IAM for “German National Research Data Infrastructure” (NFDI)

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

Jan 2024

NFDI

base4 nfdi

NFDI Background

- NFDI: National Research Data Initiative
- https://nfdi.de
- Three rounds of calls
- 27 Consortia (call 1 + call 2 + call 3)
  - To span many different scientific disciplines
    (social, humanities, engineering, earth, chemistry, physics, ...)
- ~ 90 M€/a
- 5a + (potential extension: 5a)

base4 nfdi

NFDI Background

- NFDI first focussed on consortia
  - asked (infrastructure) questions later
- Identity and Access Management
  - Initially not in focus
  - Added in 3rd call via “Base4NFDI”:
    Basic services: Persistent Identifiers (PID), Metadata, Multicloud, IAM, ...
- IAM4NFDI Project submitted (during last years fim4r)
  - Active Phase officially starts on Feb 1st 2024
  - Funding 6FTE until Jan 2026

base4 nfdi

IAM4NFDI Goals

(Based on requirement analysis run before proposal)

- **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!

base4 nfdi

Project status

- We have an architecture ✅
- We have a set of attributes ✅
- We have the initial set of policies ✅
- We have the initial documentation ✅
- We have the demonstration Community AAIs up and running ✅

All documented at https://doc.nfdi-aai.de

base4 nfdi

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.

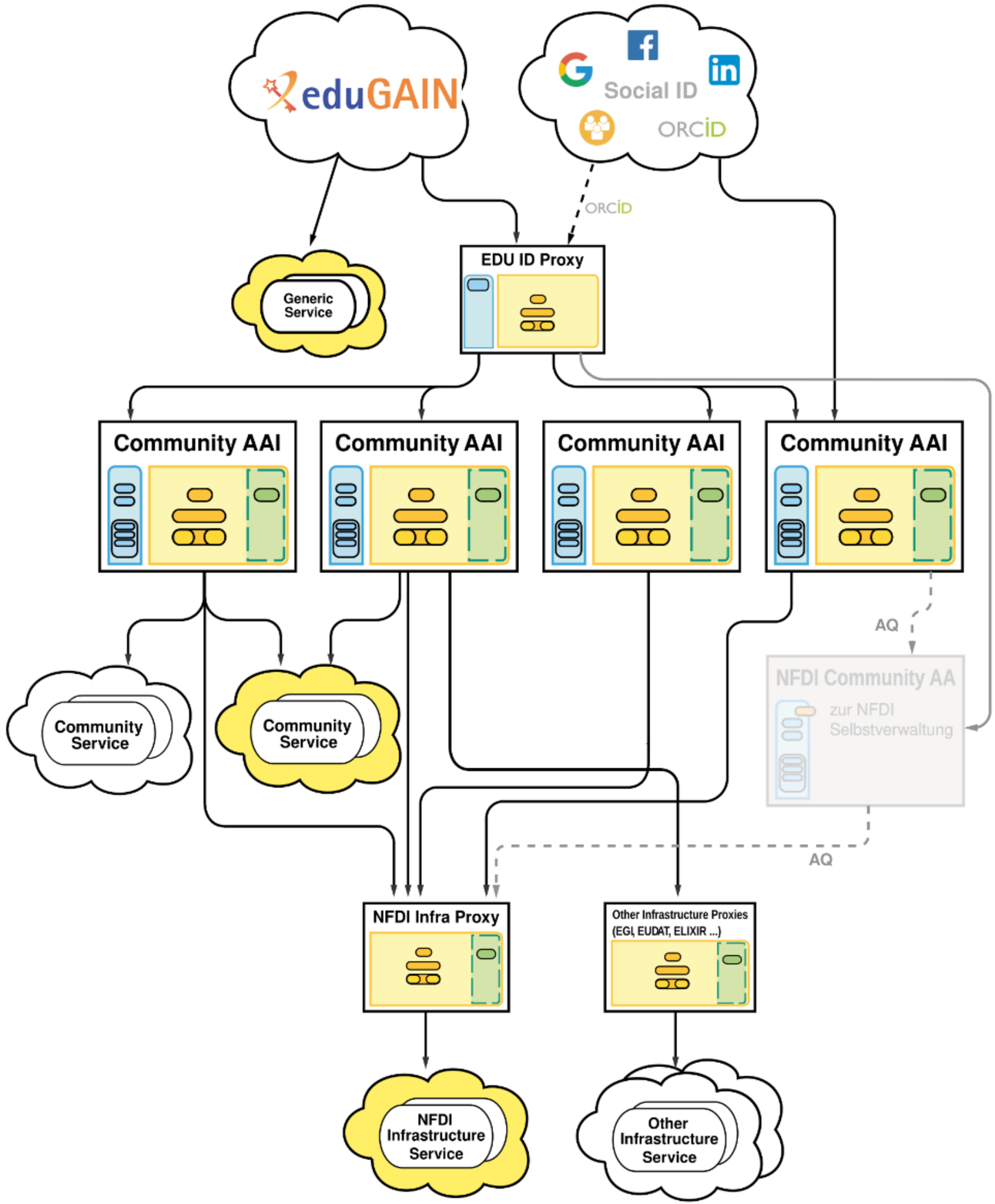
Context

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.

In the German context, several different projects have contributed their experience to this AAI:

- Helmholtz AAI by HIFIS, which uses Unity in an AARC / EOSC compatible configuration.
- AcademicID by GWDG, which is used to offer all IT services of GWDG to education in Lower Saxony.
- didmos by DAASI International, which integrates expandable open source modules that can be custom tailored to infrastructures
- RegApp by KIT, which is used to provide access to several educational and infrastructure services to academia in Baden

Architecture


eduGAIN
Social ID
ORCID
ORCID
Generic Service
EDU ID Proxy
Community AAI
Community AAI
Community AAI
Community AAI
Community Service
Community Service
AQ
NFDI Community AA
zur NFDI Selbstverwaltung
AQ
NFDI Infra Proxy
Other Infrastructure Proxies (EGI, EUDAT, ELIXIR ...)
NFDI Infrastructure Service
Other Infrastructure Service

base4nfdi

Technical Details tl;dr

- Based on AARC outputs
- Both `SAML` and `OIDC` supported
- Including the **German eduID**
- **Standardised** set of attributes
  - Following EOSC AAI spec
  - Added `ssh_public_key`
  - Pushing `voperson_external_id` (and `orcid`)
- Supporting three independent components for authorisation
  - Assurance (RAF)
  - Community Attributes (`entitlement` mainly for expressing VO/group membership)
  - Home Organisation attributes
- Well established contact mailinglists:
  - Core Team: **aai-kernteam@lists.kit.edu (email)**
  - General Information **list nfdi-aai-info@lists.kit.edu** (subscribe)

base4 nfdi

Results so far

Community AAIs

- Demonstration instances of all CAAI Softwares available
- Supported softwares:
  - AcademicID:
    - Operated and developed by **GWDG**
  - didmos:
    - Operated and Developed by **DAASI international GmbH**
  - Reg-APP:
    - Operated and developed by **KIT**
  - Unity:
    - Operated by **FZ-Jülich**
    - Developed by **BixBit** / AuthVizor

Consortia <-> CAAI map

Consortia <-> CAAI map

Fil Rediger Se Indsæt Formatér Data Værktøjer Udvidelser Hjælp

Del | Log ind

100% | Kun kommentering

A1

	A	B	C	D	E	F	G	H	I	J	K
1		Incubator	Runde	# Consortia	Academic ID	didmos	regApp	unity	LSAAI	Total	NFDI Coverage
2		13		26	1	3	2	2	1	9	34.62%
3	1		2	BERD@NFDI							
4	2		2	DAPHNE4NFDI				Prod			
5			1	DataPLANT							
6			3	FAIRagro							
7		yes	2	FAIRmat							
8			1	GHGA							
9			1	KonsortSWD							
10		yes	2	MaRDI		Started					
11		yes	1	NFDI4Biodiversity					Prod		
12			3	NFDI4BIOIMAGE							
13			1	NFDI4Cat							
14		yes	1	NFDI4Chem							
15		yes	1	NFDI4Culture		Concept					
16		yes	2	NFDI4DataScience		Considering					
17		yes	2	NFDI4Earth							
18			3	NFDI4Energy							
19			1	NFDI4Health							
20			3	NFDI4Immuno							
21		yes	1	NFDI4Ing			Prod				
22			3	NFDI4Memory							
23			2	NFDI4Microbiota							
24		yes	3	NFDI4Objects							
25		yes	2	NFDI-MatWerk			Prod				
26		yes	3	NFDIxCS							
27		yes	2	PUNCH4NFDI				Prod			
28		yes	2	Text+	Clarify!						
29											

Sheet1

Policies

- Exploiting the AARC Policy Development Kit
- Users (in Helmholtz-AAI) were unhappy with **defining the VO AUP**
  - Unsure about which responsibilities are actually taken
  - Asking their legal department for advice
  - Spending months to establish VOs
  - Way out
    - Split AUP into VO-AUP and CAAI-AUP
      - VO-AUP is minimally minimal
      - Users agree to CAAI-AUP on first login
- Users (in particular Service admins) were unhappy with “too many policies”
  - Way out
    - Colorise policy table
- Open questions
  - Should we expose SNCTFI to Home Organisations? (Experience, anyone?)

base4 nfdi

Operational Concept

- Operation of infrastructure Components (CAAIs, InfraProxy, ...)
  - Best-Effort during the project phases (5-10 a)
  - Sustainability models are being evaluated during the project
    - Along with all NFDI services at large
- Legal definition (25 pages and growing) of all AAI components
- Defines operation of CAAI for NFDI Consortia
  - Provides operations and service options:
    - “included via project funding”
    - bespoke “additional” services
- Production operation of CAAIs is currently starting

base4 nfdi

CAAI - InfraProxy

- ~27 CAAIs + 2-3 InfraProxies
- Set up a small SAML federation first
  - Make use of entity categories as part of DFN-AAI
- Later: use the setup for other protocols
  - OIDC
  - OpenID Federation
- Likely SATOSA with a small SAML federation between CAAI and InfaProxy

Tool: naco

For testing attribute release

naco - the NFDI Attribute COnformity Checker

Listed are **attribute categories** (e.g. Identifier) and the actual attributes that belong into these attribute categories. Please check the EOSC AAI Architecture 2022 and the NFDI Attribute Profile for more information.

Mandatory Attributes

Product	Identifier	Name	E-Mail	Domain of home-org	Affil. in community	Affil. at home-org	Assurance	Last Update
didmos (User Info)	sub+iss	name	email	schac_home_organization (wrong type)	eduperson_scoped_affiliation	voperson_external_affiliation	eduperson_assurance	2024-01-18 16:30
didmos (Summary)	OK	OK	OK	Wrong Type	OK	OK	OK	2024-01-18 16:30
Product	Identifier	Name	E-Mail	Domain of home-org	Affil. in community	Affil. at home-org	Assurance	Last Update
RegAPP (User Info)	sub+iss eduperson_unique_id voperson_id	name	email	schac_home_organization	eduperson_scoped_affiliation	voperson_external_affiliation	eduperson_assurance	2024-01-30 11:30
RegAPP (Access Token)	sub+iss	---	email	---	---	---	---	2024-01-30 11:30

- Nice exercise
- Learned: need more precise definition of attributes
- SAML supported (sort of)

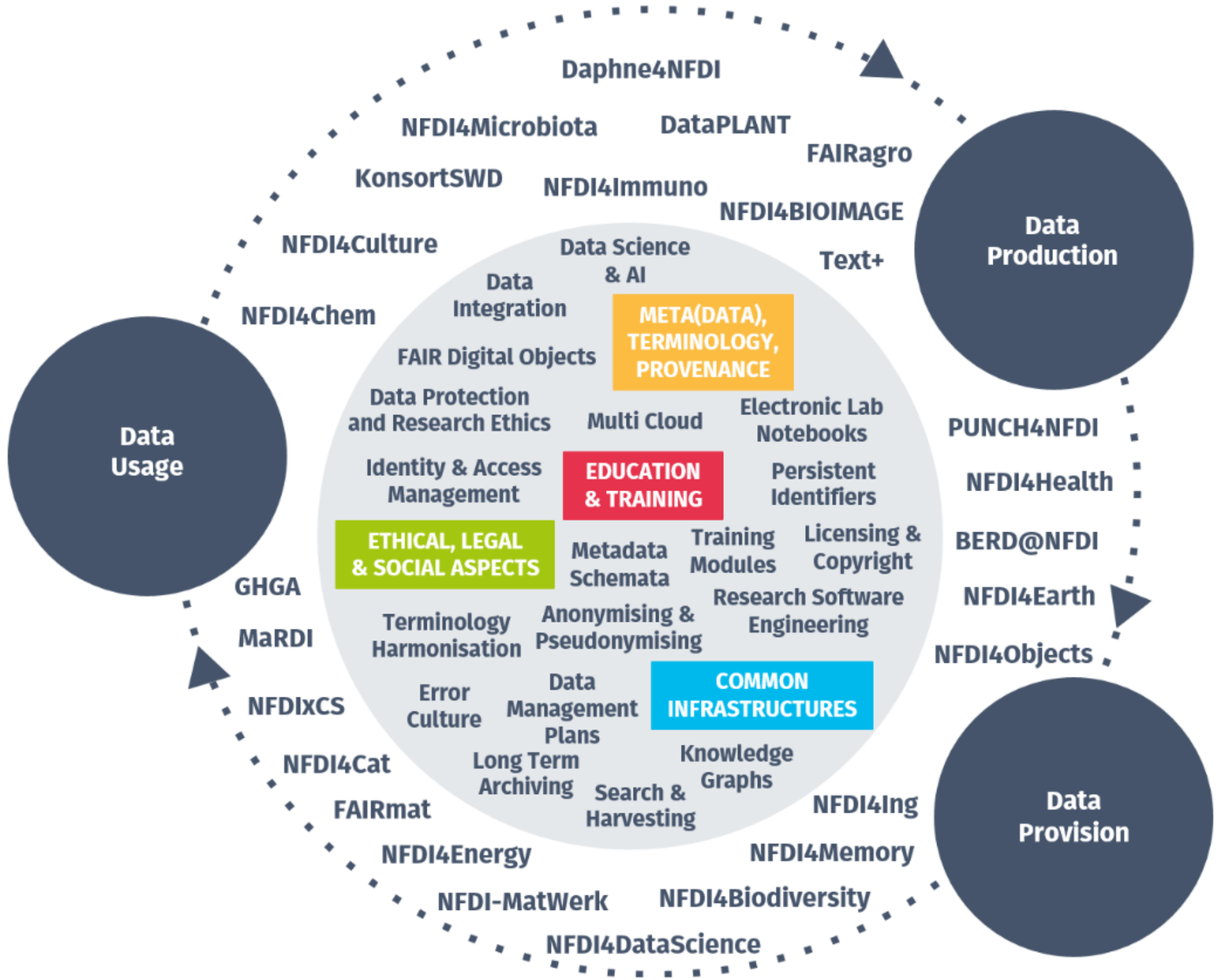
base4 nfdi

Upcoming

- Support AARC-G071 at CAAIs
- Make sure key messages are better understood:
  - We (IAM4NFDI Project) operate one of four CAAI Products as a service for each of the 27 NFDI Consortia
  - Consortia have to choose one CAAI solution
  - We develop the Infrastructure Proxy
  - Once it is there, services for multiple NFDI-Consortia are migrated from CAAI to InfraProxy

base4 nfdi

Questions?



base4 nfdi

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