SYNC&SHARE FEDERATION FOR HELMHOLTZ
Challenges, solutions and outlook
## Initial Service Portfolio

<table>
<thead>
<tr>
<th>Services</th>
<th>Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenStack</td>
<td>Jülich, Jülich (HDF), KIT, DKFZ</td>
</tr>
<tr>
<td>Storage (HDF)</td>
<td>Jülich, DESY</td>
</tr>
<tr>
<td>HAICORE (HAICU, HIP)</td>
<td>KIT, Jülich</td>
</tr>
<tr>
<td>Singularity</td>
<td>KIT, Jülich</td>
</tr>
<tr>
<td>Docker</td>
<td>DESY</td>
</tr>
<tr>
<td>GPU Compute Service</td>
<td>Jülich, HZDR</td>
</tr>
<tr>
<td>AWI Marketplace</td>
<td>AWI</td>
</tr>
<tr>
<td>GitLab</td>
<td>HZDR, KIT, Jülich, GEOMAR</td>
</tr>
<tr>
<td>JupyterHub</td>
<td>Jülich, DESY, DKFZ, HMGU</td>
</tr>
<tr>
<td>B2Share (Invenio)</td>
<td>Jülich</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Services</th>
<th>Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>JupyterHub Notebooks on HPC</td>
<td>KIT</td>
</tr>
<tr>
<td>ODV</td>
<td>AWI</td>
</tr>
<tr>
<td>RODARE</td>
<td>HZDR</td>
</tr>
<tr>
<td>Ocean and Climate Sensor Management</td>
<td>AWI</td>
</tr>
<tr>
<td>Rocket.Chat</td>
<td>Jülich</td>
</tr>
<tr>
<td>Zammad</td>
<td>HZDR</td>
</tr>
<tr>
<td>Mattermost</td>
<td>HZDR</td>
</tr>
<tr>
<td>Nextcloud</td>
<td>KIT, HZB, DESY</td>
</tr>
<tr>
<td>LimeSurvey</td>
<td>HMGU, DKFZ</td>
</tr>
<tr>
<td>Redmine</td>
<td>HZDR, HMGU</td>
</tr>
<tr>
<td>ShareLaTex</td>
<td>HZDR</td>
</tr>
</tbody>
</table>
The environment we operate in

- Over 42,000 Employees
- 18 completely independent legal entities
- 18 data protection officers
- 18 employee representatives
- 18 information security officers
Existing Sync&Share instances

- 9 Centers without local Sync&Share instance
- 9 Centers operate Sync&Share instances
  - Currently, 4 of them want to offer it on Helmholtz Cloud
    - For all of Helmholtz and external project partners
    - Federation, not Consolidation
• IdM via Helmholtz AAI
  • eduGAIN based Identity proxy
    • Also contains social IdPs
  • generating authoritative eduPersonUniqueIDs
  • VO management
  • Uses SAML2 and OIDC

• VOs are transmitted to S&S via custom SAML2 attribute
  • Format: VO#login.helmholtz.de

• AAI currently manages authorization for Sync&Share

• Policies built on WISE & AARC
IDENTITY MANAGEMENT

Providing Sync&Share to every user

WHAT WORKS

- Providing Sync&Share to whole centers without own instance

WHAT DOESN’T WORK

- Providing Sync&Share to VOs
- Results in user account redundancy over multiple instances
FEDERATION

Use cases

▪ We will try to federate all Helmholtz Sync&Share instances
  ▪ Later on: Integrate the federation with other HIFIS Service types

POSSIBLE ISSUES

▪ Large trend in VOs to work in group-based folders and calendars
  ▪ Opportunities:
    ▪ VO based quota management
    ▪ Data not bound to users

▪ Collaboration in shared files across instances needs to be possible

▪ Data protection in federation is tricky
  ▪ Protection of sensible user groups on Instances cannot be provided (e.g. Students on KIT instance)
Use cases: Technical solutions are needed

- Sync&Share instances need to recognize federation-spanning VOs
- Avoid data redundancy with group folders beyond group-based OCM sharing
- Shared files should always be opened on the sharers Office application
- Nextcloud Global Scale
  - Free-Software, but only applicable with vendor-support within bigger installations
  - Integrating lookup-Server with Helmholtz AAI is challenging
  - Does it work with other Sync&Share vendors?
- Data Protection: Allow selection on which users/groups will be shared in Federation
Data protection in a trusted environment

HIFIS Contract between all centers

- Also deals with privacy
- Contains Helmholtz AAI policies
- Emphasis on remaining open to other organizations
- Minimizing paperwork, maybe even data processing agreements
FURTHER READING

HIFIS Website:
https://hifis.net

HIFIS documentation:
https://hifis.net/doc

HIFIS Initial Service Portfolio
https://hifis.net/doc/service-portfolio

Helmholtz AAI Policies:
https://hifis.net/doc/backbone-aai/policies

AARC Blueprint VoPerson Schema:
https://github.com/voperson/voperson/blob/master/voPerson.md

AARC Guidelines:
https://aarc-project.eu/guidelines/