EISCAT 3D user authentication and authorization

Carl-Fredrik Enell

EISCAT Scientific Association

User meeting 16 Dec 2020
AA(A)I
Who is trying to access our data?

AA(A)I = Infrastructure for

1. **Authentication**: Who is the user? Identity
2. **Authorization**: Grant access to resources depending on who the user is
3. (Accounting: e.g. who has downloaded what)
Authentication
EISCAT 3D users

- EU
- China
- Japan
- US
- etc
User IDs

Who is the user

- A chain of trust
- Identity providers
  - Ultimately responsible for providing user credentials
  - Different Levels of Assurance (LoA)

Examples of ID providers

- Institutional IDs
- Social logins
- Google account
- OrcID
Connecting to ID providers: EGI Checkin as ID proxy

Figure 1: EGI Checkin, the big picture
Figure 2: Checkin login page
Figure 3: Checkin account page
<table>
<thead>
<tr>
<th>Identity Provider</th>
<th>URL</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRF</td>
<td><a href="https://idpshibboleth.irt.se/idp/shibboleth">https://idpshibboleth.irt.se/idp/shibboleth</a></td>
<td>epuid</td>
</tr>
<tr>
<td>OrcID</td>
<td><a href="https://aai.egi.eu/orcid/sam12/idp/metadata.php">https://aai.egi.eu/orcid/sam12/idp/metadata.php</a></td>
<td>epuid</td>
</tr>
<tr>
<td>Github</td>
<td><a href="https://aai.egi.eu/github/sam12/idp/metadata.php">https://aai.egi.eu/github/sam12/idp/metadata.php</a></td>
<td>epuid</td>
</tr>
<tr>
<td>Google</td>
<td><a href="https://aai.egi.eu/google/sam12/idp/metadata.php">https://aai.egi.eu/google/sam12/idp/metadata.php</a></td>
<td>epuid</td>
</tr>
<tr>
<td>Linkedin</td>
<td><a href="https://aai.egi.eu/linkedin/sam12/idp/metadata.php">https://aai.egi.eu/linkedin/sam12/idp/metadata.php</a></td>
<td>epuid</td>
</tr>
</tbody>
</table>

Figure 4: Carl-Fredrik’s IdPs
Authenticating via EGI Checkin

Figure 5: Checkin ID provider selection
Figure 6: IRF Shibboleth login page
https://docs.egi.eu/users/check-in/
Authorization
Can we grant access to this user?

- Capability based authorization
  - E.g. list of resources
- User attribute based authorization
  - E.g. Virtual Organization group membership
User attributes — Perun and VOs

VOs

- Virtual Organization
  - One for EISCAT eiscat.se (our domain name)
- VO Roles
  - VO Manager
  - VO Group manager
  - ...
- Virtual Organization groups
  - Membership = User attribute
  - EISCAT Associates and Affiliates
  - Subgroups possible

VO management

- Perun https://perun-aai.org/
Figure 7: Login page of EGI Perun instance
Figure 8: Perun VO management
### Figure 9: Groups defined in Perun: EISCAT members

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>members</td>
<td>Group containing VO members for VO eiscat.se</td>
</tr>
<tr>
<td>CN</td>
<td>EISCAT P.R. China CRiRP</td>
</tr>
<tr>
<td>CN:Experiments</td>
<td>Users who can submit experiment requests</td>
</tr>
<tr>
<td>Dev</td>
<td>System developers</td>
</tr>
<tr>
<td>DLRSO</td>
<td>EISCAT DLR-SO Germany</td>
</tr>
<tr>
<td>DLRSO:Experiments</td>
<td>Users who can submit experiment requests</td>
</tr>
<tr>
<td>Ei</td>
<td>EISCAT internal</td>
</tr>
<tr>
<td>FI</td>
<td>EISCAT Finland SA</td>
</tr>
<tr>
<td>FI:Experiments</td>
<td>Users who can submit experiment requests</td>
</tr>
<tr>
<td>JHUAPL</td>
<td>EISCAT Johns Hopkins University US</td>
</tr>
<tr>
<td>JHUAPL:Experiments</td>
<td>Users who can submit experiment requests</td>
</tr>
</tbody>
</table>
Perun groups, example of members

Figure 10: Group members: Developer group
Figure 11: Group managers: Assigned manager of SE group
EISCAT workflow in a nutshell

User

EISCAT Portal

Access attributes for authorization

User registered?

Yes

VO group attributes available?

Yes

EGI Checkin

No

Signup

ID linking

Link another ID?

Yes

User registered?

No

Email verification procedure (for some ID providers)

ID providers

Message(s) to group manager(s)

− Group manager logs in to Perun
− Group manager verifies ID of user
− Group manager rejects request or adds user to group

Perun enrolment

User registered? (for some ID providers)

No

Yes

Email verification

Yes

No
Regular mini workshops

- On Zoom
- So far, participation from
  - EGI
  - GRNET
  - U Oulu + SGO
  - IRF
- Welcome to join! Next meeting TBD