

Attribute Management pilot BBMRI

- [Introduction](#)
- [Schema](#)
- [Registration workflow](#)
- [Managing group membership/assignment of the representative to biobank](#)

Introduction

One of the AARC results is the blueprint architecture (BPA) describing how the AAI infrastructure for research communities should look 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.

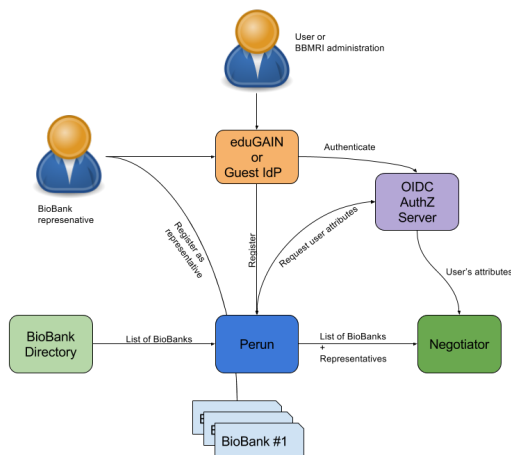
Users and representatives registering into the BBMRI are getting their BBMRI ID which is used to uniquely identify BBMRI users regardless which identity they used to access the BBMRI services (any of their home organisation identity or guest identity).

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 from eduGAIN or Guest IdP.

BBMRI-ERIC Registrar Form Submitted registrations Sign out

BBMRI-ERIC

Registration to the BBMRI support

Name * Slávek Licehammer

Email slavek.licehammer@cesnet.cz

Submit

Support: perun@cesnet.cz Powered by Perun © 2017 CESNET & CERIT-SC

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.

BBMRI-ERIC Registrar Form Submitted registrations Sign out

BBMRI-ERIC

Registration to the BBMRI support

Name * Slávek Licehammer

Email slavek.licehammer@cesnet.cz

Submit

- slavek.licehammer@cesnet.cz
- slavek@ics.muni.cz
- licehammer@cesnet.cz
- Custom ---

Support: perun@cesnet.cz Powered by Perun © 2017 CESNET & CERIT-SC

Registration is complete. You will receive a notification after VO manager approve your application.

BBMRI-ERIC Registrar Form Submitted registrations Sign out

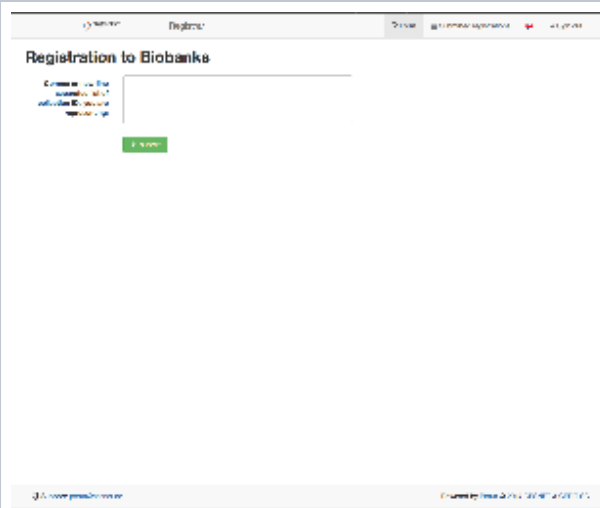
BBMRI-ERIC

✓ You have successfully applied for membership

Please wait until your application to BBMRI support will be approved.

Support: perun@cesnet.cz Powered by Perun © 2017 CESNET & CERIT-SC

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.

Perun BBMRI

Name: **Slávek Licehammer** Role: PERUN / SECURITY ADMIN Logout

Perun admin BBMRI ID: 3 Short name: bbMRI

Security admin BBMRI

VO manager

Select VO

BBMRI

Members

Groups

Resources

Applications

Application form

Settings

Managers

External sources

Overview Members Groups Resources Applications Application form Settings Managers External sources

Create... Delete Filter

<input type="checkbox"/>	Group ID	Sync	Name	Description	Count: 1081
<input type="checkbox"/>	3		members	Group containing VO members for VO BBMRI	
<input type="checkbox"/>	7		collections	Biobank collections.	
<input type="checkbox"/>	2174		collections.bbmri-eric.ID.AT_MUG.collection.all_samples	Group of people authorized to access this biobank collection.	
<input type="checkbox"/>	2175		collections.bbmri-eric.ID.AT_MUG.collection.all_samples.representatives	Group of people responsible for this biobank collection.	
<input type="checkbox"/>	2176		collections.bbmri-eric.ID.AT_MUI.collection.all_samples	Group of people authorized to access this biobank collection.	
<input type="checkbox"/>	2177		collections.bbmri-eric.ID.AT_MUI.collection.all_samples.representatives	Group of people responsible for this biobank collection.	
<input type="checkbox"/>	2178		collections.bbmri-eric.ID.AT_MUW.collection.all_samples	Group of people authorized to access this biobank collection.	

About: Perun web | Support: perun@cesnet.cz, Online help © CESNET, CERIT 2011 - 2017, version: 3.0.1 fe540 Settings

Group detail where you can see that the group currently contains no members.

Next step is click on the "Add" button.

The screenshot shows the Perun web interface for a group named "collections:bbmri-eric.ID.AT_MUG.collect...". The user is logged in as "Slávek Licehammer" with the role "PERUN / SECURITY ADMIN". The interface includes a navigation menu on the left with options like "Perun admin", "Security admin", "VO manager", "Group manager", "Facility manager", and "User". The main content area shows the group details, including a table for members. The table is currently empty, and a message states "Group has no members." Below the table, there are buttons for "Add...", "Invite member...", and "Remove".

Fill in the name of user who you want to add and click on search button.

In case there is more than one user found you have to choose from the list below.

The screenshot shows the "Add member(s)" dialog box open in the Perun web interface. The dialog has a search input field containing "prochazka" and buttons for "Search in VO", "Search globally", "List all VO members", "Add", "Invite selected", and "Close". Below the search input, a table lists search results. The table has columns for "Member Id", "User Id", "Status", "Name", "Organization", "Email", and "Count". One result is shown: Member Id 11, User Id 3, Status (green checkmark), Name "Michal Procházka", Organization, Email "prochazka.michal@gmail.com", and Count 1.

After you add user to the group. You will see pop-up notification on the top 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.

The screenshot shows the "Add member(s)" dialog box after a user has been added. A blue notification banner at the top of the dialog reads "Member: Procházka Michal added to group: bbmri-eric.ID.AT_MUG.collection.all_samples". The search input field is empty. The table below shows the "Already added" user: Member Id 11, User Id 3, Status (green checkmark), Name "Michal Procházka", Organization, Email "prochazka.michal@gmail.com", and Count 1.

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