IAM4NFDI Deliverable 1.4

Initial Concept for Rights and Roles Management

A short guide to Virtual Organisation Management within the NFDI-AAI

Version 1, October 2025

Authors: Sander Apweiler[1], Matthias Bonn[2], David Hübner[3], Thorsten Michels[4], Wolfgang Pempe[5]

Funded by DFG as part of NFDI, Grant Number: 521453681

Introduction

This document is intended as a concise introduction to the various aspects of Virtual Organisation Management in NFDI-AAI. It brings together the relevant information from the NFDI-AAI Policy Framework and provides a quick overview of the basic principles and key requirements that must be taken into account when implementing and operating a Virtual Organisation (VO). It does not release the operators of a VO from the necessity of reading the original documents, cf. [IAM-Policies].

Technical Background and Terminology

For the technical concept underlying the NFDI-AAI and the associated technical terms, see [IAM-Architecture].

What is a Virtual Organisation (VO)?

A Virtual Organisation is a group of one or more users, not necessarily bound to a single institution, organised with a common purpose, jointly granted access to one or more services. In many cases, a Virtual Organisation unites the users of a specific research

[1] Forschungszentrum Jülich
[2] Karlsruhe Institute of Technology
[3] DAASI International GmbH
[4] RPTU Kaiserslautern-Landau
[5] DFN-Verein

community represented by one of the NFDI consortia. It may serve as an entity which acts as the interface between the individual Users and an infrastructure like the NFDI and the NFDI-AAI as part of it. In general, the members of the Virtual Organisation will not need to separately negotiate access with Service Providers. A user can be a member of multiple Virtual Organisations. The Virtual Organisation must define, in its Acceptable Use Policy (AUP), its collective aims and purposes, i.e., the research or scholarship goals of the Virtual Organisation. In order to allow Infrastructures to make decisions on resource allocation, the Virtual Organisation should make this information available to them, and subsequently inform them of any material changes therein [VOMMP]. The Basic Service IAM provides templates for AUPs [IAM-Templates]. The AUP of the VO must refer to the AUP of the respective Community AAI (see next section), which allows the VO-AUP to remain very concise and focus on essential information.

How does it work technically?

The technical framework for VO management is provided by a so-called Community AAI (Authentication and Authorisation Infrastructure). Following the AARC Blueprint Architecture [AARC-BPA], it brings together user identities, community attribute services, authorisation, access protocol translation and, finally, community-specific end-services. In this respect, a Community AAI of this kind provides all the tools needed to manage a Virtual Organisation, particularly with regard to rights and role management, and the resulting access rules for community services. Details on how a VO can be rolled out in a Community AAI can be found in the IAM4NFDI Service Onboarding Handbook [IAM4NFDI-ServiceOnboarding].

How is a Virtual Organisation organised?

The Virtual Organisation must define a Virtual Organisation Management role and assign this role to two or more individuals. The Virtual Organisation Management role should be performed by individuals who can authenticate via an Identity Provider that is connected to or part of the NFDI-AAI, but local admin accounts at the respective Community AAIs can also be an option. The Virtual Organisation Management is responsible for meeting the requirements of the applicable policies of the Infrastructures, and for implementing the necessary procedures and operational requirements.

The Virtual Organisation Management does not necessarily have to be a member of the Virtual Organisation. The role may be delegated to any individual by the Virtual Organisation, including Infrastructure personnel.

The Virtual Organisation Management is responsible for registering the Virtual Organisation with the Infrastructure, i.e. the NFDI. The concrete steps and the requirements for this procedure are outlined in the VO Lifecycle Policy [VOLifecycle].

The Virtual Organisation Management must implement procedures that ensure the accuracy of individual User Registration Data for all Virtual Organisation members who act as responsible persons towards the Infrastructure. The contact information must be verified both at initial collection/registration and on an ongoing basis, and only stored and processed in compliance with applicable Data Protection legislation. Other Virtual Organisation roles, such

as additional management personnel and security contacts must be defined and assigned to individuals as required by the Infrastructure [VOMMP]. Changes in these roles must be communicated promptly.

User Management

The Virtual Organisation Management is responsible for the Virtual Organisation Membership life cycle process of its Users. This responsibility may be devolved to designated personnel in the Virtual Organisation or in the Infrastructure, and their trusted agents such as Institute Representatives or Service Managers.

The VO's membership lifecycle comprises the following aspects and related processes:

- Registration
- Assignment of Attributes
- Changes of Assurance Levels
- Renewal
- Suspension
- Termination

The individual points are described in detail in the Virtual Organisation Membership Management Policy [VOMMP]. The (personal) data collected and stored about a user must comply with the Infrastructure Attribute Profile [IAP].

Access Management - Authorisation

As mentioned at the beginning, the main purpose of a VO is to organise and manage access to community services for its users/members. As part of the User Management, users are assigned to specific groups (or roles). Depending on the granularity of access management, mere membership of a VO may be sufficient to authorise access to a specific service; otherwise, this is done on the basis of additional **group memberships** or sub-VOs.

This **membership information** is transmitted to a service via the entitlements claim (or the corresponding SAML attribute) according to a well-defined syntax. Users can be organised in hierarchical groups (i.e. VOs and sub-VOs). Each group membership claim (or attribute) value represents a particular position of the user within a VO. A user may be a member or hold more specific roles within a VO. Groups are organised in a tree structure, meaning that a group may have subgroups, which in turn may have subgroups, etc.This hierarchical structure implies that if someone is a member of a subgroup, then they are also a member of the parent group. For detailed information, please refer to the AARC Guidelines for expressing group membership and role information, AARC-G069 [AARC-G069].

Example:

"urn:geant:dfn.de:nfdi.de:<consortium>:group:<vo-name>:<sub-vo>"

Another approach is for the VO to make specific statements about what a user may do, e.g. whether or not to start VMs, or which datasets may be accessed. In this case, we talk about **Resource Capabilities**. This information is also transmitted via the `entitlements` claim, but then using the `res` and `act` keywords - see AARC-G027 [AARC-G027].

Example:

```
"urn:geant:dfn.de:nfdi.de:<consortium>:res:ant-dataset-42:act:read",
"urn:geant:dfn.de:nfdi.de:<consortium>:res:vm_xyz:act:start-vm"
```

In addition to this information managed by the VO, an authorisation decision may include data provided by external sources like an Identity Provider of a Home Organisation (Home IdP) or an identity proxy such as the DFN edu-ID Portal. In this context, usually three types of information are relevant:

- The **affiliation to a specific Home Organisation** (university, research centre) and its type, e.g. student, staff, faculty...
- **Identity assurance**, i.e. the information on how reliable a digital identity is, how the identity vetting process by the Home Organisation is organised, etc. The REFEDS Assurance Framework has become the standard here and is widely accepted nowadays [REFEDS-Assurance].
- **Authentication context**, i.e. information about how a user was authenticated, e.g. via username and password, via WebAuthn, and whether a second factor was used. As for the latter, a Community AAI could also provide a step-up authentication service for users that come with a single-factor authentication context from their Home IdP.

In the end, it is up to the respective service operator to decide, together with the VO, which information and factors are required for authorisation. It is strongly recommended to keep this as simple as possible and ideally based on **group memberships**.

Further Aspects of VO Management

Apart from the user and access management, there are some additional aspects to consider when operating a VO (for a detailed description, please refer to the Virtual Organisation Membership Management Policy [VOMMP]).

Processing of Personal Data and Data Protection

The Virtual Organisation must have policies and procedures addressing the protection of the privacy of individual users with regard to the processing of their Personal Data collected as a result of their membership in the VO and of their access to services made available by the VO. These policies must be made available in a visible and easily accessible way and users must explicitly acknowledge acceptance of these policies through the AUP and registration process.

Audit Log and Traceability

The Virtual Organisation must record and maintain an audit log of all membership lifecycle transactions (see above, User Management). At the technical level, this is usually handled by the respective Community AAI implementation. This audit log must be kept for a minimum

period consistent with the traceability and logging policies of all infrastructures that provide services to the VO.

Registry and Registration Data

The Virtual Organisation must operate, or have operated on its behalf, a registry that contains the membership data of the VO. This registry must be operated in a secure and trustworthy manner and in compliance with the security requirements of the VO and the NFDI in terms of authentication, authorisation, access control, physical and network security, security vulnerability handling and security incident handling. As for the latter, the VO must comply with the Security Incident Response Procedure Policy [SIRP], which is based on the widely-accepted Security Incident Response Trust Framework for Federated Identity (Sirtfi) [SIRTFI].

Formal Requirements

From the points discussed above and the underlying policies the following formal requirements can be derived that need to be taken into account for a Virtual Organisation:

☐ Provide an Acceptable Use Policy for the Virtual Organisation, including

- A reference to the AUP of the respective Community AAI (see Appendix)
- The email addresses of the VO Managers

(An AUP template is available at [IAM-Templates])

☐ Provide a Privacy Statement for the VO, including

- Contact data (at least email address) for data protection issues, data protection officer or the like

(Privacy Statement Templates in both German and English are available at [IAM-Templates])

☐ Check the VO Lifecycle Policy (available at [IAM-Templates]) and provide

- Contact data of VO Managers and
- A security contact (incident response)

Please note: At the time of writing this document (August 2025), the role of an NFDI VO Supervisor is not assigned yet. Please send the VO registration data to aai-helpdesk@lists.nfdi.de. The IAM project team will keep this information and pass it to the relevant person(s) as soon as the governance concept for the NFDI-AAI is fully implemented.

Bibliography

[AARC-BPA] AARC Blueprint Architecture, https://aarc-community.org/architecture/

[AARC-G027] AARC Consortium Partners, & AppInt members. (2018). Specification for expressing resource capabilities (AARC-G027). Zenodo. https://doi.org/10.5281/zenodo.2247446

[AARC-G069] Valeria Ardizzone, Dominik František Bučík, Marcus Hardt, Stefan Helmert, Jens Jensen, Ivan Kanakarakis, Christos Kanellopoulos, Nicolas Liampotis, Mikael Linden, & Mischa Sallé. (2022). Guidelines for expressing group membership and role information (AARC-G069). Zenodo. https://doi.org/10.5281/zenodo.6533400

[IAM-Architecture] NFDI-AAI Architecture, https://doc.nfdi-aai.de/architecture/

[IAM4NFDI-ServiceOnboarding] Pempe, W., Gietz, P., Michels, T., Bonn, M., Hübner, D., Apweiler, S., Hardt, M., & Wong, S.-L. (2025). IAM4NFDI Service Onboarding Handbook. Zenodo. https://doi.org/10.5281/zenodo.15629651

[IAM-Policies] IAM4NFDI Policy Framework, https://doc.nfdi-aai.de/policies/

[IAM-Templates] IAM4NFDI Policy Framework, Policy Templates at https://doc.nfdi-aai.de/policies/#nfdi-policy-templates

[IAP] IAM4NFDI, Infrastructure Attribute Policy (v0.9.4), https://doc.nfdi-aai.de/policies/#nfdi-policies

[REFEDS-Assurance] REFEDS Assurance Framework version 2.0, https://refeds.org/assurance

[SIRP], IAM4NFDI, Security Incident Response Procedure (v0.9.4), https://doc.nfdi-aai.de/policies/#nfdi-policies

[SIRTFI] Security Incident Response Trust Framework for Federated Identity (Sirtfi), https://refeds.org/sirtfi

[VOLifecycle] IAM4NFDI, Virtual Organisation Lifecycle Policy (v0.9.4), https://codebase.helmholtz.cloud/m-team/nfdi/nfdi-policies/-/jobs/artifacts/v0.9.4/raw/91_VO-lifecycle.pdf?job=build-docs

[VOMMP] IAM4NFDI, Virtual Organisation Membership Management Policy (v0.9.4), https://codebase.helmholtz.cloud/m-team/nfdi/nfdi-policies/-/jobs/artifacts/v0.9.4/raw/01_CAAI-VOMMP.pdf?job=build-docs

Appendix: Community AAI AUPs

Academic ID and Academic Cloud

- https://academiccloud.de/terms-of-use/

didmos CAAI

- https://docs.didmos.nfdi-aai.de/policy/caai-aup-en.html

NFDI RegApp Community AAI

- https://www.isb.kit.edu/english/138.php

Unity / Helmholtz AAI / Punch AAI

- https://login.helmholtz.de/unitygw/hifis/files/acceptable-use-policy.html