Life Science AAI, as described in section 4.3. Relying services may decide to make use of the Bona Fide attribute in access control enforcement.
Home Organisation	The university, research institution, company or other organisation that employs the user or where the user is otherwise affiliated with. Potentially the user's Authentication provider.
Identity, ID	Collection of attributes belonging to a certain user.
Identifier	An attribute that uniquely identifies a user.

Life Science ID	An umbrella term referring to both a Life Science user ID and a Life Science service ID.
Life Science service ID	A Life Science ID which is used by services which need to authenticate with other services. A Life Science service ID is owned by at least one Life Science user ID holder who is responsible for the service ID.
A Life Science user ID	A Life Science ID which the Life Science AAI issues to a natural person who registers to the Life Science AAI.
Relying party	An organisation that manages a Relying service.
Relying service	A service that makes use of the authentication and authorisation services of the Life Science AAI.

2. Identity and identifiers

2.1. Life Science ID

There are two kinds of identities which are commonly referred to as “Life Science IDs” or simply “users”:

- Life Science user IDs
- Life Science service IDs

Any natural person can register a Life Science user ID. Shared accounts (such as, “operations manager in-duty”) are not allowed. To register a Life Science ID a user needs to commit to an Acceptable Usage Policy (section 3.4).

A Life Science service ID can be assigned to a service. They are distinguishable from the Life Science user IDs assigned to natural persons.

2.2. User identifiers

Each user is assigned two identifiers: one Life Science Identifier and one Life Science username. Both identifiers are non-reassignable (i.e. their value cannot be later recycled to another user).

Life Science identifier is an opaque and non-revocable identifier (i.e. it cannot change over time)

- It carries the syntax of eduPersonUniqueID, which consists of “uniqueID” part and fixed scope “lifescienceid.org”, separated by at sign
- The uniqueID part contains up to 64 alphanumeric characters (a-z, A-Z, 0-9)
- N.B. eduPerson defines the comparison rule caseIgnoreMatch for eduPersonUniqueID, implying there must be no two users whose Life science identifier collides in a case insensitive comparison
- Example: 28c5353b8bb34984a8bd4169ba94c606@lifescienceid.org

Life Science username is a user selected, human-readable, revocable identifier (i.e. the user can change it)

- It carries the syntax of eduPersonPrincipalName, which consists of “user” part and fixed scope “lifescienceid.org”, separated by at sign

- the user part (syntax derived from Linux accounts (reference)) begins with a lower case letter or an underscore, followed by lower case letters, digits, underscores, or dashes. In regular expression terms: [a-z_][a-z0-9_-]*?
- Intended use: when user's unique identifier needs to be displayed in the UI (e.g. wikis or Unix accounts)
- The usernames beginning with an underscore are dedicated to Life Science service IDs.
- Example: mike@lifescienceid.org

The Life Science identifier and Life Science username "test@lifescienceid.org" are test accounts reserved for testing and monitoring the proper functioning of the Life Science AAI. The Relying parties should not authorise it to access any valuable resources.

2.3. Cardinality of identities

Each user is supposed to register only one Life Science ID which follows them during their career although they may change their affiliation (It is believed that it would be confusing for the users themselves to have several, causing extra workload in the AAI helpdesk).

The Life Science AAI will implement checks to prevent users incidentally creating parallel Life Science IDs (for instance, name and e-mail address comparisons when a new Life Science ID is registered). However, there is no way to fully prevent a user having several parallel Life Science IDs.

The administrator must have the capacity to delete a Life Science ID if a user has unintentionally created several.

3. Registering with and authenticating to Life Science AAI

3.1. Registering a Life Science ID

Registering a Life Science ID is triggered by the user themselves by

- The user browsing to "register" page, or
- A Relying service redirecting a user to register page

To start the registration process, the user needs to

1. Select their authentication provider (see the next section) and authenticate at it
2. Commit to the Acceptable Usage Policy (section 3.4) and
3. Enter their e-mail address and other necessary personal data on themselves (at least select their Life Science username)
4. Demonstrate they control the e-mail address they entered.

3.2. Supported Authentication providers and their discovery

For user authentication the Life Science AAI supports following authentication providers. The user is supposed to have an account in at least one of them and the users are supposed to link that account to their Life Science user ID:

- Identity Providers managed by researchers' Home Organization (via eduGAIN interfederation service)
- Research infrastructures (such as, ARIA)
- Commercial (such as, Google)
- ORCID

- Hostel Identity Provider (see the next section)

Apart from the Hostel Identity Provider, the Life Science AAI does not issue passwords for Life Science user IDs. Life Science service IDs can have credentials (e.g. password) associated.

The Discovery service (the UI for a user to select their Authentication provider) displays

- The user's previously used authentication provider(s) (up to 3),
- The recommended authentication provider if specified by the relying service (e.g. users authenticating via Life Science AAI to use ARIA SP should see ARIA IdP highlighted as a recommended authentication provider),
- The eduGAIN Identity Providers which
  - signal support to REFEDS Research and Scholarship entity category, or
  - signal support to GEANT Data Protection Code of Conduct entity category, or
  - have been demonstrated to release the necessary attributes. The release of such necessary attributes is checked by a user logging in to the Life Science AAI's dedicated "attribute release test" page. Users are encouraged to perform this attribute release test by clicking an "Add my institution" button in the bottom of the discovery page.
- Other authentication providers listed above

Following attributes are required from Identity Providers in eduGAIN:

- Unique user identifier (eduPersonUniqueID, SAML subject-id, eduPersonTargetedID, SAML Persistent NameID or SAML pairwise-id)
- Affiliation (eduPersonScopedAffiliation or eduPersonAffiliation)
- schacHomeOrganization

3.3. Hostel Identity Provider

The Life Science AAI manages a Hostel Identity Provider for those users who cannot use any other Authentication providers listed in the previous section. The users can self-register to the Hostel Identity Provider which issues them a username and password. The username is the user's Life Science username.

It must be possible to upgrade a self-registered user identity in Hostel Identity Provider to a verified identity (IAP/medium or IAP/high, see section 3.7) if one of the designated persons in trusted organizations (typically one of national nodes of RIs) carries out the identity proofing for the Hostel identity holder. Such verification process must be documented by that designated organization. The Hostel Identity Provider must keep logs on the upgrade process for the audit trail.

The Hostel Identity Provider must provide authentication that qualifies to the REFEDS Single-Factor Authentication profile (section 3.7).

3.4. Acceptable Usage Policy (AUP)

The Acceptable Usage Policy of the Life Science AAI may change from time to time. Any time a user logs in, the Life Science AAI verifies if the user has committed to the latest AUP version and, if necessary, asks them to do it before they can continue. User's decision to commit to the AUP is recorded for audit trail.

3.5. Account linking for Life Science user IDs

A user can link multiple accounts from multiple authentication providers (see section 3.2) to their Life Science user ID. Linking a new account is carried out by

- at first logging in using a previously linked account and subsequently the new account, or
- by demonstrating control of an e-mail account, using a procedure that is as secure as above

Account linking can be triggered by

- The user logs into their "Life Science ID management panel" (section 4.7) where they can manage their Life Science ID and start linking a new account, or
- The user is trying to log in using a previously unknown account after which the Life Science AAI provides them with two alternatives: "Create a new Life Science ID" (section 3.1) or "Link an existing account".

A user can unlink an account in the "Life Science ID management panel". After unlinking an account the user cannot use that account any more for login. The user cannot unlink their last account. If a user loses access to their last account, the Life Sciences AAI operations shall have a possibility to help them, but only according to the defined procedures which ensures there will be no security risk and only with explicit agreement from the user. All the steps must be audited.

3.6. Account management for Life Science service IDs

Each Life Science service ID must have at least one associated Life Science user ID that belongs to a natural person who manages the account and takes responsibility of the activity done using the service ID.

Any of the managers can

- Invite new managers
- Remove managers

3.7. Assurance framework

Life Science AAI supports issuing the following REFEDS Assurance Framework (RAF, https://refeds.org/assurance) ver 1.0 values to the Life Science IDs and releases them to Relying services:

eduPersonAssurance (ePA) value	Implementation in Life Science AAI	Rationale
`$PREFIX$`	Always true	Life Science AAI fulfills RAF conformance criteria
`$PREFIX$/ID/unique`	Always true	(Unique-1) will be satisfied by policy (see section 2.1) and the AUP (Unique-2) will be satisfied by e-mail handshake when user registers to Life Science AAI (section 3.1) (Unique-3) will be satisfied by policy (see section 2.2) (Unique-4) will be satisfied by Life Science attribute profile
`$PREFIX$/ID/eppn-`	Always true	Life Science AAI never reassigns ePPN (section

unique-no-reassign		2.2)
$PREFIX$/ID/eppn-unique-reassign-1y	Always missing	Excluded by the previous row
$PREFIX$/IAP/low	Always true	Guaranteed by the e-mail handshake (section 3.1) when user registers to Life Science AAI
$PREFIX$/IAP/medium	True if passed by the Authentication provider	Life Science AAI relays the value provided by the Authentication provider.
$PREFIX$/IAP/high	True if passed by the Authentication provider	Life Science AAI relays the value provided by the Authentication provider.
$PREFIX$/IAP/local-enterprise	Always missing	Not applicable for research infrastructures
$PREFIX$/ATP/ePA-1m	Always true	ePA attribute carries the person's affiliation with the infrastructure
$PREFIX$/ATP/ePA-1d	Always true	ePA attribute carries the person's affiliation with the infrastructure
$PREFIX$/profile/cappuccino	True if /IAP/medium	Compound value
$PREFIX$/profile/espresso	True if /IAP/high	Compound value

Single/multi-factor authentication

Life Science AAI supports REFEDS Single factor authentication (https://refeds.org/profile/sfa) and multi-factor authentication (https://refeds.org/profile/mfa) as follows:

Value	**Implementation in Life Science AAI**	**Rationale**
https://refeds.org/profile/sfa	True if passed by the Authentication provider	Life Science AAI is dependent on the authentication quality of the Authentication provider
https://refeds.org/profile/mfa	True if passed by the Authentication provider or Life Science AAI step-up authentication	Life Science AAI is dependent on the authentication quality of the Authentication provider. However, Life Science AAI step-up authentication (see next section) can deliver MFA authentication if the user's Authentication provider doesn't provide it.

3.8. Step-up authentication

A user can associate a second authentication factor to their Life Science ID and a Relying service can ask the Life Science AAI to perform a step-up authentication using it. The second authentication factor can for instance be a smartphone app running in the user's phone.

The Step-up authentication service first checks if the user has an Authentication provider that supports REFEDS MFA (for instance, by issuing an authentication request with requested authentication context equals REFEDS MFA). If that fails the Step-up authentication services proceeds to enroll an MFA for the user.

The enrollment of the second authentication factor must qualify at least to RAF `$PREFIX$/IAP/medium`.

4. Attributes and authorisation

In addition to the identifiers presented in section 2, the Life Science AAI can decorate Life Science IDs with attributes which are useful for the Relying parties to decide the user's permissions in their services.

Each attribute is either

- Common, which means they are visible to all Life science research infrastructures or communities, or
- Community specific, which means the attribute is visible only to the Relying services of the research infrastructure or community that manages it

4.1. Home Organisation Affiliation(s) of a user

Each user can be affiliated to one or more Home organisations (such as, a university, research institution or private company) and the user's affiliations may change over time. A Relying service wanting to couple user's permissions to their continuing affiliation can observe the Home Organisation Affiliation attribute and their changes.

The syntax and semantic of the attribute follows the eduPersonScopedAffiliation attribute defined in eduPerson schema (version 201310). If necessary, a new attribute following the eduPersonScopedAffiliation syntax will be defined. Following values are recommended for use to the left of the "@" sign:

`Faculty`	The person is a researcher or teacher in their home organization. The exact interpretation is left to the home organization, but the intention is that the primary focus of the person in his/her home organization is in research and/or education. Note. This attribute value is for users in the academic sector.
`Industry-researcher`	The person is a researcher or teacher in their home organization. The exact interpretation is left to the home organization, but the intention is that the primary focus of the person in his/her home organization is in research and/or education. Note. This attribute value is for users in the private sector.
`Member`	`Member` is intended to include `faculty`, `industry-researcher`, `staff`, `student`, and other persons with a full set of basic privileges that go with membership in the home organisation, as defined in eduPerson.

	In contrast to faculty, among other things, this covers positions with managerial and service focus, such as service management or IT support.
Affiliate	The affiliate value for eduPersonAffiliation indicates that the holder has some definable affiliation to the home organization NOT captured by any of faculty, industry-researcher, staff, student and/or member.

In other words, if a person has faculty or industry-researcher affiliation with a certain organization, they have also the member affiliation. However, that does not apply in a reverse order. Furthermore, those persons who do not qualify to member have an affiliation of affiliate.

Examples

- faculty@helsinki.fi
- industry-researcher@zeiss.com
- member@ebi.ac.uk

To become a holder of the faculty, industry-researcher or member attribute values in Life Science AAI, the user must either

- Perform federated login to the Life Science AAI using their home organisation's credentials, during which the home organization releases the related eduPersonAffiliation or eduPersonScopedAffiliation attribute, or
- Be assigned that identifier by a dedicated person in their home organisation

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

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

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

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

4.2. User's Research Infrastructures attribute

Universities, research institutions and other organisations may be affiliated with one or more research infrastructures, giving their users access to the research infrastructures' Relying services. User's Research Infrastructures attribute indicates to which research infrastructures the user's Home Organisation is affiliated with.

4.3. Researcher status and attestations

As described above, any natural person can register a Life Science ID. To narrow down the user base for Relying services limited to researchers, a user could apply for and receive further researcher qualifications, such as a "bona fide researcher" status[2].

The Life Science AAI has a service that can assign users one or more researcher qualifications based on, for instance,

- Their Home Organisation's ability to deliver faculty@<home-organisation> value (described above in section 4.1), or
- Another qualified researcher vouching for them or
- Them making an attestation that they commit to a certain community code.

[2] See Registered access: authorizing data access: https://www.nature.com/articles/s41431-018-0219-y

4.4. Groups

The Life Science AAI has a service for managing users' group memberships and roles in the groups they belong to. Management of groups is done using a web interface.

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

Groups can be one of three types:

1. Secret group (where the group is not shown to anyone and the group creator/manager adds members manually).
2. Private groups (where users can have URL to the registration form for the group, and the group manager can approve or decline membership requests).
3. Public group where users are able to register as for the private group, but will be automatically added to the group without the need for group manager approval.

Each group has one or several managers who are able to

- delegate group manager role to other users and groups
- manage the group's properties (such as name)
- invite group members (requires confirmation by the invited user)
- add group members (no confirmation needed by the invited user)
- edit the type of the group (secret, private, or public)
- add other group as group member (members from other group became members of the group as long as other group is member of the group)
- remove group members
- assign and delete additional attributes (roles) for users in the group

The group manager needs to periodically confirm that the group is still active. The members of the group may need to periodically refresh their membership.

Groups have hierarchy i.e. member of a child group is automatically a member of the parent group.

4.5. Dataset authorisation

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

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

The service has interfaces for:

- Bulk import for datasets' metadata from the data archive's catalogue for automated provisioning of the related application circulation workflows
- Launching data access application from an external source, such as the portal of the data archive
- Exporting the entitlements to an external system for access rights enforcement

4.6. Other attributes

The Life Science AAI supports adding arbitrary attributes to a Life Science ID, including

- If the Life Science ID is a user ID or a service ID
- User's name
- User's e-mail address (which is confirmed by an e-mail handshake)
- User's ORCID ID (which is recorded using ORCID APIs)
- Other wider researcher identifiers (such as, a researcher ID assigned to users by e-infrastructures) if they emerge
- The country in which the user's Home Organisation resides (if the user has several Home Organisations, the attribute may be multi-valued). This determines to what services the user has access (if at all - some services are for members only) and under what conditions (some services may be paid in the future for non-members, and discounted for observers, while free for members).
- User's public key (for SSH secure shell access)

4.7. Life Science ID management panel

Users can view their Life Science ID, attributes and linked accounts (section 3.5) and manage some of them in a dedicated web page "Life Science ID management panel".

User attributes are obtained from an Authentication provider, a Relying service or filled in by the user themselves. The user filled attributes are controlled solely by the user. Dependent on the particular attribute the user might or might not have the rights to modify it by himself, but no other role (e.g. group manager) should have rights to modify it without user's explicit permission. Ability to manipulate mentioned data by other parties creates a security risk and therefore it is strictly forbidden. The only exception from this rule is the Life Sciences AAI operations, which will have the right to modify this data, but this has to be done in accordance with the defined procedures, with explicit agreement from the user, and properly audited.

5. Access control

5.1. Active role selection

Some services expect a user to select the role they are currently acting in and couple the user's permissions to that role. For instance:

- A user is associated to several projects (represented by the group membership attribute, see section 4.4 Groups) and they need to select the project they are currently active, providing them access to only those resources assigned to the project.
- A user is affiliated to several Home Organisations (represented by the Home Organisation affiliation attribute, see section 4.1) but their access rights are coupled to their continuing affiliation with a particular Home Organisation. The user needs to select the Home Organisation to which they want to couple their access rights.

Active role selection is an additional service which the Relying Service can subscribe. The relying service identifies the attribute(s) whose active value the user needs to select when they log in. The result is then mediated to the Relying Service.

5.2. Access control enforcement during login

A Relying service can subscribe an additional service where the Life Science AAI enforces access control after authenticating the user but before the user's browser is returned to the Relying service. The access control can be based on

- The user's membership in a particular group (see section 4.4),
- The user having sufficient level of identity and authentication assurance (see section 3.7) or
- Any other attribute of the user

If the Life Science AAI learns the user does not pass the criteria, it will (depending on the configuration made for each Relying service separately)

- display "Permission denied" message, or
- display "Permission denied" message and a free text message instructing the users on how to remedy, or
- (if permission is denied due to a missing group membership) display "Permission denied" message and the list of private and public groups whose members have access to the Relying service. The user can select a group which will redirect them to the registration form of the group

5.3. Life Science AAI Test environment

Life Science AAI has a Test environment for the Relying services to test their technical integration. When a new Relying Service is registered to the Life Science AAI, it is first exposed to the Test environment. After completing the tests and committing to the Life Science AAI policies for Relying Services, they are moved to the production use. Transfer to the production environment must not require any configuration updates for the Relying Service.

The Life Science AAI enforces access control of the Test environment (see the previous section). Only users who are members of a dedicated Test user group can access the Relying Services in the Test environment. For other users, the Life Science AAI displays instructions on how to apply for membership in the Test user group (see previous section). Membership in the Test user group expires in 30 days.

6. Technical interfaces

6.1. Federated login and attribute release

The Life Science AAI provides an Identity/Service provider proxy with three primary interfaces for federated authentication and release of the attributes described in this document

- SAML 2.0, using the SAML2int profile or its successor
- OAuth2, including support to encoding attributes to access tokens as signed JWT
- OpenID Connect, including support to encoding attributes to claims in id-tokens and retrieving them from user-info endpoint.

It must be possible to configure what attributes are released to a Relying service for each Relying service separately.

The Life Science AAI pays attention to the smooth integration to the federated login with the Home Organisation credential via eduGAIN. The goal is that common end users do not need to face unnecessary technical hurdles for federated login.

6.2. Attribute retrieval from external sources

The Life Science AAI can retrieve attributes from external sources using a REST API during the OAuth2 and/or OIDC protocol flow and embed them to the claims and tokens released (see the previous section).

6.3. Credential translation

Relying Services can subscribe to the credential translation service of the Life Science AAI, allowing the users to obtain X.509 certificates based on the login described in the previous section.

6.4. User synchronisation

When needed, the Life Science AAI can synchronise users from external sources. That enables managing group membership within Life Science AAI from the external system. Users that weren't registered in Life Science AAI before, will have to approve the Acceptable usage policy before the they can utilize any services provided within Life Science AAI.

The synchronization will be done periodically in configurable time period depending on a particular use-case and the technical capabilities of connected external source.

6.5. Provisioning

Life Science AAI can provision user identities and attributes (such as, group memberships) to Relying Services. Provisioning is done either by providing attribute authority or by pushing the data directly to Relying Service. Regardless of the provisioning method, the Relying Service should obtain only data about the users who are entitled to use the service. The provided data should be limited to minimal subset which is actually required by the Relying Service.

7. Logging, statistics and data retention

- The IdP/SP Proxy must collect appropriate logs.
- The AAI must provide anonymised statistics on # of Relying services, # of identities, # of logins (live and historical), # of logins by different Identity Providers to a given Relying service
- The AAI must display a public listing of current relying services both in test (section 5.3) and production environment, including a link to their privacy policy, location and organisation responsible for the service
- The AAI must follow data retention practices. Accounts must be closed if not used for 24 months. Users must be informed of the account closure well in advance.
- All the operations within the Life Science AAI must be recorded in audit logs

8. Information security

The Life Science AAI must be operated following professional information security practices.

The Life Science AAI must follow the security incident response framework described in Sirtfi v1.0 (https://refeds.org/sirtfi).

9. Usability

9.1. Ease of use

All services and service components exposed to common end users must be easy and intuitive to use without any particular training or experience on similar services.

Help text should be provided where required to enhance the user experience.

All navigation options, buttons, and help text must be simple, clear, and concise.

All administrative interfaces (group manager, dataset authorisation, home organisation assignment) and relying service management interfaces must be easy enough to use after studying related online materials (manuals, videos, etc). Such materials should be provided in a centralised location and made accessible to all administrators.

Language should be familiar and non-technical i.e; technical terms and acronyms such as 'VO' should be avoided or explained, if avoiding is difficult.

9.2. Usability expert review

All services and service components will be exposed to a review by a usability expert and their providers are expected to implement reasonable improvements based on the review results.

9.3 Consistency

The Life Science AAI should allow templating determined by the SP that the user is coming from.

The templating should be consistent throughout navigation on Life Science AAI pages.

10. Capacity

The Life Science AAI must have sufficient capacity to serve

- 25000 logins a day
- 100000 OpenID Connect introspections a day
- A peak of 500 OIDC requests (introspection or userinfo) simultaneously (i.e. within the timeout of the components)

There should be the potential to increase this capacity to meet increasing demand as the user base and number of relying services grow.

11. Accessibility & Compatibility

The user should be able to access the Life Science AAI regardless of the device (e.g. phone, tablet, PC), the operating system (e.g. Android, Mac OS, Windows, Linux) or the browser used. Life Science AAI must have cross browser compatibility with the following:

Desktop Browsers

- Google Chrome; latest version and the previous five versions. Currently from 67.0 to 72.0
- Firefox; latest version and the previous five versions. Currently from 60.0 to 65.0
- Edge; latest version and the previous three versions. Currently from 38 to 44
- Internet Explorer; latest version and the previous three versions. Currently from v8 to v11

- Safari; latest version and the previous three versions. Currently from v10.1 to v12.0.2
- Opera; latest version and the previous three versions. Currently from v55 to v58

Mobile Browsers

Latest version and versions of the previous two years (Chrome for Android, Firefox for Android, UC browser for Android, IE Mobile, and iOS Safari)

Cross browser compatibility with other browsers should be on a best-effort basis. The Life Science AAI should also ensure compatibility with any new browsers which obtain greater than 1% global browser usage.

Large mouse pointers should be enabled, and large targets or hotspots provided.

Menus and controls should be accessible from the keyboard.