

White Paper on a NFDI4Biodiversity AAI

Barbara Ebert, Martin Zurowietz



NFDI 4
BIODIVERSITY
BIODIVERSITY, ECOLOGY & ENVIRONMENTAL DATA

Imprint

This White Paper is published in April 2025 as part of Task Area 4 Measure 5 in the NFDI4Biodiversity work programme 2020-2025. It is the result of Action 2: Authentication and Authorisation Infrastructure.

NFDI4Biodiversity is funded by the German Research Foundation (DFG) within the framework of an agreement between the Federal Government and the Länder on the establishment and funding of the National Research Data Infrastructure (NFDI) of 26 November 2018 (grant number [442032008](#)).

Cite as

Ebert, Barbara & Zurowietz, Martin: White Paper on a NFDI4Biodiversity AAI. Bremen, 2025, 10 p. [DOI: 10.5281/zenodo.15125477](https://doi.org/10.5281/zenodo.15125477)

Reuse

This work is licensed under a Creative Commons Attribution International License ([CC-BY 4.0](#))



Title illustration

Element from the explainer movie “NFDI4Biodiversity”, produced by Spread the Nerd for NFDI4Biodiversity.

Publisher

GFBio – Gesellschaft für Biologische Daten e.V.
Mary-Somerville-Str. 2-4,
28359 Bremen
Web: www.gfbio-ev.de
E-Mail: info@gfbio.org

Introduction.....	3
I. Starting position.....	3
Solutions currently in use by community members.....	4
DFN-AAI.....	4
Life Science Login.....	5
GFBio SSO.....	5
Solutions being developed for the NFDI: IAM4NFDI.....	5
II. Developing the NFDI4Biodiversity AAI.....	6
Goal 1: Established AAI.....	6
Goal 2: Compatibility with IAM4NFDI.....	6
Goal 3: Consistent user experience.....	7
Goal 4: Centralized authorization.....	8
III. Conclusion.....	9
IV. Outlook.....	9
Acknowledgments.....	10
References.....	10

Introduction

NFDI4Biodiversity is a distributed expert and resource provider network in Germany with a variety of service providers ranging from universities, scientific IT centers, expert organisations and authorities. Our goal in NFDI4Biodiversity (and the NFDI in general) is to provide a coherent [service catalog \[1\]](#) for data providers and users in the community as well as a cloud-based community infrastructure, the [Research Data Commons \(RDC\) \[2\]](#). For the services in this catalog, we aim to improve the accessibility by easy sign-on options. To achieve this, we need to understand how the current practice of authentication and authorisation impacts the user experience. On the provider side, we have to assess the local impacts of introducing a joint authentication and authorisation infrastructure (AAI). The frameworks include provider-oriented identity federations (such as DFN-AAI), two domain-specific IAM systems (GFBio SSO and Life Science Login) as well as local IAM solutions. This report describes the solutions currently used by providers in the wider community and explores options for the introduction of a joint “NFDI4Biodiversity AAI”.

I. Starting position

The full NFDI4Biodiversity service portfolio includes over 90 services from more than 20 providers from universities, scientific IT centers, expert organisations and authorities. A subset of 20 services has been formally onboarded by NFDI4Biodiversity into the public service catalog, which ensures certain standards regarding documentation and operation.

Out of these 20, ten services are web based and require user accounts. These services are the primary focus of this document, outlining the plan for an NFDI4Biodiversity AAI that will be one of the building blocks of the emerging RDC.

Solutions currently in use by community members

Most services of the NFDI4Biodiversity service portfolio and catalog that require user accounts implement “local accounts” that are only valid for the respective service. More than half of the relevant services of the service catalog also support access through federated accounts via GFBio SSO (including DFN-AAI) or Life Science Login (see Table 1). These three solutions are described in more detail below.

Table 1: List of NFDI4Biodiversity catalog services that require user accounts and their respective authentication methods.

Service Name	Authentication Method(s)
Aruna	Life Science Login, GFBio SSO
BEXIS Training Environment	Local Account
BEXIS2	Local Account
BIIGLE	Local Account, Life Science Login
BiodivPortal	Local Account
BioMe	Local Account, Helmholtz ID (AAI)
Diversity Workbench Training Environment at GWDG	GFBio SSO
e!DAL-PGP	Life Science Login
GFBio Submission	GFBio SSO, GitHub, ORCID, Google
VAT	GFBio SSO

DFN-AAI

[DFN-AAI \[3\]](#) is the national German identity federation operated by the DFN e.V., a not-for-profit association providing the German National Research and Education Network. The initial focus of DFN-AAI was to provide access to digital resources such as academic journals or databases. It is well-established in Germany and supports login via more than 400 German universities and research institutes. It also participates in [eduGAIN \[4\]](#), which enables login via another approx. 6,000 organisations worldwide. DFN-AAI is one of the building blocks of the upcoming NFDI AAI (see “Solutions being developed for the NFDI: IAM4NFDI” below) and enables researchers from all over the world to authenticate via their organisations. The organisations acting as “Identity Providers” provide user data such as the

users' names, email addresses or their so-called "affiliations" at their organisations (e.g. "student", "member", "staff", etc.). Support is available via hotline@aai.dfn.de.

Life Science Login

[Life Science Login](#) [5] is the AAI system developed and used by the European Life Science Research Infrastructures and EOSC-Life. It is the AAI system of the [ELIXIR](#) [6] research infrastructure, of which [de.NBI](#) [7] is the German node. The de.NBI cloud is currently the fundamental infrastructure for storage and compute resources in the consortium. Life Science Login offers a wide range of authentication options, supporting eduGAIN, Google, GitHub or ORCID. Life Science Login and the underlying Perun software are operated by Masaryk University, Czech Republic. Support is available via support@aai.lifescience-ri.eu.

GFBio SSO

GFBio SSO is a solution developed and used by [GFBio](#) [8], the German Federation for Biological Data. It enables access to almost 40 internal working environments and external services for scientific end users provided by GFBio and its members. It is based on the [AcademicID](#) [9] software maintained by GWDG, which means the accounts can also be managed by authorised users through the Identity Management Portal of the GWDG. In addition to dedicated GFBio Accounts, which are currently used by more than 75% of the users, GFBio SSO also offers federated login options via DFN-AAI and Life Science Login. GFBio SSO is used to manage access to the internal project management platform of NFDI4Biodiversity as well as some of the catalog services (see Table 1). It is jointly managed by GFBio e.V. and GWDG. Support is available via helpdesk@gfbio.org.

Solutions being developed for the NFDI: IAM4NFDI

The [IAM4NFDI basic service](#) [10] of Base4NFDI develops a common architecture for an AAI connecting all NFDI consortia and their resources and services. Each NFDI consortium is encouraged to adopt a "Community AAI" system. The basic service initially integrates four AAI software products that are developed and maintained by organisations in Germany, one of which is AcademicID. In addition to the Community AAI architecture, IAM4NFDI propagates a set of policies that are required to establish trust between users, communities (resp. virtual organisations), identity providers and service providers both inside and outside of the emerging AAI architecture. In order to enable internal and external interoperability (e.g. with EOSC), the policy framework specifies a common attribute profile. To establish a common "NFDI AAI", the basic service also provides an "NFDI Infra Proxy" (see Figure 1). When a service supports this proxy as an authentication option, any authorized user of a Community AAI can access this service, regardless of which NFDI consortium they belong to.

II. Developing the NFDI4Biodiversity AAI

The original NFDI4Biodiversity project proposal envisioned Life Science Login (formerly ELIXIR AAI) as the solution for the emerging RDC. However, analyses of the service landscape revealed that offering only Life Science Login would be too limiting and not compatible with the plans of the IAM4NFDI basic service. Using AcademicID via the existing GFBio SSO would provide a better basis for the NFDI4Biodiversity AAI. This solution offers the best of all worlds: It is based on a Community AAI software supported by IAM4NFDI, it supports authentication via Life Science Login, addressing users of the de.NBI cloud, and the need to migrate existing services or users is kept to a minimum. Furthermore, it presents a central location to implement possible authorization rules, which may become important in the developing RDC.

In the following sections, this decision is explained based on four main goals that the AAI should fulfill.

Goal 1: Established AAI

We want to adopt an AAI system that is well established in the community and among the consortium partners. In addition, the system should also be accessible to users without an academic affiliation.

Right from the start of NFDI4Biodiversity, GFBio SSO was used as the mechanism to authenticate partners and users with consortia services. It is backed by the AcademicID software which is maintained by partner organization GWDG. While by default, GFBio SSO requires the creation of a dedicated GFBio Account, it also offers federated login options via DFN-AAI and Life Science Login. DFN-AAI supports a wide range of universities and other academic institutions in Germany. Life Science Login expands the scope to the European level and also non-academic users. Supporting Life Science Login is crucial, as it is the only available method to access de.NBI Cloud resources. de.NBI is currently the most important partner of NFDI4Biodiversity in terms of the provided storage and compute infrastructure for the emerging RDC. GFBio SSO combined with DFN-AAI and Life Science Login can serve all existing and future community members and partners of NFDI4Biodiversity.

Goal 2: Compatibility with IAM4NFDI

We want to adopt an AAI system that is compatible with the architecture proposed by IAM4NFDI. In particular, users of other NFDI consortia should be able to access relevant services offered by NFDI4Biodiversity.

AcademicID is the foundation of the GFBio SSO. It is one of the four AAI software solutions that IAM4NFDI recommends and supports as Community AAI for each NFDI consortium. As such, it directly complies with the vision of the "NFDI AAI" architecture developed by the basic service (see Figure 1). With GFBio SSO as the Community AAI of NFDI4Biodiversity, it can be used to allow access both to

community services, which are only relevant for the single consortium, as well as services that are relevant for multiple consortia via the “NFDI Infra Proxy”.

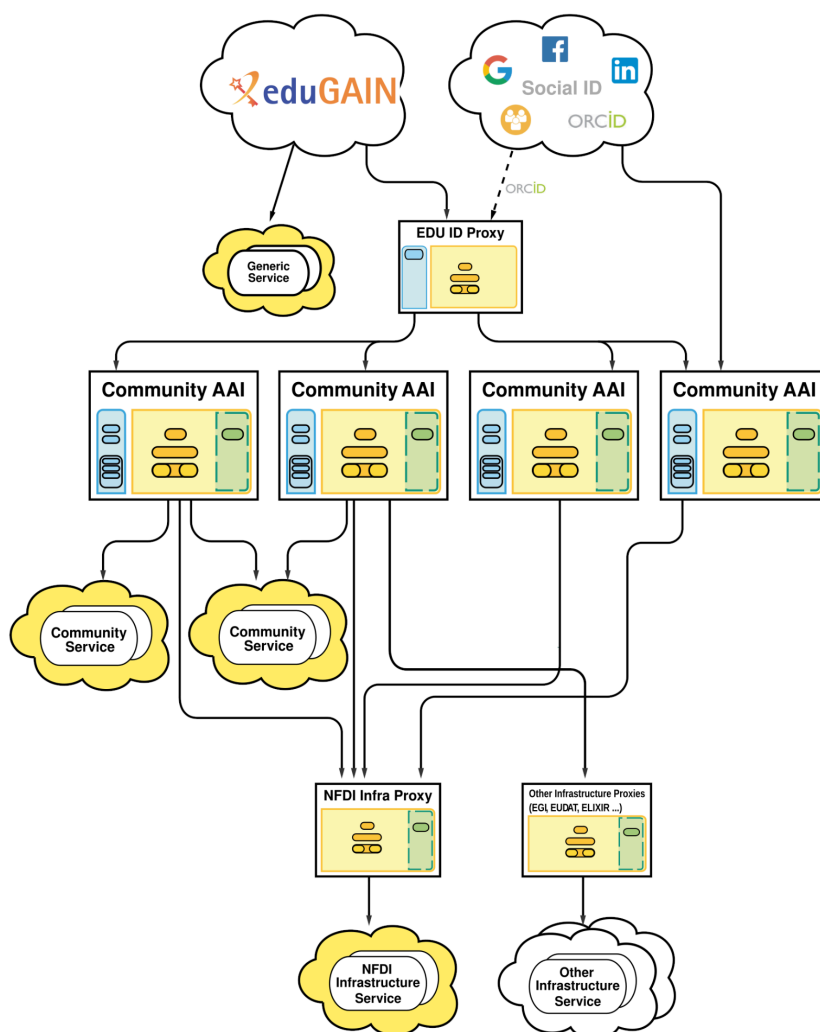


Figure 1. IAM4NFDI architecture v2.5 of Community AAIs that feed into the NFDI Infra Proxy. [CC BY-SA 3.0](#) IAM4NFDI.

Goal 3: Consistent user experience

We want to offer a consistent user experience across different services developed and maintained by the consortium. This means that users should be able to log in to the services by using the same single sign-on mechanism everywhere.

One of the main goals of an AAI in general is to make it easier for users to sign up to services by reusing the same account and credentials. While this is possible with any AAI solution, too many supported AAI systems can provide a bad user experience. On the one hand, users now have to decide which AAI to use and on the other hand, service providers have to decide which AAI to support.

While with GFBio SSO users still have the choice between three different options (DFN-AAI, Life Science Login, GFBio Account), service providers can support only GFBio SSO as single option for authentication to serve the whole NFDI4Biodiversity community. This is an acceptable tradeoff, as established services cannot and should not be easily replaced in a federated network of AAI.

In addition, there is now the opportunity to rebrand GFBio SSO as “NFDI4Biodiversity AAI”. This would highlight its importance for consortium services, take future use cases with centralized authentication into account (see below) and enable clear communication in the context of IAM4NFDI.

Goal 4: Centralized authorization

We want to adopt an AAI system that offers flexible mechanisms for authorization.

One aspect of AAI that has yet to be fully explored is the possibility to implement centralized or federated authorization mechanisms between services. A centralized authorization mechanism manages user group memberships, entitlements or attributes at a single location. Services can request this information from the central location to make authorization decisions (e.g. access to the service itself or resources in the service). A federated authorization mechanism usually employs user attributes to enable authorization decisions. Attributes can be passed on through a chain of different AAI systems, hence the federation. A centralized authorization mechanism is typically more powerful and allows more fine-grained authorization rules than a federated mechanism. As a hybrid solution, federated attributes could also be used to tell services “where to look” for more fine-grained authorization rules at one of several central locations. The level of complexity increases from attribute-based authorization over fine-grained centralized authorization to the most complex hybrid approach.

In a dedicated Resource Provider Workshop held in March 2023 we learned about the authorization capabilities of Life Science Login and presented first ideas for the implementation of authorization mechanisms in our NFDI4Biodiversity services. These ideas followed the common use case where a new user signs up for a service but has to be manually authorized by service administrators before they gain access to certain resources in the service (e.g. file uploads). With an attribute-based AAI authorization mechanism, these authorization decisions could be automated, relieving service administrators of the additional manual work.

In a follow-up discussion with selected RDC service providers we identified a number of use cases for more complex authorization mechanisms. While these use cases are not fleshed out yet, we agreed that we should adopt an AAI system that offers sufficient flexibility in terms of authorization. Even more important than the technical flexibility is to use only a single central service to implement authorization rules. All users who use GFBio SSO are managed by the AcademicID software, even if they log in via a federated account through DFN-AAI or Life

Science Login. This enables central authorization management for all users of NFDI4Biodiversity services in a single location.

III. Conclusion

Following the points above, we conclude that AcademicID via the existing GFBio SSO should be adopted as the Community AAI of NFDI4Biodiversity, under the requirement that the technical provider GWDG ensures the persistent functional integration of DFN-AAI and Life Science Login in GFBio SSO.

To ensure a successful implementation, we recommend that:

- a) The GWDG and GFBio are formally asked to provide the service for the consortium, including documentation and guidance for its use and implementation.
- b) Any service qualifying for the Research Data Commons is required to support the NFDI4Biodiversity Community AAI or the NFDI Infra Proxy.
- c) Providers of services in the NFDI4Biodiversity service catalog in particular (see Table 1) and consortium services in general are actively encouraged to implement support for either the NFDI4Biodiversity Community AAI or the NFDI Infra Proxy. They are offered a dialogue to assess the impact of these decisions on the provision of their services, including opportunities offered by a centralized authorization mechanism. This holds true for existing as well as future services and could be done as part of the service portfolio management activities of NFDI4Biodiversity.
- d) A rebranding of GFBio SSO and a redesign of its login page is considered to better match the (visual) identity of the consortium. The name “GFBio Account” should be kept as an identity that is recognizable by existing users.

IV. Outlook

The selection of a community AAI is an important milestone for the Research Data Commons and the consolidated service provider network envisaged in NFDI4Biodiversity. A continued engagement in the NFDI and ELIXIR activities will help to monitor other national and international efforts that may be relevant for a further integration, like the development of the IAM4NFDI Infra Proxy and the developing EOSC Node federation. Furthermore, the NFDI4Biodiversity AAI could be an option for other NFDI consortia from the life sciences that have not chosen a dedicated community AAI, yet. This would support the notion of a “community AAI as a service” of IAM4NFDI. In summary, we believe that the implementation of the NFDI4Biodiversity AAI, as outlined in this document, will be an important step towards a well-integrated service landscape for research data infrastructures in Germany and beyond.

Acknowledgments

We thank Manuel Feser (IPK Gatersleben), Frank Förster (JLU Gießen), Maria Meister (GFBio e.V.), Wolfgang Pempe (DFN-AAI), Uwe Scholz (IPK Gatersleben), Philipp Wieder (GWDG) and See-Ling Wong (GWDG) for their contributions to this document.

References

1. <https://nfdi4biodiversity.org/de/services/>
2. <https://kb.gfbio.org/pages/viewpage.action?pageId=113904360>
3. <https://www.aai.dfn.de/>
4. <https://technical.edugain.org/>
5. <https://lifescience-ri.eu/ls-login/>
6. <http://elixir-europe.org/>
7. <https://www.denbi.de/>
8. <https://gfbio.org/>
9. https://docs.gwdg.de/doku.php?id=en:services:general_services:academicid:s tart
10. <https://doc.nfdi-aai.de/>