Contribution ID: **132** Type: **Presentation**

Applications of the AARC Blueprint Architecture - Migration to a IdP-SP-proxy in the DARIAH AAI

Wednesday, 10 October 2018 11:45 (15 minutes)

The DARIAH Research Infrastructure (RI) provides, among other things, digital services for researchers in arts and humanities. It offers an authentication and authorisation infrastructure (AAI), the DARIAH AAI, to enable researchers to login into these services with their own campus account, providing a Single Sign-On experience. The DARIAH AAI supplies additional information, such as group memberships specific to the DARIAH community, which can be used by services for authorisation decisions. Historically, the DARIAH AAI is composed of different components:

- a self-service interface which allows for the registration of DARIAH accounts;
- the DARIAH IdP, which serves as both an Identity Provider (IdP) for these DARIAH accounts, as well as an attribute authority (AA) that releases DARIAH-specific attributes for users authenticating via their home organisation‘s IdP;
- a group membership management system for both these types of accounts;
- and the DARIAH service providers (SP) that each need to query the AA and check for DARIAH-specific attributes.

The Blueprint Architecture (BPA), which was developed in the EC-funded AARC (Authentication and Authorisation for Research and Collaboration) project, recommends an IdP-SP-proxy, which serves as a gateway between service providers of the research infrastructure and identity providers and attribute sources. This approach takes away a lot of the complexity services would have to deal with in a traditional full mesh federation, and allows for a central place for policy decisions. It thus offers a scalable solution to problems such as aggregation of attributes from different sources, and account linking.

In order to allow services to connect to the DARIAH AAI in a much simpler fashion, and to allow for interoperability with other e- and research infrastructures, and to create the foundation for new features, such as account linking in the future, the DARIAH AAI was recently extended by an AARC BPA-compliant IdP-SP-proxy component. Since the DARIAH AAI is already largely based on Shibboleth products, we decided to implement this proxy solution based on Shibboleth, as opposed to SimpleSAMLphp or SATOSA, which offer proxy functionality by default. While this solution integrates nicely into the existing DARIAH AAI ecosystem, it provided some technical challenges in actually turning the Shibboleth products into an IdP-SP-proxy.

This talk will illustrate the main advantages of, and experiences with the adoption of the AARC BPA from the point of view of the DARIAH research community and showcase our technical solution based on Shibboleth (i.e. how Shibboleth IdP and SP can be used to build a proxy component). We can also give insight into how to migrate from an existing AAI to a proxy-based infrastructure, while ensuring backwards compatibility with legacy use cases.

Type of abstract

Presentation

Summary

The DARIAH Research Infrastructure has recently integrated a IdP-SP-proxy into its authentication and authorization infrastructure. This proxy follows the recommendations and guidelines from the AARC Blueprint Architecture (BPA) and allows for easier integration of services, additional features and interoperability with other infrastructures.

The talk will illustrate the technical implementation of the proxy component (based on Shibboleth products) and our experience with the migration process in general, including challenges like policy decisions and ensuring backwards compatibility. We will also talk about our future plans in the DARIAH AAI, which are enabled by the integration of the proxy.

Primary authors: Mr HÜBNER, David (DAASI International GmbH); Mr GIETZ, Peter (DAASI International GmbH)

Presenter: Mr HÜBNER, David (DAASI International GmbH)

Session Classification: Towards an AAI service for research communities