DARIAH - Pilot Overview

Pilot Description

The pilot's goal is to first extend the existing DARIAH AAI with a SP-IdP-proxy according to the AARC BPA to allow for interoperability with other infrastructures, such as EGI. Afterwards this interoperability is proven by connecting the DARIAH proxy with EGI Check-In in order to allow DARIAH users access to EGI resources.

Pilot goals

The AARC2 pilot consists of two individual goals:

1. Implementation of an SP-IdP proxy within the DARIAH AAI

According to the AARC Blueprint Architecture (BPA) communication between infrastructures should happen through dedicated infrastructure proxies. During this pilot, DARIAH implemented their own proxy solution based on Shibboleth. This proxy will be compliant to all relevant recommendations and guidelines developed within AARC and therefore this pilot can be seen as a real-world example of the architecture work within AARC. As a side effect DARIAH-internal services will benefit from this solution as well, as it will move a lot of the previously needed complexity away from the individual services to the central proxy component.

2. Interoperability pilot between EGI and DARIAH

To showcase successful implementation of the DARIAH SP-IdP proxy, the second part of this pilot deals with interoperability between the DARIAH research infrastructure and the EGI e-infrastructure. The goal is to allow DARIAH users to transparently access EGI resources through EGI's own proxy solution (EGI CheckIn). As an initial use case, selected DARIAH users should be able to deploy and access virtual machines in the EGI infrastructure.

Description

Introduction to DARIAH

DARIAH is an ERIC, a pan-European infrastructure for arts and humanities scholars working with computational methods. It supports digital research as well as the teaching of digital research methods. It connects several hundreds of scholars and dozens of research facilities in currently 17 European countries, the DARIAH member countries. In addition, DARIAH has several cooperating partner institutions in countries not being a member of DARIAH, and strong ties to many research projects across Europe. People in DARIAH provide digital tools and share data as well as know-how. They organize learning opportunities for digital research methods, like workshops and summer schools, and offer training materials for Digital Humanities.

In AARC2, DARIAH is represented by DAASI International. The tasks of DAASI International in DARIAH include:

- Constructing and operating an AAI (Authentication and Authorization Infrastructure).
- Integrating new technologies like the management of virtual organizations via attribute aggregations.
- Developing a long-lasting and comprehensive operating unit.
- Conceptioning and developing the DARIAH storage infrastructure.

How the AARC BPA helped this pilot

The DARIAH research infrastructure offers the DARIAH AAI as one of the core technical services for researchers in arts and humanities. This enables researchers to log in to various services offered within DARIAH, by either using their own campus account or an account registered at the DARIAH home IdP. The DARIAH AAI adds information, such as group memberships specific to the DARIAH community or approval of general and optionally service specific terms of use, which can be used by services for authorisation decisions. Version 1 of the DARIAH AAI has been in production for multiple years and required every service to implement several details by themselves, e.g. connection to eduGAIN, attribute query to DARIAH for the additional attributes, validation of policy attributes, and blocking and redirecting the user to the DARIAH self service portal if any of the information was missing or out of date.

In order to improve these limitations, be in line with the Blueprint Architecture (BPA) by AARC and therefore allow interoperability with other infrastructures, we decided to implement the DARIAH AAI version 2 as part of this pilot. In this version 2, which was created during this pilot, a central proxy component, which follows the proxy layer of the AARC BPA was added to complete the first goal (Implementation of an SP-IdP proxy within the DARIAH AAI) of the pilot. We were able to base the infrastructure on the building blocks of the BPA and also follow various guidelines from the AARC project on how to convey information to other infrastructures. Examples include the unique identifier or how to express group memberships in order to allow DARIAH users access to EGI resources.

Components

The components are as follows:
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Why did we choose It?</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>RCAuth</td>
<td>Token Translation. Used to generate x509 certificates for access to legacy services</td>
<td>EU wide, sustainable infrastructure component</td>
<td><a href="https://rcauth.eu">https://rcauth.eu</a></td>
</tr>
<tr>
<td>EGI-Check-in</td>
<td>BPA-compliant proxy within EGI and membership management component</td>
<td>Implements multiple components, easier maintenance. Product used by other communities.</td>
<td><a href="https://www.egi.eu/services/check-in/">https://www.egi.eu/services/check-in/</a></td>
</tr>
<tr>
<td>DARIAH Proxy</td>
<td>BPA-compliant SP-IDP-Proxy implemented within DARIAH AAI, based on Shibboleth IDP and SP</td>
<td>Interoperability with other Infras (e.g. EGI Check-in)</td>
<td><a href="https://aaiproxy.de.dariah.eu/idp/shibboleth">https://aaiproxy.de.dariah.eu/idp/shibboleth</a></td>
</tr>
<tr>
<td>DARIAH Group Management and User Registry</td>
<td>Management of internal DARIAH users and groups, as well as groups used for access to EGI resources</td>
<td>Access management to EGI resources is managed by DARIAH</td>
<td><a href="https://auth.de.dariah.eu/cgi-bin/selfservice/ldapportal.pl">https://auth.de.dariah.eu/cgi-bin/selfservice/ldapportal.pl</a></td>
</tr>
</tbody>
</table>

**EGI group management Modules configuration**

You need **admin privileges** to perform the following:

**Add a pipeline**

Select <collaboration> -> Configuration -> Pipelines -> Add Pipeline

See screenshot below for configuration settings

![Add a pipeline screenshot](image-url)

**Add Organisational Identity Source**

Select <collaboration> -> Configuration -> Organisational Identity Sources -> Add Organisational Identity Source

See screenshots below for configuration settings

![Add Organisational Identity Source screenshot](image-url)
Create RCAuth Enrollment Flow

Select <collaboration> -> Configuration -> Enrollment Flows -> Add Enrollment Flow

See screenshots below for configuration settings
Add and Configure VOMs Provisioning Plugin

Select <collaboration> -> Configuration -> Provisioning Targets -> Add Provisioning Target

See screenshots below for configuration settings

<table>
<thead>
<tr>
<th>Environment</th>
<th>Issuer DN</th>
</tr>
</thead>
<tbody>
<tr>
<td>AARC pilot (e.g. LS AAI, WLCG)</td>
<td>{{/O=AARC/OU=AAI-Pilot/CN=AARC Simple Demo CA}}</td>
</tr>
<tr>
<td>Production</td>
<td>{{/DC=eu/DC=rcauth/O=Certification Authorities/CN=Research and Collaboration Authentication Pilot G1 CA}}</td>
</tr>
</tbody>
</table>
Architecture

The following (slightly simplified) diagram shows the interaction between the various components of the DARIAH AAI (green), home organisation IdPs (yellow) and EGI (red):
The central component, which is being implemented in this pilot, is the DARIAH SP-IdP proxy. The proxy implements the AARC BPA and serves as an AAI gateway for two scenarios:

1. To allow users to authenticate at DARIAH services using their preferred authentication method (e.g. eduGAIN IdPs or the DARIAH homeless IdP).
2. In the inter-infrastructure use-case the DARIAH proxy connect directly to the proxy of EGI (or other infrastructures in the future).

AARC BPA version:
Use Cases

Allow DARIAH users to transparently access EGI resources through EGI's own proxy solution (EGI CheckIn)

Create DARIAH Enrollment Flow

Select <collaboration> -> Configuration -> Enrollment Flows -> Add Enrollment Flow

Configure DARIAH Enrollment Flow

<Name>, e.g. Confirm request for accessing EGI resources
>Status> => Active
<Petitioner Enrollment Authorization => Authenticated User
<Identity Matching> => None
<Email Confirmation Mode> => None
<Terms and Conditions Mode> => Explicit Consent
<Finalization Redirect URL> => The URL of the enrollment petition to follow. For this case the enrollment to follow is the RCAuth enrollment

See screenshots below for configuration settings
See screenshots below for co persons profile after finishing DARIAH Enrollment

Demo Videos can be found [here](#)

- User accessing Dariah service
- Expunging a user from Group Management Framework removes the user from VOMS as well

**Login flow from the PoV of a DARIAH User**

A demo of the login experience for a DARIAH user can be found in these slides:
Further information

Results and sustainability plans

The implementation of the proxy was completed in mid-2018 and since then all DARIAH services have been moved behind the proxy. Since the architecture was designed with backwards compatibility in mind, the transition process did not create any major issues. Using the proxy to connect to federated AAI is now much simpler for service operators, hence we've already connected additional services to the DARIAH AAI and intend to continue doing so. For the second part of the pilot we've successfully finished connecting the DARIAH proxy with the development instance of EGI check-in. This includes attribute and entitlement mapping between DARIAH and EGI, as well as on the fly user provisioning within EGI. For this some plugins to the existing EGI check-in infrastructure were developed.

Within DARIAH the new proxy component is now part of the core AAI and will be operated as such in the future. The EGI Check-In framework also follows the AARC BPA philosophy and therefore will continue to be operated as part of the EGI organisation. This also included the enrollment workflows for DARIAH users.