Authentication and Authorization in Collaborative Organizations
Attribute management, aggregation and consumption

www.aarc-project.eu

Use cases & aims

In a federated environment Identity Providers and Service Providers establish a trust framework to handle **Authentication** based on institutional accounts. Today this approach (see scenario 1) is common practice and even global IdP - SP scenarios become mainstream using eduGAIN as an interfederation vehicle.

Authentication infrastructures have proven to be useful in collaborative organizations (COs) but in those scenarios there is a strong need for additional attributes (e.g. entitlements) to handle **Authorizations** in a scalable and federated way as well (see scenario 2). In addition, there is a growing need to include users with **guest/social identities** but at the same time establish a sufficient level of trust for such identities.

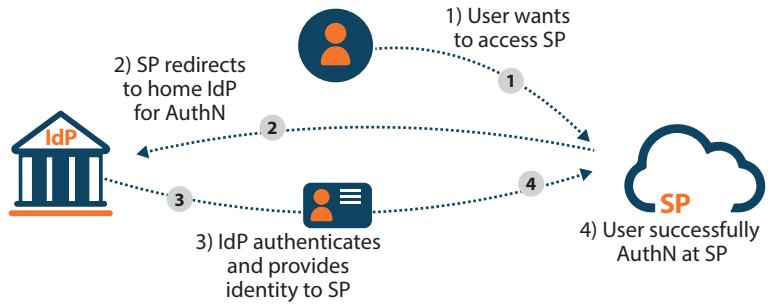
The pilots presented here provide clues to (1) establish external CO managed Attribute Authorities (AAs), (2) to aggregate attributes from different sources in a central proxy, (3) forward the enriched set of attributes in such a way that they can easily be consumed by Service Providers (SPs) upon which these SPs can make authorization decisions and (4) to provide suitable approaches to include users in the CO who own only a social identity by integrating multiple authentication technologies like OIDC and OAuth2 with SAML.

In the first pilot (scenario 2) we investigated the suitability of SAML based AAI components to use externally managed attributes to provide and restrict access to cloud services. We provide a demo where attribute management is based on COmanage and a user is able to access an OpenStack Liberty based cloud service.
Demonstrator: https://wiki.geant.org/x/LAH5Aw

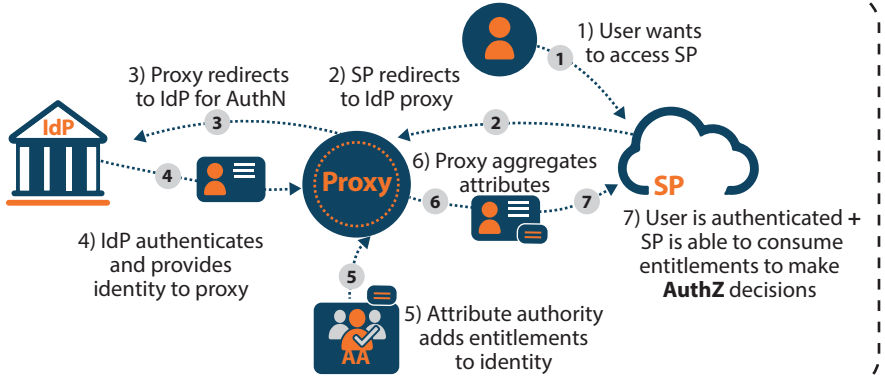
In the second pilot (scenario 3) we demonstrate possible mechanisms to include social identities in the Authentication and Authorisation flow to provide access to resources for users who lack an institutional account. In this context, we explored mechanisms to enhance the Level of Assurance (LoA) of users with a social identity who need to participate in research collaborations.
Demonstrator: https://wiki.geant.org/x/ZIqSAw

In the third pilot we applied the principles of scenarios 2 and 3 to the AAI use case of the BBMRI ERIC. We demonstrate how an existing architecture can be applied to existing services. The pilot integrated pre-existing solutions like PERUN for federated identity management, the aggregation of authentication and authorization information with the aim to provide an aggregate of attributes to service providers in a transparant way.
Demonstrator: https://wiki.geant.org/x/HgD5Aw

1 Basic - common - scenario



2 Collaboration scenario



3 Collaboration scenario including social identities