



# IRISCC

## D6.1

# **Landscape analysis of AAI at RIs and cookbook for connecting to the AAI federation**



Disclaimer: Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

## Abstract

### Key words

Landscape analysis, RIs, Federated AAI, Access

This report gives an overview of possible AAI systems in place for **digital** services as provided by the RIs in the IRISCC landscape. It includes an analysis if these AAI systems are already connected to a federated AAI service or fit to be connected. The target is that all digital services with AAI in IRISCC become federated through EGI Check-in, which serves as federated AAI service for EOSC. For the second group, a cookbook is provided on how to connect their AAI service to EGI Check-in. There are also AAI systems in use which are not yet fit for such a federation. Therefore, the cookbook includes recommendations to set-up and deploy a new local AAI service, using KeyCloak, that then will be fit for EGI Check-in federation.

## Revision History

Version	Date	Description	Author/Reviewer
V 0.1	28/07/2024	First Draft	Dick M.A. Schaap (MARIS), Valeria Ardizzone (EGI)
V 0.2	15/08/2024	Second Draft	Tjerk Krijger (MARIS)
V 0.3	19/08/2024	Review	Ville Terhunen (EGI) Ulrich Bundke (FZJ)
V 1.0	26/08/2024	Submitted version	Dick M.A. Schaap (MARIS), Tjerk Krijger (MARIS)

## Document Description

Landscape analysis of AAI at RIs and cookbook for connecting to the AAI federation

Work Package Number 6


### Document Type

Report

### Document Status

UNDER EC REVIEW

Version 1.0

Dissemination Level	Public
Copyright Status	 <p>This material by Parties of the IRISCC Consortium is licensed under a <a href="https://creativecommons.org/licenses/by/4.0/">Creative Commons Attribution 4.0 International License</a>.</p>
Lead partner	MARIS
Document Link	
DOI	<a href="https://doi.org/10.5281/zenodo.13375311">https://doi.org/10.5281/zenodo.13375311</a>
Main Author(s)	<ul style="list-style-type: none"> <li>• Dick M.A. Schaap (MARIS) and Valeria Ardizzone (EGI)</li> </ul>
Contributing Authors	<ul style="list-style-type: none"> <li>• Tjerk Krijger (MARIS)</li> <li>• Contact persons of digital RI services:             <ul style="list-style-type: none"> <li>○ Charles Troupin (ULiege)</li> <li>○ Antti Hyvärinen (FMI)</li> <li>○ Alessandro Spinuso (KNMI)</li> <li>○ Stephan Kindermann (DKRZ)</li> <li>○ Damien Boulanger (CNRS)</li> <li>○ Markus Fiebig (NILU)</li> <li>○ Hajo Boomgaarden (UNIVIE)</li> <li>○ Davide Di Cioccio (EMBRC-ERIC)</li> <li>○ Gerard van der Schrier (KNMI)</li> <li>○ Dennis Abel (GESIS)</li> <li>○ Michel Boer (AnaEE-ERIC)</li> </ul> </li> </ul>
Reviewers	<ul style="list-style-type: none"> <li>• Ville Tenhunen (EGI)</li> <li>• Ulrich Bundke (FZJ)</li> </ul>
Approved by:	<ul style="list-style-type: none"> <li>• Päivi Haapanala (Luke)</li> </ul>
Estimated Delivery date	August 2024 (M5)
Actual Delivery date	27/08/2024

<b>Terminology / Acronyms</b>	
Term/Acronym	Definition
AAI	Authentication and Authorization Infrastructure
AARC	Authentication and Authorisation for Research and Collaboration. The AARC initiative was first launched in May 2015 to address the increased need for federated access and for authentication and authorisation mechanisms by research and e-infrastructures. The AARC Blueprint Architecture and the accompanying set of policies ensure interoperability among AAI, streamline researchers' access to resources and offer a single integration point to resource providers.
IAM	Identity and Access Management
IdP	identity provider
RI	Research Infrastructure
SAML	Security Assertion Markup Language
SP	Service Provider
SSO	Single-Sign-On: allowing to login and access to different AAI systems of multiple digital services with the same user ID - password
TA	Transnational Access
VA	Virtual Access
VO	Virtual Organisation
VRE	Virtual Research Environment
WPS	Web Processing Service

# CONTENT

Executive summary .....	5
1. Objective of this report.....	6
2. EGI-Check-in as preferred AAI federation service for IRISCC.....	7
2.1. Identity and access management service solution .....	7
2.2. EGI-Check-in architecture .....	8
2.3. Virtual Organisation .....	10
3. Landscape analysis of AAI systems used for digital services by RIs in IRISCC.....	11
3.1. List of digital services in IRISCC and AAI survey .....	11
3.3 Preliminary conclusions .....	21
4. Integration with EGI Check-in.....	24
4.1 Integration options .....	24
4.1.1 EGI Check-in as community AAI.....	24
4.1.2 EGI Check-in as an AAI proxy for services or resource providers .....	25
4.1.3 EGI Check-in as a bridge to EGI services and resources .....	25
4.2 Deployment types .....	25
4.3 Integration steps.....	25
4.4 Authentication and Authorization with EGI Check-in.....	26
4.5 Using Keycloak as AAI service .....	26
5. Conclusions.....	28
6. References.....	30
Annex 1 – Survey results.....	31

# Executive summary

The overall objective of IRISCC WP6 is to harmonise transnational and virtual access (TA and VA) policies and procedures for efficient access management and provision, as well as for positive user experience to access installations and digital services, and to deploy and provide the technical interoperability framework for integrated IRISCC services.

Task 6.1 is aimed at harmonisation of access policies and procedures to IRISCC digital services. It should facilitate easy access to IRISCC digital services by adopting a federated Authentication and Authorization Infrastructure (AAI) to support the sign-in to the range of digital services within the IRISCC landscape with the same account. This is called 'Single-Sign-On (SSO)'.

This Deliverable D6.1 gives an overview of the AAI systems in place for **digital** services as provided by the Research Infrastructures (RIs) in the IRISCC landscape. It includes an analysis if these AAI systems are already connected to a federated AAI service or fit to be connected. The target is that all digital services with AAI in IRISCC become federated through EGI Check-in, which serves as federated AAI service for EOSC. For the second group, a cookbook is provided on how to connect their AAI service to EGI Check-in. There are also AAI systems in use which are not yet fit for such a federation. Therefore, the cookbook includes recommendations to set-up and deploy a new local AAI service, using KeyCloak, that then will be fit for EGI Check-in federation.

This report gives the conclusions with the preliminary results of the landscape analysis and indicates which RI digital services are already OK, and which might have to undertake action. The analysis and drafting of the Deliverable D6.1 have been undertaken by IRISCC partners MARIS and EGI, supported by managers of RIs, completing the Task 6.1 AAI survey. While the review of D6.1 has been performed by IRISCC partners FZ and EGI.

A follow-up will be given by MARIS and EGI by organising an online workshop where the findings per service will be presented and discussed for finalising conclusions on the current situation and required actions. The workshop will also provide information and guidance on how to connect local AAI services to EGI Check-in. This way, the workshop will lead to a refinement of actions and will pave the way towards SSO for all RI services.

The resulting actions should then be performed by RI service operators, supported by MARIS and EGI, aiming for delivery before M11 (end of February 2025), and whereby the action results will be reported in Deliverable D6.5 - Report on accessibility of IRISCC services through EOSC federated AAI - planned for M12 (end of March 2025).

# 1. Objective of this report

The overall objective of IRISCC WP6 is to harmonise transnational and virtual (TA and VA) access policies and procedures for efficient access management and provision, as well as for positive user experience to access installations and digital services, and to deploy and provide the technical interoperability framework for integrated IRISCC services.

Task 6.1 is aimed at harmonisation of access policies and procedures to IRISCC digital services. It should facilitate easy access to IRISCC digital services by adopting a federated Authentication and Authorization Infrastructure (AAI) to support the sign-in to the range of digital services within the IRISCC landscape with the same account. This is called 'Single-Sign-On (SSO)'.

This Deliverable D6.1 should give an overview of the AAI systems in place for **digital** services as provided by the Research Infrastructures (RIs) in the IRISCC landscape. An analysis will be made if these AAI systems are already connected to a federated AAI service or already fit to be connected. The target is that all digital services with AAI in IRISCC become federated through EGI-Check-in, which is operated by IRISCC partner EGI, and which serves as federated AAI service for EOSC. For the second group of RIs, a cookbook will be provided on how to connect their AAI service to EGI-Check-in. While there might also be AAI systems in use which are not yet fit for such a federation. Therefore, the cookbook will give guidance on how to set-up and deploy a new local AAI service, that will be fit for EGI-Check-in federation. The report should assess possible actions to be undertaken by selected RIs before M12, the deadline for achieving SSO capabilities for using all digital services of RIs in the IRISCC portfolio.

## 2. EGI-Check-in as preferred AAI federation service for IRISCC

The aim of Task 6.1 is to establish Single-Sign-On (SSO) for users of the IRISCC digital services for those digital services that are operated with an Authentication and Authorization Infrastructure (AAI) service. SSO can be established by connecting the various AAI services to a federated AAI service. For IRISCC the target is to make use of EGI Check-in of partner EGI as the IRISCC federated AAI service. The following paragraphs give more information about EGI-Check-in.

### 2.1. Identity and access management service solution

A Research Infrastructure (RI) providing services and resources to end-users has to deal with the control of the access to these services and resources: the identity of the users needs to be verified, and once this is done successfully, the proper rights have to be granted to the users to perform the operations they are supposed to do. Identity and Access Management (IAM) is an approach that manages and organises all identities into one system with a consistent set of rules and policies. The purpose is to ensure that the right users have the right access to the right resources at the right time. IAM includes systems and processes that work together to assign a single digital identity to each user. The user is authenticated when they log in and authorised for specific access. IAM also monitors and manages those identities throughout their life cycles.

With the growth of international research collaboration, users are accessing external systems which are fundamentally outside their domain of control and external users are accessing internal systems. The need for managing user identity across borders between organisations, domains, and services, leads to the creation of federated identity environments. A federation is a system of trust between two parties for the purpose of authenticating users and conveying information needed to authorise their access to resources. In this system, an identity provider (IdP) is responsible for user authentication, and a service provider (SP), such as a service or an application, controls access to resources.

[EGI Check-in](#)<sup>1</sup> is a service solution for federated identity management based on the AARC Blueprint Architecture (AARC-BPA) and a service of the existing [eduGAIN](#)<sup>2</sup> Interfederation. By integrating with EGI Check-in, users do not need to create any additional user names/passwords and can easily get access to services with their institution accounts; users without institutional accounts can access through social media or other external



accounts, including ORCID, GitHub, Google, LinkedIn, etc. EGI Check-in manages users and their respective roles and other authorization-related information. The adoption of standards and open technologies, including SAML 2.0, OpenID Connect 1.0, OAuth 2.0 and X.509v3, facilitates interoperability and integration with the existing AAIs of other e-infrastructures and research communities.

## 2.2. EGI-Check-in architecture

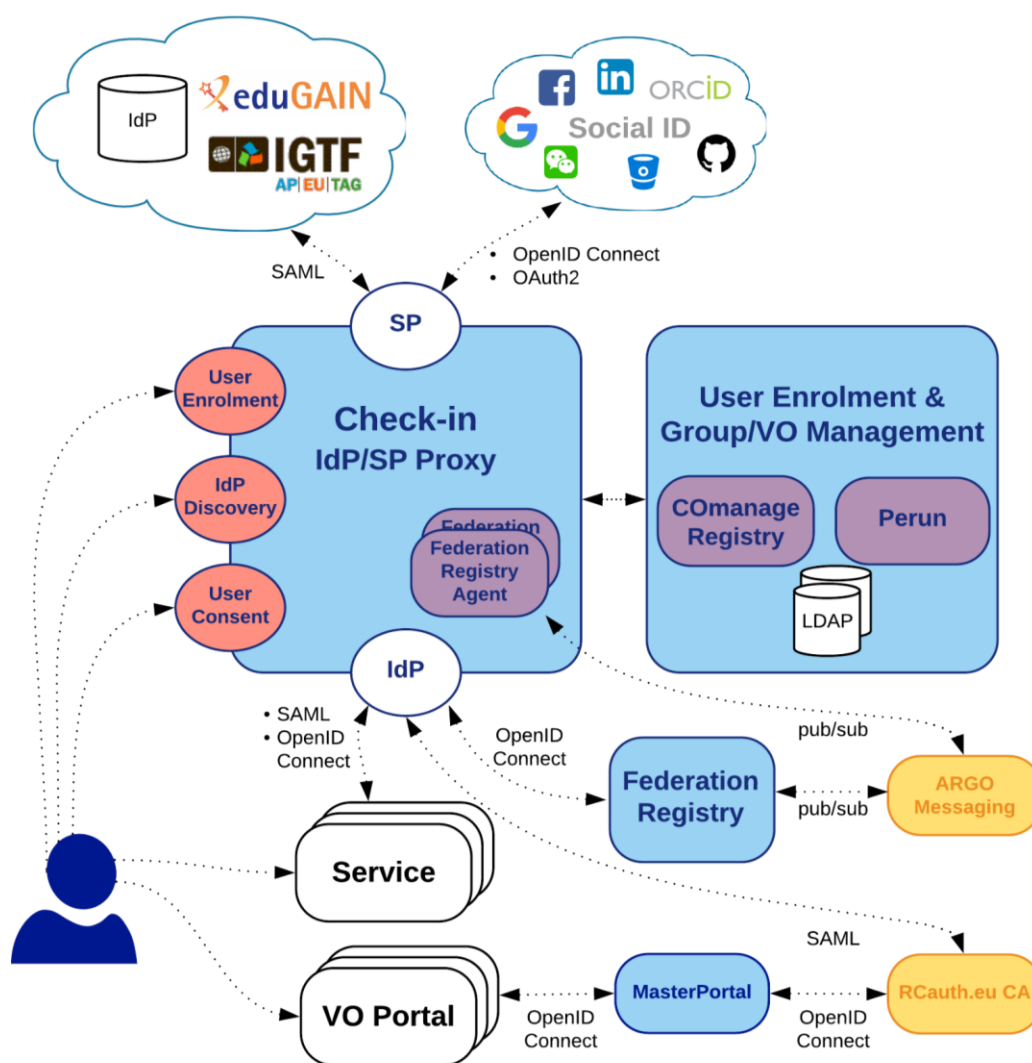


Figure 1 Architecture of EGI Check-in service

The architecture of EGI Check-in service is shown in Figure 1. In a nutshell, EGI Check-in is a proxy service that operates as a central hub to connect federated Identity Providers (IdPs) with Service Providers (SPs). EGI Check-in allows users to select their preferred IdP so that they can access and use services in a uniform and easy way. For the user the feature is transparent: as soon as their IdP is integrated with the proxy, they are redirected by the

service to their own IDP. Once integrated the IDP with the proxy, all the services using the IDP proxy will be available. The service providers will get all the authentication and authorisation information needed from the IdP Proxy (in the form of attributes), without the need to deal with individual IdPs.

Main characteristics of EGI Check-in are the following:

- Enables multiple federated authentication sources using different technologies
- Increased productivity and security
- Federated in eduGAIN as a service provider, publishing [REFEDS RnS](#) and [Sirtfi](#) compliance
- User registration portal to allow accounts-linking
- Combines user attributes originating from various authoritative sources (IdPs and attribute provider services) and delivers them to the connected service providers in a transparent way.

In the core of EGI Check-in are three main components -- the IdP/SP Proxy, the User Enrolment and Group Management and the Federation Registry.

- The **IdP/SP Proxy** component acts as a bridge between the services and external authentication sources and identity providers. This decoupling of the internal services and external authentication sources/identity providers, reduces the complexity of the service implementation as it removes dependencies on the heterogeneity of multiple IdPs, Federations, Attribute Authorities and different authentication and authorization technologies. This complexity is handled centrally by the proxy.
- The **User Enrolment and Group Management** component supports the management of the full life cycle of user accounts including the initial user registration, the acceptance of the terms of use of community services, account linking, group and user management, delegation of administration of groups to authorised users and the configuration of custom enrolment flows for groups via an intuitive web interface. For Virtual Organisations (VOs), operating their own Group/VO Management system, the Check-in service has a comprehensive list of connectors that allows integrating their systems as externally managed Attribute Authorities.
- The **Federation Registry**<sup>3</sup> provides a secure web interface through which SP owners can register and manage their OpenID Connect and SAML based Services: users in this portal can view and also manage their Services through creating and submitting Service Requests. There are three types of requests that can be made: registration, reconfiguration and deregistration. Once a request is submitted users with reviewing privileges are notified and can view and review it. If a petition is approved then it is deployed to the requested integration environment (development, demo and production).

## 2.3. Virtual Organisation

A *Virtual Organisation*, by concept, is a set of cooperating independent organisations which to the outside world provide a set of services as if they were one organisation. It is worth noting that EGI Check-in group management is built on the structure of EGI Virtual Organisation (VO). EGI is a multi-disciplinary e-Infrastructure, that means the same resources are shared among different research communities. Research communities access the e-Infrastructure by grouping their users into VOs. Usually there is one-to-one mapping between research communities and VOs. This is not mandatory. There are cases such as a big community enabling multiple VOs for different disciplines. These VOs are basically groups of users and they are enabled on the EGI resources (i.e., Grid or Cloud) attached to the VOs. In this way, users are not individually enabled on the resources but through VOs. On the other hand, a user can belong to different VOs, e.g., s/he works with different communities.

The control of the VO is fully managed by the community - an admin role will be created and assigned to a community representative who responds to approve user registrations and grant rights for access to resources and services attached to the community VO.<sup>3</sup> Landscape analysis of AAI systems used for digital services by RIs in IRISCC.

# 3. Landscape analysis of AAI systems used for digital services by RIs in IRISCC.

## 3.1. List of digital services in IRISCC and AAI survey

On 17<sup>th</sup> June 2024, MARIS circulated to identified contact persons for RIs in IRISCC a survey to gather answers about IRISCC installations as mentioned under VA and other digital services provided by RIs. It was explained that the ultimate goal of Task 6.1 in IRISCC is to make the digital services and digital installations provided by the RIs accessible via a federated AAI (through EGI-Check-in) with single-sign-on (SSO). The survey serves to perform a landscape analysis of AAI at RIs concerning connecting to EGI Check in for establishing AAI federation for all digital services in IRISCC.

The survey is available at: <https://forms.gle/a5ZN2EFoZtjRgYaX7><sup>3</sup>

Since 17<sup>th</sup> 2024, 3 reminders have been sent out in order to reach out and get answers from most of the IRISCC RIs providing access through IRISCC Online Service Facility and other RIs involved in the project. In total we received answers from 12 respondents providing us with answers to 14 out of 20 installations and RIs:

- Table 1 gives an overview of the RI installations that will receive funding via the project to provide VA to their digital services.
- Table 2 gives on overview of the other participating RIs in IRISCC that do also provide VA but will not receive funding for this as part of the VA Calls.

**Table 1. Overview of contacted organizations providing funded VA through a RI participating to IRISCC.**

RI installation	Research Infrastructure (full name)	Installation organisation (VA)
IAGOS Data Centre	In-service Aircraft for a Global Observing System	CNRS
IAGOS Data Centre	In-service Aircraft for a Global Observing System	KIT
ACTRIS Data Centre	Aerosol, Clouds and Trace gases Research Infrastructure	NILU
ACTRIS Data Centre	Aerosol, Clouds and Trace gases Research Infrastructure	CNR
ACTRIS Data Centre	Aerosol, Clouds and Trace gases Research Infrastructure	CNRS
ACTRIS Data Centre	Aerosol, Clouds and Trace gases Research Infrastructure	FMI
ICOS Carbon Portal	Integrated Carbon Observation System	ULUND
IS-ENES	European Network for Earth System Modelling	DKRZ
IS-ENES	European Network for Earth System Modelling	KNMI
ECA&D	European Climate Assessment & Dataset	KNMI
EIRENE data center	Environmental Exposure Assessment Research Infrastructure	UU

**Table 2. Overview of IRISCC RIs providing non-funded VA**

RI acronym	Research Infrastructure (full name)	Contact organisation
SeaDataNet - CDI	Pan-European Infrastructure for marine and ocean data management – CDI Data Discovery & Access Service	MARIS
SeaDataNet - DIVAnd	Pan-European Infrastructure for marine and ocean data management – DIVAnd - Data Interpolating Variational Analysis	ULiege
AnaEE	Analysis and Experimentation of Ecosystems	AnaEE-ERIC
eLTER	European Long-Term Ecosystem, Critical Zone and Socio-ecological Research Infrastructure	FC.ID
EMBRC	European Marine Biological Resource Centre	EMBRC-ERIC
OPTED	Observatory for Political Texts in European Democracies	UNIVIE
GESIS	research-based infrastructure institution for the social sciences	GESIS
ECMWF	European Centre for Medium-range Weather Forecasts	ECWMF

### 3.2 AAI Survey results

Table 3 gives the answers as received from each of the contacts. It is remarked that for ICOS Carbon Portal the responses are taken from a recent survey conducted as part of the ENVRI-Hub NEXT project with similar questions.

**Table 3. Summary of survey answers**

RI/Installation organization	Description	AAI status
IAGOS – CNRS (installation)	<p>Name: Climatologies and anomalies of selected ECVs in the troposphere by IAGOS-DC-CNRS.</p> <p>Description: This service will provide diagnostics and statistics for a better understanding of the long time series, offering the possibility of the creation of a “tailored data set for ESM evaluation/improvement”. This service is currently under development and will be ready for the first release. A very similar service can be found here: <a href="https://services.iagos-data.fr/atmo-access/footprint">https://services.iagos-data.fr/atmo-access/footprint</a></p>	<p>Using an AAI provided by AERIS (French Data and Services cluster for Atmosphere) based on Keycloak. The AAI is registered as a Service Provider of eduGAIN.</p>
IAGOS – KIT (installation)	<p>Name: Climatologies and anomalies of selected VOCs in the troposphere by IAGOS-DC-KIT.</p> <p>Description: This service will provide a time series of organic compounds and auxiliary species (such as O<sub>3</sub>, CO and NO<sub>y</sub>) in the troposphere and lowermost stratosphere tagged with the impact of biomass burning / fires.</p> <p>This service is under development and will be provided for the first release.</p> <p>We (in IAGOS-CARIBIC) don't have a data provision chain comparable with the typical much bigger RIs in the environmental domain. Up to now we provide our data via two channels:</p> <ol style="list-style-type: none"> <li>1. A subset is offered via the IAGOS DC in Toulouse, as described in the table below by Damien</li> <li>2. The full dataset is accessible via Zenodo and a local THREDDS server</li> </ol>	<p>Currently we don't have our own AAI. We are currently waiting on the answer by our computing centre, whether it could be implemented with moderate efforts.</p>

RI/Installation organization	Description	AAI status
ACTRIS – NILU (installation)	Data access service.	Data access service does not have its own AAI.
ACTRIS – CNR (installation)	<p><u>No answer to the survey.</u></p> <p>Own research found: ACTRIS Data Centre node for aerosol remote sensing profiling (ARES<sup>1</sup>). This node is physically hosted at CNR in Potenza, Italy, where all the data are stored and made available. CNRS is responsible for the combined lidar-photometer processing which is executed in Lille, France. The EARLINET <sup>2</sup>Single Calculus Chain (SCC) is a tool for the automatic analysis of aerosol lidar measurements. Its development started in the framework of EARLINET-ASOS (European Aerosol Research Lidar Network – Advanced Sustainable Observation System), it is now a major component of the ACTRIS Aerosol Remote Sensing Node (ARES) responsible for the curation and the processing of the ACTRIS aerosol remote sensing data.</p> <p>For non ACTRIS/EARLINET lidar stations: the usage/testing of the SCC is possible also for not ACTRIS stations! If you are interested, please, request the access to SCC as ACTRIS DC-ARES service following ACTRIS-IMP instructions<sup>34</sup>.</p>	Login required to access EARLINET (SCC).

<sup>1</sup><https://www.actris.eu/topical-centre/data-centre/ares-aerosol-remote-sensing-data-centre-unit>

<sup>2</sup>[https://www.earlinet.org/index.php?id=earlinet\\_homepage](https://www.earlinet.org/index.php?id=earlinet_homepage)

<sup>3</sup><https://www.actris.eu/sites/default/files/inline-files/Guidance%20notes%20to%20ACTRIS%20IMP%20user%20application%20form%202021.pdf>

<sup>4</sup><https://www.actris.eu/access-services/apply-tna>



RI/Installation organization	Description	AAI status
ACTRIS – CNRS (installation)	<p><u>No answer to the survey.</u></p> <p>Own research found:</p> <ul style="list-style-type: none"> <li>• GRES data centre (<a href="https://gres.aeris-data.fr/">https://gres.aeris-data.fr/</a>) unit provides data curation service for reactive trace gases remote sensing data.</li> <li>• The ASC data centre unit provides data curation service for data obtained from experiments in atmospheric simulation chambers (ACTRIS exploratory platforms). It is making use of the EUROCHAMP database (<a href="https://data.eurochamp.org/">https://data.eurochamp.org/</a>), which is hosted by AERIS infrastructure.</li> </ul>	<p>GRES data centre catalogue uses an AAI provided by AERIS (French Data and Services cluster for Atmosphere) based on Keycloak. The AAI is registered as a Service Provider of eduGAIN.</p>
ACTRIS – FMI (installation)	<p>Palla-Sodankylä: TNA access &amp; Pallastunturi-Sodankylä VA access</p>	<p>Palla-Sodankylä: TNA access &amp; Pallastunturi-Sodankylä VA access both do not have an own AAI.</p>
ICOS – ULUND (installation)	<p><u>No answer to the survey.</u></p> <p>ICOS Carbon portal</p> <p>Answer taken from ENVRI-HUB Next questionnaire</p>	<p>Answer taken from ENVRI-HUB Next questionnaire: ICOS has an AAI, needed for authorisation of uploads and other admin tasks.</p> <p>Registration of users to add extra functionality and store acceptance of data licence.</p> <p>Authentication options include Institutional accounts (eduGAIN), ORCID, social media, local login using email/password.</p>

RI/Installation organization	Description	AAI status
IS-ENES – DKRZ (installation – data access service)	IS-ENES data access service <a href="https://esgf-metagrid.cloud.dkrz.de/search">https://esgf-metagrid.cloud.dkrz.de/search</a>	Has an AAI, currently working on an integration with the EGI checkin AAI and are currently experimenting with a keycloak based test service at UKRI / CEDA, which will later be replaced by the European proxy solution. So the plan is to move completely to OpenID connect and OAuth2 in Europe.
IS-ENES – DKRZ (installation – web processing service)	ENES RI Web processing service	Service has an AAI, experimenting with different AAI solutions also in connection to keycloak, yet the WPS services currently in production do not rely on an own AAI integration but rely on the AAI solution which is provided by the virtual research environments they are integrated in. E.g. the (load balanced) WPS service which is provided for COPERNICUS, relies on the AAI solution of Copernicus and the WPS integration is based on firewall configuration to allow only requests coming from copernicus processing nodes. This is probably also the initial approach we will follow in IRISCC for the D4Science integration.

RI/Installation organization	Description	AAI status
IS-ENES – KNMI (installation)	<p>IS-ENES offers Data discovery, access and analysis of Climate Models Data via different programmatic and interactive systems.</p> <p>Climate4Impact is a VA service managed and operated by KNMI as part of the ENES RIs and IRISCC initiatives. It offers interactive virtual access to global ESGF CMIP5/6 data and includes a personal workspace for data analysis  <a href="https://www.climate4impact.eu/c4i-frontend/">https://www.climate4impact.eu/c4i-frontend/</a>.</p> <p>The personal workspace consists of a VRE developed with the SWIRRL Technology  <a href="https://gitlab.com/KNMI-OSS/swirrl/swirrl-api">https://gitlab.com/KNMI-OSS/swirrl/swirrl-api</a></p> <p>C4I enables users to navigate the portal using either a Guest account or a Registered User account. The type of services accessible varies based on these profiles, as detailed on the portal's home page.</p>	<p>Service has an AAI. It's in the plan to federate the AAI across all the ESGF data, metadata and services. However, IS-ENES focuses on services at European level, thereby we are keen in considering possibilities offered by IRISCC (e.g. EGI Check-in), as long as these are interoperable with global standards and come with a sustainability plan. This is in alignment with the current organisation hosting the AAI server (CEDA – <a href="https://www.ceda.ac.uk/">https://www.ceda.ac.uk/</a>). C4I implements SSO via this AAI server.</p>
ECA&D – KNMI (installation)	<p>ECA&amp;D – European Climate Assessment &amp; Dataset, <a href="https://www.ecad.eu">https://www.ecad.eu</a></p> <p>ECA&amp;D provides daily data for in-situ meteorological stations across Europe sourced from the National Meteorological Services and other data holding entities. Based on these data, pan-European derived data products are provided.</p>	<p>The service does not currently have an AAI.</p>
EIRENE – UU (installation)	<p><u>No answer to the survey.</u> Unknown</p>	

RI/Installation organization	Description	AAI status
SeaDataNet (RI – CDI)	SeaDataNet with CDI Data Discovery & Access Service ( <a href="https://cdi.seadatanet.org/search">https://cdi.seadatanet.org/search</a> ) for marine and ocean data sets	We use Marine-ID (see: <a href="https://www.marine-id.org">https://www.marine-id.org</a> ) which is not yet fully part of a federation and somewhat outdated in technology. We would like to upgrade this to a modern AAI service which could then be easily federated through EGI-Check-in.
SeaDataNet (RI – DIVAnd)	SeaDataNet - DIVAnd: spatial interpolation of in situ measurements using the Data-Interpolating Variational Analysis in n dimensions (DIVAnd) method.	This service does not have an AAI.
AnaEE (RI)	Services in experimental ecology anaee.eu	This service does not have an AAI.
eLTER (RI)	<p><u>No answer to the survey.</u></p> <p>Own research resulted in at least the following services accessible via eLTER-RI:</p> <ul style="list-style-type: none"> <li>• DEIMS-SDR (<a href="https://deims.org/">https://deims.org/</a>) (Dynamic Ecological Information Management System - Site and dataset registry) is an information management system powered by eLTER. It allows you to discover long-term ecosystem research sites around the globe, along with the data gathered at those sites and the people and networks associated with them</li> <li>• eLTER Spatial Data Processor (Cookie Cutter). Use this 'cookie cutting' tool to crop spatial data (e.g. modelled air quality data) or socio-economic</li> </ul>	<ul style="list-style-type: none"> <li>• DEIMS-SDR uses an AAI that allows for logging in with email/username.</li> <li>• for the Spatial Data Processor, you will need a DataLabs account.</li> <li>• EcoSense does not have an AAI.</li> <li>• DEIMS-enriched does not have an AAI.</li> </ul>

	<p>statistical data to the boundaries of a chosen eLTER Site or Platform.</p> <ul style="list-style-type: none"> <li>• EcoSense (<a href="https://ecosense.biosense.rs/#/home">https://ecosense.biosense.rs/#/home</a>). Visualise remote sensing data and time-series data with EcoSense, a tool developed by eLTER and eShape.</li> <li>• DEIMS-enriched (<a href="https://elter-enrich.datalabs.ceh.ac.uk/">https://elter-enrich.datalabs.ceh.ac.uk/</a>). DEIMS-enriched extends your LTER Site and Platform search capabilities by enabling you to combine existing DEIMS site metadata with your own data.</li> </ul>	
EMBRC (RI)	EMBRC – services for marine biology and ecology	This service has an AAI that allows for logging in with ORCID, sodanet, LS login. Uses aria ( <a href="https://aria.structuralbiology.eu/">https://aria.structuralbiology.eu/</a> ), see this <a href="#">example</a> .
OPTED (RI)	Data on political and/or public discourses around different climate risks/hazards in relation to geographical locations.	This service does not have an AAI. They are looking into offering AAI through the federation in an update next year.
GESIS (RI)	Finding and accessing data from more than 6500 national and international studies	Service has an AAI, the login-solution is hosted by ourselves and operated independently. It is implemented based on Keycloak ( <a href="https://www.keycloak.org">https://www.keycloak.org</a> ).

RI/Installation organization	Description	AAI status
ECMWF (RI)	<p><u>No answer to the survey.</u></p> <p>Own research concluded that an ECMWF account enables you to:</p> <ul style="list-style-type: none"> <li>• access open data more quickly</li> <li>• register for events</li> <li>• enrol on online courses</li> <li>• access training resources</li> <li>• create and track service requests</li> </ul> <p>And in order to check if you are eligible for more features you can read about <a href="#">access to forecast data</a> and <a href="#">access to our computing facilities</a>.</p>	ECMWF uses an <b>AAI</b> that allows you to login with your email or password.

Individual answers per RI and digital service are included in Annex 1.

## 3.3 Preliminary conclusions

For 14 out of 20 installations and RIs we received an answer to the survey, despite the summer holiday period. However, a number of answers are not sufficient to make conclusions about the fact whether their AAI service is already part of the EGI Check-in federated AAI service or otherwise fit for connecting to EGI Check-in. This will require further refinement. Finally, there are also a number of RI services that do not use an AAI service for giving access. These will require no further action, as everyone will be able to easily access these services and no further access harmonization is required. Preliminary conclusions of AAI landscape analysis of IRISCC RIs listed in Table 4.

**Table 4. Summary of survey answers**

RI/Installation organisation	Conclusion
IAGOS – CNRS (installation)	Uses a solution that is fit to be connected through EGI Check-in. Steps are still required for integration.
IAGOS – KIT (installation)	Does currently not use an AAI, no further action required.

RI/Installation organisation	Conclusion
ACTRIS – NILU (installation)	Does currently not use an AAI, no further action required.
ACTRIS – CNR (installation)	The EARLINET component uses an AAI that is not fit for connecting its AAI service to EGI Check-in.
ACTRIS – CNRS (installation)	The GRES data centre catalogue uses an AAI that is fit to be connected through EGI Check-in. Steps are still required for integration.
ACTRIS – FMI (installation)	Both installations currently do not use an AAI, no further action required.
ICOS – ULUND (installation)	The ICOS Carbon portal requires a cookbook for connecting its AAI service to EGI Check-in but looks fit to be connected through EGI Check-in.
IS-ENES – DKRZ (installation – data access service)	Working on an integration with the EGI Check-in AAI.
IS-ENES – DKRZ (installation – web processing service)	Requires cookbook for connecting its AAI service to EGI Check-in, but is already experimenting with a connection to Keycloak. Rely on the AAI solution that is provided by the Virtual Research Environment (VRE).
IS-ENES – KNMI (installation)	Requires cookbook for connecting its AAI service to EGI Check-in.
ECA&D – KNMI (installation)	Does currently not use an AAI, no further action required.
EIRENE – UU (installation)	Unknown (no answer to the survey)
SeaDataNet (RI – CDI)	Will implement a solution that is fit to be connected through EGI Check-in.
SeaDataNet (RI – DIVAnd)	Does currently not use an AAI, no further action required.

<b>RI/Installation organisation</b>	<b>Conclusion</b>
AnaEE (RI)	Does currently not use an AAI, no further action required.
eLTER (RI)	Two separate AAI services require a cookbook for connecting their AAI services to EGI Check-in.
EMBRC (RI)	Uses the AAI service called aria, which is an IdP of EGI Check-in.
OPTED (RI)	Does currently not use an AAI. Wants to include AAI next year, requiring a cookbook for connecting its AAI service to EGI Check-in.
GESIS (RI)	Uses a solution that is fit to be connected through EGI Check-in.
ECMWF (RI)	Requires cookbook for connecting its AAI service to EGI Check-in.



# 4. Integration with EGI

## Check-in

Depending on concrete requirements, there are three options for a community when considering to integrate with EGI-Check-in.

### 4.1 Integration options

#### 4.1.1 EGI Check-in as community AAI

A community can use Check-in to manage its users and enable multiple federated authentication sources using different technologies.

##### How to set-up an AAI from scratch

- **Authentication:** EGI Check-in accepts federated identity credentials to enable users to re-use institutional log-ins
  - IdP/SP proxy to aggregate authentication information from multiple sources, including eduGAIN IdPs, social media credentials, and ad-hoc configured IdPs upon request
- **Authorization:** EGI Check-in manages group membership information according to services
  - Built-in group management tools to create and manage a Virtual Organisation (VO) and subgroups, add and remove users, and manage user consent and the VO acceptable usage policy

##### Improves existing AAI tools

- A community that already operates a group management tool does not need to change any of their workflows to be interoperable with EGI Check-in. EGI Check-in can play different roles based on the requirements of the community:
  - Use it as an identity provider proxy to enable federated access to the community group management tool
  - Integrate it with the group management tool of the community to implement community-based authorization in the EGI services

## 4.1.2 EGI Check-in as an AAI proxy for services or resource providers

Service or resource provider can connect their services or resources to EGI Check-in to enable Single Sign-On (SSO) through eduGAIN, social and custom identity providers. In this case, EGI Check-in acts as an identity provider proxy. Service providers can configure it as a normal SAML or OpenID Connect identity provider and let EGI Check-in handle external identity providers. EGI Check-in will provide all the required authentication and authorization information to service providers in a single assertion.

The advantage for service providers include:

- Users can use their existing accounts from the eduGAIN identity provider interederation, social media, and ORCID;
- Community services can become available to new identity providers added to Check-in;
- Users can link different accounts and access community services with a single user identifier.

## 4.1.3 EGI Check-in as a bridge to EGI services and resources

In this case, a community operating its own AAI connected to EGI Check-in as an Identity Provider Proxy can allow its users to access EGI services and resources.

# 4.2 Deployment types

When a community wants to use EGI Check-in as a full community AAI solution, there are two options for deploying the service:

- 1) **Shared Instance.** A catch-all Check-in instance is deployed on the EGI resource. This production service is used by EGI users to access EGI services and resources.
- 2) **Dedicated Instance.** This is to deploy an EGI Check-in instance on community resources.

# 4.3 Integration steps

In general, integration of EGI Check-in needs a combination of the following steps:

- **Set up a community VO<sup>4</sup>** -- EGI team will set up a new VO for a new community and configure it with Check-in.

- **Integration with IdPs<sup>5</sup>** -- Community organisations need to connect their IdPs with Check-in to allow their users to access any community services or EGI services that have enabled Check-in as an authentication provider.
- **Integration with SPs<sup>6</sup>** -- Community services need to connect to Check-in IdP as SP. Both SAML and OpenID Connect protocols are supported by Check-in.
- **Group management and user enrollment<sup>7</sup>** -- A community administrator needs to decide community group structure and user enrolment workflow, and organize the membership information using Check-in.

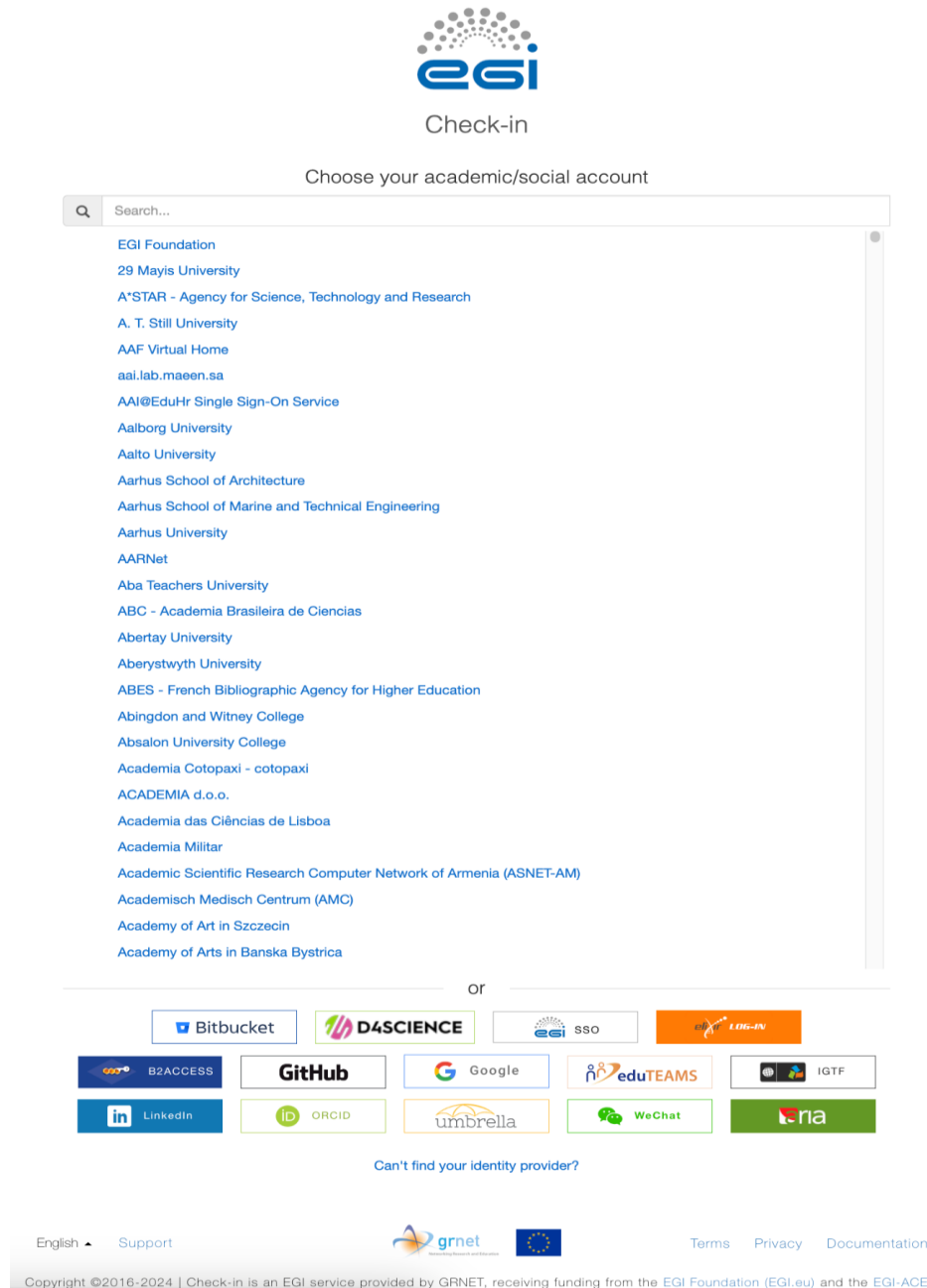
## 4.4 Authentication and Authorization with EGI Check-in

In a simple scenario, EGI-Check-in can be provided, for example, as a logIn button on the community service webpage. Showing in Figure 2. users can browse through the list of Identity Providers to find their Home Organisations (Note that the names are localised based on the selected language). Users can also select one of the social media/other external IdPs at the bottom. A pop-up window will allow users to input their organizational credentials (i.e., their university user account) -- in this way, no new account needs to be created to access the service.

EGI Check-in will contact the IdP of the user' home organisation to approve the user and grant access to the service.

## 4.5 Using Keycloak as AAI service

In case a RI is operating an AAI service which is not fit for connecting to EGI Check-in, then there is a good solution available by installing and configuring an instance of Keycloak. It provides open-source identity and access management. It can add authentication to applications and secure services with minimum effort. Keycloak provides user federation, strong authentication, user management, fine-grained authorization, and more. And it is fit for connecting to EGI Check-in. More information about Keycloak can be found at its website<sup>8</sup>.



The screenshot displays the EGI Check-in user login interface. At the top center is the EGI logo, consisting of a semi-circle of dots above the lowercase letters 'egi'. Below the logo is the text 'Check-in' and the instruction 'Choose your academic/social account'. A search bar with a magnifying glass icon and the placeholder text 'Search...' is positioned above a scrollable list of institutions. The list includes: EGI Foundation, 29 Mayıs University, A\*STAR - Agency for Science, Technology and Research, A. T. Still University, AAF Virtual Home, aai.lab.maaen.sa, AAI@EduHr Single Sign-On Service, Aalborg University, Aalto University, Aarhus School of Architecture, Aarhus School of Marine and Technical Engineering, Aarhus University, AARNet, Aba Teachers University, ABC - Academia Brasileira de Ciencias, Abertay University, Aberystwyth University, ABES - French Bibliographic Agency for Higher Education, Abingdon and Witney College, Absalon University College, Academia Cotopaxi - cotopaxi, ACADEMIA d.o.o., Academia das Ciências de Lisboa, Academia Militar, Academic Scientific Research Computer Network of Armenia (ASNET-AM), Academisch Medisch Centrum (AMC), Academy of Art in Szczecin, and Academy of Arts in Banska Bystrica. Below the list, the word 'or' is centered. A grid of identity provider logos follows, including Bitbucket, D4SCIENCE, EGI SSO, EGI-ACE, B2ACCESS, GitHub, Google, eduTEAMS, IGTF, LinkedIn, ORCID, umbrella, WeChat, and ria. A link 'Can't find your identity provider?' is located below the grid. At the bottom, there is a footer with 'English' and 'Support' on the left, the GRNET logo and the European Union flag in the center, and 'Terms', 'Privacy', and 'Documentation' on the right. A copyright notice at the very bottom reads: 'Copyright ©2016-2024 | Check-in is an EGI service provided by GRNET, receiving funding from the EGI Foundation (EGI.eu) and the EGI-ACE'.

Figure 2: EGI Check-in user Login interface

## 5. Conclusions

This Deliverable D6.1 gives an overview of the AAI systems in place for **digital** services as provided by the RIs in the IRISCC landscape. It includes an analysis if these AAI systems are already connected to a federated AAI service or are already fit to be connected. The target is that all digital services with AAI in IRISCC become federated through EGI Check-in, which serves as federated AAI service for EOSC.

For the second group, a cookbook is provided on how to connect their AAI service to EGI Check-in. There are also AAI systems in use which are not yet fit for such a federation. Therefore, the cookbook includes recommendations to set-up and deploy a new local AAI service, using KeyCloak, that then will be fit for EGI Check-in federation.

Table 5 gives the preliminary results of the landscape analysis and indicates which RI digital services are already OK, and which might have to undertake action. The analysis and drafting of the Deliverable D6.1 have been undertaken by IRISCC partners MARIS and EGI, supported by managers of RIs, completing the Task 6.1 AAI survey. While the review of D6.1 has been performed by IRISCC partners FZ and EGI.

Table 5. EGI Check-in fitness for federation and actions	
Fitness for federation with EGI Check-in	Installations, RIs
Not fit yet for federation, i.e. requiring substantial effort for integration.	<ul style="list-style-type: none"> <li>● ACTRIS-CNR               <ul style="list-style-type: none"> <li>○ EARLINET AAI seem to use a home-made AAI service</li> </ul> </li> <li>● IS-ENES-DKRZ (Web Processing Service (WPS))               <ul style="list-style-type: none"> <li>○ WPS services rely on the AAI solutions provided by the VREs in which they are integrated</li> </ul> </li> <li>● eLTER               <ul style="list-style-type: none"> <li>○ DEIMS-SDR seem to use a home-made AAI service</li> <li>○ Spatial Data Processor requires a DataLabs account</li> </ul> </li> <li>● OPTED               <ul style="list-style-type: none"> <li>○ No AAI currently, but looking into offering AAI through federation</li> </ul> </li> <li>● ECMWF               <ul style="list-style-type: none"> <li>○ ECM WF RI seem to use a home-made AAI service</li> </ul> </li> </ul>

<p>Fit for federation but still requiring steps to be undertaken, i.e. uses Keycloak, registered as Service Provider of eduGAIN.</p>	<ul style="list-style-type: none"> <li>● IAGOS-CNRS           <ul style="list-style-type: none"> <li>○ AAI is registered as a Service Provider of eduGAIN</li> </ul> </li> <li>● ACTRIS-CNRS           <ul style="list-style-type: none"> <li>○ AAI is registered as a Service Provider of eduGAIN</li> </ul> </li> <li>● ICOS-ULUND           <ul style="list-style-type: none"> <li>○ For the ICOS Carbon portal, Authentication options include eduGAIN and ORCID</li> </ul> </li> <li>● IS-ENES-KNMI           <ul style="list-style-type: none"> <li>○ Service uses an AAI hosted by CEDA</li> </ul> </li> <li>● SeaDataNet-CDI           <ul style="list-style-type: none"> <li>○ Service will incorporate Keycloak</li> </ul> </li> <li>● EMBRC           <ul style="list-style-type: none"> <li>○ Service uses aria, which is an IdP of EGI Check-in</li> </ul> </li> <li>● GESIS           <ul style="list-style-type: none"> <li>○ Service has an AAI that is based on Keycloak</li> </ul> </li> </ul>
<p>Already part of EGI-Check in or already in progress of becoming part.</p>	<ul style="list-style-type: none"> <li>● IS-ENES-DKRZ (DAS)           <ul style="list-style-type: none"> <li>○ Service is working on an integration with EGI-Check in</li> </ul> </li> </ul>
<p>No AAI, no further steps needed.</p>	<ul style="list-style-type: none"> <li>● IAGOS-KIT</li> <li>● ACTRIS-NILU</li> <li>● ACTRIS-FMI</li> <li>● ECA&amp;D-KNMI</li> <li>● SeaDataNet-DIVAnd</li> <li>● AnaEE</li> <li>● eLTER           <ul style="list-style-type: none"> <li>○ EcoSense does not have an AAI</li> <li>○ DEIMS-enriched does not have an AAI</li> </ul> </li> </ul>
<p>Unknown status.</p>	<ul style="list-style-type: none"> <li>● EIRENE-UU</li> </ul>

A follow-up will be given by MARIS and EGI by organising an online workshop where the findings per service will be presented and discussed for finalising conclusions on the current situation and required actions. The workshop will also provide information and guidance on how to connect local AAI services to EGI Check-in. This way, the workshop will lead to a refinement of actions and will pave the way towards SSO for all RI services.

The resulting actions should then be performed by the RI service operators, supported by MARIS and EGI, aiming for delivery before M11 (end of February 2025), and whereby the action results will be reported in Deliverable D6.5 - Report on accessibility of IRISCC services through EOSC federated AAI - planned for M12 (end of March 2025).

# 6. References

Reference	
No	Description/Link
1	EGI Check-in <a href="https://www.egi.eu/service/Check-in/">https://www.egi.eu/service/Check-in/</a> (visited 23.8.2024)
2	eduGAIN: <a href="https://edugain.org/">https://edugain.org/</a> (visited 23.8.2024)
3	EGI Check-in Federation Registry documentation: <a href="https://docs.egi.eu/providers/Check-in/sp/#service-provider-integration-workflow">https://docs.egi.eu/providers/Check-in/sp/#service-provider-integration-workflow</a>
4	<b>A request should be sent to EGI: <a href="https://www.egi.eu/contact-us/">https://www.egi.eu/contact-us/</a></b>
5	Guide for Check-in integration with Identity Providers is at: <a href="https://docs.egi.eu/providers/Check-in/idp/">https://docs.egi.eu/providers/Check-in/idp/</a>
6	Guide for Check-in integration with Service Providers is at: <a href="https://docs.egi.eu/providers/Check-in/sp/">https://docs.egi.eu/providers/Check-in/sp/</a>
7	Guide for group management with Check-in is at: <a href="https://docs.egi.eu/users/aa/Check-in/">https://docs.egi.eu/users/aa/Check-in/</a>
8	<a href="https://www.keycloak.org/">https://www.keycloak.org/</a>

# Annex 1 – Survey results

CNRS – IAGOS	
Questions	Answers
<b>What kind of service does your RI or installation offer (name + description)?</b>	<p>Name: Climatologies and anomalies of selected ECVs in the troposphere by IAGOS-DC-CNRS.</p> <p>Description: This service will provide diagnostics and statistics for a better understanding of the long time series, offering the possibility of the creation of a “tailored data set for ESM evaluation/improvement”.</p> <p>This service is currently under development and will be ready for the first release. A very similar service can be found here: <a href="https://services.iagos-data.fr/atmo-access/footprint">https://services.iagos-data.fr/atmo-access/footprint</a></p> <p>We are using an AAI provided by AERIS (French Data and Services cluster for Atmosphere) based on keycloak. A migration is planned in the next months: same solution (keycloak) but reorganization.</p>
<b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b>	VA
<b>Does your service have its own AAI?</b>	Yes
<b>Is the AAI already part of a federation and/or are there plans to federate it in the future?</b>	The AAI is registered as a Service Provider of eduGAIN.
<b>What authentication options are available within the AAI?</b>	Institutional accounts (eduGAIN), ORCID



<b>Which attributes are required by the AAI to identify the user?</b>	Name (First / Last name), Email
<b>How does the AAI handle authorisation?</b>	Based on the user's membership in group(s)
<b>What authentication &amp; authorisation protocols does the AAI currently support?</b>	OpenID Connect/OAuth 2.0
<b>Does the AAI implement the AARC Blueprint Architecture?</b>	Considering implementing the AARC BPA. (This reflects an interest in potentially using the AARC BPA)
<b>Is there a GDPR Data Controller designated for the AAI?</b>	Yes
<b>Has the AAI designated a security contact to handle security incidents?</b>	Yes: securite@aeris-data.fr
<b>Does the AAI adhere to SIRTFI or other recognised security frameworks?</b>	Yes

KIT – IAGOS	
Questions	Answers
<b>What kind of service does your RI or installation offer (name + description)?</b>	<p>Name: Climatologies and anomalies of selected VOCs in the troposphere by IAGOS-DC-KIT.</p> <p>Description: This service will provide a time series of organic compounds and auxiliary species (such as O<sub>3</sub>, CO and NO<sub>y</sub>) in the troposphere and lowermost stratosphere tagged with the impact of biomass burning / fires.</p> <p>This service is under development and will be provided for the first release.</p> <p>We (in IAGOS-CARIBIC) don't have a data provision chain comparable with the typical much bigger RIs in the environmental domain.</p> <p>Up to now we provide our data via two channels:</p> <ol style="list-style-type: none"> <li>1. A subset is offered via the IAGOS DC in Toulouse, as described in the table below by Damien</li> <li>2. The full dataset is accessible via Zenodo and a local THREDDS server</li> </ol>
<b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b>	VA
<b>Does your service have its own AAI?</b>	Currently we don't have our own AAI. We are currently waiting on the answer by our computing centre, whether it could be implemented with moderate efforts.

<b>NILU – ACTRIS</b>	
<b>Questions</b>	<b>Answers</b>
<b>What kind of service does your RI or installation offer (name + description)?</b>	Data access
<b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b>	Regular Access
<b>Does your service have its own AAI?</b>	No

<b>FMI – ACTRIS</b>	
<b>Questions</b>	<b>Answers</b>
<b>What kind of service does your RI or installation offer (name + description)?</b>	Palla-Sodankylä: TNA access & Pallastunturi-Sodankylä VA access
<b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b>	Palla-Sodankylä: TNA access & Pallastunturi-Sodankylä VA access
<b>Does your service have its own AAI?</b>	No for both

**ICOS – ULUND (Remark: the answers are taken over from a recent survey for the ENVRI-Hub NEXT project )**

Questions	Answers
<b>What kind of service does your RI or installation offer (name + description)?</b>	
<b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b>	
<b>Does your service have its own AAI?</b>	Yes, needed for authorisation of uploads and other admin tasks. Registration of users to add extra functionality and store acceptance of data licence.
<b>Is the AAI already part of a federation and/or are there plans to federate it in the future?</b>	
<b>What authentication options are available within the AAI?</b>	Institutional accounts (eduGAIN), ORCID, social media, local login using email/password
<b>Which attributes are required by the AAI to identify the user?</b>	Email
<b>How does the AAI handle authorisation?</b>	[Based on user capabilities defining specific resources a user is allowed to access or perform certain actions], [Based on identity assurance (e.g. level of identity proofing, freshness of affiliation information)], [Based on the authentication method (e.g. Multi-Factor Authentication - MFA)]

<b>What authentication &amp; authorisation protocols does the AAI currently support?</b>	OpenID Connect/OAuth 2.0, SAML2
<b>Does the AAI implement the AARC Blueprint Architecture?</b>	Considering implementing the AARC BPA. (This reflects an interest in potentially using the AARC BPA)
<b>Is there a GDPR Data Controller designated for the AAI?</b>	No
<b>Has the AAI designated a security contact to handle security incidents?</b>	No
<b>Does the AAI adhere to SIRTFI or other recognised security frameworks?</b>	I don't know / I need more reflection on this

### DKRZ – IS-ENES (data access service)

Questions	Answers
<b>What kind of service does your RI or installation offer (name + description)?</b>	<p>IS-ENES data access service <a href="https://esgf-metagrid.cloud.dkrz.de/search">https://esgf-metagrid.cloud.dkrz.de/search</a></p> <p>We are currently in a transition phase to a new federation AAI solution which is based on globus AAI integration in the US (see <a href="https://aims2.llnl.gov/search">https://aims2.llnl.gov/search</a> --&gt; login)</p> <p>In Europe we are currently working on an integration with the EGI checkin AAI and are currently experimenting with a keycloak based test service at URKRI / CEDA, which will later be replaced by the European proxy solution. So the plan is do move completely to</p>

	<p>OpenID connect and OAuth2 in Europe. this is work in progress and the people at UKRI are in contact with the EGI / EOSC people on this.</p> <p>all data is now changed to open access - so the AAI solution is not used for data access grant decisions (as in the old ENES solution based on OpenID 2.0 an a proprietary group membership based data access solution)</p>
<b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b>	Regular access
<b>Does your service have its own AAI?</b>	Yes
<b>Is the AAI already part of a federation and/or are there plans to federate it in the future?</b>	yes, global ESGF / ENES RI AAI
<b>What authentication options are available within the AAI?</b>	OpenID
<b>Which attributes are required by the AAI to identify the user?</b>	Name (First / Last name), Email, Affiliation with the home institute, users are not forced to provide information, core data collections are open for download without registration
<b>How does the AAI handle authorisation?</b>	Based on the user's membership in group(s)
<b>What authentication &amp; authorisation protocols does the AAI currently support?</b>	OpenID Connect/OAuth 2.0
<b>Does the AAI implement the AARC</b>	In the process of implementing the AARC BPA. (This shows an ongoing effort to adopt the AARC BPA)

<b>Blueprint Architecture?</b>	
<b>Is there a GDPR Data Controller designated for the AAI?</b>	No
<b>Has the AAI designated a security contact to handle security incidents?</b>	No
<b>Does the AAI adhere to SIRTFI or other recognised security frameworks?</b>	Partially

### DKRZ – IS-ENES (web processing service)

Questions	Answers
<b>What kind of service does your RI or installation offer (name + description)?</b>	<p>ENES RI Web processing service.</p> <p>Also for the WPS we are experimenting with different AAI solutions also in connection to keycloak, yet the WPS services currently in production do not rely on an own AAI integration but rely on the AAI solution which is provided by the virtual research environments they are integrated in. E.g. the (load balanced) WPS service which is provided for COPERNICUS, relies on the AAI solution of Copernicus and the WPS integration is based on firewall configuration to allow only requests coming from copernicus processing nodes. (Similarly the integration of WPS services into the KNMI Climate4Impact portal/VRE is done) This is probably also the initial approach we will follow in IRISCC for the D4Science integration.</p> <p>essentially we would need full support for access rights delegation to integrate WPS services into VREs .. we currently do not have this ..</p>

	<p>example links:</p> <ul style="list-style-type: none"> <li>- GUI access</li> </ul> <p><a href="https://clint.dkrz.de/processes/execute?wps=a588f4a229ae479fbcfb3bb12cde4235&amp;process=hello">https://clint.dkrz.de/processes/execute?wps=a588f4a229ae479fbcfb3bb12cde4235&amp;process=hello</a></p> <ul style="list-style-type: none"> <li>- access via client in jupyter notebook</li> </ul> <p><a href="https://nbviewer.org/github/roocs/rooki/blob/master/notebooks/demo/demo-rooki-subset-by-point.ipynb">https://nbviewer.org/github/roocs/rooki/blob/master/notebooks/demo/demo-rooki-subset-by-point.ipynb</a></p>
<p><b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b></p>	<p>VA</p>
<p><b>Does your service have its own AAI?</b></p>	<p>Yes</p>
<p><b>Is the AAI already part of a federation and/or are there plans to federate it in the future?</b></p>	<p>there are plans to federate, there is a federated operational European installation to support Copernicus, yet based on a low-level AAI solution (firewall config etc.)</p>
<p><b>What authentication options are available within the AAI?</b></p>	<p>GitHub</p>
<p><b>Which attributes are required by the AAI to identify the user?</b></p>	<p>depends on use case, generally globally unique identifier</p>
<p><b>How does the AAI handle authorisation?</b></p>	<p>Based on the user's membership in group(s)</p>



<b>What authentication &amp; authorisation protocols does the AAI currently support?</b>	some protocols were tested, no fully operational solution by now
<b>Does the AAI implement the AARC Blueprint Architecture?</b>	Considering implementing the AARC BPA. (This reflects an interest in potentially using the AARC BPA)
<b>Is there a GDPR Data Controller designated for the AAI?</b>	No
<b>Has the AAI designated a security contact to handle security incidents?</b>	Yes
<b>Does the AAI adhere to SIRTFI or other recognised security frameworks?</b>	Partially

<b>KNMI – IS-ENES</b>	
<b>Questions</b>	<b>Answers</b>
<b>What kind of service does your RI or installation offer (name + description)?</b>	<p>IS-ENES offers Data discovery, access and analysis of Climate Models Data via different programmatic and interactive systems.</p> <p>Climate4Impact is a VA service managed and operated by KNMI as part of the ENES RIs and IRISCC initiatives. It offers interactive virtual access to global ESGF CMIP5/6 data and includes a personal workspace for data analysis</p> <p><a href="https://www.climate4impact.eu/c4i-frontend/">https://www.climate4impact.eu/c4i-frontend/</a>.</p> <p>The personal workspace consists of a VRE developed with the SWIRRL Technology  <a href="https://gitlab.com/KNMI-OSS/swirrl/swirrl-api">https://gitlab.com/KNMI-OSS/swirrl/swirrl-api</a></p>

	C4I enables users to navigate the portal using either a Guest account or a Registered User account. The type of services accessible varies based on these profiles, as detailed on the portal's home page.
<b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b>	Regular access
<b>Does your service have its own AAI?</b>	Yes
<b>Is the AAI already part of a federation and/or are there plans to federate it in the future?</b>	TBD. It's in the plan to federate the AAI across all the ESGF data, metadata and services. However IS-ENES focuses on services at European level, thereby we are keen in considering possibilities offered by IRISCC (eg. EGI Check-in), as long as these are interoperable with global standards and come with a sustainability plan. This in alignment with the current organisation hosting the AAI server (CEDA - <a href="https://www.ceda.ac.uk/">https://www.ceda.ac.uk/</a> ). C4I implements SSO via this AAI server.
<b>What authentication options are available within the AAI?</b>	ORCID, GitHub, Google
<b>Which attributes are required by the AAI to identify the user?</b>	Email
<b>How does the AAI handle authorisation?</b>	Based on the user's membership in group(s)?, Before granting access to analysis resources, users submit a motivation request, which is then validated from the administrators of the Climate4Impact service at KNMI. IS-ENES is keen in considering the possibilities offered by IRISCC. The current system could be aligned with solutions proposed by the project (EGI/EOSC), as long as it is interoperable with global standards and come with a sustainability plan.
<b>What authentication &amp; authorisation protocols does the AAI currently support?</b>	OpenID
<b>Does the AAI implement the AARC</b>	Yes, partially compliant. (This signifies some implementation of the AARC BPA principles, but with deviations)

<b>Blueprint Architecture?</b>	
<b>Is there a GDPR Data Controller designated for the AAI?</b>	TBD. Currently there is no official IS-ENES contact. However, internally to KNMI there is a designated data controller for GDPR issues related to those services hosted locally.
<b>Has the AAI designated a security contact to handle security incidents?</b>	TBD. Currently there is no official IS-ENES contact. KNMI falls-back on our internal security contact to perform security audits and address issues that exclusively related to the access of the C4I services within the KNMI Cloud Infrastructure (AWS).
<b>Does the AAI adhere to SIRTFI or other recognised security frameworks?</b>	TBD. IS-ENES is interested in aligning on this with the possibilities offered by IRISCC (eg. EGI Check-in), as long as it is interoperable with global standards and come with a sustainability plan.

<b>KNMI – ECA&amp;D</b>	
<b>Questions</b>	<b>Answers</b>
<b>What kind of service does your RI or installation offer (name + description)?</b>	ECA&D - European Climate Assessment & Dataset, <a href="https://www.ecad.eu">https://www.ecad.eu</a> ECA&D provides daily data for in-situ meteorological stations across Europe sourced from the National Meteorological Services and other data holding entities. Based on these data, pan-European derived data products are provided.
<b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b>	Regular Access
<b>Does your service have its own AAI?</b>	No

SeaDataNet CDI	
Questions	Answers
<b>What kind of service does your RI or installation offer (name + description)?</b>	SeaDataNet with CDI Data Discovery & Access Service ( <a href="https://cdi.seadatanet.org/search">https://cdi.seadatanet.org/search</a> ) for marine and ocean data sets
<b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b>	Regular access
<b>Does your service have its own AAI?</b>	Yes
<b>Is the AAI already part of a federation and/or are there plans to federate it in the future?</b>	We use Marine-ID (see: <a href="https://www.marine-id.org">https://www.marine-id.org</a> ) which is not yet fully part of a federation and somewhat outdated in technology. We would like to upgrade this to a modern AAI service which could then be easily federated through EGI-Check-in.
<b>What authentication options are available within the AAI?</b>	You can only register and get an MARINE-ID account. No exchanges with other systems.
<b>Which attributes are required by the AAI to identify the user?</b>	Name (First / Last name), Email, Affiliation with the home institute
<b>How does the AAI handle authorisation?</b>	Once registered, the MARINE-ID user needs to agree with the SeaDataNet access policy after which the MARINE-ID users become a SeaDataNet user
<b>What authentication &amp; authorisation protocols does the AAI currently support?</b>	PWM and LDAP for User self-registration ; CAS for Authentication and Single Sign On; SugarCRM for Accounting. Shibboleth is used as a middleware to connect EUDATs B2ACCESS and Marine-ID. It is an open-source implementation for identity management and

	federated identity-based authentication and authorisation. It is based on the Security Assertion Markup Language (SAML).
<b>Does the AAI implement the AARC Blueprint Architecture?</b>	No, using a different AAI architecture. Please briefly describe or provide links to the AAI architecture you are using below.
<b>Is there a GDPR Data Controller designated for the AAI?</b>	Officially not
<b>Has the AAI designated a security contact to handle security incidents?</b>	I do not know
<b>Does the AAI adhere to SIRTFI or other recognised security frameworks?</b>	No

**SeaDataNet – DIVAnd**

Questions	Answers
<b>What kind of service does your RI or installation offer (name + description)?</b>	SeaDataNet - DIVAnd: spatial interpolation of in situ measurements using the Data-Interpolating Variational Analysis in n dimensions (DIVAnd) method.
<b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b>	VA
<b>Does your service have its own AAI?</b>	No

<b>AnaEE</b>	
<b>Questions</b>	<b>Answers</b>
<b>What kind of service does your RI or installation offer (name + description)?</b>	Services in experimental ecology anaee.eu
<b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b>	Regular access
<b>Does your service have its own AAI?</b>	No

<b>EMBRC</b>	
<b>Questions</b>	<b>Answers</b>
<b>What kind of service does your RI or installation offer (name + description)?</b>	EMBRC - services for marine biology and ecology
<b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b>	Regular access
<b>Does your service have its own AAI?</b>	Yes
<b>Is the AAI already part of a federation and/or</b>	

<b>are there plans to federate it in the future?</b>	
<b>What authentication options are available within the AAI?</b>	ORCID, sodanet, LS login
<b>Which attributes are required by the AAI to identify the user?</b>	Name (First / Last name), Email
<b>How does the AAI handle authorisation?</b>	
<b>What authentication &amp; authorisation protocols does the AAI currently support?</b>	I am not sure which protocol ARIA uses
<b>Does the AAI implement the AARC Blueprint Architecture?</b>	I am not sure which architecture ARIA uses
<b>Is there a GDPR Data Controller designated for the AAI?</b>	Yes
<b>Has the AAI designated a security contact to handle security incidents?</b>	as far as I can see from the ARIA contract, only for bugs and issues. I am not sure if this is related to the AAI system or to the "access system" itself
<b>Does the AAI adhere to SIRTFI or other recognised security frameworks?</b>	I am not sure which framework ARIA uses

<b>OPTED</b>	
<b>Questions</b>	<b>Answers</b>
<b>What kind of service does your RI or installation offer (name + description)?</b>	Data on political and/or public discourses around different climate risks/hazards in relation to geographical locations.
<b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b>	Regular access
<b>Does your service have its own AAI?</b>	No
<b>Is the AAI already part of a federation and/or are there plans to federate it in the future?</b>	We are looking into offering AAI through federation in an update next year

<b>GESIS</b>	
<b>Questions</b>	<b>Answers</b>
<b>What kind of service does your RI or installation offer (name + description)?</b>	Finding and accessing data from more than 6500 national and international studies
<b>Is the service accessible via regular access (through RIs) or via VA as part of IRISCC VA Calls?</b>	Regular access



<b>Does your service have its own AAI?</b>	Yes
<b>Is the AAI already part of a federation and/or are there plans to federate it in the future?</b>	No. Our login-solution is hosted by ourselves and operated independently. It is implemented based on Keycloak ( <a href="https://www.keycloak.org">https://www.keycloak.org</a> ).
<b>What authentication options are available within the AAI?</b>	Setting up profile on GESIS website ( <a href="https://login.gesis.org/">https://login.gesis.org/</a> ); Depending on the level of access categories of the dataset, user is required to fill out a data usage agreement for off-site or on-site usage of data
<b>Which attributes are required by the AAI to identify the user?</b>	Name (First / Last name), Email, Affiliation with the home institute, Postal address
<b>How does the AAI handle authorisation?</b>	Based on the user's membership in group(s)?, Based on user capabilities defining specific resources a user is allowed to access or perform certain actions?, Based on affiliation of the user with their home institute?
<b>What authentication &amp; authorisation protocols does the AAI currently support?</b>	Keycloak generally supports these protocols but since our implementation is based on direct registration with us, it does not apply.
<b>Does the AAI implement the AARC Blueprint Architecture?</b>	We cross-checked this question with our IT department and they are not aware of it. So: No.
<b>Is there a GDPR Data Controller designated for the AAI?</b>	Yes
<b>Has the AAI designated a security contact to handle security incidents?</b>	Yes

<b>Does the AAI adhere to SIRTFI or other recognised security frameworks?</b>	No. Since we are not part of a federation, we are also not in a network which investigates security incidents in a federation.
---	--