HELMHOLTZ

RESEARCH FOR
GRAND CHALLENGES

HIFIS | HELMHOLTZ FEDERATED IT SERVICES

Helmholtz-AAI

Marcus Hardt (on behalf of the HIFIS AAI Task)

March 2021

Organisation

- Helmholtz-AAI - Driven and maintained by HIFIS
  - Operated by FZ-Jülich
  - Developed by KIT, FZJ and Unity Developers
  - **Long term commitment** for operation via Helmholtz Programme
- Tailored for needs of Helmholtz
  - Still: **General Approach** (no specific organisational structure imposed)

Technical Basis

Integration

- Multiple solutions from different sectors integrated
  - Europe: AARC Blueprint Architectures + Policies
    - Compatible with EOSC
  - HPC: Integration of b2access
  - Germany: DFN-AAI (and its implied assurance)
  - Baden-Württemberg-IDM: Home-IdP based authorisation
- => Ensure state-of-the-art AAI for researchers

Helmholtz-AAI Instance

- Helmholtz-AAI implements a **Community AAI**
  - Supporting international collaboration (by enabling eduGAIN
  - Connects services
    - Directly
    - Via “Infrastructure Proxies”
- Based on Unity (b2access)
- Support for **web and non-web**
  - Web Applications
  - REST APIs
  - Delegation scenarios
- Available at https://login.helmholtz.de

Assurance

- We support **explicit assurance**
- Levels of Assurance according REFEDS Assurance Framework
  - via decoding implicit federation information (e.g. DFN-AAI-Member)
  - via explicit definition at home IdP
- Allows services to distinguish users
  - Passport seen
  - Work contract available
  - Member of Home Organisation
  - Social Media
- Used at Provisioning Services:
  - Feudal, Local-Agent
- Benefit
  - AAI can host “lesser-than-maximum” users
  - Scientists only need to upgrade their identity, if necessary to access service

Authorisation

- Integration of two concepts:
- Virtual Organisation approach
  - VOs are managed centrally in the AAI
  - VOs are managed by decentral PIs
  - *Automatic VO*: Each user is a member of a VO that corresponds to the Home-Organisation
- **Home-IdP based** approach
  - Home IdP can assert complementary information
  - Employee / Student / Guest
  - Home-Org may assert users eligibility to use certain resources (BW use case)

Customer Perspectives

Benefits for Services

- Services have **full control about authorisation** decision:
  - **Straightforward integration**
  - Multi protocol approach: SAML, OIDC (even X.509)
  - Guaranteed attribute release
  - Precise attributes about users (Assurance, Authorisation, Home-Org, ...)
  - Easily distinguish
    - Helmholtz / non-Helmholtz users
    - Student / Staff
    - Scientific User / Social IdP
    - Passport-vetted, ...

More benefits for Services

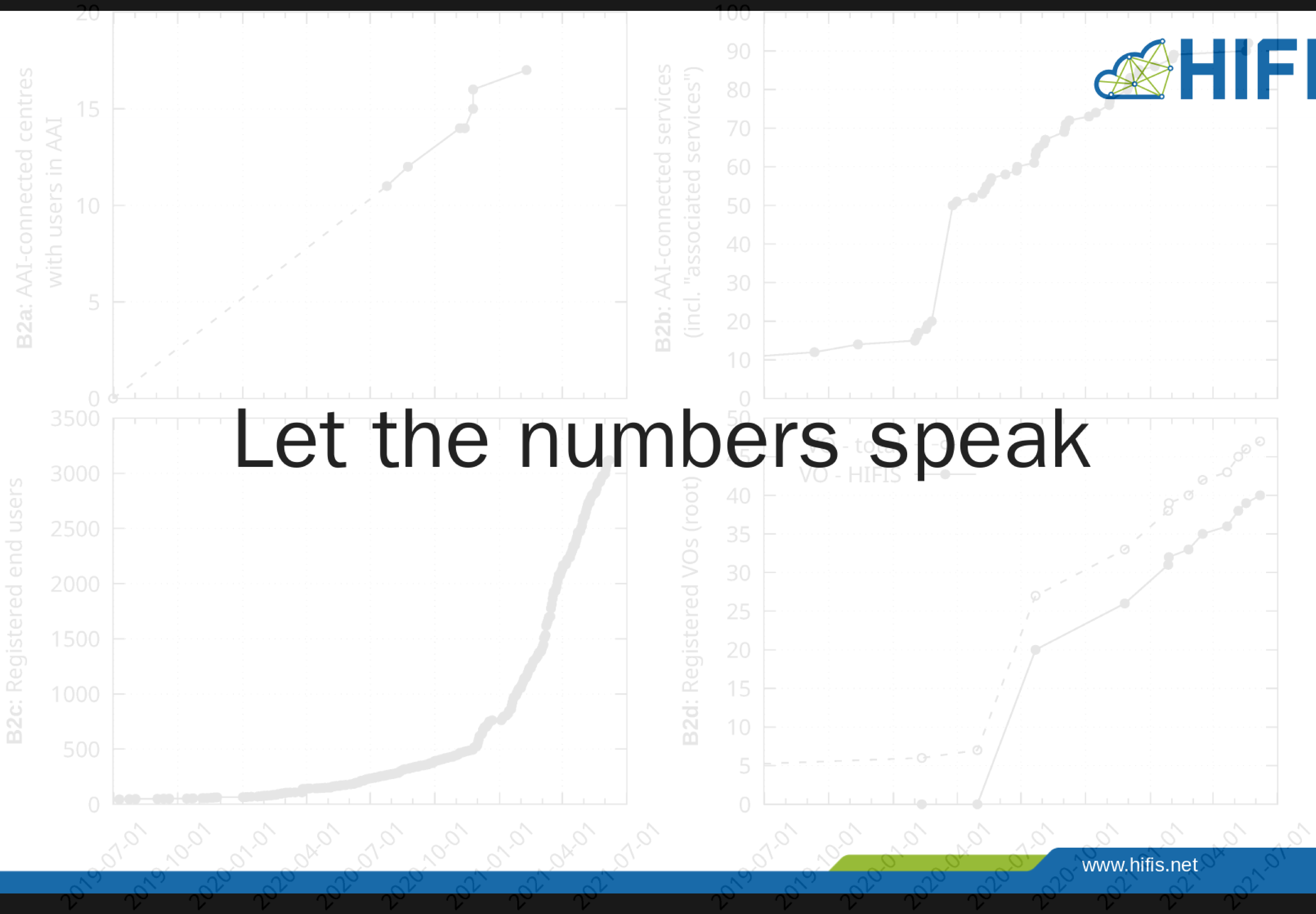
- Standards Compliance
  - Attributes comply with AARC / AEGIS recommendations
  - => Services may support Helmholtz-AAI next to other AAIs
- Non-web extends spectrum of available services
  - Delegation + API-Access
    - Opens gate to new world of computing (from a SAML perspective)

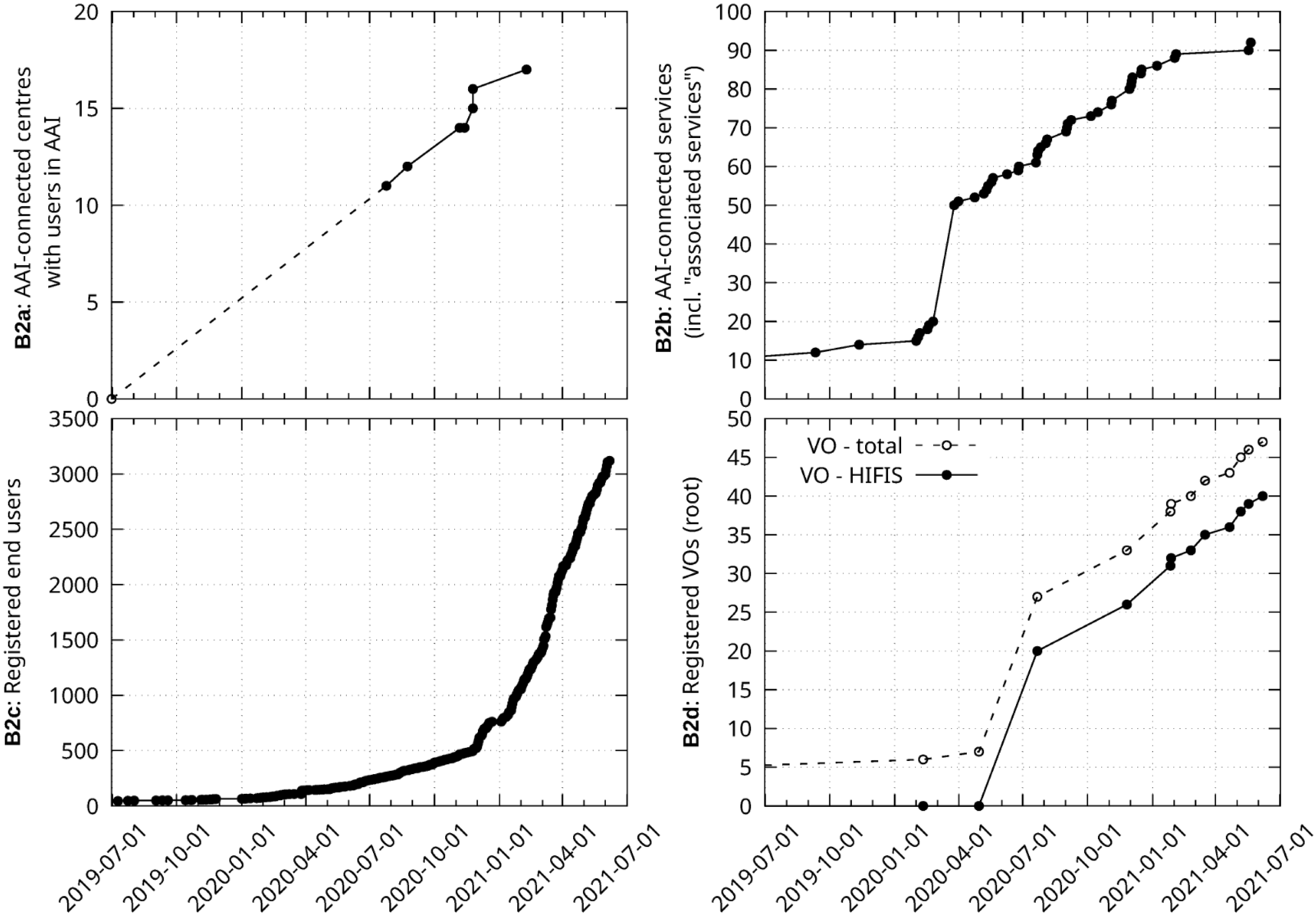
List of connected services: https://aai.helmholtz.de/services/

Benefits for Users

- Easy-Access to a wealth of services
  - Compute: OpenStack, Kubernetes, JupyterHub
  - Storage: dCache, FTS,
  - Tools: GitLabs, NextClouds, Rocketchat, Mattermost, Helpdesk, ...
  - Account Provisioning: RegAPP/FeLS, Feudal
  - Development: OIDC-Agent, Orpheus, ...
- Virtual Organisations allow **self management** of groups
  - Traditionally, a lot more difficult
- Driver for sharing data and computing with peers

Let the numbers speak




B2a: AAI-connected centres with users in AAI
0
5
10
15
20
B2b: AAI-connected services (incl. "associated services")
0
10
20
30
40
50
60
70
80
90
100
B2c: Registered end users
0
500
1000
1500
2000
2500
3000
3500
B2d: Registered VOs (root)
0
5
10
15
20
25
30
35
40
45
50
VO - total
VO - HIFIS
2019-07-01
2019-10-01
2020-01-01
2020-04-01
2020-07-01
2020-10-01
2021-01-01
2021-04-01
2021-07-01

Developments from Helmholtz-AAI

- Provisioning of accounts
  - FEUDAL
  - SSH with OIDC Tokens
  - 2nd Factor SSH
- Deprovisioning
  - Inform interested services
  - Today: VO based
  - Future: Home-Org based

General Remarks

- Helmholtz-AAI is
  - Free of charge
  - Long term funded
  - Used by **30+ services**, and **3000+ users**
- Managing Risk:
  - Some initiatives consider building their own AAI
  - Risk of fragmentation
    - User identity is different per Community
    - Cross Community Access is not specified by AARC yet

HIFIS

https://aai.helmholtz.de