OPERAS-P

Open Scholarly Communication in the European Research Area for SSH - Preparation

AAI Service Specifications

10.11.2020

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871069

OPERAS-P

OPEN SCHOLARLY COMMUNICATION IN THE EUROPEAN RESEARCH AREA FOR SSH - PREPARATION

Deliverable 4.2

AAI Service Specifications

Grant Agreement number	:	871069
Project acronym	:	OPERAS-P
Project title	:	Open Scholarly Communication in the European Research Area for SSH - Preparation
Funding Scheme	:	INFRADEV-02-2019-2020
Project's coordinator Organization	:	CNRS-OpenEdition
E-mail address	:	pierre.mounier@openedition.org
Website	:	www.operas-eu.org
WP and tasks contributing	:	WP4, T4.2
WP leader	:	CNRS
Dissemination level	:	Public
Due date	:	31 Oct 2020
Delivery date	:	10 Nov 2020
Authors	:	Yin Chen (EGI.eu) Yoann Moranville (DARIAH) Valeria Ardizzone (EGI.eu)

Contents

Executive summary

To support a transparent and seamlessly access to the OPERAS platforms and to external sources of data, including services, compute and storage, T4.2 aims to align and integrate the platforms with the EGI Check-In service (also called EGI AAI proxy) as Authentication and Authorisation Infrastructure (AAI) within the OPERAS Research Infrastructure (OPERAS RI).

Check-In provides an identity and access management solution that facilitates the access to services and resources using the federated authentication mechanisms. Through the EGI AAI proxy, users will be able to authenticate with the credentials provided by the Identity Providers (IdP) of their Home Organisation (e.g. via eduGAIN), as well as using social identity providers, or other selected external identity providers.

Check-In is adopted by many European Research Infrastructures, i.e. ELIXIR, EISCAT-3D, WeNMR. It is one of the EOSC AAI solutions. Integration with EGI Check-in keeps OPERAS well interoperable with EOSC AAI. The potential benefits are: being a OPERAS user, s/he can also access EOSC/EGI services. On the other hand, EOSC/EGI SSH researchers and other Science communities users by default become OPERAS users and are able to use the OPERAS platform -- this will enlarge OPERAS user base and make OPERAS more visible to European science communities.

The report provides technical details about Check-In and the integration options, that serves as a guideline for OPERAS service providers for integration work.

Although Check-In is powerful and flexible, there are specific requirements of OPERAS services. One of the contributions of this report is to develop an understanding of OPERAS' needs for AAI, capture various integration scenarios of SSH services, and identify the Check-In solutions. Technical details are discussed, e.g., protocols, standards, configurations, etc. These experiences from OPERAS are useful and can be shared with other SSH communities and beyond. On the other hand, it provides the EGI Check-In team a better understanding of different service scenarios from the SSH community.

We would like to share our experiences and promote these results to other SSH communities and EGI communities. For example, OPERAS is invited by the EGI conference 2020[1], to present the Check-In integration experiences in the AAI workshop. An abstract of TRIPLE integration with Check-In is also accepted by the conference that provides a good opportunity for making OPERAS/TRIPLE visible to the EGI user community.

[1] EGI conference 2020, 2-5 Nov: https://indico.egi.eu/event/5000/overview

I.Introduction

This deliverable reports tasks conducted in T4.2 - User Authentication Implementation (AAI service). The aim of the task is to support secure and seamless access to the OPERAS platforms and external resources (service, compute and storage).

The chosen technology is the EGI check-in service, an authentication/authorisation mechanism, providing identity and access management components that facilitate users to access the community services and resources. Through Check-in, users do not need to create new logIn names and passwords, but be able to use their Home Organisation credentials (e.g., eduGAIN accounts), as well as social media accounts (i.e., google, facebook, LinkedIn).

Check-in is adopted by many European Research Infrastructures, i.e. ELIXIR, EISCAT-3D, WeNMR. It is one of the EOSC AAI solutions. Integration with EGI Check-in keeps OPERAS well interoperable with EOSC AAI. The potential benefits are: being a OPERAS user, s/he can also access EOSC/EGI services. On the other hand, EOSC/EGI SSH researchers and other Science communities users by default become OPERAS users and are able to use the OPERAS platform -- this will enlarge OPERAS user-based and make OPERAS more visible to European science communities.

Different OPERAS services have different requirements for AAI. One of the contributions of this report is to develop an understanding of OPERAS' needs for AAI, capture the various integration scenarios with different SSH services, and identify the Check-In solutions. We also discussed the technical details for integrations, e.g., protocols, standards, configurations, etc. These experiences can be shared with other SSH communities and beyond.

The rest of the report is organized as follows: Section II gives an overview of the EGI Check-In service, describing the architecture and its service components; Section III discusses the AAI requirements of OPERAS community; Section IV describes the configuration setup for OPERAS Check-In, presents the initial integration results of Check-in with Pathfinder, a new service developed by T4.1. It also discusses the implementation status and issues with other OPERAS services; finally, we summarize the work in Section V.

II.EGI Check-In

A. A Service Solution for Federated Identity Management

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.

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. In the case of OPERAS-P, a project that develops services for OPERAS Research Infrastructure, there are 16 partner organisations coming from 11 countries: together they are developing services and platforms aimed to support SSH researchers and professionals (scholars, publishers, librarians and other professionals) across Europe and beyond. The need for managing user identity across borders between organisations, domain and services, leads to the creation of federated identity environments.

An Identity federation is a group of Identity and Service Providers that sign up to an agreed set of policies for exchanging information about users and resources to enable access to and use of the resources. Home organisations (e.g. a university, library, research institute, etc.), who operate an Identity Provider (IdP)[2], register users by assigning a digital identity -- in this way, they are able to authenticate their users and provide a limited set of attributes that characterise the user in a given context. Service Providers (SPs) delegate the authentication to IdP, in order to control access to the provided resources.

Check-in is a service solution for federated identity management, building on the existing eduGAIN[3] interfederation. By integrating with Check-In, OPERAS users do not need to create any additional user names/passwords and can easily get access to OPERAS services with their own institution accounts; users without institutional accounts can access through social media or other external accounts, including Google, Facebook, LinkedIn,

[2] By definition, an IdP is a system that creates, maintains, and manages identity information for principals (users, services, or systems) and provides principal authentication to other service providers (applications) within a federation or distributed network.

[3] eduGAIN: https://edugain.org/. It already comprises over 60 participant federations connecting more than 5,000 Identity and Service Providers.

Github, Bitbucket, WeChat or ORCID[4]. Check-in manages users and their respective roles and other authorisation-related information. The adoption of standards and open technologies, including SAML 2.0, OpenID Connect, OAuth 2.0 and X.509v3, facilitates interoperability and integration with the existing AAIs of other e-Infrastructures and SSH research communities.

B. Check-In Architecture

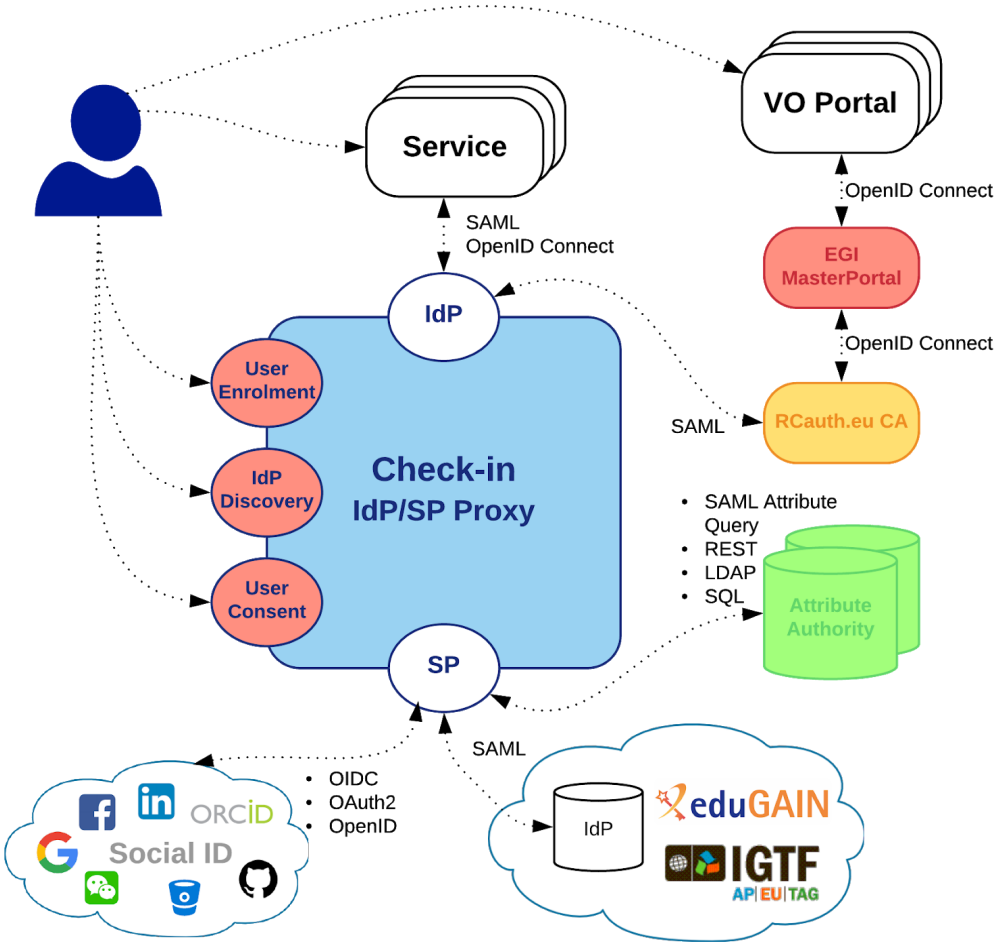

Fig 1. Architecture of EGI Check-in service

[4] Note, other social external accounts (Twitter, ResearchGate, Academia, etc…) are not implemented in Check-In, yet.

The architecture of Check-In service is shown in Fig 1. In a nutshell, Check-in is a proxy service that operates as a central hub to connect federated Identity Providers (IdPs) with Service Providers (SPs). 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.

The core of Check-in are two main components -- the IdP/SP Proxy, and the User Enrolment and Group Management.

- 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 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 authorized users and the configuration of custom enrolment flows for groups via an intuitive web interface.

C. Virtual Organisation

It is worth noting that Check-In group management is built on the structure of EGI Virtual Organisation (VO). A *Virtual Organisation*, by concept, is a set of cooperating independent organizations which to the outside world provide a set of services as if they were one organisation. 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 Virtual Organizations (VOs). Usually there is one-to-one mapping between research communities and Virtual Organizations. 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.

D. Integration with Check-In

1. Service Options

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

1) **Check-In as community AAI**. A community can use Check-In to manage its users and enable multiple federated authentication sources using different technologies. Check-In enables users to re-use their academic and social accounts for authentication. It can also manage community/group membership information to control access to services. Built-in group management tools are provided for creating and managing a Virtual Organisation (VO) and (sub)groups, adding and removing users, and managing user consent and the VO acceptable usage policy.
2) **Check-In as an AAI proxy for services or resource providers**. In this case, Check-In acts as an identity provider proxy. Service providers can configure it as a normal SAML or OpenID Connect identity provider and let Check-In handle external identity providers. 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 interfederation, social media, and ORCID; Community services can become available to new identity providers added to Check-In; Users can link different accounts and access the community services with a single user identifier.
3) **Check-In as a Bridge to EGI services and resources**. In this case, a community operating its own AAI connected to Check-In as an Identity Provider Proxy can allow its users to access EGI services and resources.

OPERAS requires a full community AAI solution, and the option 1) is the choice.

2. Deployment Types

When a community want to use 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 a Check-In instance on community resources.

In OPERAS, after comparing pros and cons, we decided to go for option 1). Comparing to option 2), it is much more easy to setup the service; OPERAS doesn't need to find additional resources, nor technical staffs for maintenance (i.e., service updates, resolving technical issues, etc.); the service is already in production level, and used by the EGI community (over 70,000 users). Many other communities (i.e., EISCAT-3D, WeNMR, EOSC portal, etc.) also choose for this setup, showing it is capable to support large-sale community users.

However, by choosing option 1), there is a concern that in future, if OPERAS wants to move out from the EGI Check-In integration, it needs a migration process to export the community information. It's unclear how much it would cost. On the other hand, it may not be a risk in the next couple of years -- OPERAS has signed a Memorandum of Understanding (MoU) with EGI in Jun 2020, and will receive technical support through the newly funded project, EGI-ACE (2021-2023). During the EGI-ACE project, OPERAS will continue to receive support (i.e., new integration requests, technical issues -- including migration requests, etc.) from the Check-In team for free.

3. Integration Steps

In general, integration of Check-In needs the following steps:

- **Set up a community VO**[5] -- EGI team will set up a new VO for a new community and configure it with Check-In. For OPERAS, the VO is created as vo.operas-eu.org.
- **Integration with IdPs**[6] -- 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**[7] -- Community services need to connect to Check-in IdP as Service Provider (SP). As mentioned above, both SAML and OpenID Connect protocols are supported by Check-In
- **Group management and user enrollment**[8] -- A community administrator needs to

[5] A request should be sent to EGI help desk: https://helpdesk.egi.eu/
[6] Guide for Check-In integration with Identity Providers is at: https://wiki.egi.eu/wiki/AAI_guide_for_IdPs
[7] Guide for Check-In integration with Service Providers is at: https://wiki.egi.eu/wiki/AAI_guide_for_SPs
[8] Guide for group management with Check-In is at: https://wiki.egi.eu/wiki/AAI_guide_for_VO_managers

decide community group structure and user enrolment workflow, and organize the membership information using Check-In.

E. Authentication and authorization with Check-In

In a simple scenario, Check-In can be provided, for example, as a logIn button on the community service webpage. Showing in Fig 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 organisational credential (i.e., their university user account) -- in this way, no new account needs to be created to access the service.

Check-In will contact the IdP of the user' Home Organisation to approve the user and grant access to the service.

Fig 2: Check-In user LogIn interface

III. OPERAS Community Requirements

Section II describes the generic Check-In integration scenarios. In the case of OPERAS, there are specific requirements from the SSH community. This session discusses the OPERAS's needs for Check-In.

Core services developed in OPERAS include Publication Service Portal (PSP), Metrics, DOAB, and Discovery Service. Different services have different integration requirements.

A. PSP

The OPERAS Publication Service Portal (PSP) also called Pathfinder, collects the publishing and scholarly communication services that OPERAS members offer and gives access to their description from a single access portal. The portal service is hosted by the University of Turin. The PSP composes two parts: a presentation of the services as a catalog, and a wizard that walks researchers through a series of questions towards the service offering that best fits their needs.

The requirement of PSP is simple -- it only needs Check-In to be served as the user log-in of the service website. In this case, PSP connects Check-in as a Service Provider using OpenID connect protocol, and the configuration is straightforward following the generic scenario described in the previous section.

B. Metrics

Metrics is a service that collects usage and impact metrics related to Open Access monographs from many different sources and allows for access, display and analysis from a single access point.

Different from other OPERAS services, Metrics is API-based. The main users of Metrics are publishers. At the moment, Metrics uses the Token-based authentication -- a `tokens_api`[9] is provided that issues JSON Web Tokens to the registered users/publishers, and the access to *Altmetrics API* will need to be validated with a JSON Web Token obtained from `tokens_api`. Metrics has its own database for user information, hirmeos/tokens_db, that keeps user registration information. Fig 3 depicts the interaction flow between a user application and Metrics API interfaces.

[9] Metrics `tokens_api`: https://metrics.operas-eu.org/docs/tokens-api

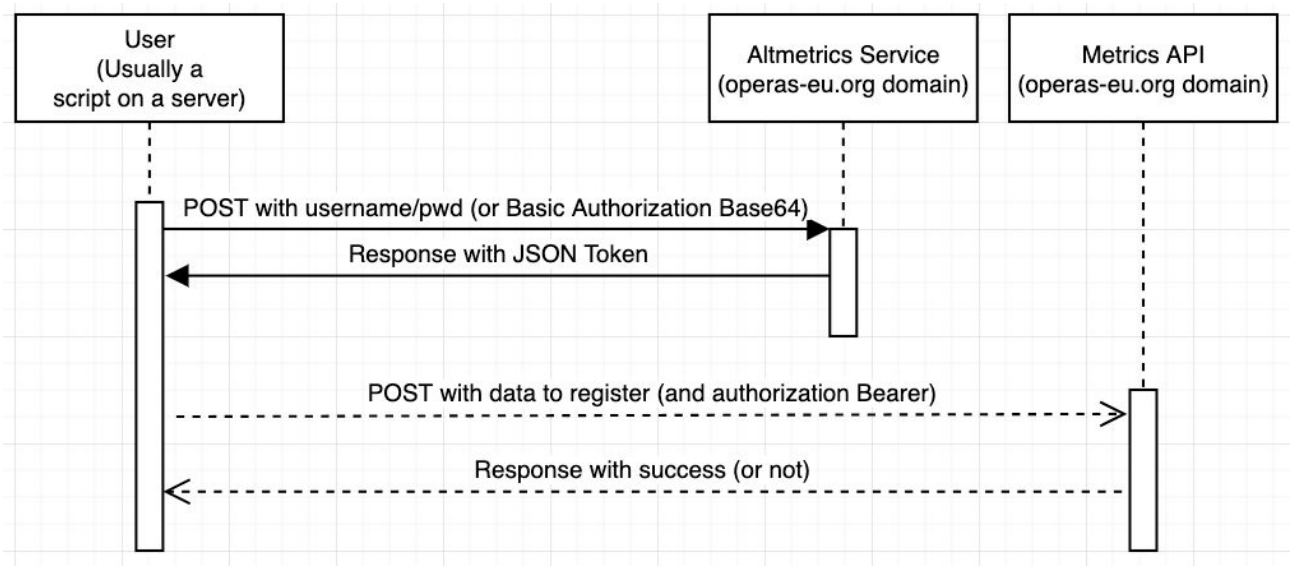

Fig 3: Authentication interactions flow of the Metrics Service

C. Certification Service (DOAB)

The Certification Service aims to certify Open Access (OA) book publishers, based on their publishing practices, in particular their peer review procedures and licensing policies. The goal is to support trust in OA book publishing, by improving transparency around quality assurance of OA book publishers and their publications. The service is intended to certify publishers at both the publisher level and the individual publication level.

Operated by the DOAB Foundation, the Certification Service serves as a quality insurance service for the benefit of readers and the service providers working with them, such as the libraries. With the efforts of Task 4.5, this service is already registered to the EOSC Marketplace[10] in early 2020.

The Certification Service uses DSpace[11] for building the open digital repository, and integrated with Shibboleth for identity management. Shibboleth itself is an open-source web single sign-on system with rich attribute-exchange based on open standards.

Since Shibboleth is one of the major SAML2.0 solutions that is naturally supported by Check-In, the integration should be straightforward. DSpace v6.x has an existing plugin to make use of Shibboleth and this will be used, and we will configure Shibboleth, SAML2.0 and EGI Check-in for this integration.

[10] The OPERAS Certification Service entry in EOSC Marketplace: https://marketplace.eosc-portal.eu/services/operas-certification-doab
[11] DSpace: https://duraspace.org/dspace/

D. Discovery Service

OPERAS discovery service is a platform providing European Researchers a single point to discover SSH open scholarly resources such as data, publications, and other researchers and projects. The Discovery Service is currently under development thanks to the Horizon 2020 TRIPLE project[12] and it is based on ISIDORE[13], which has been operated by Huma-Num since 2017. The new design and development in TRIPLE will make it much easier for scientists, citizens and business organisations to access scientific publications, data, data processing platforms and data processing services and therefore to benefit from Open Science. In the new TRIPLE platform, ISIDORE will be one of the main aggregators of data sources.

In addition to the TRIPLE Core platform, its frontend interface and a set of innovative tools (visualisation, annotation, trust building system, crowdfunding, social network and recommender system) are being deployed, but not all will have or need to be integrated with EGI Check-In. Indeed, for services that are being deployed at the core of TRIPLE, no direct user interaction will happen, therefore, no authentication is needed.

In performing Check-In integration with TRIPLE innovation services, issues have been identified -- when a new user registers to, s/he also needs to register as an EGI member. This is because Check-in is designed for higher Authentication and Authorization needs and has to satisfy the EGI e-Infrastructure service access policy. However, those services want to be as open (public access) as possible. There is a need to make the registration process of new users as simple and immediate as possible, while maintaining compliance with the authentication and identification standards, and that is the main goal of the Check-in integration work with TRIPLE. In order to address this specific requirement, a new registration workflow in Check-in now integrates a much simpler registration process for users, that can largely help those public access platforms, similar to TRIPLE, who want to ease the user onboarding process (in particular for non-academic users). This will allow users to be very quickly active on the services.

[12] The TRIPLE project: https://www.gotriple.eu/

[13] ISIDORE, https://isidore.science/, is a platform and a search engine allowing the access to digital data of Humanities and Social Sciences. Open to all and especially to teachers, researchers, PhD students and students, it relies with enrichments on the principles of semantic web and provides access to data in open access. ISIDORE proposes more than 5 millions of ressources of the whole world and enrichments are available in 3 languages : French, English and Spanish.

IV. Integration of Check-in for OPERAS

A. Check-in protocols used in OPERAS

Check-in provides interfaces for 2 authentication protocols: SAML2.0 and OpenID Connect. The more simple configuration use of EGI Check-in would be to use OpenID Connect, which is why it was chosen for most OPERAS services, or at least, when possible. However, for the use of Check-in within the Certification Service, we had to use the SAML2.0 protocol, and therefore Shibboleth. The reason being that DSpace Repository (which is used by the Certification Service) already allows its users to use SAML2.0 via a plugin but not OpenID Connect (yet).

B. VO and User groups and Managers on different levels (nested management)

OPERAS and its service need special requirements and the idea to have a nested structure of management became clear: an OPERAS VO that contains groups that are related to each service of OPERAS in which subgroups are created for each role of the specific service. This is needed because OPERAS is a distributed infrastructure and therefore services are being operated by its members and not centrally. So, the managers of the services and therefore the managers of the user base, are all distributed to OPERAS members. The groups of users are then provided from Check-in to the services via attribute values called “entitlement”.

Table 1: Configuration of OPERAS VO and the nested Group structure

Requirements	**Entitlements (Attribute Values)**
OPERAS VO	urn:mace:egi.eu:group:vo.operas-eu.org
-- PSP	urn:mace:egi.eu:group:vo.operas-eu.org:PSP
---- Administrators	urn:mace:egi.eu:group:vo.operas-eu.org:PSP:Admins.PSP
---- Service providers	urn:mace:egi.eu:group:vo.operas-eu.org:PSP:ServiceProviders.PSP
-- DOAB	urn:mace:egi.eu:group:vo.operas-eu.org:DOAB
---- Administrators	urn:mace:egi.eu:group:vo.operas-eu.org:DOAB:Admins.DOAB
---- Publishers	urn:mace:egi.eu:group:vo.operas-eu.org:DOAB:Publishers.DOAB
-- TRIPLE	urn:mace:egi.eu:group:vo.operas-eu.org:TRIPLE
---- Administrators	urn:mace:egi.eu:group:vo.operas-eu.org:TRIPLE:Admins.TRIPLE
---- Providers	urn:mace:egi.eu:group:vo.operas-eu.org:TRIPLE:Providers.TRIPLE

A very simple description of how these entitlements work or are used is:

- A service will receive the entitlement of a user when logging in
- A service will decide based on these entitlements received what are the roles of such logged in user
- A service will be able to attribute special rights to such user without having to change anything in the service's configuration

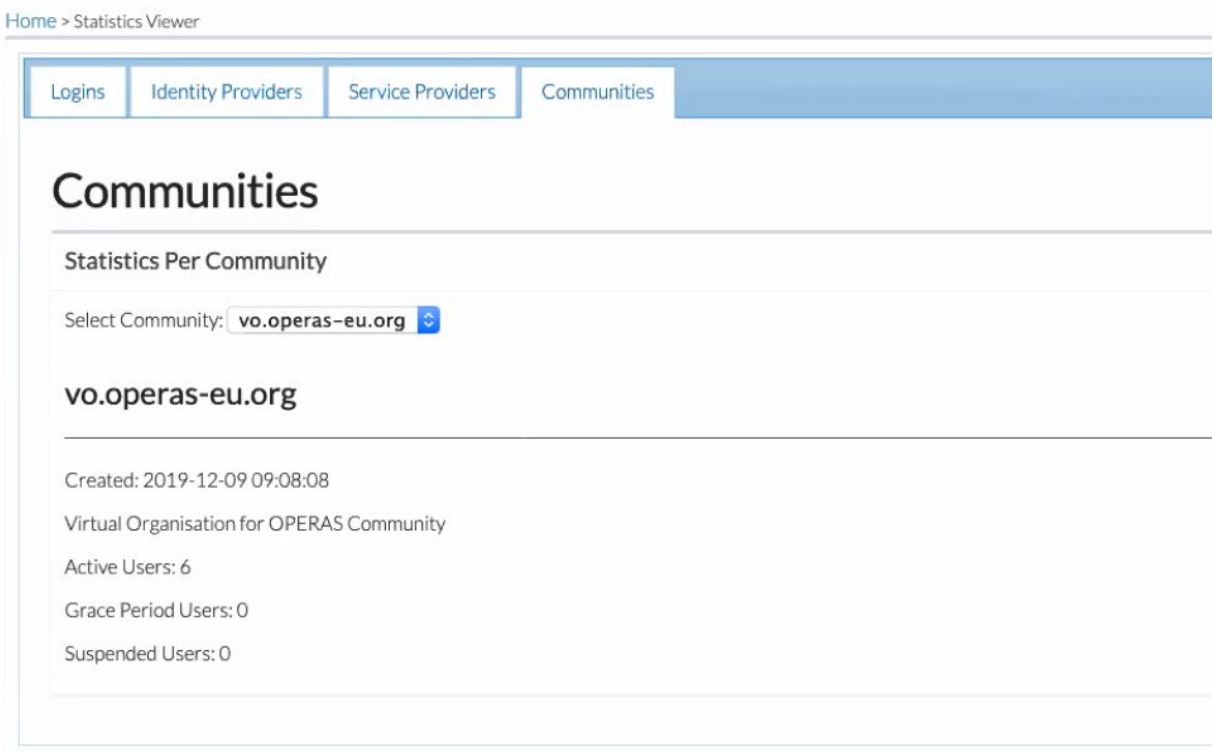

Fig 4: OPERAS VO information

Fig 4 shows the OPERAS VO information page within Check-in. Here, an overview of the OPERAS VO community (vo.operas-eu.org), and the statistics (i.e., active users, suspended users) are available in the interface.

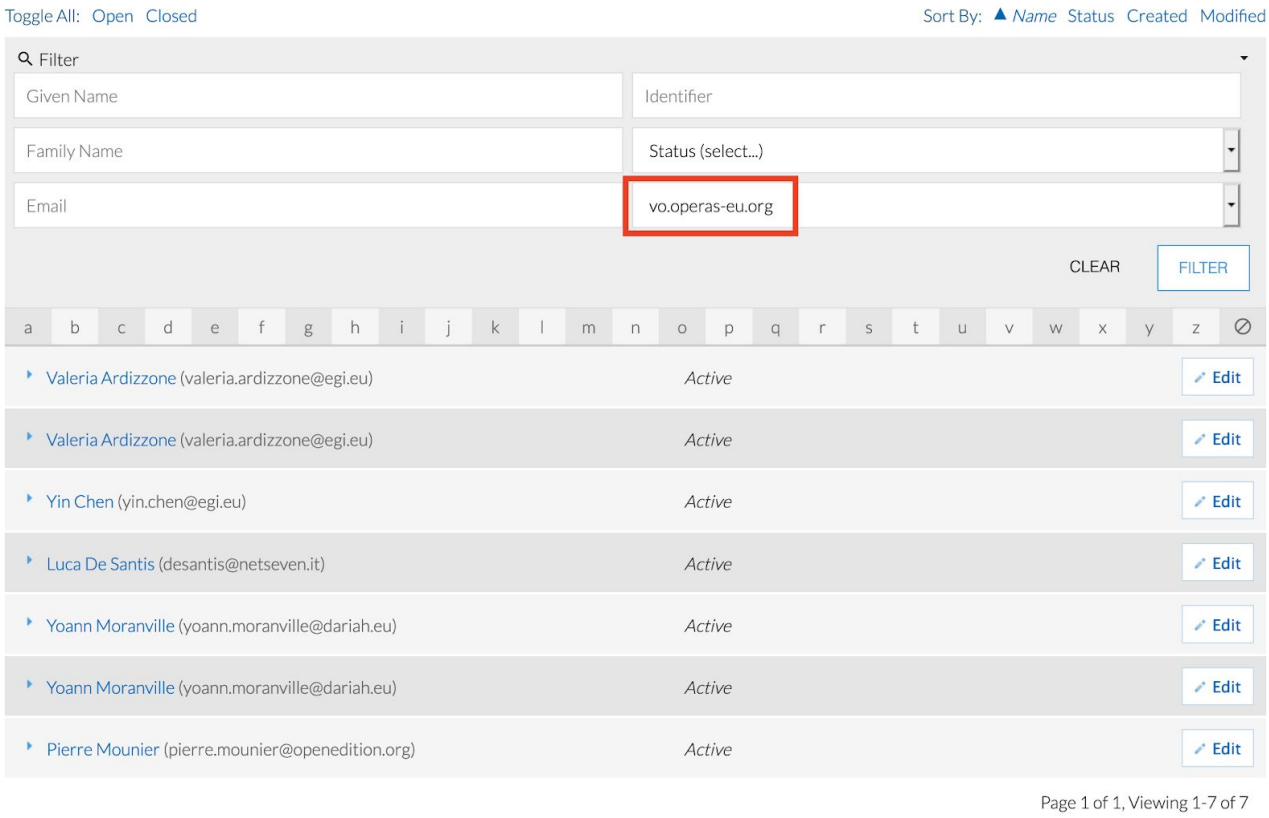

Fig 5: Managing OPERAS Groups and Users with Check-In

Fig 5 shows the Check-in interface for OPERAS user group management. All the EGI Check-in users that are part of the OPERAS VO are listed. On the left panel, it lists the OPERAS groups and sub-groups. A OPERAS admin can select one of the (sub-)groups, add users to it and assign the role and grant access rights.

C. Publication Service Portal (Pathfinder)

The Publication Service Portal has been developed within the OPERAS-P project, for its design phase which includes a prototype. This prototype has been linked to the EGI Check-in service for its login functionality (currently using the EGI Check-in DEV environment[14]). In order to do so, and as Check-in proposes 2 different protocols to connect: SAML2 and OpenID Connect, we opted to use the OpenID Connect, which provides a simpler (but at least as robust) communication protocol between the Service Provider and the Identity Provider.

As for other programming languages, PHP also has libraries to make use of OpenID

[14] https://aai-dev.egi.eu

Connect without rewriting the logic ourselves. A new Check-in client was created in the administration interface which provided us a key and a secret, and following the documentation and the Check-in endpoint, the configuration of the service was made to make use of Check-in within this service.

Fig 6 shows the Pathfinder user login page. Check-in is provided as a second login option, by clicking the button '*LOGIN WITH EGI*', a user will be directed to the Check-in interface (Fig 2), where (s)he can use their organisation credential to login. Once authentication is approved, the user will be directed back to Pathfinder and use the service.

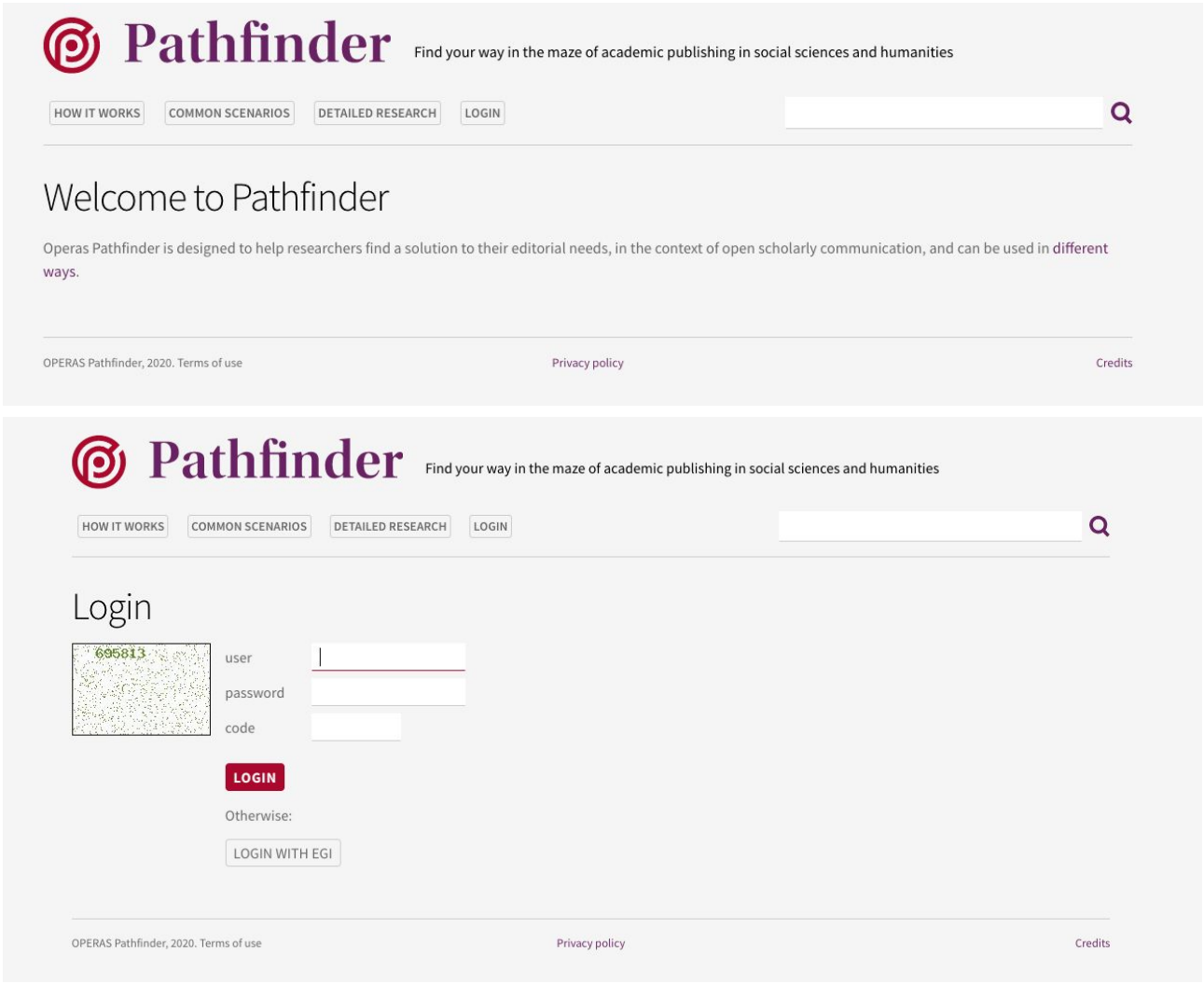

Fig 6: Pathfinder User Login interface

D. Future Integrations

a. Certification Service (DOAB)

The DOAB (Directory of Open Access Books, doabooks.org) is currently being redeveloped within the OPERAS-P project and will rely on the DSpace

(https://duraspace.org/dspace/) repository system. The OPERAS Certification Service, being part of DOAB and being provided by DOAB Foundation, will also rely on the DSpace repository. At the time of writing, it is not yet sure how the API will provide information to the users, since it is being developed, but it is clear that the use of it will be partly public, and partly behind authentication. To make the matter simpler, the whole DOAB will be using EGI Check-in for the authentication and authorization of its users.
However, because of the use of DSpace, technological problems have forced us to not use OpenID Connect protocol, but SAML2.0 and Shibboleth. This is due to the fact that DSpace 6.x already provides an optional plugin to connect to Shibboleth SP, and that will be used instead of creating a new OpenID Connect plugin.

b. Metrics Service

A specificity of the Metrics service is that it is basically an API, and that user authentication is directly done on the API with a username and password. The API offers a public access but also a restricted access. This restricted access is used by publishers (data providers) that would provide their data to the service. All other accesses, which is reading and retrieving data, is done anonymously by any users.
This integration is for the moment on hold, and is being taken into consideration by the Metrics team. If a simple integration between Metrics and Check-in is found, then a plan to move from the current username/password authentication to Check-in will be put forward. Today, a potential integration proposed by the EGI Check-in development team is to use *OAuth2 Device Authorization Grant*[15] (previously known as *Device Code Flow*). This flow enables OAuth clients on devices that lack a browser (e.g. Command Line based client applications) to obtain user authorisation to access protected resources (e.g. APIs) by using a user agent (i.e. a browser) on a separate device. Specifically, instead of interacting directly with the end user's browser, the device client instructs the end user to use another device and connect to the authorisation server to approve the access request. If the client is granted access, the authorization server responds with an access token and, optionally a refresh token. A refresh token is a special kind of token that can be used to obtain a renewed access token until the refresh token expires or gets revoked. Refresh tokens improve the authentication experience significantly. The user has to authenticate through an interactive web authentication process only once. Subsequent re-authentication can take place without user interaction, This would allow users of the Metrics service to only have to follow a web authentication process to obtain those refresh tokens very seldom, up to 13 months, which is the maximum expiry time of refresh tokens. So the services that are contacting the Metrics API would require very limited user interaction. This is definitely a solution to be considered by the Metrics team.

c. Research for Society

Research for Society is based on an already existing service, Hypotheses.org which is operated by OpenEdition. The service will be updated and upgraded within the COESO

[15] https://oauth.net/2/device-flow/

project which will start early 2021, in which we may open it up to Check-in, but that is to be seen with the SP of the currently used Hypotheses.org platform and the COESO project consortium.

d. GOTRIPLE service

GOTRIPLE is divided by Core, and innovative services. The core service will be using Check-in! The innovative services, depending on their integration with GOTRIPLE, will have the choice to do so or not. Examples already: 1. TBS will be integrated fully in the code of TRIPLE Core, which means no integration with Check-in (or any authentication service), 2. Pundit annotation service will be fully integrated with different authentication services, including Check-in with OpenID Connect.

V. Conclusion and future work

In this deliverable, we provided information about EGI Check-in, the technical details and integration options. The aim is to provide a guideline for OPERAS service providers for future integration work.

We also captured the OPERAS requirements for AAI and discussed Check-in solutions. These are useful experiences from OPERAS that can be shared with other SSH communities and beyond. On the other hand, it provides the Check-in team a better understanding of community service scenarios.

We reported the integration progress, provided technical information on VO configuration, group and user management, and a demonstrator on how Check-In works with OPERAS service, Pathfinder, developed in T4.1.

In the next step, we will continue integrating with other OPERAS services (Certification service, Metrics, Research for Society, and GOTRIPLE). We will also promote the results to other SSH communities and EGI communities. For example, OPERAS is invited to present the Check-in integration experiences in EGI conference 2020[16], AAI workshop. An abstract of TRIPLE integration with Check-in is also accepted by the conference that provides a good opportunity for making OPERAS/TRIPLE visible to the EGI user community.

[16] EGI conference 2020, 2-5 Nov: https://indico.egi.eu/event/5000/overview