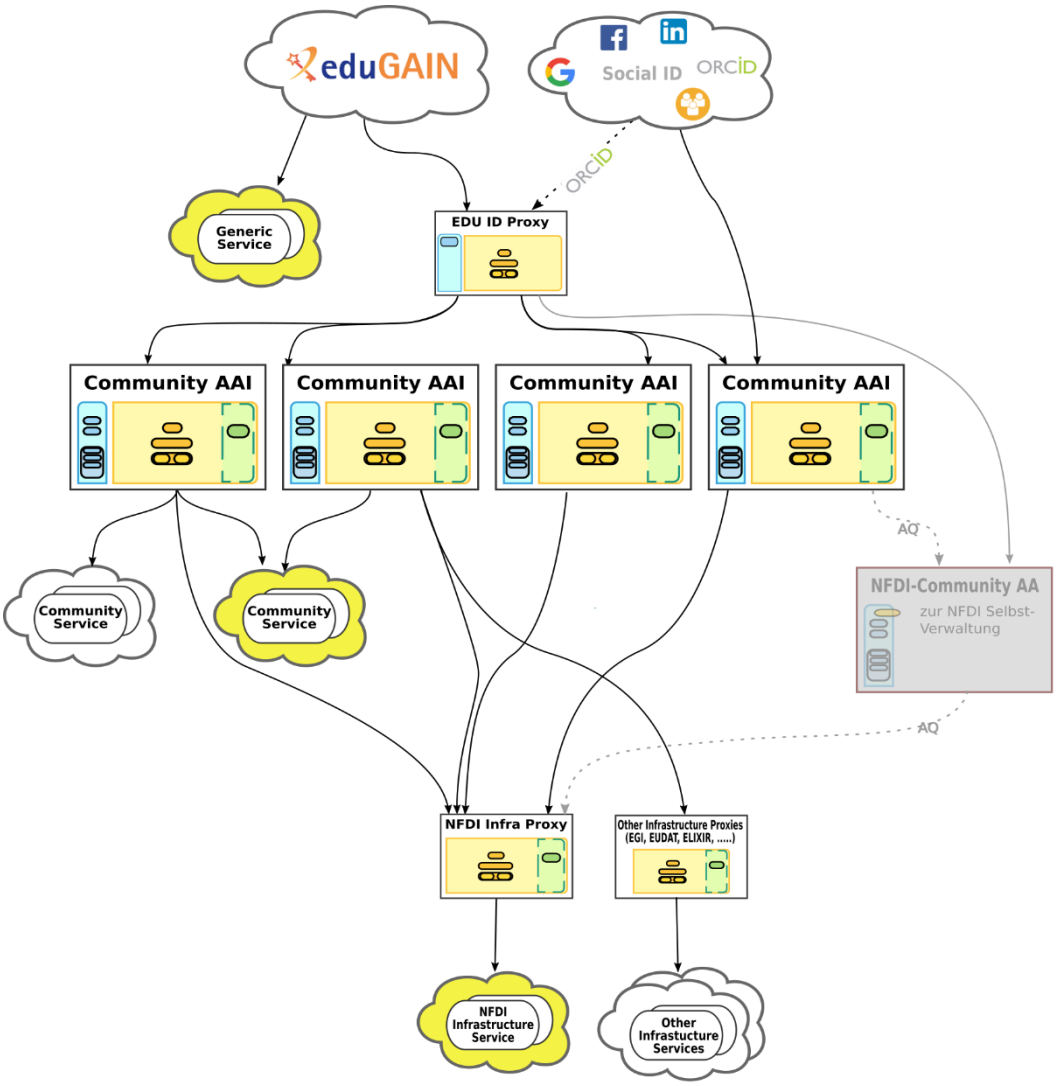
IAM4NFDI

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



Proposal for the Initialization and Integration Phases of Base4NFDI

Submitted: February 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)
  - Politze, Marius (RWTH)
- Participating institutions

Principal Investigator	Institution, location	Contact E-mail	Member in [consortium][1]
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	Base4NFDI

Table 1: List of participating institutions

- Planned runtime of the project
  - Initialisation phase: 6 months
  - 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. In order 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. In order to achieve this, a

[1] Name one DFG-consortium the institution is or has a route to become a member of and through which funds should be appropriated if this proposal is approved.

decentralised, federated Identity and Access Management 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. 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. 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 Identitäts- und Zugangsmanagement 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. 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. State of the Art of Proposed Basic Service

Background and Motivation

Federated Identity and Access Management allows managing who may access consortium services by making use of Virtual Organisations (VOs). Compared to conventional approaches, the suggested IAM basic service integrates existing solutions to provide a more scalable solution. It will be better suited than existing solutions for authorisation for three reasons: First, the use of federated identities allows scientists to use their home organisation accounts, rather than creating new accounts for individual services. This simultaneously unburdens service operators and users. Second, the Virtual Organisation approach introduces an authorisation concept that is decoupled from individual services. This allows services to authorise groups of federated identities rather than individual ones. The benefit for users is that their VO membership can be organised along structures of their scientific communities. It is thus independent of structures imposed by an employer or a service. Another user benefit is the single sign-on experience. In addition, IAM will create a reliable trust framework and enhance the general security of connected systems, by following established recommendations by international bodies, such as FIM4R [5], WISE [6], and AEGIS [7] (i.e. the AARC community). This will also ensure compatibility with currently partially adopted IAM solutions for some consortia, such as DARIAH AAI, Helmholtz AAI and Life Science AAI (formerly ELIXIR AAI). Finally, with this approach, compatibility with EOSC services will be ensured.

Expertise of the partners

Several members of this group have been active members for many years in international federations, initiatives, and projects like FIM4R, AARC, AEGIS, REFEDS [8], and others that serve as a forum for research infrastructures to formulate their IAM requirements. With this background, these members joined the Section Common Infrastructures and formed the Identity and Access Management Working Group (WG IAM).

These partners are well networked inside various NFDI initiatives (including PUNCH4NFDI, DAPHNE, Text+, NFDI4Ing, NFDI-MatWerk, NFDI4Biodiversity, NFDI4Culture, NFDIxCS), as well as expert in various community specific solutions Helmholtz AAI via HIFIS, ELIXIR/Life Science AAI, and B2Access). Experience covers the integration of services, as well as the enhancement of scientific applications, workflows, and services required to be able to cope with AAI requirements.

Operational expertise

- DFN: Operation of an Identity Federation (DFN-AAI), IdP hosting, federating Services

- ZKI AK IAM community of IAM operators at German universities
- DAASI: Expert in agile development and Continuous Integration. Development and operation of the didmos IAM solution. Implementer of the Textgrid AAI and DARIAH AAI (still in use in CLARIA DE). Represented DARIAH in AARC, FIM4R workshops, FIM4L etc.
- KIT: Development and operation of regApp for Identity Management of 10,000 employees and 30,000 students (bw.IDM)
- RWTH: IDM.nrw, development and operation of local IDM for 10,000 employees and 47,000 students
- FZJ: Operation of the Helmholtz-AAI within HIFIS (13,000 users), EUDAT's B2ACCESS, and the PUNCH4NFDI AAI.
- GWDG: Development and operation of AcademicID, an IAM solution for universities, research and higher education institutes in Lower Saxony (120,000 identities), operation of DARIAH AAI (Text+)

State of the art

As for research community AAIs, the AARC Blueprint Architecture (BPA) [9] has established itself as a best practice solution over the last years in several research communities and projects, e.g. in Life Science AAI (formerly ELIXIR AAI). Many research communities and projects participating in EOSC are based on this model. Furthermore, several recommendations of the AARC community define a set of common, widely accepted baseline standards enabling international cross-community interoperability. Lower-level standards such as SAML2 [10] , OIDC [11], OAuth2 [12] or X.509 [13] are well established and well-integrated into the above.

Own Preparatory Work for the Basic Service

The IAM Basic Service is considered to be urgently required by many consortia. In order to get an overview of the requirements and the current state in terms of IAM within the NFDI, the Working Group IAM of the Section Common Infrastructures conducted a survey among the NFDI consortia in 2021, including the upcoming consortia of the third round. Based on the findings of this survey and other feedback from the community, the editorial team of this proposal has started the activity by defining an initial set of key concepts and guidelines for the upcoming NFDI-AAI. Furthermore, in June 2022, the group hosted a three-day workshop in Karlsruhe to advance the work on the AAI architecture. This preparatory work already covers the milestones 1 (AAI Implementation Guidelines - except the data protection aspects), 2 (Identity Space Baseline Scheme) and 4 (IAM Architecture for "one NFDI") of the work plan of the Working Group IAM [14] [15]. It comprises

- a set of policy documents that provide the necessary organisational framework and regulations for operating an AAI. This includes specific points to address GDPR requirements,
- an architecture concept that extends the 2019 version of the AARC Blueprint Architectures to foster the collaboration among NFDI consortia,
- the mandatory and optional sets of attributes that are required to sustain interoperable operation in the NFDI and EOSC contexts, and
- a list of frequently asked questions that were raised during dialogues with NFDI consortia.

To accomplish this, the partners held weekly calls, and one face to face meeting. The invested manpower amounts to roughly 2.5 Person Months, or €16,000.

Current Technical Readiness Level (TRL) of the proposed Basic Service

The IAM Basic Service consists of multiple technical components (see below, section 4) at different TRLs:

- Community AAI as a Service (CAAIaaS)
    - Ordering part (Demonstrator, aaS-style delivery): TRL 4
    - Technical solutions for setting up individual Community AAIs (AcademicID, didmos, RegApp, Unity): TRL 9
- Infrastructure Proxy: TRL 3
- NFDI Community Attribute Authority (AA): TRL 6
- edu-ID Proxy: TRL 4

3. SWOT Analysis

Internal	Strengths 1. in total more than 40 person-years of professional AAI Expertise on Architecture, Policy and Implementation 2. Most of the IAM-related guidelines and policy templates for NFDI AAI have already been provided by the project group. 3. Trust in the expertise of core partners is already well established. 4. Reliable networks (national + international) 5. German eScience AAI Landscape is well organised and interconnected via DFN-AAI (and not divided into clusters) …	Weaknesses 1. Lack of manpower / overloaded individuals 2. Finding new staff for the community is difficult 3. 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 (cf. "AAI und Datenschutz" [16])
External	Opportunities 1. Promote IAM interfaces for cross-organisational and international collaboration 2. Harmonise access to German research infrastructures and services 3. Harmonise and simplify access policies 4. Harmonise and improve security incident response procedures and contacts 5. Reduce administrative cost of existing Access Management	Threats 1. NFDI Consortia implement their own IAM solutions and cause a fragmentation of the NFDI landscape 2. The barrier to federating services and implementing IAM policies may be too high for some consortia

Table 2: SWOT Analysis

4. Working Concept for the development of the Basic Service (max 2.5 pages)

The necessity of an internationally interoperable, and hence scalable, Identity and Access Management (IAM) Basic Service is undisputed and initial requirements have been identified already. The NFDI AAI architecture does not only address access to services within the NFDI, but also access to and exchange with external infrastructures such as the European Open Science Cloud (EOSC), international collaborations (such as CERN, ELIXIR, DARIAH, EGI, PRACE, or ACCESS, formerly XSEDE), national resources such as NHR (National High Performance Computing), HIFIS (Helmholtz Federated IT Services), and, potentially, the GAIA-X ecosystem (e.g. FAIR Data Spaces).

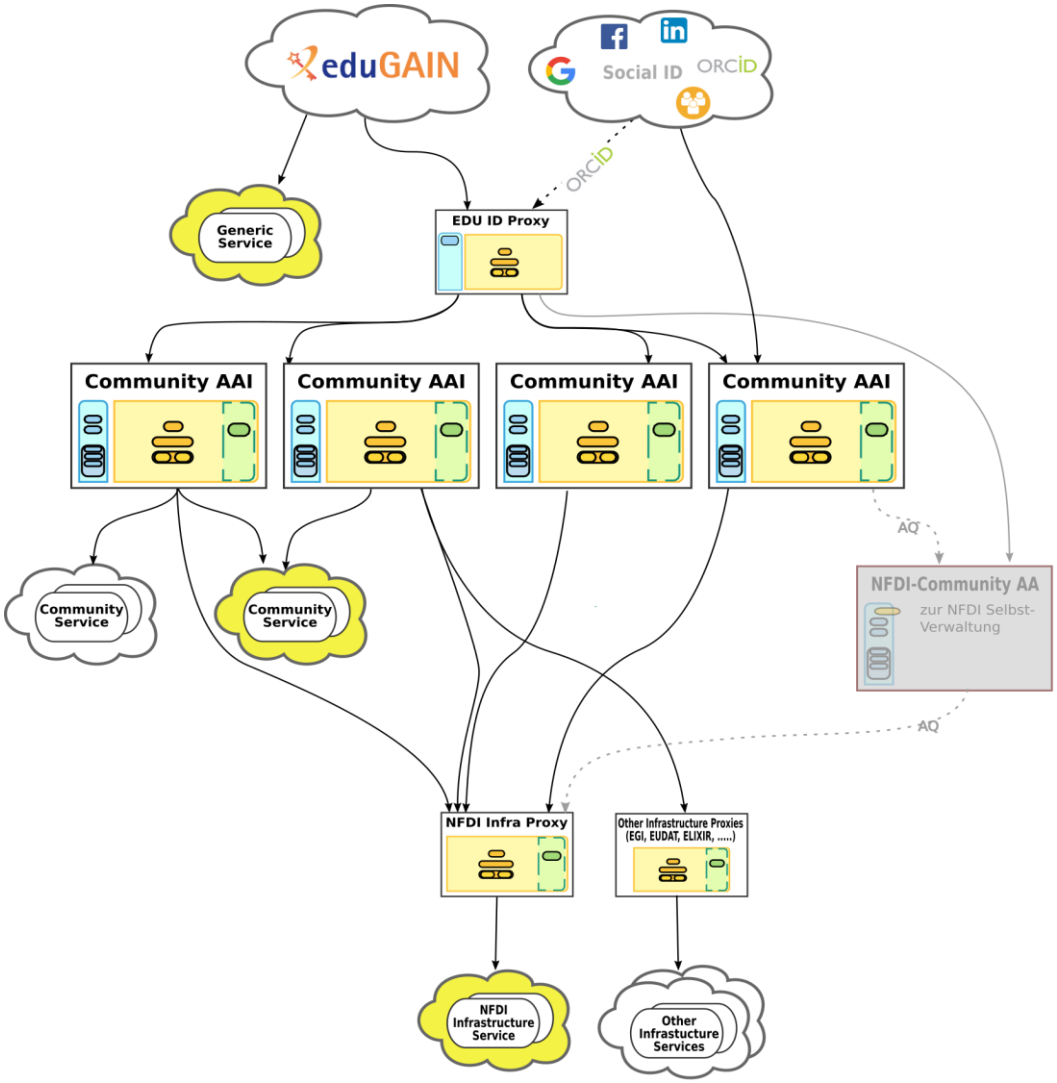


Figure 1: The NFDI Extension of the AARC Blueprint Architecture

In a preparatory phase, the architecture sub-group of the WG IAM analysed an initial questionnaire (see above, Own Preparatory Work for the Basic Service) and aligned the identified

requirements with the approaches defined by the AARC Blueprint Architectures [17], and the EOSC-AAI Roadmap (See figure). As such, the plans for this Basic Service are well embedded within the European and global ecosystem of Federated Identity Management. This preparatory work resulted in an Architecture, which is believed to be scalable, and adaptable to a large span of community requirements. Furthermore, detailed sets of attributes that describe user identities, as well as operational policies, that describe the organisational and operational procedures for making the IAM Services work are already available. The results of the preparatory phase are Documented on a project website [15].

Project goals beyond the State of the Art

With this project, we propose to bring the described architecture to life with particular focus on three key goals:

1. International interoperability for services and users.
2. High Availability and Fault Tolerant operation.
3. Sustainable implementation on state-of-the-art Identity and Access Management. This, probably the hardest goal, can only be achieved, if the benefits of using the Basic Service are evident for the communities. Only this will guarantee future acceptance and funding for continuously operating and developing the IAM Basic Service.

All proposal partners are institutions with a strong track record in the field of IAM. The strength of this group is that it includes all four relevant providers of Community-AAI products, as well as architecture-, and policy experts. The fact that all four different German technical implementations of community AAIs participate in this proposal is of particular importance. The collaboration among these - otherwise competing - solutions addresses environments that we observe on the international level:

- Researchers need to access services that are provided by multiple different Communities.
- Services need to be available to many communities.

The envisaged architecture (Fig 1) enables this cross-community support. The IAM Basic Service proposal is committed to using this multi-community as a strength, by extending the individual technical Community AAI solutions to a) be flawlessly interchangeable and work together, and b) be available to the NFDI-Consortia also in an “as a Service” fashion, known from many popular cloud services.

The Community-AAI-as-aService (CAAIaaS) concept is the best option in the long term.

Given the long term vision of the NFDI, long-term benefits of the CAAIaaS concept, and its diversity of solutions are evident:

- It allows adequate support for different types of user communities with diverse requirements.
- It ensures the NFDI IAM infrastructure will adequately cope with an even more heterogeneous international landscape.
- Trust of an NFDI consortium in any given solution will always include the institution providing that solution. Excluding any German Community AAI from the NFDI solution is therefore not an option.
- Georeplication among all CAAI providers is one key element of the fault tolerance approach in this project.
- A variety of choice for consortia increases their Digital Sovereignty.

Despite all diversity, the strict adherence to architecture, attributes, policies and governance model ensures sustainability, interoperability, and is one key to allow the CAAIaaS concept to work.

Service integration: Unique approach

An additional 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 with support from the Operations in WP4.

Following the successful Incubator concept of GEANT4-3 project in WP5 Task 2 [18], which became mandatory for each WP in GEANT5-1, we also foresee an Incubator in Work Package 3. 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 that will be addressed in the incubator will be agreed upon in joint meetings with B4N/IAM and the IAM representatives of the NFDI Consortia.

Additional technical components

To support advanced use-cases, additional infrastructure components are required.

The **Infrastructure Proxy** provides several technical capabilities. First, it allows the connection of services which need to be accessible for several NFDI Consortia, without specific development on the service side. Second, an Infrastructure Proxy is one place at which authorisation may be enforced, e.g., in cases where a connected service itself is not capable of doing so. In the more distant future, the Infrastructure Proxy may also be the place at which "Identity Linking", e.g., for individuals that use different technical identities, may be applied.

Since the Infrastructure Proxy will need to be integrated from a set of existing components, it will become available during the project. Migration of services from Community-AAI to the Infrastructure Proxy will be possible. The Infrastructure Proxy will be operated in a distributed and fault-tolerant manner.

The **edu-ID Proxy** [19] is a component 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. The edu-ID Proxy is - again - another SP-IdP-Proxy, just as the Community AAI, or the Infrastructure Proxy, with a specific purpose.

The **NFDI Community Attribute Authority** is 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, which are required for a scalable operation and organisation of the NFDI.

Service initialisation concept

Implementations and Installations of the four Community AAI solutions exist. For the NFDI initialisation, those will be installed as demonstration versions for the NFDI consortia to test.
During that testing phase the Community AAI as a Service (CAAIaaS) will be implemented by the supported softwares.
Once this is established, the planned integration and development for the infrastructure proxy will be started.

Development and integration outlook

Own developments are foreseen to be limited to missing components and integration. As such, integration of NFDI-consortia-operated services, as well as the realisation of required features on the infrastructure proxy will be the places where most development will take place.

5. Work Programme

The project as outlined in this document is separated into two project phases. The first phase is planned for six months and contains the immediate steps for initialising the NFDI-AAI, by providing the initial set of policies to the NFDI consortia, setting up an initial demonstration infrastructure for the consortia to get started with, and to provide feedback on the overall architecture. Furthermore, the first Phase will see the initialisation of the operational procedures for the infrastructure, as well as the initialisation of the incubator programme.

The second phase (integration) is planned for two years (month 7 - month 30). At the end of this period, all NFDI consortia will be using production quality AAI services. To minimise further delay, the consortia will be able to use those CAAI services early on in the project, while additional features, and operational hardening will be worked on during the project lifetime. Workplans and cost calculations for this phase are estimates based on current knowledge and might need slight revision towards the end of the first phase.

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 WP5, as well as Dissemination, Training, and Community Engagement in WP5.

Detailed work programme

Overview - Gantt Chart

The Gantt Chart is submitted in the appendix for better legibility.

WP1: Policy, Governance, and Legal Aspects

WP lead: DFN, RWTH

Phase	**DFN**	DAASI	FZJ	GWDG	KIT	**RWTH**	RPTU	**Total**
Initialization (M1-M6)	(2)	0.5	0.5	0.5	0.5	1	-	**5**
Integration Year 1 (M7-M30)	(2)	1	1	1	1	2	2	**10**

Phase	**DFN**	DAASI	FZJ	GWDG	KIT	**RWTH**	RPTU	**Total**
Integration Year 2 (M7-M30)	(2)	1	1	1	1	2	2	**10**

Values in parentheses denote in kind contributions by the partner from existing funding.

This work package will establish a set of binding policies and policy templates, as well as the governance structure of the NFDI AAI. This involves the establishment of clear procedures for transparent decision processes. 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. Starting as early as possible, a clear organisational scheme will be 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 will implement the recommendations of WISE, Sirtfi [22], and Snctfi [23], as it will be 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 General Data Protection Regulation (GDPR), some aspects in the operation of some services in the scientific service landscape are not yet fully understood from a legal point of view. For this purpose, the activities for processing personal data must first be documented. As a further step, a legal opinion on Federated Identity Management and Attribute Release in AAI will be obtained. Depending on the results of the legal opinion, further steps will be taken, like contacting one or more state Data Protection Officers (DPOs) or developing a binding data protection MoU 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
M1.1			Approval of the Policy Documents by the NFDI community	Month 2
	D1.1		VVT[2] / Register of FIM-related data processing operations	Month 2
	D1.2		Finalised Policy Documents, especially the Privacy Policy and Acceptable Use Policy (AUP) templates	Month 3
	D1.3		Legal Opinion on FIM and Attribute Release in AAI context	Month 6
	D1.4		Initial concept for rights and roles management (-> VOs)	Month 16
M1.2			Consultation with key stakeholders	Month 18
	D1.5		Updated VO concept, which supports advanced requirements	Month 26
	D1.6		Specification of a community process for further development of the NFDI AAI policy framework	Month 30
			Project Coordination	

WP2: AAI Architecture and Implementation

WP lead: KIT

Phase	DFN	DAASI	FZJ	GWDG	**KIT**	RWTH	RPTU	**Total**
Initialisation (M1-M6)	(1)	1	1	1	2	1	-	**7**
Integration Year 1 (M7-M30)	(2)	3	3	3	4(+1)	-	-	**15**
Integration Year 2 (M7-M30)	(2)	2	2	2	3(+1)	1	-	**12**

Values in parentheses denote in kind contributions by the partner from existing funding.

This work package focuses on aligning all architecture related aspects with two key stakeholders: The implementation on one hand and the international standards on the other hand.

[2] Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO

In line with the initially defined AAI Architecture [15], this work package will lead the participating Community AAIs to an interoperable mode of operation, which - by the end of the initialisation phase - will be available in a modern, “as a Service” fashion to NFDI Consortia (Community AAI as a Service - CAAIaaS).

Two additional key components 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, we foresee that services are first integrated with the Community AAIs directly, since those will be operational about one year before the infrastructure proxy. A smooth transition of services between Community AAIs and the Infrastructure Proxy will be achieved, by using a standardised attribute set.

Milestones and Deliverables

Milestone	Deliverable	Type	Description	Due end of
M2.1			Approval of the Architecture by the NFDI community	Month 2
M2.2		DEM	Early Adopter 1: Collaboration with Basic Service DMP and implementation of RDMO instances as Community AAI services	Month 3
M2.3		DEM	Early Adopter 2: Collaboration with Basic Service KGI and implementation of KGI instance as Community AAI service	Month 5
M2.4		DEM	Demonstration Instances of all CAAIs available	Month 6
M2.5		DEM	Relevant Policies implemented in all CAAIs	Month 12
	D2.1	DOC	Hosting of CAAIs available as a service	Month 14
M2.6		DEM	Infrastructure Proxy PoC connected to CAAIs Development	Month 14
M2.7		DEM	Infrastructure Proxy initial version operational and connected to most CAAI Instances	Month 18
M2.8		DEM	Integration of edu-ID Proxy	Month 18

Milestone	Deliverable	Type	Description	Due end of
M2.9		DEM	NFDI-Community-AA PoC connected to CAAI	Month 22
M2.10			All AAI Services operational and initial NFDI Services integrated	Month 26
	D2.2	DOC	Final documentation on integration of NFDI services with the NFDI-AAI as a whole.	Month 30

WP3: Incubator

WP lead: RWTH

Phase	DFN	DAASI	FZJ	GWDG	KIT	**RWTH**	RPTU	**Total**
Initialisation (M1-M6)	-	0.5	0.5	0.5	0.5	0.5	-	**2.5**
Integration Year 1 (M7-M30)	(0.5)	3	3	3	3	3	-	**14.5**
Integration Year 2 (M7-M30)	(0.5)	3	3	3	3	2	-	**13.5**

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.

To guarantee an efficient and targeted use of resources, it is foreseen that a decision process will be defined and approved by the NFDI TEC with D3.1 in Month 4. This decision process will involve AAI experts of the NFDI consortia, the section common infrastructures, and the Base4NFDI consortium. Criteria for selection will 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 focussed development, incubator projects are limited to a lifetime of 6 months. At the end of a project, the developments 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.
Appendix IV shows the workflow for the selection of incubator projects in the GN4-3 project, which will serve as a starting point for the definition within this project.
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

Milestones and Deliverables

Milestone	Deliverable	Type	Description	Due end of
	D3.1	Doc	Approval of the precise decision process for the incubator projects by the NFDI TEC	Month 4
M3.1			Decision on first Incubator Cycle projects	Month 6
M3.2		Doc/ Dem	End Incubator Cycle 1	Month 12
M3.3		Doc/ Dem	End Incubator Cycle 2	Month 18
M3.4		Doc/ Dem	End Incubator Cycle 3	Month 24
M3.5		Doc/ Dem	End Incubator Cycle 4	Month 30

WP4: Operations

WP lead: GWDG, DAASI

Phase	DFN	**DAASI**	FZJ	**GWDG**	KIT	RWTH	RPTU	**Total**
Initialization (M1-M6)	(0.5)	2	-	1	-	-	-	**3.5**
Integration Year 1 (M7-M30)	(0.5)	3	3	4	3	-	-	**13.5**
Integration Year 2 (M7-M30)	(2)	3	3	4	3	-	-	**15**

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 Community AAI implementations. The main goals of this work package are:

- to provide Continuous Integration and Delivery 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.

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 Continuous Integration (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.

For operations, Continuous Delivery (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, we will make use of 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 has to 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. Last but not least, this work package will 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.

Milestones and Deliverables

Milestone	Deliverable	Type	Description	Due end of
M4.1			Identification of software components to be developed and/or operated for NFDI IAM.	Month 2
	D4.1	Doc	Concept for the operation of developed and hosted software components. Review policies	Month 4
M4.2			PoC hosting environments for development and staging of NFDI IAM components	Month 6
M4.3			PoC for CI/CD pipelines for NFDI IAM components	Month 9
M4.4			PoC load balancing and proxying for high availability	Month 12
	D4.2		Service Onboarding Handbook	Month 12
M4.5			Service Desk operational.	Month 12
M4.6			Key Infrastructure operationally hardened: ● Load tests ● Recovery installation from Backup ● Monitoring Start of regular operation.	Month 18
	D4.3	Doc	Security Audit	Month 20
	D4.4	Doc	Documentation of the Standard Operational Procedures (SOP).	Month 24
	D4.5	Doc	Administrative Handbook ● Description of Infrastructure setup ● error situations / how to fix errors	Month 24
M4.7			One year of regular operation.	Month 30

WP5: Dissemination, Training, and Community Engagement

WP Lead: RPTU

Phase	DFN	DAASI	FZJ	GWDG	KIT	RWTH	**RPTU**	**Total**
Initialisation (M1-M6)	(1)	-	-	-	-	-	1	**2**
Integration Year 1 (M7-M30)	(1)	2	2	2	1(+1)	1	4	**13**
Integration Year 2 (M7-M30)	(3)	3	3	3	2(+1)	1	4	**19**

Values in parentheses denote in kind contributions by the partner from existing funding.

After a respective requirements analysis, a dissemination plan and workshop curriculum will be specified. In order to validate the work results and to gather further feedback, the IAM-Team will conduct infoshare meetings within the Section Common Infrastructures on a regular basis. Those infoshares will 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 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 community AAI implementations.

These events will be conducted in collaboration with the Section Training & Education.

Milestones and Deliverables

Milestone	Deliverable	Type	Description	Due end of
M5.1		Info	Community Infoshare, presentation of the current work plan for the IAM basic service, NFDI AAI architecture, preliminary announcement of workshops	Month 2
M5.2		WS	IAM basics (explain, present the current architecture as of https://nfdi-aai.de)	Month 3
	D5.1	Doc	Specification of dissemination strategy and workshop curriculum	Month 8
M5.3		WS	Community AAI implementations	Month 9
M5.4		Info	Community Infoshares	ongoing
M5.5		Info	Community Workshops	ongoing

Please note: Further workshops and Infoshares will be organised according to demand.

7. Required Support Actions from Base4NFDI / NFDI Sections / NFDI consortia

Support from	Work package	Contact Person Basic Service
Basic Service DMP	WP2: Early adopter, RDMO instances as first NFDI community AAI services	Jürgen Windeck,, David Wallace juergen.windeck@tu-darmstadt.de, david.wallace@tu-darmstadt.de
Basic Service KGI	WP2: Early adopter, enable login to MediaWiki /Wikibase software with NFDI AAI account	Lozana Rossenova Lozana.Rossenova@tib.eu

Table 8: Support request

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/. [Zugriff am 14 February 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. [Zugriff am 14 February 2023].

[3] DFN e.V:, [Online]. Available: https://www.aai.dfn.de/. [Zugriff am 14 February 2023].

[4] Géant Association, „eduGain," [Online]. Available: https://technical.edugain.org. [Zugriff am 14 February 2023].

[5] FIM4R, „Federated Identity Management - For Research," [Online]. Available: https://fim4r.org/. [Zugriff am 14 Febuary 2023].

[6] WISE, „Wise Information Security for Collaborating E-infrastructures," [Online]. Available: https://wise-community.org. [Zugriff am 14 Feburary 2023].

[7] AARC, „AARC Engagement Group for Infrastructures," [Online]. Available: https://aarc-project.eu/about/aegis/. [Zugriff am 14 Febuary 2023].

[8] REFEEDS, „The Voice of Research and Education Identity Federations," [Online]. Available: https://refeds.org/. [Zugriff am 14 Febuary 2023].

[9] AARC, „AARC Blueprint Architecture," [Online]. Available: https://aarc-project.eu/architecture/. [Zugriff am 14 Febuary 2023].

[10] OASIS Open, „Security Assertion Markup Language (SAML) v2.0," [Online]. Available: https://www.oasis-open.org/standard/saml/. [Zugriff am 14 Febuary 2023].

[11] OpenId, „OpenID Connect Core 1.0 incorporating errata set 1," [Online]. Available: https://openid.net/specs/openid-connect-core-1_0.html. [Zugriff am 14 Febuary 2023].

[12] D. Hardt, „The OAuth 2.0 Authorization Framework," 2012. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6749. [Zugriff am 14 Febuary 2023].

[13] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Husley und W. Polk, „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," 2008. [Online]. Available: https://www.rfc-editor.org/rfc/rfc5280. [Zugriff am 14 Febuary 2023].

[14] W. Pempe und M. Politze, „Concept for Setting up a Working Group in the NFDI Section "Common Infrastructures"," 2022. [Online]. Available: https://doi.org/10.5281/zenodo.6421866.

[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. [Zugriff am 14 Febuary 2023].

[16] DFN e.V., „77. Betriebstagung," [Online]. Available: https://www.dfn.de/event/77-betriebstagung/. [Zugriff am 14 Febuary 2023].

[17] N. Liampotis, „AARC Blueprint Architecture 2019," 2019. [Online]. Available: https://doi.org/10.5281/zenodo.3672785.

[18] Géant Association, „Incubator Dashboard,“ [Online]. Available: https://wiki.geant.org/display/gn43wp5/Incubator+Dashboard. [Zugriff am 14 Febuary 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.

[20] SWITCH, „About SWITCH edu-ID,“ [Online]. Available: https://www.switch.ch/edu-id/about/. [Zugriff am 14 Febuary 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.

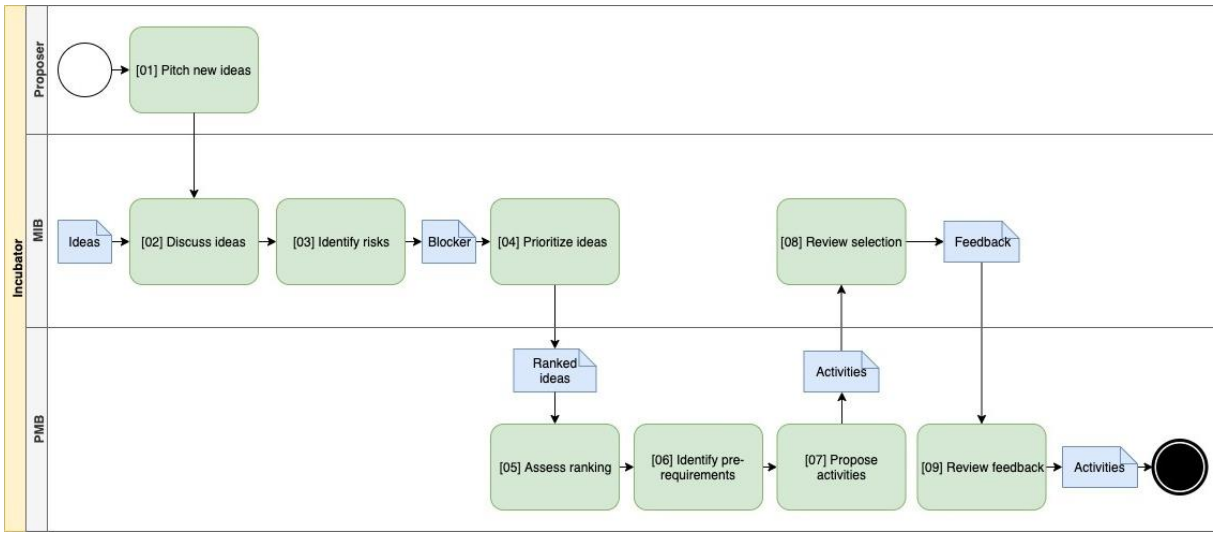
[22] REFEEDS, „SIRTIFI,“ [Online]. Available: https://refeds.org/sirtfi. [Zugriff am 14 Febuary 2023].

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

IV GEANT Incubator Template

Using the GEANT Incubator cycle as a template, this is how we currently envisage the selection process of the incubators:

Here we describe the selection of ideas for an Incubator cycle. Ideas gathered during the year are listed and evaluated by the Main Incubator Board (MIB). Every proposer has to join a MIB meeting at least once to pitch his/her idea to the MIBs. Once the Activitiy Selection process has been completed, the Proposers are required to finalize the project description.



Details about the GEANT incubator process can be found here.

The Incubator Activity Template collecting a reasonable amount of information, when an incubator project is being submitted. We will use this form as our starting point. The form is available at https://wiki.geant.org/x/drAuBw

V Project Gantt Chart

Basic Service IAM Gantt	2023												2024												2025											
	Mar	Apr	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						
Work Packages	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24	M25	M26	M27	M28	M29	M30						
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 framework																																				
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 the NFDI TEC																																				
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																																				