External identity provider pilot

- Introduction
- Detailed description
- Demonstration portal
  - Registration/Login Workflow
  - Identity Linking Workflow
- Components

Introduction

This pilot aims at demonstrating possible mechanisms to include Social Identities in the Authentication and Authorization process for providing federated access to resources within a given research collaboration, exploiting mechanisms to enhance the LoA of the users. The idea is to be able to support individual researchers that are not affiliated with any of the traditional home organisations, as well as those users whose Identity Providers are not part of any of the eduGAIN participating federations.

The pilot showcases how to cater for these cases by enabling a research collaboration, namely the AARC Pilot User Community, to use social networks as third party Identity Providers. The key factors in enabling such Guest Identity services is to be able to support multiple technologies and flexible policies in a scalable and trustworthy manner. In this context, the pilot is based on an SP-IdP proxy architecture (see also AARC Blueprint Architecture) through which users are able to authenticate with the credentials provided by the IdP of their Home Organisation (e.g. via eduGAIN), as well as using Social Identity providers, or other selected external identity providers. Specifically, the proxy has built-in support for SAML, OpenID Connect and OAuth2 providers and enables user logins through Facebook, Google, LinkedIn, and ORCID. The proxy is then responsible for enriching the identity information that comes from these external IdPs with additional attributes, including the following:

- a unique, persistent, non-reassignable user identifier (namely AARC ID, expressed as an eduPersonUniqueID attribute scoped at "@aarc-project.eu");
- assurance level (expressed as an eduPersonAssurance attribute);
- community membership roles and groups (expressed through eduPersonEntitlement attribute values).

Note that a user cannot access federated resources until they obtain an AARC ID through enrollment in the AARC Pilot User Community. In addition, we have defined a minimum set of attributes required for registering for an AARC ID. The SP-IdP proxy will attempt to retrieve these attributes from the user’s Home Organisation. If this is not possible, then the user will be asked to provide the missing attribute values and the request to join the collaboration will need to go through a verification process by the collaboration’s Sponsors.

Detailed description

A detailed description of the aim and approach of this pilot and how it maps to the AARC Blueprint Architecture is available here

Demonstration portal

For the purpose of this pilot, we have enabled federated access to the dashboard of a demo OpenStack Cloud deployment. Specifically, the pilot IdP proxy has been configured to authenticate users and communicate the result of the authentication to OpenStack’s Identity service (Keystone) using SAML assertions. The SAML assertions are then mapped to keystone user groups, based on which, the authenticating user can access cloud resources using their federated AARC ID.

Registration/Login Workflow
1. Access OpenStack's Dashboard (Horizon) at https://am02.pilots.aarc-project.eu/horizon

2. Click **Connect** and select your Identity Provider from the discovery page (WAYF). You may select any of the following options:
   - Institutional IdP: **AARC DIY Identity Provider** (considered an institutional IdP for demo purposes only)
   - Social IdPs: **Facebook**, **Google**, **LinkedIn**
   - **ORCID**
3. Enter your login credentials to authenticate yourself with the IdP of your Home Organisation (e.g. Google)

4. After successful authentication, you may be prompted by your Home Organisation to consent to the release of personal information to the EGI AAI Service Provider Proxy.

5. On the EGI AAI Consent about releasing personal information page, click Yes, continue to consent to the release of personal information to the EGI User Account Registry. If you select the Remember option, your browser will remember your choice unless you clear your cookies or restart the browser.

6. If this is your first time logging in, you will be redirected to the AARC Pilot User Community Sign Up page after successful authentication. Alternatively, you may access the sign up page directly by visiting:

   https://aai-dev.egi.eu/join-aarc
1. Depending on the LoA and/or attributes released by your Home IdP, there are two sign up workflows:

   1. If the LoA is substantial and all required attributes are released: **Self-service Sign Up** (typically for users coming from eduGAIN IdPs, or the AARC DIY Identity Provider for the purpose of this demo)
   2. If the upstream IdP cannot provide all attributes, or the LoA is low: **Approval-based Sign Up**. For example, in the case of Social IdPs the Affiliation Attribute will be missing; thus, you will be asked to provide any missing attribute values yourself.

8. On the registration form, click **Review Terms and Conditions**

9. If you agree to the Terms of Use, select the **I Agree** option. **Important:** You will not be able to agree to the terms until you review them!
Finally, click **Submit** to submit your request. **Important:**
You will not be able to submit your request until you agree to the terms!

After submitting your request, you will receive an email with a verification link in it. After you click that link, you'll be taken to the request confirmation page.
After reviewing your request, click Confirm and re-authenticate yourself using the Identity Provider you selected in Step 2.

If your sign up request requires approval (see Step 7), the Sponsor(s) of the VO will be notified via email. You will need to wait for a Sponsor to approve your request to join the AARC Pilot User Community. Upon approval, you will receive a notification email.
After your registration has been completed, you can manage your profile through the Account Registry portal at https://aai-dev.egi.eu/registry

Relogin to OpenStack's dashboard at https://am02.pilots.aarc-project.eu/horizon. You will be mapped to a Keystone user group based on the values of the eduPersonEntitlement attribute

Identity Linking Workflow

Identity linking allows users to access federated resources with their existing personal AARC ID, using any of the login credentials they have linked to their account. To link a new organisational or social identity to your AARC account:
1. Enter the following URL in a browser: https://aai-dev.egi.eu/registry

2. Click **Login** and authenticate using any of the login credentials already linked to your AARC account

3. Navigate to **My AARC Pilot User Community Account** page in any of the following ways:
   - hover over your display name next to the gear icon on the top right corner of the page;
   - or, alternatively,
   - select **AARC Pilot User Community** from the list of available Collaborations and then click **My AARC Pilot User Community Account** from the **People** menu

4. Under the **Organisational Identities** section of your profile page, click **Link New Identity**.

5. On the introductory page for Identity Linking, click **Begin**

6. On the Link New Identity form, click **Review Terms and Conditions**
7. After reviewing the Terms and Conditions, click **OK**.

<table>
<thead>
<tr>
<th>GRID ACCEPTANCE USE POLICY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last updated:</strong> 8 Jul 2016</td>
</tr>
<tr>
<td>The Grid Acceptable Use Policy (&quot;GAUP&quot;) defines the terms and conditions (the &quot;Terms and Conditions&quot;, or &quot;Conditions of Use&quot;) that have to be accepted by all users (the &quot;Users&quot;) during their registration as a user of the Grid. Please read these terms and conditions carefully before using the EGI AAI (the &quot;Service&quot;) operated by EGI.eu (&quot;us&quot;, &quot;we&quot;, or &quot;our&quot;). By using the Service, you agree to the latest version of the GAUP (<a href="https://documents.egi.eu/document/74">https://documents.egi.eu/document/74</a>).</td>
</tr>
<tr>
<td><strong>GRID ACCEPTANCE USE POLICY</strong></td>
</tr>
<tr>
<td>By registering as a Grid user you shall be deemed to accept these Conditions of Use:</td>
</tr>
<tr>
<td>1. You shall only use the Grid to perform work, or transmit or store data consistent with the stated goals, policies and conditions of use as defined by the body or bodies granting you access.</td>
</tr>
<tr>
<td>2. You shall not use the Grid for any unlawful purpose and not (attempt to) breach or circumvent any Grid administrative or security controls.</td>
</tr>
<tr>
<td>3. You shall respect intellectual property and confidentiality agreements.</td>
</tr>
<tr>
<td>4. You shall protect your access credentials (e.g. private keys or passwords).</td>
</tr>
<tr>
<td>5. You shall immediately report any known or suspected security breach or misuse of the Grid or access credentials to the incident reporting locations specified by the Grid and to the relevant credential issuing authorities.</td>
</tr>
<tr>
<td>6. You must notify the Registrar of any changes to your Registration Information.</td>
</tr>
<tr>
<td>7. Use of the Grid is at your own risk. There is no guarantee that the Grid will be available at any time or that it will suit any purpose.</td>
</tr>
<tr>
<td>8. Logged information, including information provided by you for registration purposes, is used for administrative, operational, accounting, monitoring and security purposes only. This information may be disclosed, via secured mechanisms, only for the same purposes and only as necessary to other organisations cooperating with the Grid. Although efforts are made to maintain confidentiality, no guarantees are given.</td>
</tr>
<tr>
<td>9. The access-granting bodies and Resource Providers are entitled to regulate, suspend or terminate your access, within their domain of authority, and you shall immediately comply with their instructions.</td>
</tr>
</tbody>
</table>

8. If you agree to the Terms and Conditions, select the **I Agree** option. **Important:** You will not be able to agree to the terms until you review them.

<table>
<thead>
<tr>
<th>Agree to Terms and Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>You must agree to the following Terms and Conditions before continuing.</td>
</tr>
<tr>
<td>You must review the T&amp;C before you can click I Agree, and you must agree before you can submit.</td>
</tr>
<tr>
<td><strong>I Agree</strong></td>
</tr>
<tr>
<td>* denotes required field</td>
</tr>
</tbody>
</table>

9. Finally, click **Submit** to submit your request. **Important:** You will not be able to submit your request until you agree to the terms.
After submitting your request, you will receive an email with a link in it. After you click that link, you’ll be taken to the Link New Identity confirmation page.

On the Link New Identity confirmation page, click Confirm.

After confirmation, you will need to sign in using the login credentials from the Institutional/Social Identity Provider you want to link to your account.
1. After successful authentication, you'll be able to access federated resources with your existing personal AARC ID using the login credentials of the Identity Provider you selected in the previous step.

2. You've been logged out successfully.

Components

- SimpleSAMLphp (version 1.14.5)
  - simplesamlphp-module-openidconnect (commit affb54a)
  - simplesamlphp-module-authfacebook (commit d8dc33c)
  - simplesamlphp-module-authlinkedin (branch rc/authlinkedin)
  - simplesamlphp-module-authorcid (master branch)
- COmanage Registry (version 1.0.4)
- Shibboleth (Service Provider version 2.5.3)
- Memcached (version 1.4.21)
- PostgreSQL (9.4)
- OpenStack