Attribute Management pilot BBMRI

Introduction

One of the AARC results is the blueprint architecture (BPA) describing how the AAI infrastructure for research communities should looks like. In this pilot we deployed identity and access management software Perun for BBMRI research infrastructure according to the BPA. The goal of the pilot was to demonstrate how data from different sources can be aggregated in form of attributes and then distributed to the services. Perun is a part of the eduTEAMS initiative from GEANT. We have successfully demonstrated that combination of existing components and data sources can fulfil needs of research community, in this case represented by BBMRI. The result of this pilot has been transferred into the production service used by the BBMRI.

Detailed description

BBMRI use case for attribute management was to combine data about biobanks, their representatives and users in order to feed the Negotiator service which requires authenticated users, list of biobanks and their representatives. We have configured two registration workflows in Perun system which is used to register users of Negotiator service and representatives of biobanks. Users go through normal registration which requires just their contact information. Representatives register as normal users plus they provide which biobanks they represent. BBMRI administration checks the registration form for representatives and approve their request to be representative. Perun system gathers data from biobank directory and represents them as a groups. Representatives are then automatically put into subgroup of the group representing biobank. Mapping of representatives and biobanks is then pushed into the Negotiator service, so every biobank has its own representatives assigned. Negotiator is accessible just via OpenID Connect protocol, so OIDC authorisation server communicates with Perun system to get attributes about users.

Users and representatives registering into the BBMRI are getting their BBMRI ID which is used to uniquely identify BBMRI users regardless which identity they used to access the BBMRI services (any of their home organisation identity or guest identity).

The whole attribute aggregation is transparent from the user point of view, so they just register into the BBMRI and then use Negotiator service.

Perun system is doing the attribute aggregation as well as identity linking together with support of the whole user life cycle we can ensure that users are automatically added or removed into/from the BBMRI and all the data for authorisation decisions are available.

The whole pilot has been done on https://perun.bbmri-eric.eu and https://negotiator.bbmri-eric.eu. The Perun service for BBMRI has been connected to the eduGAIN, therefore most of the BBMRI users can access the service without any burden.

Schema
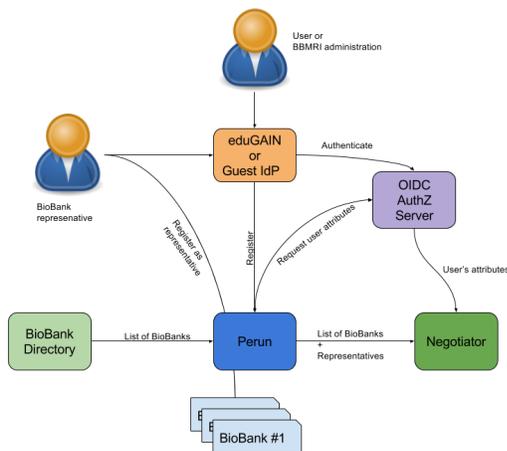
Registration workflow

Enrollment form. Name and email fields are pre-filled with attributes form eduGAIN or Guest IdP.	
You can easily select different mail from list obtained from eduGAIN or you can write down custom one. If you fill in the custom email, you have to verify it by clicink on the link that will be send to provided email address.	
Registration is complete. You will receive a notification after VO manager approve your application.	

Registration form for biobank representatives where they are providing list of biobanks.	
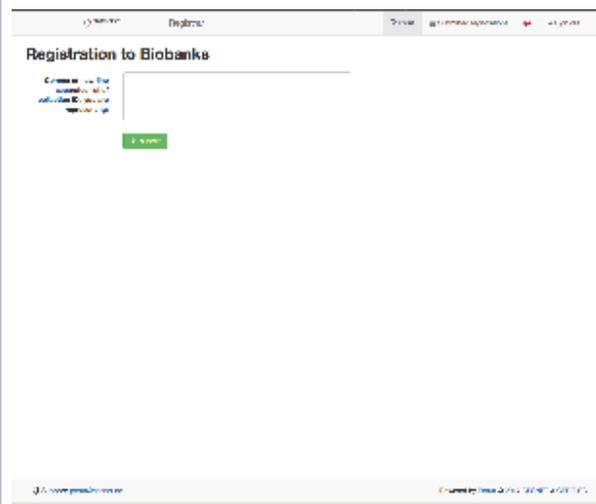
Managing group membership/assignment of the representative to biobank

Select group from the list of all groups within the VO. Group representing biobank. Next step is to select a group.	

Group detail where you can see that the group currently contains no members.	
Next step is click on the "Add" button.	

Fill in the name of user who you want to add and click on search button.	
In case there is more then one user found you have to choose from the list below.	

After you add user to the group. You will see pop-up notification on the tom and then you can search and add more users.	
After adding new user to the group, new access control configuration will be provisioned to all affected services.	

Data about representatives and biobanks are now pushed into the Negotiator service. Users then can see who is representing particular biobank.	