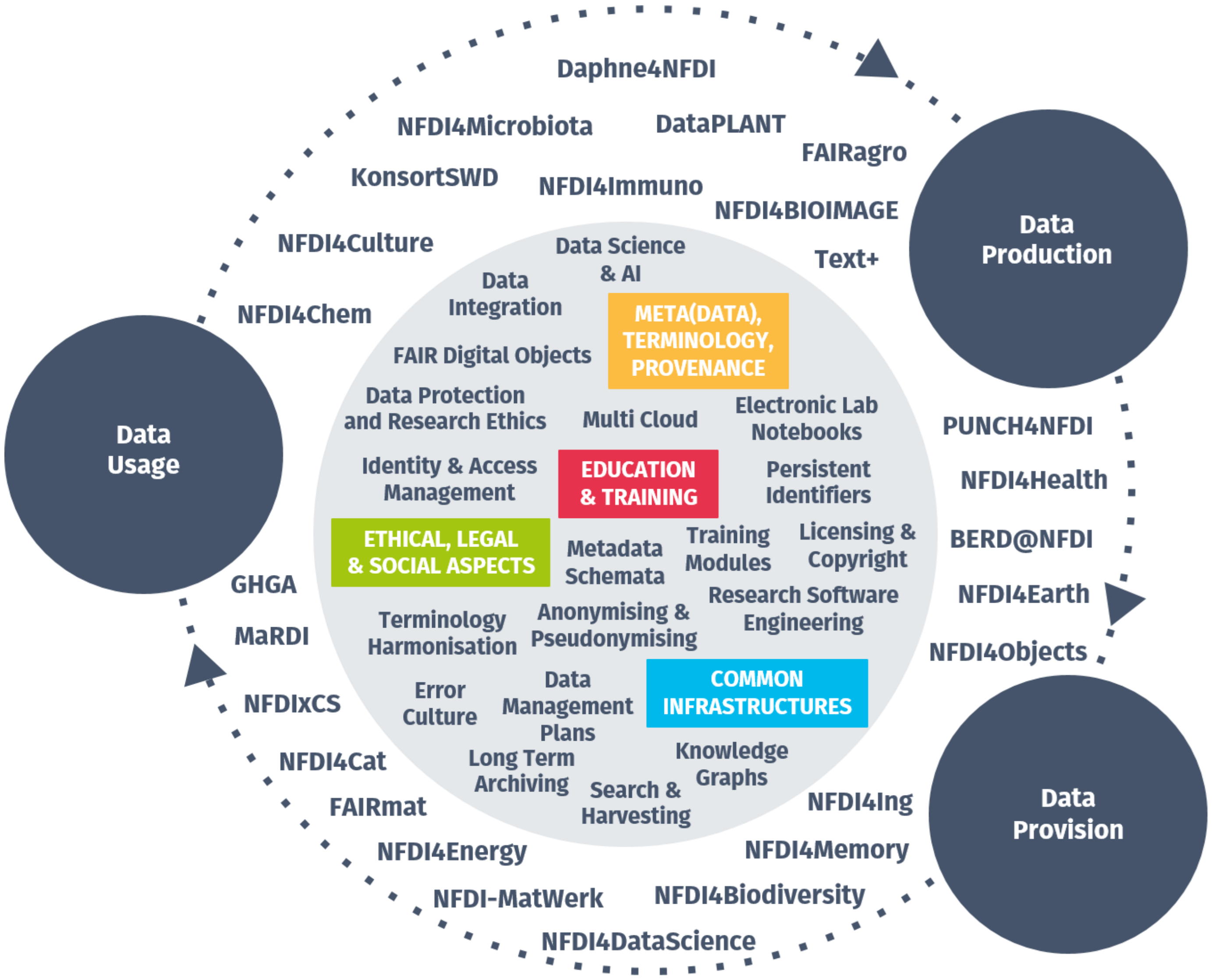
Basic Services for NFDI

IAM4NFDI – Identity Management Service for NFDI

Sander Apweiler, Matthias Bonn, Peter Gietz, Jacqueline Gottowik, Marcus Hardt, David Hübner, Thorsten Michels, Wolfgang Pempe, Christof Pohl, Marius Politze

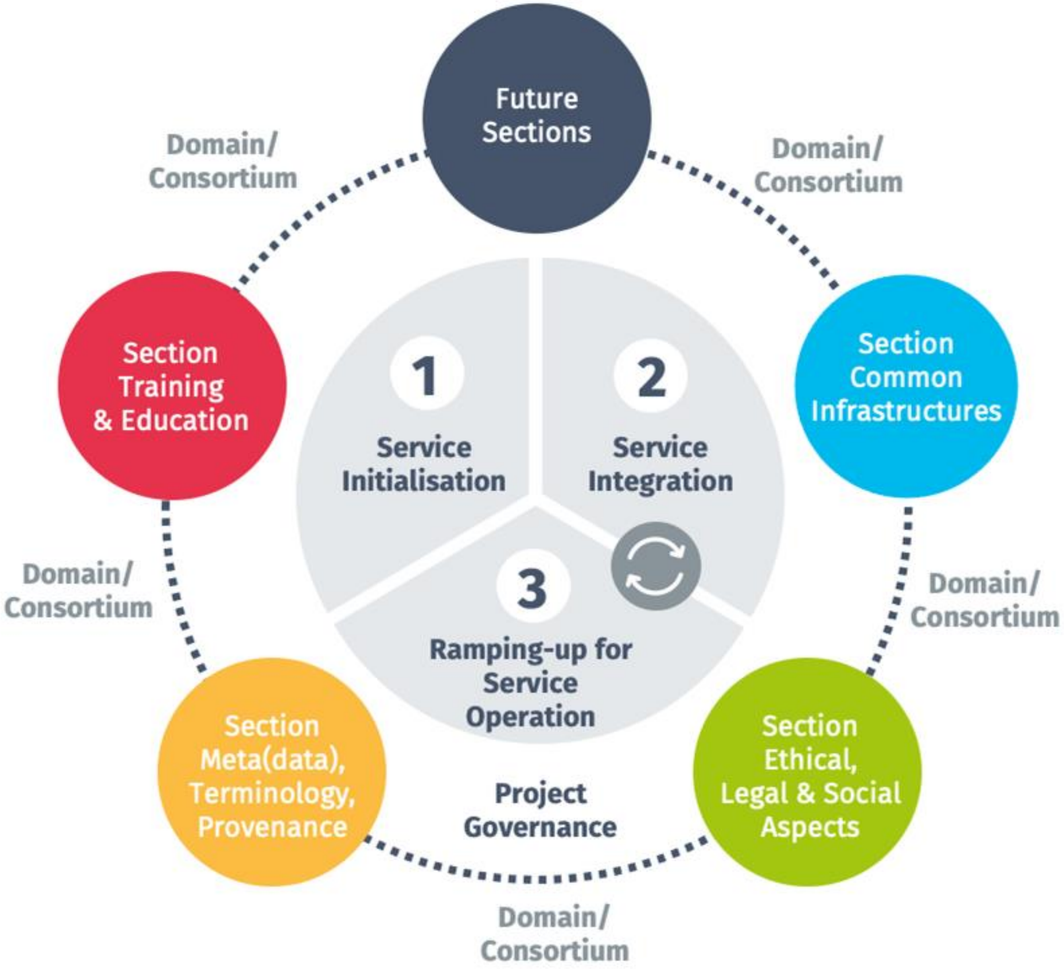


Funded by **DFG** as part of **NFDI**.
Grant Numbers: 521453681, 521460392, 521462155, 521463400, 521466146, 521471126, 521473512, 521474032, 521475185, 521476232

About Base4NFDI

What Base4NFDI will do

Translate needs & topics in basic services

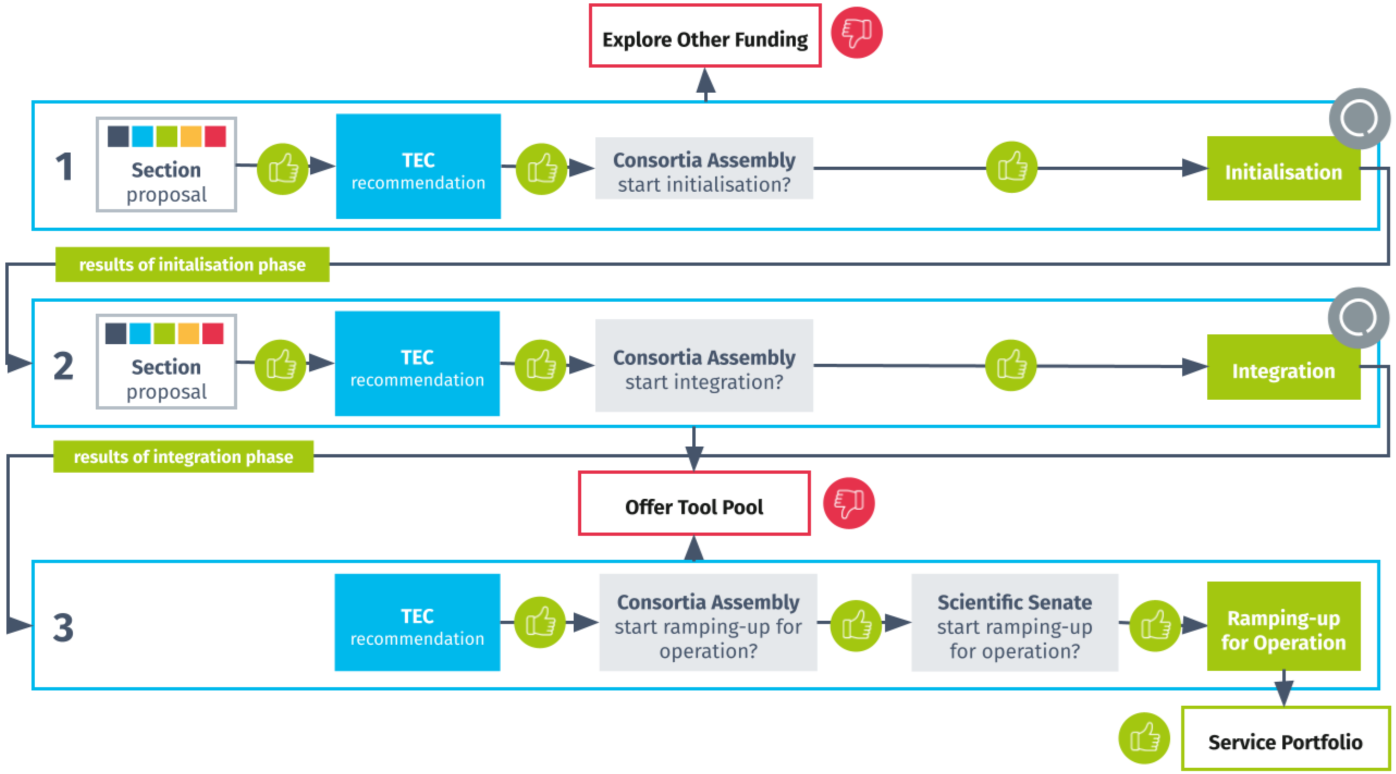

Future Sections
Domain/ Consortium
Domain/ Consortium
Section Training & Education
1
Service Initialisation
2
Service Integration
Section Common Infrastructures
3
Ramping-up for Service Operation
Domain/ Consortium
Domain/ Consortium
Section Meta(data), Terminology, Provenance
Project Governance
Section Ethical, Legal & Social Aspects
Domain/ Consortium

Base4NFDI provides the framework for

- defining potential basic services
- user-driven requirements analysis
- stepwise development for integrating and ramping-up basic service candidates
- setting up NFDI-wide basic service portfolio
- monitoring and evaluation
- transparent allocation of flexible funding
- consensus building

How Base4NFDI will decide
Tightly embedded in the NFDI Association

- Each development step is subject to evaluation and joint agreement on next steps
- Proposals are initiated and coordinated by NFDI Sections
- Proposals are evaluated by Technical Expert Committee (TEC), Consortia Assembly and Scientific Senate


Explore Other Funding
1
Section proposal
TEC recommendation
Consortia Assembly start initialisation?
Initialisation
results of initalisation phase
2
Section proposal
TEC recommendation
Consortia Assembly start integration?
Integration
results of integration phase
Offer Tool Pool
3
TEC recommendation
Consortia Assembly start ramping-up for operation?
Scientific Senate start ramping-up for operation?
Ramping-up for Operation
Service Portfolio

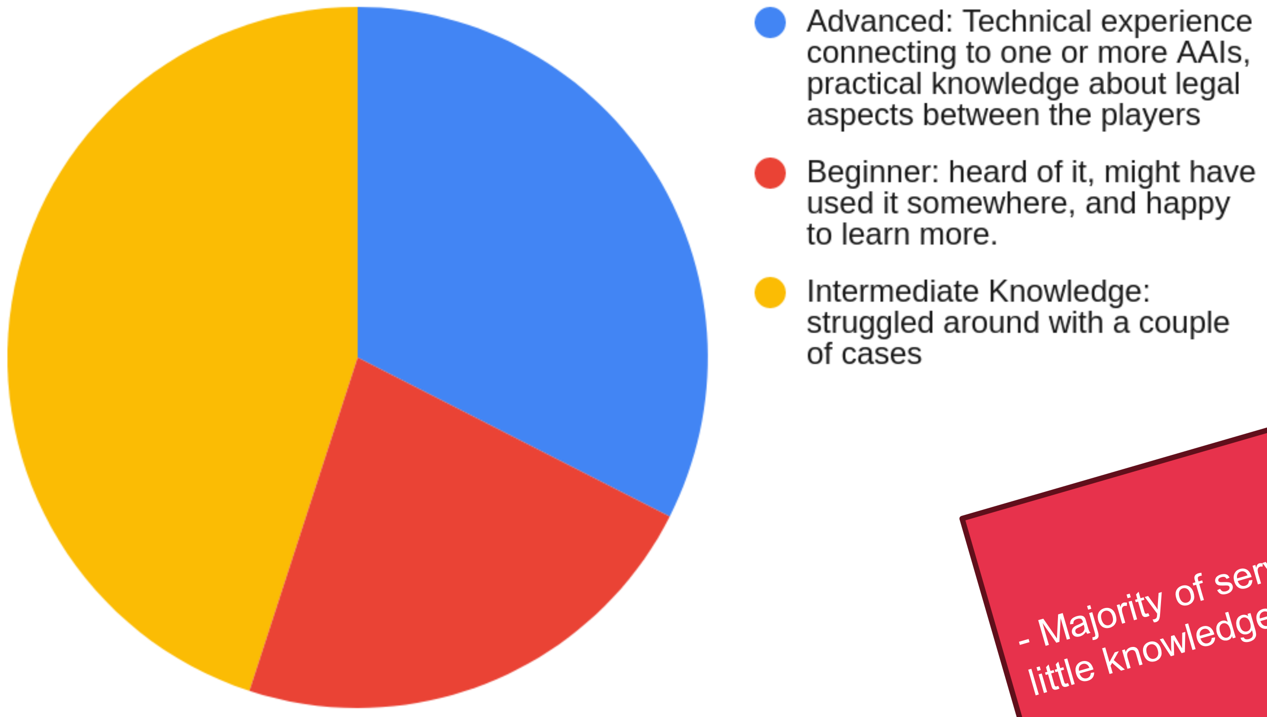
AAI Requirements Analysis

Selected questions from questionnaire run by WG IAM of NFDI Section Common Infrastructures in January 2022

All results https://docs.google.com/presentation/d/1sIXHiJybg7ewgCV53VoaeVgzlPNzfvv8AE6dYSoUNLw/edit

Requirements Analysis

Level of expertise in AAI



● Advanced: Technical experience connecting to one or more AAIs, practical knowledge about legal aspects between the players

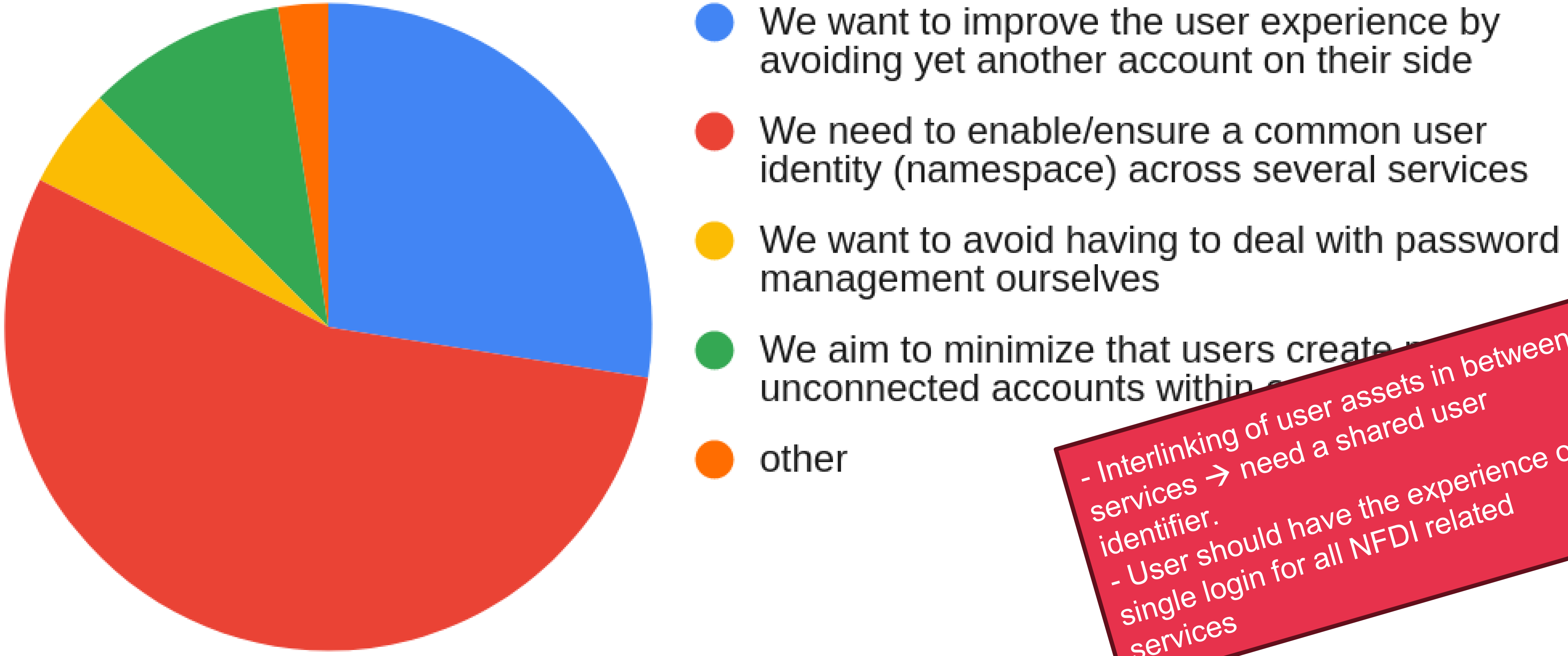
● Beginner: heard of it, might have used it somewhere, and happy to learn more.

● Intermediate Knowledge: struggled around with a couple of cases

- Majority of service providers have little knowledge about AAI!

Requirements Analysis

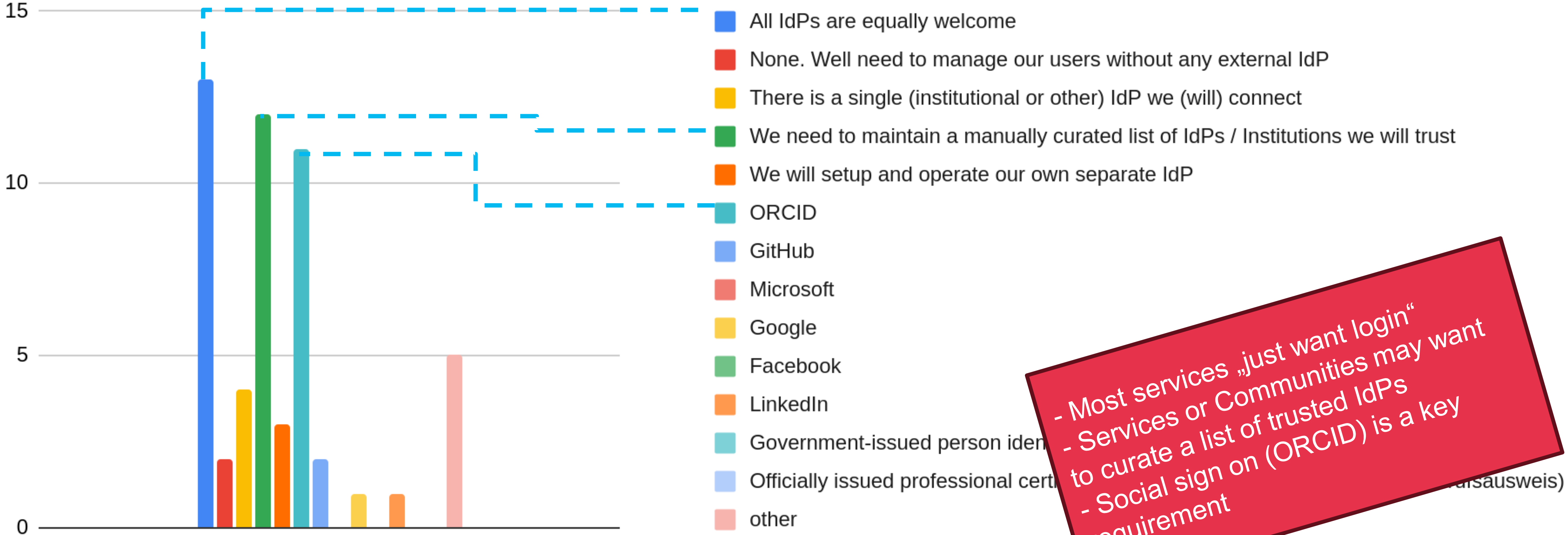
Why is your service interested in the Authentication aspects of AAI



- Interlinking of user assets in between services → need a shared user identifier.
- User should have the experience of a single login for all NFDI related services

Requirements Analysis

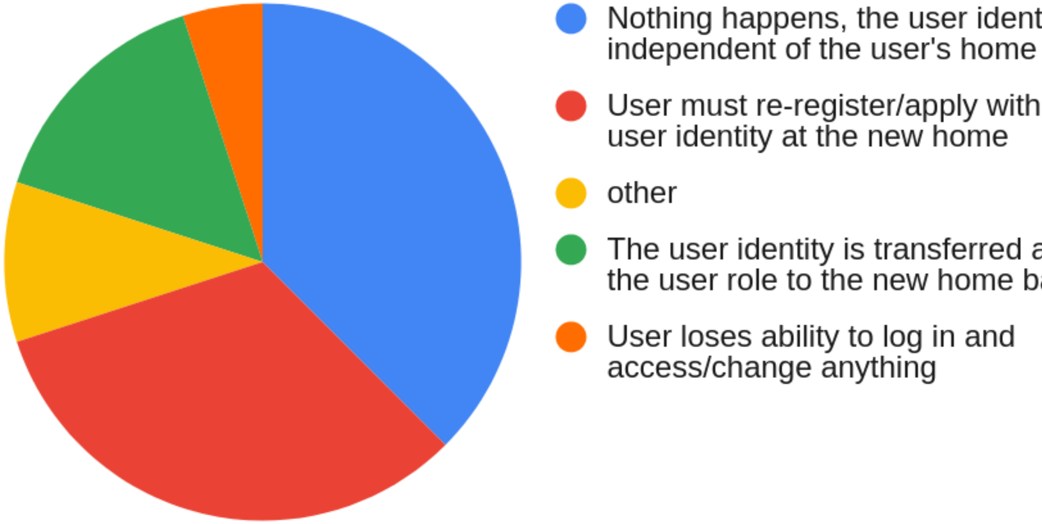
Preferred Identity provider for users

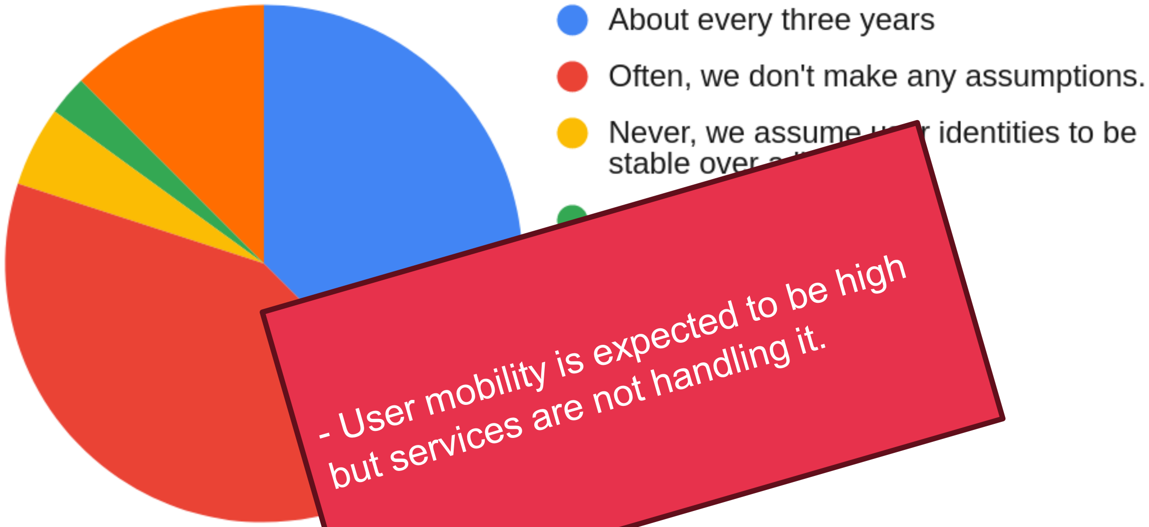


- Most services „just want login“
- Services or Communities may want to curate a list of trusted IdPs
- Social sign on (ORCID) is a key requirement

Requirements Analysis

Consequence and Frequency of user mobility

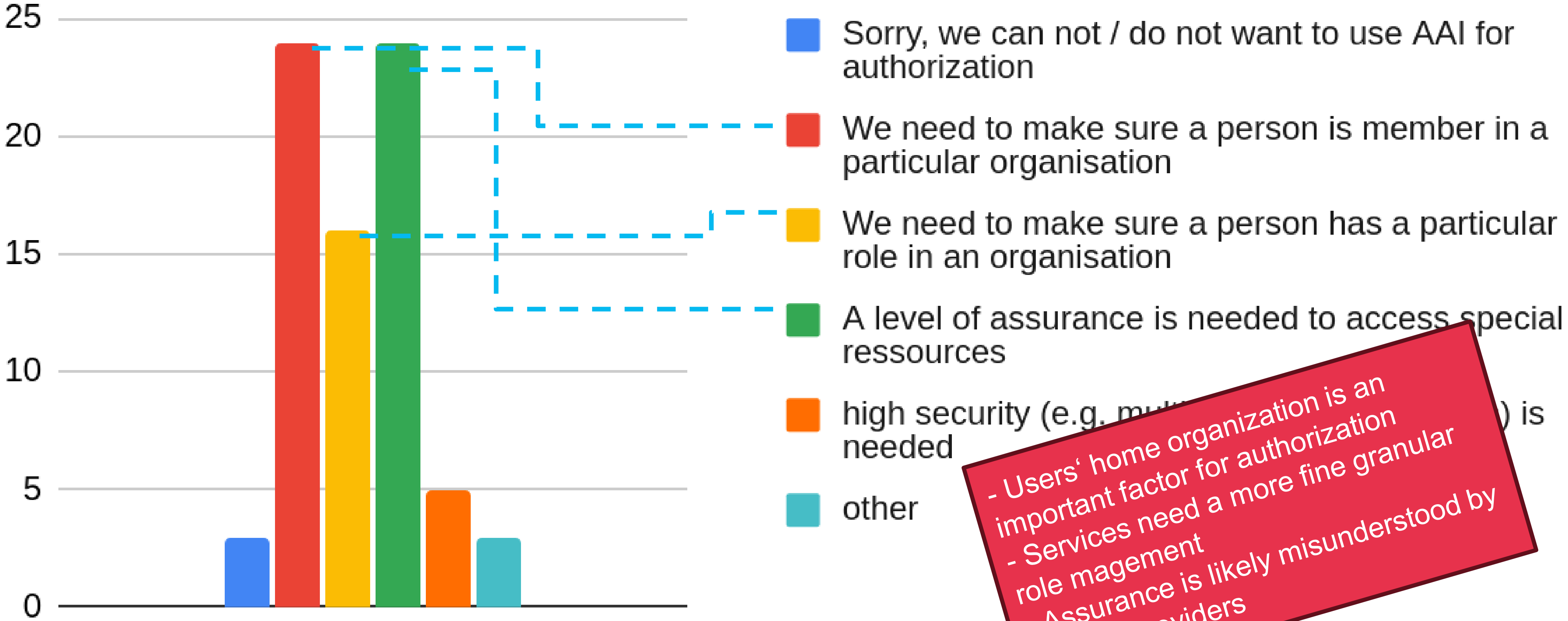




- User mobility is expected to be high but services are not handling it.

Requirements Analysis

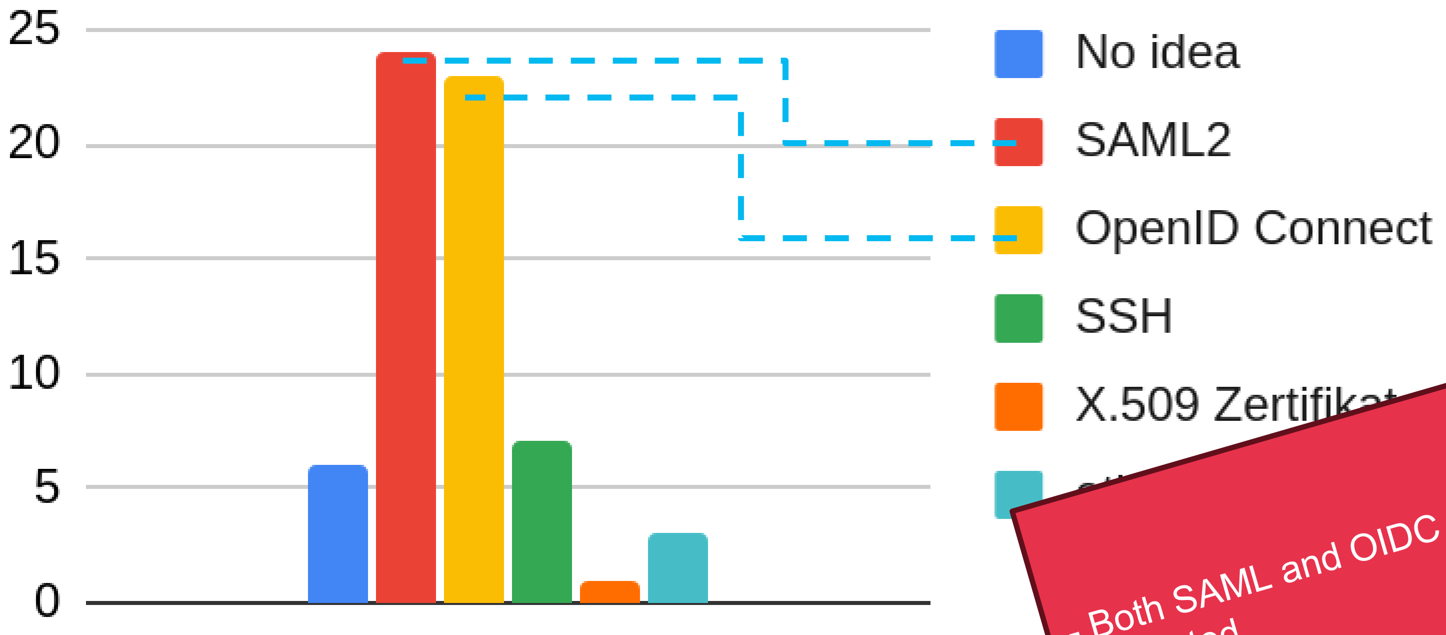
Why is your service interested in the Authorization aspects of AAI?



- Users' home organization is an important factor for authorization
- Services need a more fine granular role magement
- Assurance is likely misunderstood by service providers

Requirements Analysis

Which login standards / protocols are being used



- Both SAML and OIDC need to be supported

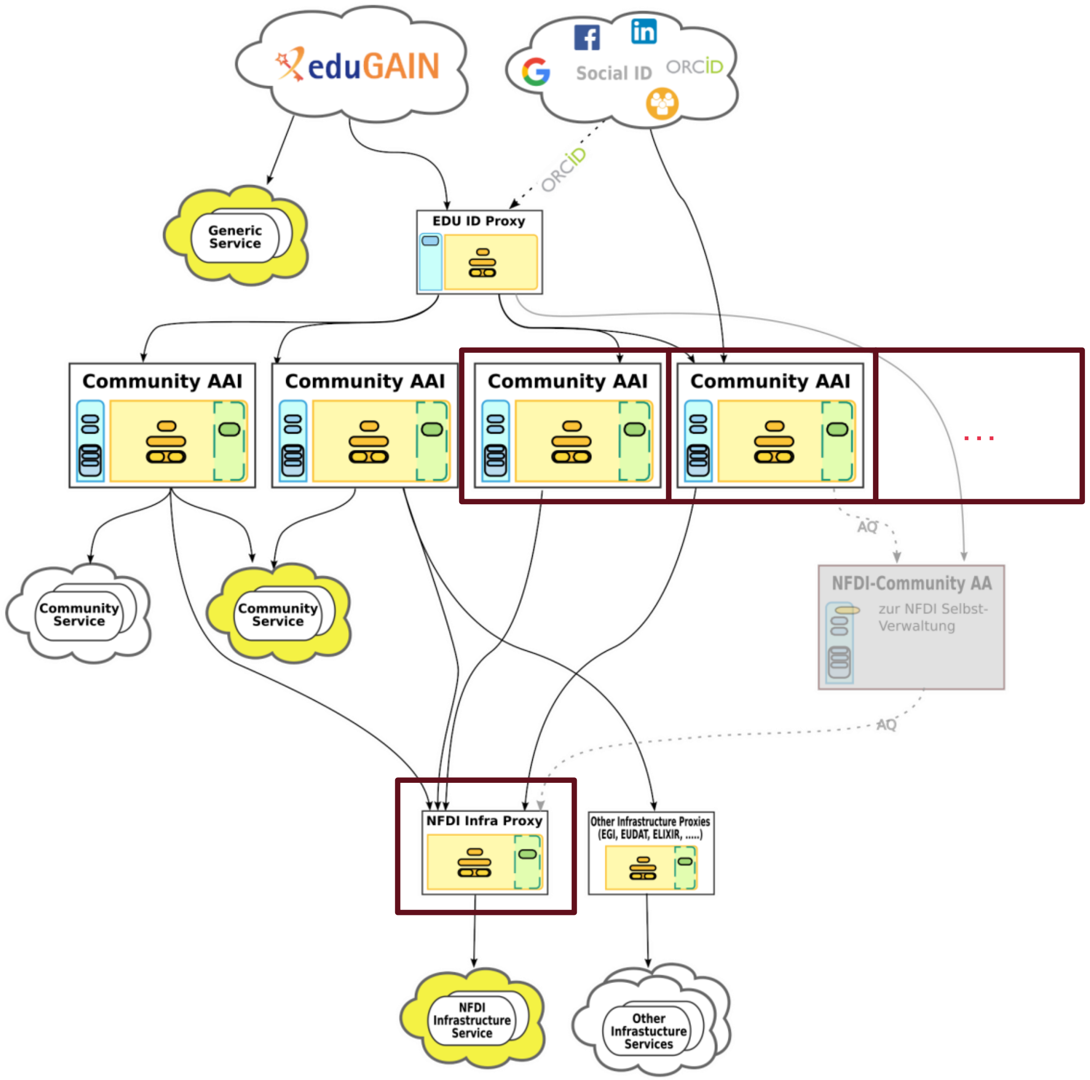
IAM4NFDI

Goals and Structure

- Provide state of the art IAM to all NFDI Consortia
- Use home organisation identity
- Enable delegated group management (Virtual Organisations)
- Open for NFDI and beyond
- Compatible with AARC / EOSC
- Community AAI as a Service!

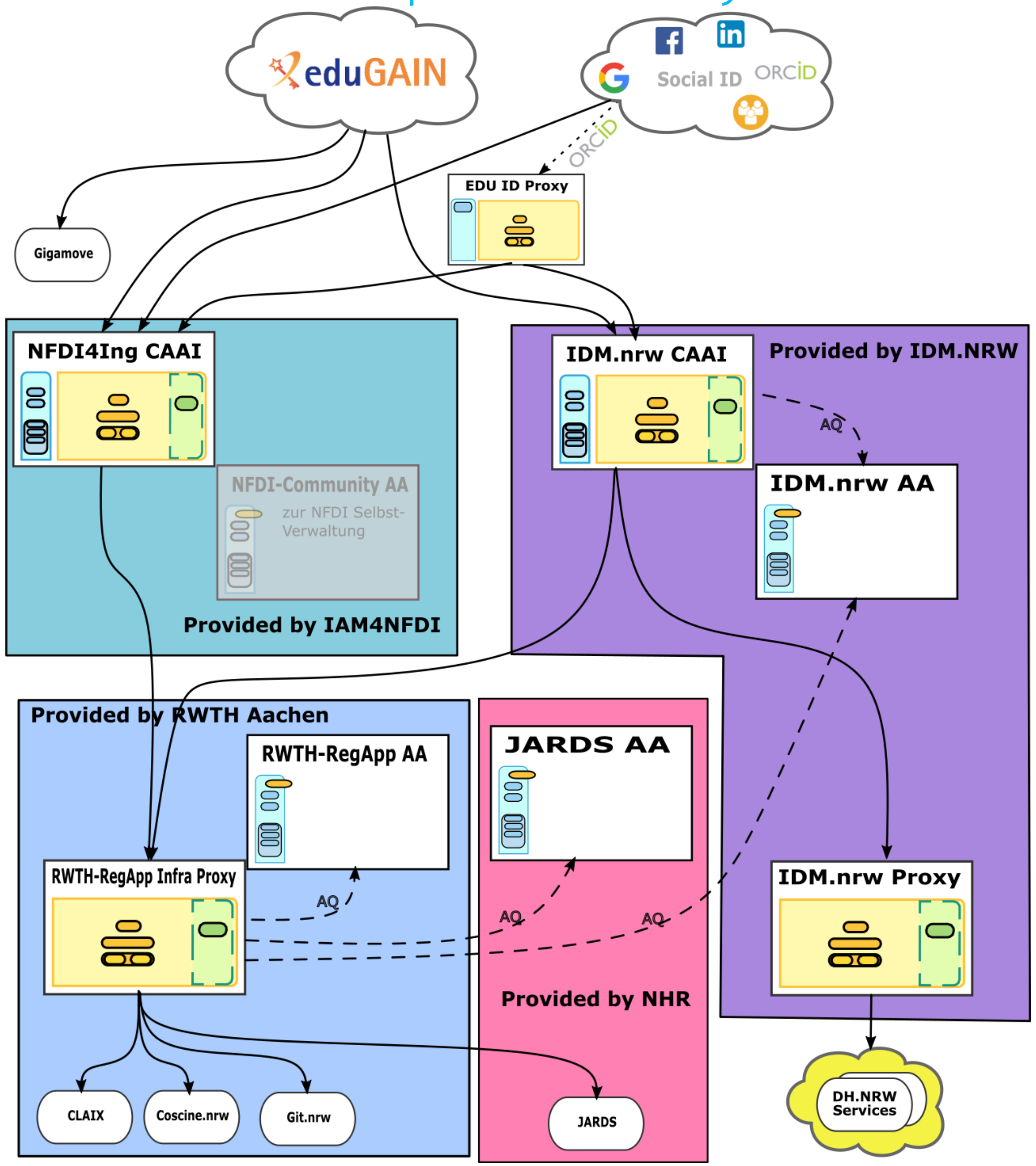
Architecture

Based on AARC II BPA



Architecture

A (very) Opionionated Interpretation by Me*



* As of 2023-09-21. Changes are subject to further enlightenment and insights. Interpretation is not necessarily (even quite unlikely) shared within the IAM4NFDI project. Zu Risiken und Nebenwirkungen Fragen Sie einen Informatiker Ihres Vertrauens.

Profile [WIP]

Basic Attribute Profile

- User identifier (created by CAAI)
  - Non-reassignable
  - and persistent
  - and unique
- Name information
- Email information
- Home Organisation information
- Affiliation within the community
- Affiliation at the Home-Organisation
- Assurance

Discussion currently ongoing to align with specifications from EOSC, Cern, NFDI consortia and German state initiatives

Profile [WIP]

Extended Attribute Profile

- Groups and roles: `eduPersonEntitlement`
- Capabilities `eduPersonEntitlement` [AARC-G027]
- Assurance (see above)
- Agreement to policies
- ORCID identifier
- Supplemental Name Information
- Authentication Profiles
- External Identifier
- SSH-Keys

Discussion currently ongoing to align with specifications from EOSC, Cern, NFDI consortia and German state initiatives

Authorization [WIP]

aka „VO Concept“

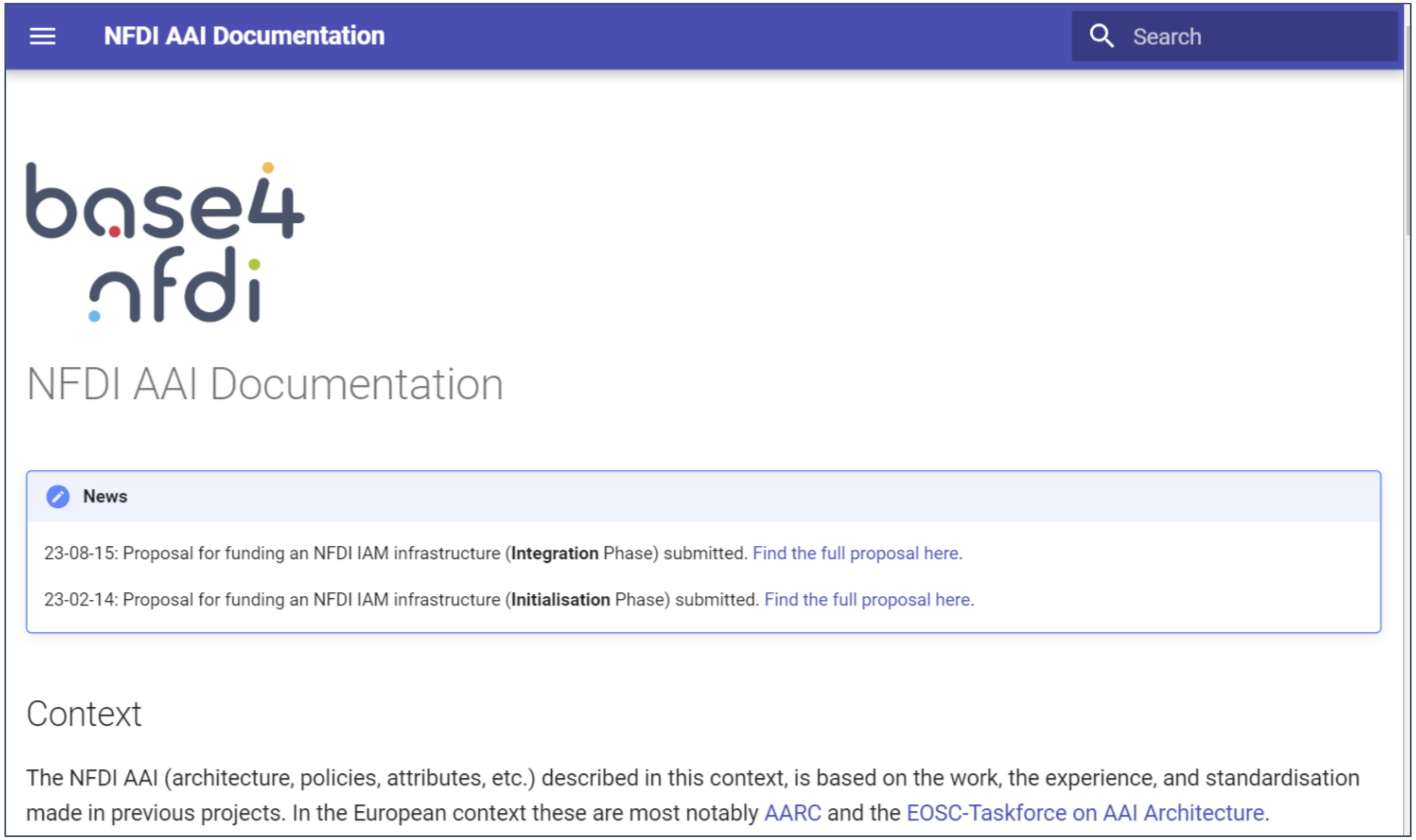
- Allow NFDI Consortia to define VOs on their behalf (within community AAI)
- Services may decide to support VOs
- This should be part of the „Community AAI as a Service“
- Caveats
  - NFDI Consortium is an AAI Community
  - NFDI Community is an AAI VO

Policies [WIP]

- Essential: Concept of Policy Frameworks
  - SIRTFI
  - SNCTFI
- Actual policies need to follow the Policy Framework
  - Top Level Infrastructure Policy (TLP)
  - Security Incident Response Policy (SIRP)
  - Policy on the Processing of Personal Data (PPPD)
  - Virtual Organization (VO) Membership Management Policy (VOMMP)
  - Virtual Organisation (VO) Life Cycle Management (VOLCM)
  - Service Access Policy (SAP)
  - Privacy Policy Template (PP (per VO / per Service))
  - Acceptable Use Policy Template (AUP (per VO / per Service))

Documentation

→ https://doc.nfdi-aai.de



NFDI AAI Documentation

News

23-08-15: Proposal for funding an NFDI IAM infrastructure (**Integration** Phase) submitted. Find the full proposal here.

23-02-14: Proposal for funding an NFDI IAM infrastructure (**Initialisation** Phase) submitted. Find the full proposal here.

Context

The NFDI AAI (architecture, policies, attributes, etc.) described in this context, is based on the work, the experience, and standardisation made in previous projects. In the European context these are most notably AARC and the EOSC-Taskforce on AAI Architecture.

Implementations and Test Instances

- Academic ID (GWDG)
- Didmos (DAASI)
- Reg-App (KIT)
- Unity (FZ-Jülich)

Thanks for listening!

Marius Politze

iD 0000-0003-3175-0659

politze@itc.rwth-aachen.de

base4nfdi