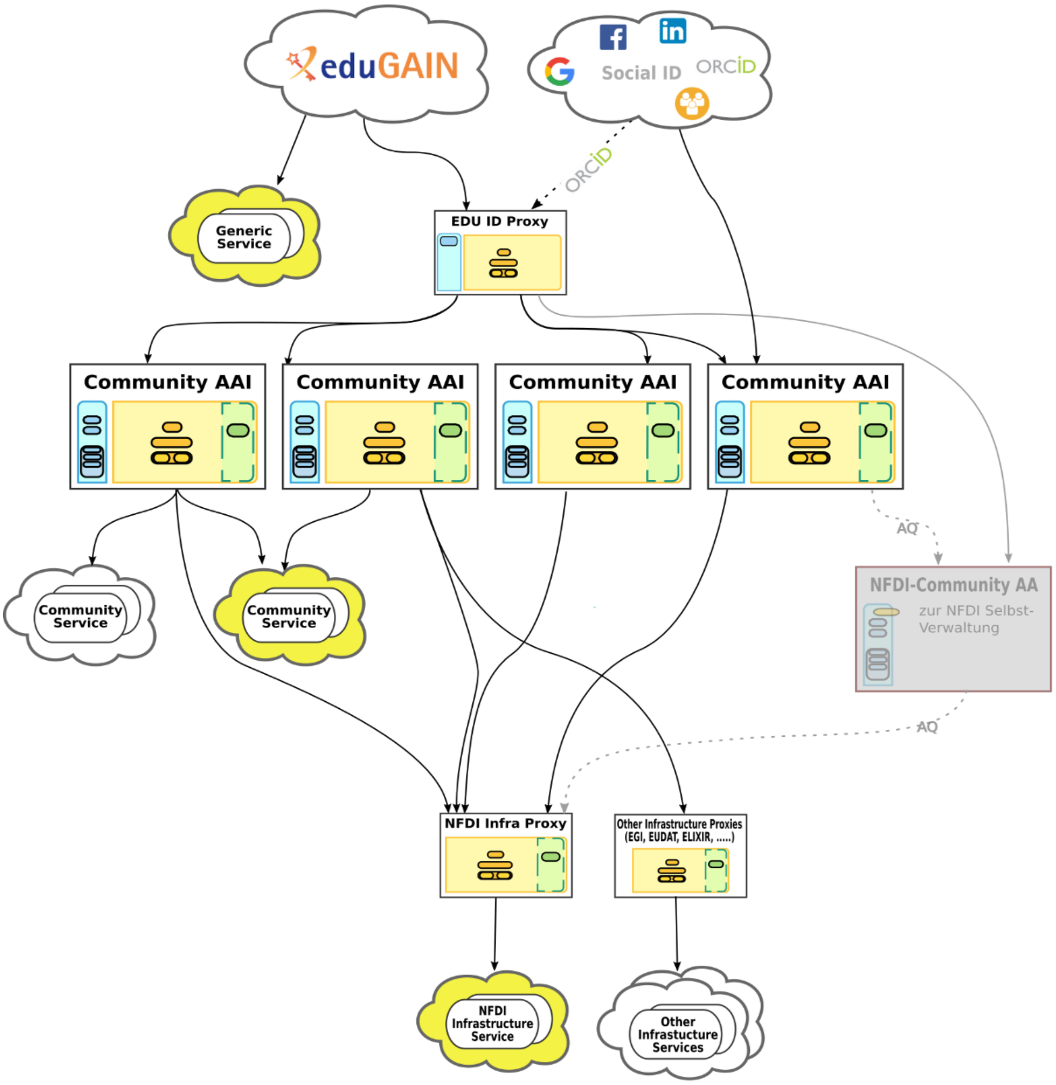
IAM4NFDI – Integration Phase

Basic Service ‘Identity and Access Management’ for the German National Research Data Infrastructure



Proposal for the Initialization and Integration Phases of Base4NFDI

Submitted: August 15th, 2023

On behalf of: WG Identity and Access Management, Section Common Infrastructures

1. General Information

- Name of proposed Basic Service (in English)

  Identity and Access Management

- Acronym of the proposed Basic Service

  IAM4NFDI

- Service "subtitle" explaining key functionality

  Management of digital identities and federated access to resources within and across the NFDI consortia

- Lead institution
  - DFN-Verein, Alexanderplatz 1, 10178 Berlin
  - RWTH Aachen, Templergraben 55, 52056 Aachen

- Name of lead institution principal investigator
  - Pempe, Wolfgang (DFN) – pempe@dfn.de
  - Politze, Marius (RWTH) - politze@itc.rwth-aachen.de

- Participating institutions

Principal Investigator	Institution, location	Contact E-mail	Member in [consortium]
Wolfgang Pempe	DFN	pempe@dfn.de	NFDI4Ing
Peter Gietz	DAASI	p.gietz@daasi.de	NFDI4Ing via GWDG
Sander Apweiler	FZJ	sa.apweiler@fz-juelich.de	Punch4NFDI
Christof Pohl	GWDG	christof.pohl@gwdg.de	NFDI4Ing
Marcus Hardt	KIT	hardt@kit.edu	NFDI4Ing
Marius Politze	RWTH	politze@itc.rwth-aachen.de	NFDI4Ing
Thorsten Michels	RPTU	michels@rptu.de	DataPlant

Table 1: List of participating institutions

- Planned runtime of the project
  - Integration phase: 24 months

- Summary of the proposal in English and German

Identity and Access Management (IAM) is concerned with the processes, policies, and technologies for managing digital identities and their access rights to specific resources [1]. A

central goal within NFDI is to enable unified access to data, software, and compute resources, as well as sovereign data exchange and collaborative work. To achieve this, it will be necessary to connect and expand existing and emerging IAM systems in a way that researchers from different domains and institutions are able to access digital resources existing within NFDI as easily as possible, including access to and exchange with external infrastructures and resources. Interoperability is therefore a central requirement. To achieve this, a decentralised, federated IAM is required. The technical and organisational framework for a federated IAM is a so-called Authentication and Authorisation Infrastructure (AAI) [2]. The task of the Basic Service IAM is to establish and provide a state-of-the-art AAI, that fosters cross-consortial and international collaboration. This NFDI Community AAI will be connected to the national identity federation DFN-AAI [3]. Through its participation in the international interfederation eduGAIN [4], the DFN-AAI facilitates international, cross-federation, and cross-community usage scenarios, including the connection to the EOSC AAI. This way, users from approx. 400 German research and higher education institutions plus approx. 4800 home organisations worldwide will be able to access services and resources provided by the NFDI Community AAI.

Identity- und Access-Management (IAM) befasst sich mit den Prozessen, Policies und Technologien zur Verwaltung digitaler Identitäten und deren Zugriffsrechten auf bestimmte Ressourcen [1]. Ein zentrales Ziel innerhalb der NFDI ist es, einen einheitlichen Zugriff auf Daten, Software und Rechenressourcen sowie einen souveränen Datenaustausch und kollaboratives Arbeiten zu ermöglichen. Um dies zu erreichen, ist geplant, bestehende und neu entstehende IAM-Systeme so zu verbinden und zu erweitern, dass Forschende aus verschiedenen Bereichen und Institutionen so einfach wie möglich auf digitale Ressourcen innerhalb der NFDI zugreifen können, einschließlich des Zugangs zu und des Austauschs mit externen Infrastrukturen und Ressourcen. Interoperabilität ist daher eine zentrale Anforderung. Um dies zu erreichen, ist ein dezentrales, föderiertes IAM erforderlich. Der technische und organisatorische Rahmen für ein föderiertes IAM ist eine sogenannte Authentifizierungs- und Autorisierungsinfrastruktur (AAI) [2]. Die Aufgabe des Basisdienstes IAM ist es, eine dem Stand der Technik entsprechende AAI aufzubauen und bereitzustellen, die eine Konsortien-übergreifende und internationale Zusammenarbeit ermöglicht. Diese AAI der NFDI-Community wird mit der nationalen Identitätsföderation DFN-AAI [3] verbunden sein. Durch die Beteiligung an der Interföderation eduGAIN [4] ermöglicht die DFN-AAI internationale, föderations- und community-übergreifende Nutzungsszenarien, inklusive der Anbindung an die EOSC AAI. Auf diese Weise können Nutzende aus ca. 400 deutschen Forschungs- und Hochschuleinrichtungen sowie aus ca. 4800 Heimatorganisationen weltweit auf die Dienste und Ressourcen der NFDI Community AAI zugreifen.

2. Summary of Initialisation Phase Results

Change in Background and Motivation since the Start of the Initialisation Phase

There are no changes compared to the proposal in the initialisation phase.

Results of Initialisation Phase

Based on community feedback and extensive preparatory work as outlined in the proposal for the initialisation phase [24], the project team has identified the following goals for the implementation of the NFDI-AAI architecture:

1. International interoperability for services and users.
2. High availability and fault tolerant operation.
3. Sustainable implementation of state-of-the-art IAM.

The core components of the NFDI-AAI are the concept of a Community AAI (CAAI), based on the AARC Blueprint Architecture [17], a set of attribute profiles [15] based on AARC Guidelines and the EOSC AAI Architecture, and a policy framework inspired by the Helmholtz AAI. Insofar, the underlying concepts for this Basic Service are well embedded within the European and global ecosystem of Federated Identity Management.

The CAAI solutions that have been put in place during the integration phase comprise all four products, which are developed or operated in Germany (AcademicID, didmos, RegAPP, Unity) [25].

With the initialisation phase, the goal 1 - international interoperability - was achieved, both technically and in terms of policies, due to the results of Work Packages 1 (WP1) and WP2, for details, see below. Furthermore, thanks to the results of the same work packages, the foundations for the third objective - state-of-the-art IAM - could be laid. Achieving the second goal - high availability and fault tolerant operation - is one of the main objectives of WP4 in the upcoming integration phase.

Detailed Results of the Initialisation Phase

WP1 - Policy, Governance, and Legal Aspects

Main objective: Laying the basis for the NFDI IAM governance structure: Initial version of the NFDI-AAI policy framework, including a privacy statement template for services and proxies compliant with the General Data Protection Regulation (GDPR).

Target audience: end users, spokespersons, legal staff, service operators

All required milestones will be achieved by the end of the initialisation phase:

- M1.1 Approval of the policy documents by the NFDI community
- D1.1 Register of FIM-related data processing operations
- D1.2 Finalized policy documents
- D1.3 Legal opinion on FIM and attribute release in AAI context

WP2 - AAI Architecture and Implementation

Main Objective: Establishing the technical basis (architecture, attribute profiles) for the NFDI-AAI and the operation of CAAIs.

Target audience: service operators, system administrators, software architects, IAM experts

The following milestones will be achieved by the end of the initialisation phase:

- M2.1 Approval of the architecture by the NFDI community
- M2.4 Demonstration instances of all CAAIs available

Due to the fact that the planned basic services DMP and KGI have not been granted in March 2023, Milestone M2.3 (Early Adopter 2: Basic Service KGI) could not be implemented. As for M2.2 (Early Adopter 1: Basic Service DMP), the RDMO instances of NFDI4Ing operated by TU Darmstadt could successfully be connected to one of the CAAIs already in use.

Additional results:

- Integration of several technical services (oidc-agent, mytoken, orpheus, naco - an OIDC/SAML attribute checker)

WP3 - Incubator

Main Objective: Development and implementation of solutions for specific requests from the community, e.g., integration of complex services, or the development of new features.

Target audience: service operators, software architects, IAM experts

All required milestones will be achieved by the end of the initialisation phase:

- D3.1 Approval of decision process for the incubator projects by Base4NFDI
- M3.1 Decision on first incubator cycle projects

WP4 - Operations

Main objective: Provide professional operation of the key infrastructure components, i.e., the infrastructure proxy, the NFDI Attribute Authority and instances of the four CAAI implementations.

Target audience: service operators, system administrators, software architects

All required milestones will be achieved by the end of the initialisation phase:

- M4.1 Identification of software components to be developed and/or operated for NFDI IAM
- D.4.1 Concept for the operation of developed and hosted software components
- M4.2 Proof of Concept (PoC) hosting environments for development and staging of NFDI IAM components

Additional results:

- Preparation of infrastructure for continuous integration (CI) and delivery (CD)
- Evaluation of support options (e.g., help desk and managed services)

WP5 - Dissemination, Training, and Community Engagement

Main objective: Information and training for the target groups, validate project results, and gather community feedback.

Target audience: service operators, spokespersons, software architects, IAM experts

All required milestones will be achieved by the end of the initialisation phase:

- M5.1 Community infoshare
- M5.2 Workshop IAM basics
- M5.4 Community infoshare #2

Additional results:

- Establishing communication channels with the target groups of the Basic Service IAM, namely all IAM/AAI spokespersons of all consortia plus all persons working in the field of IAM in NFDI

Updated current Technology Readiness Level (TRL) of the proposed Basic Service

In addition to the **Community AAIs**, the NFDI-AAI architecture consists of three more technical components:

- **Infrastructure Proxy:** Allows the connection of services which need to be accessible for several NFDI Consortia, without specific development on the service side. It is also a place at which authorisation may be enforced, e.g., in cases where a connected service itself is not capable of doing so.
- **NFDI Community Attribute Authority:** An information system, in which the roles and corresponding access rights of the NFDI itself are defined and provided to all AAI components that require it. This includes, for example, the information whether a user is allowed to create or manage virtual organisations (VO), which are required for a scalable operation and organisation of the NFDI.
- **edu-ID Proxy:** Currently developed and deployed at DFN-CERT. Inspired by the SWITCH edu-ID Service [20], the concept of a German edu-ID was developed by a ZKI working group [21] after gaining an overview of the landscape of digital identities in Germany and Europe [19]. It is the concept of a self-managed, institution-independent, and lifelong digital identity for the field of research and education. The edu-ID system is intended as a place where people can bring together, i.e., link information about their identities (Home Organisation, ORCID, …) in a way that enables seamless and long-term use of the resources relevant to them. While the IdPs of the Home Organisations can still be used as authentication and basic attribute source, the edu-ID Proxy generates lifelong-valid identifier attributes/claims. In the context of NFDI, it addresses the concept known as “researcher mobility”, which reflects the fact that scientists work at several different institutions along their career. Furthermore, the edu-ID service can be used as a Homeless/Guest IdP.

At the end of the initialisation phase, the TRLs of the technical components of the NFDI-AAI are as follows:

- Community AAI as a Service (CAAIaaS)

  Technical solutions for setting up individual CAAIs including demonstrator (AcademicID, didmos, RegApp, Unity): TRL 8
- Infrastructure Proxy: TRL 6
- NFDI Community Attribute Authority (AA): TRL 6
- edu-ID Proxy: TRL 5

3. Working Concept for the Development of the Basic Service

The focus of the integration phase will be to operationalise the IAM, to ensure support for as many NFDI use-cases as possible. This requires several steps, addressed in the different work packages of this project. The core concept foresees that the CAAI software will be operated as a service by IAM4NFDI for the NFDI Consortia. The professional operation (HA/FT/security) will be addressed by WP4, the required policies to provide a solid legal foundation are established (with external legal counselling) in WP1. The architecture, attributes, and international compatibility are ensured and verified within WP2. WP3, the incubator, will handle special requests (e.g., integration of complex services that are not easy to support within the AAI). WP5 will communicate the necessary knowledge and organise the projects' workshops and infoshares.

Service Integration Concept

A key concept of this proposal is to ensure the integration of a large variety of different services in the NFDI-AAI. While some services may directly be integrated by appropriate configuration, other services may require minor adjustments, and certain services will require a considerable development effort so that they can be appropriately integrated.

These three different kinds of services are addressed by different work packages and actions within this project. The first kind of services can be integrated by the NFDI consortia themselves, simply by following the documentation provided by WP5. Services that require more know-how of the technology stacks used are going to be integrated in WP4. Following the successful incubator concept of the GEANT project [18], an incubator is established in WP3. This is the place in which the community-driven development for the integration of specific services and extensions of existing solutions will take place. The topics addressed in the incubator will be agreed upon in joint meetings with IAM4NFDI, and the IAM representatives of the NFDI Consortia. The process for the onboarding of incubator candidates will be agreed upon with Base4NFDI. An initial set of incubator projects has already been identified in the initialisation phase, cf. section 5.2.3.

To ensure the inclusion of the consortia, they are involved in the project right from the beginning and are invited to contribute and provide feedback. There were already two workshops successfully carried out, one before the start of the project and one during the initialization phase. In addition, a more general infoshare was held, where interested members of the NFDI consortia obtained a detailed overview of the architecture, attribute profiles and policies.

Future Development and Ramp-Up Outlook

The general topic “Federated Identity and Access Management” is being discussed by various bodies within the German, European and worldwide research community (e.g., DFN, ZKI, GÉANT, AEGIS, REFEEDS) as well as industrial standardisation bodies (e.g., OASIS, OIDF, W3C). The topic is also a central point of discussion in the projects shaping the European IT-service-landscape like EOSC and Gaia-X. Already during the current initialization phase, IAM4NFDI takes part in the discussion with these communities and standardisation bodies. Until the ramp-up this should be intensified. The proposed and partially implemented architecture for the NFDI-AAI is based on the AARC Blueprint Architecture (BPA) - a result of the AARC II project that is also a central element in the upcoming EOSC AAI. The proposed protocols for implementation, SAML and OIDC are widely standardised and in use by other implementers of the BPA. The envisioned architecture - the CAAIs and Infrastructure Proxy - is therefore already fully compatible with existing international infrastructures. This wider level of international standards should be brought into the NFDI consortia using the CAAIaaS. Until the ramp-up phase, the service offer should be stable and support necessary features relevant for the NFDI communities - this is addressed by the incubator projects during the integration phase. NFDI4IAM further extends the group of users applying federated IAM technologies which were previously “from-experts-for-experts” and now gradually transition to “from-experts-for-novices”. This is on the one hand addressed during the integration phase with pilot use cases and infoshares that help building a knowledge base and on the other hand by operationalizing CAAIaaS service delivery by selecting and building implementations, service providers and processes.

Risks and challenges

The following table lists the main risks of the project. Appropriate measures will be defined to minimize the probability of occurrence and reduce the possible impact on the project.

Description of Risk	WPs involved	Proposed Risk-Mitigation Measures
Lack of person power, overloaded individuals **Likelihood**: Medium **Impact**: High	all	The project partners will do everything necessary to recruit sufficient staff. Appropriate support from the respective management levels is assured.
Finding new staff for the community is difficult. **Likelihood**: High **Impact**: Medium	WP3 WP4 WP5	To compensate this situation at least a bit, IAM4NFDI can take over development and integration tasks in WP3 (Incubator), offers the hosting of a CAAI (CAAIaaS) in WP4 and training for existing staff in WP5.

Despite a well understood legal situation (GDPR), some Home Organisations (i.e., IdP Operators) refuse to release attributes to e-Science services without additional paperwork [16] **Likelihood**: Medium **Impact**: High	WP1 WP2	Addressing those legal issues is one of the main objectives in WP1. Furthermore, ZKI (represented by RPTU) and DFN will work in the German AAI community to dispel the legal concerns regarding attribute release. The attribute profiles specified by WP2 are already designed to be as data-minimizing as possible.
NFDI consortia implement their own IAM solutions and cause a fragmentation of the NFDI landscape. **Likelihood**: Medium **Impact**: Medium	WP2 WP5	Implementing own IAM solutions is not necessarily a problem. In such cases, the project team (supported by Base4NFDI and the section Common Infrastructures) will work towards implementing the attribute profiles and the policy framework to ensure interoperability within the NFDI-AAI.
The barrier to federating services and implementing IAM policies may be too high for some consortia. **Likelihood**: Medium **Impact**: Medium	WP3 WP4 WP5	To relieve the burden on consortia and their staff, IAM4NFDI takes over development and integration tasks in WP3, offers the hosting of a CAAI (CAAIaaS) in WP4 and training for the technical staff in WP5.

Table 2: Risks and proposed Measures

4. Support Actions from Base4NFDI / NFDI Sections, and Integrating NFDI Consortia / Efforts

Support from	involved effort	Consortium (contact)
Base4NFDI	Support in addressing the target groups. Guidance on and support with the implementation of processes for • onboarding of incubator candidates. • further development of the policy framework. • cross-consortia rights and role management.	base4nfdi-office@lists.nfdi.de
Section Common Infrastructures	Gather input and feedback for the development of the Basic Service, point of contact with the relevant working groups	
NFDI top level	Provide visibility of the importance of the IAM topic, e.g., by talks at conferences.	

Table 3: Contributions required from Base4NFDI / NFDI Sections

Support from	Work package	Contact Person Basic Service
Juypiter4NFDI (Basic Service)	WP3 – M.3.2	[redacted]
NFDI4Memory	WP1-5	[redacted]
NFDI4Culture	WP1-5	[redacted]
PUNCH4NFDI	WP1-5	[redacted]
FAIRagro	WP1-5	[redacted]
NFDI4ING	WP1-5	[redacted]
KonsortSWD	WP1-5	[redacted]
NFDI4Microbiota	WP1-5	[redacted]

Table 4: Support needs from integrating consortia and other Basic Services

5. Work Programme

Overview of Work Packages

All the different aspects for a successful AAI are guaranteed by the individual work packages. This comprises policy, governance, and legal aspects in WP1, the architecture and attributes in WP2, incubator cycles for addressing complex service integration tasks and new features in WP3, production quality operations in WP4, as well as dissemination, training, and community engagement in WP5.

For a more structured overview all project partners working in a work package and the institution leading the work package are listed in the detailed description of each work packages just as the milestones and deliverables. For a general overview of the timelines, please refer to the Gantt Chart (section IV). It summarises the duration, deliverables, and milestones of all work packages.

Detailed Work Programme

Detailed descriptions of each work package are provided in the following subsections.

5.2.1 WP1: Policy, Governance, and Legal Aspects

WP Lead: DFN, RWTH

Phase	**DFN**	DAASI	FZJ	GWDG	KIT	**RWTH**	RPTU	**Total**
Year 1 (M1-M12)	2	1	1	1	1	2	2	**10**
Year 2 (M13-M24)	3.5	1	1	1	1	1.5 (0.5)	1.5 (0.5)	**10.5 (1)**

Table 5: WP1 - Contribution by project partners in person months (values in parentheses denote in kind contributions by the partner from existing funding)

Based on a set of binding policies and policy templates established in the initialisation phase, this work package aims to establish a governance structure of the NFDI AAI. This involves the establishment of community-based and well- defined decision processes for the further development of this structure and the policy framework. To achieve this, a close collaboration with Base4NFDI as focal point of community engagement is required.

One key part of this activity is to ensure that AAI policies will be supported, and adhered to, by all consortia, their representatives, as well as their services, and users. For this purpose, a clear organisational scheme is being developed to identify responsibilities, regulations, and guidance for interaction with domain specific consortia, regarding

- delegation of authorisation management.
- implementation of essential policies to establish trust and common procedures.
- integration of services of consortia.
- integration of global users (e.g., from other countries and trust domains).
- integration of guest users (e.g., citizen scientists).
- authorisation management for subject-specific, generic and cross-consortia resources (e.g., communication services).

This work implements the recommendations of WISE, Sirtfi [22], and Snctfi [23], as it is based on the AARC Policy Development Kit, to ensure interoperability with international initiatives, such as EOSC. Across the three project phases, these activities will lead to the establishment of an appropriate governance structure and processes for the access and rights management of the NFDI IAM that will implement the topics listed above in a sustainable way. Clearly defined structures and responsibilities in terms of IAM will help to connect NFDI with the relevant international initiatives and infrastructures like EOSC, HPC compute/storage projects and the life sciences communities.

The other key aspect of this work package is to improve the legal basis (defined by the policies) on which the services operate, especially in terms of clarifying possible privacy issues. Despite the GDPR, some aspects in the operation of some services in the scientific service landscape had to be clarified from a legal point of view. For this purpose, the activities for processing personal data had been documented and a legal opinion on federated identity management and attribute release in AAI obtained during the initialisation phase. Based on the results of the legal opinion, further steps will be taken, like contacting one or more state data protection officers and - if necessary - developing a binding data protection memory of understanding for the NFDI-AAI.

The project team is aiming for a cooperation with the Section Ethical and Legal Aspects.

Milestones and Deliverables

Milestone	Deliverable	Type	Description	Due end of
	D1.4	DOC	Initial concept for rights and roles management (-> VOs)	Month 10

M1.2			Consultation with key stakeholders	Month 12
	D1.5	DOC	Updated VO concept, which supports advanced requirements	Month 20
	D1.6	DOC	Specification of a community process for further development of the NFDI AAI policy framework	Month 24
			Project Coordination	

Table 6: WP1 - Milestones and Deliverables

5.2.2 WP2: AAI Architecture and Implementation

WP Lead: KIT

Phase	DFN	DAASI	FZJ	GWDG	**KIT**	RWTH	RPTU	**Total**
Year 1 (M1-M12)	2	2.5 (0.5)	2.5 (0.5)	2.5 (0.5)	4 (1)	-	-	**13.5 (2.5)**
Year 2 (M13-M24)	2	2	2	2	3 (1)	1	-	**12 (1)**

Table 7: WP2 - Contribution by project partners in person months (values in parentheses denote in kind contributions by the partner from existing funding)

This work package coordinates all architecture related aspects focusing on the implementation on one hand and the international standards on the other hand. In line with the initially defined AAI Architecture [15], this work package will lead the participating CAAIs to an interoperable mode of operation, which will provide a modern, “as a Service” fashion to NFDI consortia (CAAIaaS).

Two focal points for the integration phase in this work package are the “NFDI Community Attribute Authority”, and the “Infrastructure Proxy”. The NFDI-Community-AA implements the NFDI-wide organisation structure (who is entitled to manage a VO, or a Consortium).

The infrastructure proxy is the architectural component that allows advanced features for users and services. Services that provide services to more than a single NFDI-consortium benefit from simplified integration by the infrastructure proxy. Users and services may benefit from features such as account-linking, which is best done at the infrastructure proxy. The infrastructure proxy is a novel component in the architecture and requires an initial development phase.

To support a short time to market, it is foreseen that services are first integrated with the CAAIs directly, since those will be operational about one year before the infrastructure proxy. A smooth transition of services between CAAIs and the infrastructure proxy will be achieved, by using a standardized attribute set.

Milestones and Deliverables

Milestone	Deliverable	Type	Description	Due end of
M2.5		DEM	Relevant policies implemented in all CAAIs	Month 6
	D2.1	DOC	Hosting of CAAIs available as a service	Month 8
M2.6		DEM	Infrastructure proxy PoC connected to CAAIs Development	Month 8
M2.7		DEM	Infrastructure proxy initial version operational and connected to most CAAI Instances	Month 12
M2.8		DEM	Integration of edu-ID Proxy	Month 12
M2.9		DEM	NFDI-Community-AA PoC connected to CAAI	Month 16
M2.10			All AAI Services operational and initial NFDI services integrated	Month 20
	D2.2	DOC	Final documentation on integration of NFDI services with the NFDI-AAI as a whole.	Month 24

Table 8: WP2 - Milestones and Deliverables

5.2.3 WP3: Incubator

WP Lead: RWTH

Phase	DFN	DAASI	FZJ	GWDG	KIT	**RWTH**	RPTU	**Total**
Year 1 (M1-M12)	0.5	2.5 (0.5)	2.5 (0.5)	2	2 (1)	3	-	**12.5 (2)**
Year 2 (M13-M24)	0.5	2.5 (0.5)	2.5 (0.5)	2	2 (1)	1 (1)	-	**10.5 (3)**

Table 9: WP3 - Contribution by project partners in person months (values in parentheses denote in kind contributions by the partner from existing funding)

The novel instrument of an incubator facilitates a flexible and user-driven innovation cycle. In this project, the incubator will ensure that specific advanced requests from the community can be fulfilled. Such requests could concern the deeper integration of complex services, or the development of new features. This typically requires a considerable amount of work and is ideally implemented together with communities.

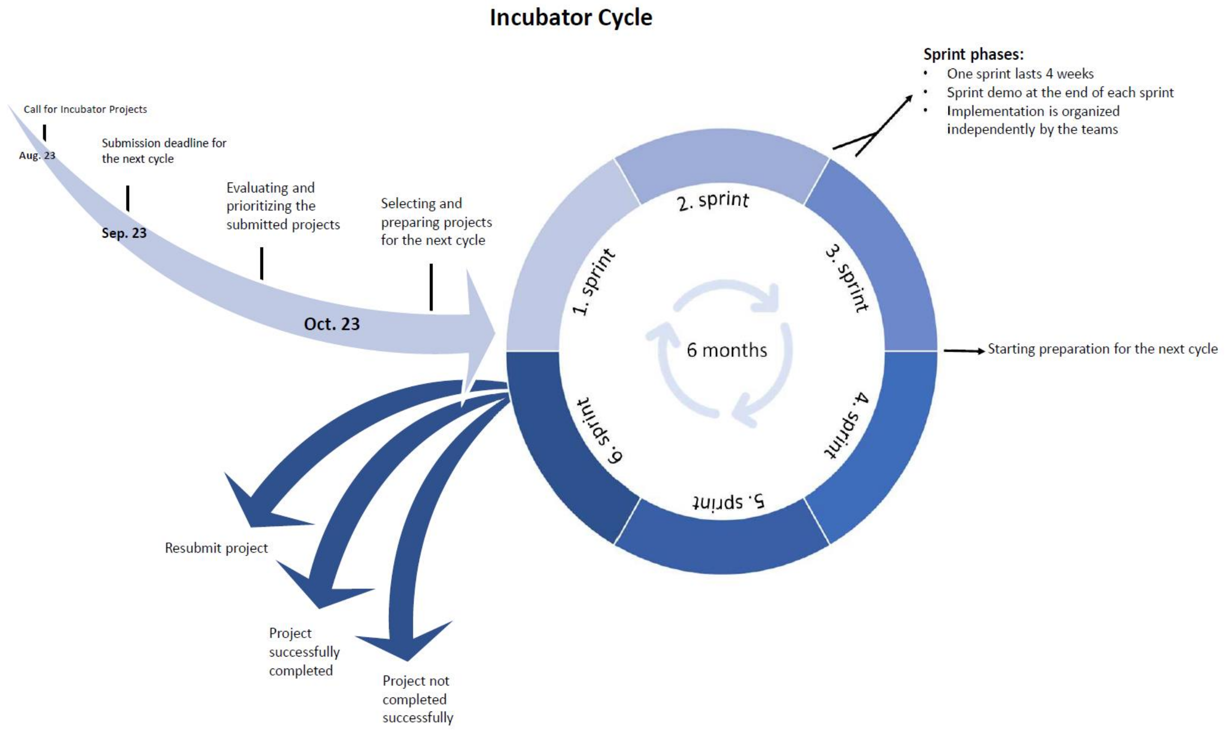

Incubator Cycle
Sprint phases:
• One sprint lasts 4 weeks
• Sprint demo at the end of each sprint
• Implementation is organized independently by the teams
Call for Incubator Projects
Aug. 23
Submission deadline for the next cycle
Sep. 23
Evaluating and prioritizing the submitted projects
Oct. 23
Selecting and preparing projects for the next cycle
1. sprint
2. sprint
3. sprint
4. sprint
5. sprint
6. sprint
6 months
Starting preparation for the next cycle
Resubmit project
Project successfully completed
Project not completed successfully

Figure 1: Incubator cycle (not yet approved by Base4NFDI)

The decision process will be defined as part of the project work and approved by Base4NFDI as one result of the initialisation phase. It consists of the rough depiction of the cycle (shown in figure 1) and a detailed description of the process. This decision process involves AAI experts of the NFDI consortia, the section common infrastructures, and the Base4NFDI consortium. Criteria for selection include the general applicability of requested features to NFDI as a whole and the extent to which the NFDI consortia are willing to support it.

For enabling focused development, incubator projects are limited to a lifetime of 6 months. At the end of a project, the results and the experiences gained will be documented. They may then either be handed over to the appropriate stakeholders or be discarded.

This work package has important interfaces to two other packages: WP4 - Operations, which may need to include the results of an incubator into its operational procedures, and documentation. WP5 - Community Engagement, which will advertise the incubator cycles, as well as include their results in the dissemination and training efforts.

A list of potential topics for incubator projects is:

- Targeted development for the deeper integration of services (e.g., VO support in GitLab etc.)
- Management of organisational structures, information, and roles
- Deprovisioning of identities/accounts
- Account/Identity linking, e.g., ORCID integration
- General identity assurance step-up service
- General Authentication step-up service (a.k.a. “second factor as a service”)
- Exploration of self-sovereign identity (SSI) technologies

In the initialisation phase the first potential incubator projects could be identified (cf. Table 10). It will be evaluated, if these projects are suitable for implementation within the incubator framework otherwise it will be defined how to integrate them into the project.

	Planned for	Contact	Member in
Jupyter4NFDI Connect a central Jupyter service to the infrastructure proxy component	M3.2 Incubator Cycle 2	[redacted]	PUNCH NFDI4ING
NFDI Nextcloud Connect the central NFDI Nextcloud instance to the infrastructure proxy	M3.2 Incubator Cycle 2	[redacted]	NFDI Directorate
Coscine Login to the research data management platform		[redacted]	NFDI4ING NFDI-MatWerk
JARVES Login to the content-management-system		[redacted]	NFDI4ING
MaRDI Login to the research data portal		[redacted]	MaRDI

Table 10:Identified incubator projects

Milestones and Deliverables

Milestone	Deliverable	Type	Description	Due end of
M3.2		DOC/ DEM	End incubator cycle 1	Month 6
M3.3		DOC/ DEM	End incubator cycle 2	Month 12
M3.4		DOC/ DEM	End incubator cycle 3	Month 18
M3.5		DOC/ DEM	End incubator cycle 4	Month 24

Table 11: WP3 - Milestones and Deliverables

5.2.4 WP4: Operations

WP Lead: GWDG, DAASI

Phase	DFN	**DAASI**	FZJ	**GWDG**	KIT	RWTH	RPTU	**Total**
Year 1 (M1-M12)	0.5	3	2.5 (0.5)	3 (1)	2.5 (0.5)	-	-	**11.5 (2)**
Year 2 (M13-M24)	0.5	3	2.5 (0.5)	3 (1)	3	-	-	**12 (1.5)**

Table 12: WP4 - Contribution by project partners in person months (values in parentheses denote in kind contributions by the partner from existing funding)

This work package handles all work items needed to provide professional operation of the key infrastructure components, i.e., the infrastructure proxy, the NFDI Attribute Authority and single, central instances of the four CAAI implementations, as well as processes to setup single-tenant CAAI implementations for larger communities. The main goals of this work package are:

- to provide CI and CD methods for the software components of the NFDI IAM (hosted as well as specifically developed components),
- to set up and operate an agile, three tier hosting environment for development, staging and production, and
- to design, implement, and maintain common operational functions for the NFDI IAM, e.g., availability management, service continuity management, capacity, and performance management, monitoring and event management, incident management, service level management and 2nd level support.

- to set up a scalable process for the individual components that allows NFDI consortia to obtain CAAI and infrastructure proxies as single-tenant or multi-tenant capable instances (aaS style delivery).

The construction of a secure, reliable, and scalable environment for operations goes hand in hand with the actual implementations and needs to be started early accordingly. This is especially true in the field of CI for the software components of the NFDI IAM, namely the Infrastructure Proxy and potential add-ons, the NFDI Attribute Authority as well as the software that will be created in the incubator projects. CI is a prerequisite for agile software development and secure operations alike, where it is vital to update software components as fast as possible in case of security vulnerabilities. CI tools will also be used to maintain the currency of the handbooks. To ensure undisrupted availability of all functionalities of the NFDI AAI components, an automated software testing during CI for critical components will also be integrated.

For operations, CD allows for automated provisioning, configuration, and scaling of hardware resources as well as the actual deployment of the software components. In this work package, operational models such as container orchestration (e.g., Kubernetes) and automated configuration of runtime environments (e.g., Puppet or Ansible) will be leveraged to meet the requirements regarding availability and performance of the NFDI IAM. Certain components of the NFDI IAM, especially the infrastructure proxy, are necessary for users to log in to and use a majority of NFDI services and therefore need to be highly available. While this also must be considered during implementation, this work package needs to design and provide suitable measures for high availability, e.g., proxying and load balancing user requests on distributed, geo redundant clusters operated by different computing centers.

As to security, it is also planned to have a respective audit of the key components before the actual operation phase. Testing is an important part of development work. In this work package, final system acceptance tests especially with regards to performance, load and fault tolerance will be performed. As a key part of service continuity, backup and recovery strategies will be designed, implemented, and tested. The key components need also to be integrated in monitoring infrastructures so that any incidents and errors can be detected and addressed as early as possible. Finally, all these operational aspects need to be documented in the form of an administration handbook, which will describe potential error situations and how to fix such errors.

This work package will also set up a Service Desk to provide 2nd level support and consulting for the NFDI IAM, e.g., for integrating further NFDI Service- and Identity-Providers and processing service and support requests from administrators and end users, as well as evaluate sustainable business models of the NFDI AAI components.

Milestones and Deliverables

Milestone	Deliverable	Type	Description	Due end of
M4.3			PoC for CI/CD pipelines for NFDI IAM components	Month 3
M4.4			PoC load balancing and proxying for high availability	Month 6
	D4.2		Service Onboarding Handbook	Month 6
M4.5			Service Desk operational.	Month 6
M4.6			Key Infrastructure operationally hardened: ● Load tests ● Recovery installation from Backup ● Monitoring Start of regular operation.	Month 11
	D4.3	DOC	Security Audit	Month 13
	D4.4	DOC	Documentation of the Standard Operational Procedures (SOP).	Month 18
	D4.5	DOC	Administrative Handbook ● Description of Infrastructure setup ● error situations / how to fix errors	Month 18
M4.7			One year of regular operation.	Month 24

Table 13: WP4 - Milestones and Deliverables

5.2.5 WP5: Dissemination, Training, and Community Engagement

WP Lead: RPTU

Phase	DFN	DAASI	FZJ	GWDG	KIT	RWTH	**RPTU**	**Total**
Year 1 (M1-M12)	1	2	2	2	1 (1)	1	4	**13 (1)**

Phase	DFN	DAASI	FZJ	GWDG	KIT	RWTH	**RPTU**	**Total**
Year 2 (M13-M24)	2 (1)	2 (1)	3	3	2 (1)	1	3 (1)	**16** **(4)**

Table 14: WP5 - Contribution by project partners in person months (values in parentheses denote in kind contributions by the partner from existing funding)

To validate the work results and to gather further feedback, the project team conducts infoshare meetings within the Section Common Infrastructures on a regular basis.

During the initialisation phase the following infoshares/workshops were accomplished:

- IAM Basics #1 (07.03.2023 - preparatory phase)
- Infoshare (19.06.2023)
- IAM Basics #2 (24.08.2023)

Those events usually focus on a particular aspect of the IAM service, providing insights in the current state of the service development. Such dissemination activities will be supported by the incubator projects in WP3 that provide respective information material.

Another work item is the organisation and hosting of workshops and training events addressing both the basics of federated identity management / IAM and the installation, configuration, and management of the CAAI implementations.

The continuous workshops and infoshares enable the consortia to play an active role in the development of the NFDI-AAI. These events will be designed and organized in collaboration with the Base4NFDI project team and will be organised according to demand.

Milestones and Deliverables

Milestone	Deliverable	Type	Description	Due end of
	D5.1	DOC	Specification of dissemination strategy and workshop curriculum	Month 2
M5.3		WS	Community AAI implementations	Month 3
M5.4		INFO	Community Infoshares	ongoing
M5.5		INFO	Community Workshops	ongoing

Table 15: WP5 - Milestones and Deliverables

III Appendix

a) Bibliography and list of references

[1] ZKI e.V., „Arbeitskreis Identity und Access Management,“ [Online]. Available: https://www.zki.de/ueber-den-zki/arbeitskreise/arbeitskreis-identity-und-access-management/. [Retrieved August 14, 2023].

[2] DFN e.V., „Dokumentation DFN-AAI, DFN-PKI und eduroam,“ 2023. [Online]. Available: https://doku.tid.dfn.de/de:aai:about#aai_und_identity_management_idm. [Retrieved August 14, 2023].

[3] DFN e.V:, [Online]. Available: https://www.aai.dfn.de/. [Retrieved August 14, 2023].

[4] Géant Association, „eduGain,“ [Online]. Available: https://technical.edugain.org. [Retrieved August 14, 2023].

[15] M. Hardt, S. Apweiler, M. Bonn, P. Gietz, D. Hübner, T. Michels, W. Pempe, C. Pohl und M. Politze, „NFDI AAI Documentation,“ [Online]. Available: https://doc.nfdi-aai.de. [Retrieved August 14, 2023].

[16] DFN e.V., „77. Betriebstagung,“ [Online]. Available: https://www.dfn.de/event/77-betriebstagung/. [Retrieved August 14, 2023].

[17] N. Liampotis, „AARC Blueprint Architecture 2019,“ 2019. [Online]. Available: https://doi.org/10.5281/zenodo.3672785. [Retrieved August 14, 2023].

[18] Géant Association, „Incubator Dashboard,“ [Online]. Available: https://wiki.geant.org/display/GWP5/Incubator+Dashboard. [Retrieved August 14, 2023].

[19] G. Bacharach, P. Gietz, G. Gragert, A. Gündogan, M. Hardt, T. Michels, B. Oberknapp, W. Pempe, R. Pfeiffer, M. Smidt und E. Soldo, „Whitepaper der ZKI AG edu-ID zur Verortung des Konzepts einer edu-ID in der aktuellen Landschaft digitaler Identitäten in Deutschland und Europa,“ 2022. [Online]. Available: https://doi.org/10.5281/zenodo.7425176. [Retrieved August 14, 2023].

[20] SWITCH, „About SWITCH edu-ID,“ [Online]. Available: https://www.switch.ch/edu-id/about/. [Retrieved August 14, 2023].

[21] J. Brauckmann, R. Fischer, P. Gietz, G. Gragert, S. Hofmann, D. Hübner, H. Kaufmann, W. Kuiper, T. Michels, B. Oberknapp, W. Pempe, R. Pfeiffer, F. Schreiterer und E. Soldo, „Eine edu-ID für die Wissenschaft in Deutschland – technisches Konzept,“ 2022. [Online]. Available: https://doi.org/10.5281/zenodo.7418055. [Retrieved August 14, 2023].

[22] REFEEDS, „SIRTIFI,“ [Online]. Available: https://refeds.org/sirtfi. [Retrieved August 14, 2023].

[23] AARC, „Snctfi,“ [Online]. Available: https://aarc-project.eu/policies/snctfi/. [Retrieved August 14, 2023].

[24] IAM4NFDI project team, “Basic Service ‘Identity and Access Management’ for the German National Research Data Management Infrastructure (Initialisation Phase),” public version available: https://doc.nfdi-aai.de/documents/iam4nfdi_initialization.pdf [Retrieved August 14, 2023]

[25] M. Hardt, S. Apweiler, M. Bonn, P. Gietz, D. Hübner, T. Michels, W. Pempe, C. Pohl und M. Politze, „NFDI AAI Documentation,“ [Online]. Available: https://doc.nfdi-aai.de/community-aai-software/. [Retrieved August 14, 2023].

IV Project Gantt Chart

Basic Service IAM Gantt	Initialisierungsphase						kostenneutrale Verl.			Integrationsphase																							
	2023						2023		2024	2024											2025												2026
	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dez	Jan
Work Packages	**M1**	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**	**M9**	**M1**	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**	**M9**	**M10**	**M11**	**M12**	**M13**	**M14**	**M15**	**M16**	**M17**	**M18**	**M19**	**M20**	**M21**	**M22**	**M23**	**M24**
WP1 - Policy, Governance, and Legal Aspects	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
M1.1 Approval of the Policy Documents by the NFDI community	■	■					▨	▨	▨																								
D1.1 Register of FIM-related data processing operations		■					▨	▨	▨																								
D1.2 Finalised Policy Documents		■	■				▨	▨	▨																								
D1.3 Legal Opinion on FIM and Attribute Release in AAI context			■	■	■	■	▨	▨	▨																								
D1.4 Initial concept for rights and roles management in VOs							▨	▨	▨	■	■	■	■	■	■	■	■	■	■														
M1.2 Consultation with key stakeholders							▨	▨	▨											■	■												
D1.5 Updated VO concept, which supports advanced requirements							▨	▨	▨													■	■	■	■	■	■	■	■				
D1.6 Specification of a community process for further development of the NFDI AAI policy							▨	▨	▨																				■	■	■	■	■
WP2 - AAI Architecture and Implementation	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
M2.1 Approval of the Architecture by the NFDI community	■	■					▨	▨	▨																								
~~M2.2 Early Adopter 1: Basic Service DMP~~	■	■	■				▨	▨	▨																								
~~M2.3 Early Adopter 2: Basic Service KGI~~				■	■		▨	▨	▨																								
M2.4 Demonstration Instances of all CAAIs available	■	■	■	■	■	■	▨	▨	▨																								
M2.5 Relevant Policies implemented in all CAAI Instances							▨	▨	▨	■	■	■	■	■	■																		
D2.1 Hosting of CAAIs available as a service							▨	▨	▨					■	■	■	■																
M2.6 Infrastructure Proxy PoC connected to CAAIs							▨	▨	▨						■	■	■																
M2.7 Infrastructure Proxy initial version operational and connected to most CAAI Instances							▨	▨	▨									■	■	■	■												
M2.8 Integration of edu-ID Proxy							▨	▨	▨											■	■												
M2.9 NFDI-Community-AA PoC connected to CAAI							▨	▨	▨													■	■	■	■								
M2.10 All AAI Services operational and initial NFDI Services integrated							▨	▨	▨																■	■	■	■	■				
D2.3 Final documentation on integration of NFDI services with the NFDI-AAI as a whole							▨	▨	▨																					■	■	■	■
WP3 - Incubator	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
D3.1 Approval of decision process for the incubator projects by Base4NFDI			■	■			▨	▨	▨																								
M3.1 Decision on first Incubator Cycle projects					■	■	▨	▨	▨																								
M3.2 Incubator Cycle 1							▨	▨	▨	■	■	■	■	■	■																		
M3.3 Incubator Cycle 2							▨	▨	▨							■	■	■	■	■	■												
M3.4 Incubator Cycle 3							▨	▨	▨													■	■	■	■	■	■						
M3.5 Incubator Cycle 4							▨	▨	▨																			■	■	■	■	■	■
WP4 - Operations	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
M4.1 Identification of software components to be developed and/or operated for NFDI IAM	■	■					▨	▨	▨																								
D.4.1 Concept for the operation of developed and hosted software components		■	■	■			▨	▨	▨																								
M4.2 PoC hosting environments for development and staging of NFDI IAM components				■	■	■	▨	▨	▨																								
M4.3 PoC for CI/CD pipelines for NFDI IAM components							▨	▨	▨	■	■	■																					
M4.4 PoC load balancing and proxying for high availability							▨	▨	▨			■	■	■	■																		
D4.2 Service Onboarding Handbook							▨	▨	▨	■	■	■	■	■	■																		
M4.5 Service Desk							▨	▨	▨	■	■	■	■	■	■																		
M4.6 Key Infrastructure operationally hardened							▨	▨	▨						■	■	■	■	■	■													
D4.3 Security Audit							▨	▨	▨												■	■											
D4.4 Documentation of the Standard Operational Procedures							▨	▨	▨														■	■	■	■	■						
D4.5 Administrative Handbook							▨	▨	▨																■	■	■						
M4.7 One year of regular operation							▨	▨	▨																								■
WP5 - Dissemination, Training, and Community Engagement	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
M5.1 Community Infoshare	■	■					▨	▨	▨																								
M5.2 IAM Basics			■				▨	▨	▨																								
D5.1 Specification of dissemination strategy and workshop curriculum							▨	▨	▨	■	■																						
M5.3 Community AAI implementations							▨	▨	▨			■																					
M5.4 Community Infoshares						■	▨	▨	▨			■			■			■			■												
M5.5 Community Workshops / Hackathons							▨	▨	▨															■			■			■			■