Federation as a Service training
21-22th April 2015, Vienna

User Interface exercise book

Authors:
Nebojša Ilić, AMRES
Marina Vermezović, AMRES

Contents

Exercise 1: User Interface walkthrough

For this training, you will exercise on the FaaS instance that is already installed and prepared for your NREN, in form https://nren-training.faas.geant.net (provided on the training).

NOTE: FaaS UI is available only on HTTPS!

Login to your own prepared NREN instance with account: admin/to-be-provided-on-training. Use the “Login with local account” option.

Spend some time to get familiar with the UI!

Exercise 2: Users, Roles and managing accounts

In this exercise you will learn how to create local user accounts for the registry application.

1. Create new user

Create new user account with the Member role for one participant:

- Navigate to the top menu “Administration/Users”
- Click on “Add user” button on upper right corner and enter data about new user
- As username enter the *eduPersonPrincipleName* of that user (username@domain) (for the latter federated authentication). This will not be relevant during the training as you will not be connecting your IdP, but this will be the way that you should create accounts in practice.
- As access type choose „local and federated“. This will allow the user to login with the federated identity later and get the same privileges as he had with the local account. However, the *eduPersonPrincipleName* from the federated identity must be the same as the local account username (this is how the local and federated identities are later linked).
- Enter your real email address so that you can keep track of the email notifications from the application.

Create another user account with the Administrator role for second participant in the same manner. In order to assign user the Administrator role, navigate to the top menu “Administration/Users” and click on the just created user. Go to „Assigned roles“ column, click on the „Manage roles“ button and add the „Administrator“ privilege.

Navigate to the top menu “Administration/Users” and explore the created accounts.

2. Delete generic admin user

Login as just created Administrator user. Delete the generic admin account by navigating to the top menu “Administration/Users”. First you will have to remove the „Administrator“ privilege of the admin user by changing it to “Guest” or “Member”. Return to “Administration/Users” and delete the admin user by clicking on the Trash icon in the „Action“ column.

3. Add notifications to the Administrator user

Registry application supports email notifications about new IdP/SP registrations, requests to join federation etc. In order for the Administrator user to get the email notifications about requests coming from the registry application, you must enable notifications on the user account level. Navigate to the top menu “Administration/Users” and click on the Administrator user. Go to „Notifications“ row, click on the „My notifications“ button and add the „ System Notifications and all other requests/alerts “. In this way the Administrator user will get all the notifications coming from the registry application.

Exercise 3: Register basic sample IdP and SP

In this exercise you will learn how to register IdP and SP with default basic metadata. You will see how this task is looking for the IdP/SP owner and for you as Federation Operator.

If you have two participants from your NREN, divide the roles so that one will play the role of IdP/SP owner and login with Member user account and the other will play the role of Federation operator and login with Administrator user account. If you are the single participant from your NREN, then you will have to play the both roles from two different browsers!

1. IdP owner registers sample IdP (Member user)

Go to the https://test.faas.geant.net/md/example-idp.xml and copy the sample IdP basic metadata. Navigate to top menu "Register/Identity Provider". Paste the XML metadata, and click on "Next" button. Revise the already existing data and add the following data:

- "Organization" tab – in following fields add in at least one language: "Name of organization", "DisplayName of organization", "URL to information about organization";
- "Contact" tab – add one or more contact persons.

These are the minimal data that the registry application is requesting to have for any IdP/SP. Additional data can be added at this point or later by editing a registered IdP/SP. You will do this in the next exercise.

Click on the "Register" button at the end of the page. The request for the registration of the new IdP will be sent for approval to the Administrator user. Check if the email notification has been sent to the Administrator.

2. Federation operator approves the registration (Administrator user)

As Administrator user, you will see the new coming notification in the top right corner. You have to go to the requests queue (red circle in the top right corner) and approve the IdP registration.

3. Federation operator leverages the permissions to manage IdP to the IdP owner (Administrator user)

As Administrator user, you need to add the privileges to the Member user to edit and manage the IdP that was just registered (currently it's not done automatically!). Go to top menu "Identity Providers" and click on the IdP that was just registered. Navigate to "Management" tab and click on the "Display access." Allow the write and manage permissions to the Member user by clicking on the "Allow" buttons.

4. Explore the metadata of registered IdP

Navigate to top menu "Identity Providers" and click on the just registered IdP. Go to the "Metadata" tab and explore all available data. See how the generated metadata is looking like (the first icon before the "Organization" tab).

Repeat steps 1-4 and register sample SP which basic metadata is available at https://test.faas.geant.net/md/example-sp.xml

Extra exercise: If you have more time, try to register IdP/SP from your own federation.

Exercise 4: Edit registered IdP and SP metadata

In this exercise you will learn how to change and add more stuff to the metadata of the IdP and SP that were just registered.

1. IdP owner amends basic IdP metadata (Member user)

As Member user, go to the top menu "Identity providers" and click on the just registered basic IdP. Click on the "Edit provider" which appears in the cogwheel menu. You will now enter in the mode for editing the IdP where you can in:

- "Organization" tab – add data about organization in multiple languages;
- "Contact" tab – add more contact persons;
- "UI Information" – in one or more languages add data important for UI representation of the IdP:
    - "Name of organization";
    - "Description of user community serviced";
    - "URL to information about the Identity Provider";
    - "URL to Privacy Policy of the Identity Provider";
    - "Logo" – you can use sample logo available at https://test.faas.geant.net/images/geant.jpg
- „UI Hints" – add hints for used for IdP discovery which could be used as hints in determining with which IdP the user may be associated:
    - "DNS domain associated with, or serviced by, the entity";
    - "IPv4 and IPv6 CIDR blocks associated with, or serviced by, the entity";
    - "GeoLocation";
- "Entity Categories" – you can assign REFEDS Research and Scholarship for IdP entity category. It will not be added to the metadata until it is approved by the Federation Operator.

Data in the "SAML" and "Certificate" tabs contain all operational metadata stuff and IdP owner will need only to change them if there is a change in IdP configuration such as adding new endpoints or certificate rollover.

2. Federation operator approves the Entity Category for IdP (Administrator user)

As Federation operator, you need to approve the application of the IdP to the Entity Category. You will do this by accessing the request queue in top right corner and approving the request.

After doing this, explore the metadata of the registered IdP and identify all the metadata elements and attributes that were added.

3. SP owner amends basic SP metadata (Member user)

As Member user, go to the top menu "Service providers" and click on the just registered basic SP. Click on the "Edit provider" which appears in the cogwheel menu. You will now enter in the mode for editing the SP where you can in:

- "Organization" tab – add data about the organization who is running the SP in multiple languages;
- "Contact" tab – add more contact persons;
- "UI Information" – in one or more languages add data important for UI representation of the SP:

  - "Name of the Service";
  - "Description of the Service";
  - "URL to information about the Service";
  - "URL to Privacy Policy of the Service";
  - "Logo" – you can use sample logo available at https://test.faas.geant.net/images/geant.jpg
- "Entity Categories" – you can assign REFEDS Research and Scholarship for SP and GÉANT Data Protection Code of Conduct for SP entity categories. It will not be added to the metadata until it is approved by the Federation Operator.
- "Other Forms/Requested attribute" you can add attributes desired or required by the SP. You can add the reason for requiring the attribute and that is not published in metadata but used for Federation Operator to review the attribute requirements. Try to modify or to remove the required attribute. Note that for REFEDS Research and Scholarship for SP entity category, SP SHOULD request a subset of R&S Category Attributes that represent only those attributes that the SP requires to operate its service https://refeds.org/category/research-and-scholarship/

Data in the "SAML" and "Certificate" tabs contain all operational metadata stuff and SP owner will need only to change them if there is a change in SP configuration such as adding new endpoints or certificate rollover.

4. Federation operator approves the Entity Category (Administrator user)

As Federation operator, you need to approve the application of the SP to the Entity Category. You will do this by accessing the request queue in top right corner and approving the request. Check if the SP has also defined required attributes which are subset of R&S Category Attributes.

After doing this, explore the metadata of the registered SP and identify all the metadata elements and attributes that were added.

Exercise 5: Explore registered Federations

There are two federations registered in the registry application and that is all that you will need!

- NREN federation – which is your local NREN federation to which all IdPs and SPs will join;
- eduGAIN – GÉANT interfederation to which IdPs and SPs that want to interfederate will join.

1. Explore the data of the federations (Administrator user)

As Federation operator you can view and edit data of the defined federations. Navigate to the top menu „Federation" and choose one of the federations. Explore the data presented in the "General" tab.

- "Federation name" serves only as a federation display name in the registry application;
- "Name in metadata" and "Publisher" function only for display purposes in the registry application. The metadata aggregator is NOT using these values, but the values that are configured in the metadata aggregator configuration file on the server. If you ever need to change these values, you will have to notify FaaS team and then also change the value presented in the registry application.

Explore what are the values defined for NREN federation and eduGAIN?

In edit mode you can change data of the federation, but currently everything is pre-set for the training so you don't need to do this. In the real, you would define your own values once on setting up your federation.

2. Explore where generated metadata is published

Navigate to the "Metadata" tab and note where the metadata is published for each federation:

- for NREN federation metadata - https://server-name.faas.geant.net/md/federation-downstream.xml - contains IdPs/SPs from the registry which have joined NREN federation + complete eduGAIN metadata

- for the eduGAIN (upstream) metadata - https://server-name.faas.geant.net/md/edugain-upstream.xml – contains IdPs/SPs from the registry which have joined eduGAIN. Since in this moment there are no entities which have joined eduGAIN federation, this file will not exist.

If you wish to publish metadata on your own webserver, you can pull from these locations. Then you will also need to change this location in the UI by editing the Federation in „General" tab in the „Metadata publication URL" field.

Extra exercise: explore how to change Metadata publication URL

Exercise 6: Join IdP and SP to NREN federation and to eduGAIN

In this exercise you will learn how IdP/SP owner joins the IdP/SP to the NREN federation and to eduGAIN and how the Federation Operator approves it. After joining the IdP/SP to the federations, you will explore how the published metadata is looking like.

1. IdP/SP owner joins the IdP and SP to the federation (Member user)

Federation memberships on the IdP/SP level are managed in the respective IdP/SP "Membership" tab. Join the registered IdP and SP to the NREN federation and to eduGAIN by clicking on the button „Manage membership (joining)". You have to pick the federation you want to join from the dropdown list and to fill in the "Message" that will be presented to the Federation operator who has to approve the registration.

2. Federation operator approves the IdP/SP registration to the federation

As Federation operator, you need to approve the request to join the IdP/SP to the Federation. You will do this by accessing the request queue in top right corner and approving the request.

After doing this, explore the metadata of the NREN federation and the eduGAIN (upstream) federation, on the Metadata publication URL that was presented in Exercise 5.

Identify Entities descriptor, Publication info and Registration info in Entity descriptor which are added by aggregating the federation metadata.

Exercise 7: Management of registered IdP and SP

In this exercise you will learn how to do basic management tasks on the registered IdP and SP such as changing IdP/SP status, defining who can access the IdP/SP and changing the Registration Policies.

1. IdP/SP owner manages the IdP/SP status (Member user)

Login as a Member user, navigate to the top menu "Identity Providers", click on registered IdP and go to the "Management" tab. Here you can:

- Manage status of the IdP by clicking on the arrow next to „Lock/Unlock Enable/Disable ":
  - Lock/Unlock IdP – if IdP is Locked, you cannot change its metadata. Try to Lock the IdP and then try to edit metadata of that IdP. What happens? Don't forget to unlock the entity after.
  - Enable/Disable IdP: if the IdP is disabled, it will not appear in any federation metadata. Try to disable the entity and explore what will happen in the eduGAIN and NREN federation metadata (note that metadata is being refreshed every 15 mins counting from the full hour).
- Remove IdP from the system – in order to do so, the IdP must first be disabled. To remove IdP you would need to click on the arrow next to "Remove provider from system" and enter entityID of the IdP. Do not do this in the exercise as you will lose your IdP!

Extra exercise: If you have more time, repeat this exercise with Service Provider, or register new sample IdP/SP so that you can try to remove it.

2. IdP/SP owner manages who can access the IdP/SP (Member user)

Login as Administrator user and create new Member user, like it is explained in Exercise 2. This Member user by default will only have the read privileges on registered IdPs and SPs.

Login as IdP/SP owner (old Member user) and add more permissions to the new created Member user by:

- Navigating to the top menu „Identity Providers" and selecting the IdP;
- In the „Management tab"click on „Display access";
- "deny" or "allow" some of the read/write/manage permissions privileges to the new Member user and see what happens.

3. IdP/SP owner adds Registration Policy to the registered IdP (Member user)

As Member user navigate to top menu "Identity Providers", click on the registered IdP and go to the "Management" tab.

Under "Registration Policies" section click on "edit" button and select the pre-defined registration policy (as the example the ACOnet registration policy is used). Registration Policy will not be added to the metadata until it is approved by the Federation Operator.

4. Federation operator approves the Registration Policy for IdP (Administrator user)

As Administrator user, you need to approve the application of the IdP for assigning Registration Policy. You will do this by accessing the request queue in top right corner and approving the request. After doing this, explore the metadata of the registered IdP and identify all the metadata elements and attributes that were added.