

VO-Management

Marcus Hardt
for the IAM4NFDI Team

June 2026

Struktur

- VOs beschreiben **organisatorische Einheiten**
 - Communities
 - Gruppen
 - HPC Rechenzeitprojekte
 - Alles mögliche
- VOs haben “Chefs”: **die VO Manager**
 - VO Manager entscheiden über **Mitgliedschaft**
 - VO Manager entscheiden über **Policies**
- VO Mitgliedschaft wird Diensten über Attribute mitgeteilt
- Dienste geben Nutzungskontingente an VOs heraus
 - VO Manager und Dienst Admin regeln die Details
 - Rechenzeit
 - Speicher
 - **Kosten**

Skalierbarkeit

Viele Dienste + Viele VOs

- VOs immer dann, wenn einfache Attribute nicht ausreichen
 - Studenten, Gäste, Administratoren, ...
- Dienste **brauchen keine individuelle Nutzerverwaltung**
 - (Nutzerkennungen werden weiterhin an Dienste übermittelt)
- Egal wie viele Dienste von eine VO nutzbar sind
 - **Eine einzige Mitgliedschaftsentscheidung** reicht für Nutzung aus
 - **Substrukturierung der VOs** ist selbsterständig möglich

Neue Möglichkeiten

VOs erlauben...

- ...dezentrale Zugriffskontrolle
- ...gruppenbasiertes Accounting (DSGVO konform)
- ...vielfältige KPI
 - Dienstnutzung
 - allgemein / pro VO
 - VO Aktivität
- ...und vermutlich mehr

Wichtig

- Fallstrick: VOs beschreiben **nicht** den Dienstzugriff

Eine VO Namens “OpenStack” ist ein Holzweg!!

Technik

- Attribute für Eigenschaften der Nutzer
 - Für VO Mitgliedschaft
 - [AARC-G069](#) Entitlement
 - Status an der Heimateinrichtung ([AARC-G025](#))
 - Student / Staff / ...
 - Qualität der Identität (LOA) ([AARC-G021](#))
 - Social Media (low)
 - Uni hat den Ausweis gesehen (medium)
 - Darf an der Uni Personaldaten einsehen ()
 - Ausweis wurde gegen eine aktuelle Datenbank geprüft (high (Uganda + US NIH))
 - Multi-Faktor ([REFEDS-MFA](#))
- Details: <https://doc.nfdi-aai.de/attributes>

Policies [1/2]

Was muss wer machen?

- Bitte nicht mit der Rechtsabteilung sprechen
 - Hier werden **keine Verträge** unterschrieben
 - Es geht um **Spielregeln**
- Ziele: **Vertrauen schaffen** (ohne ~~Waffen~~ Verträge)
 1. **Beschreibung von Vorgehensweisen**
 - durchaus verbindlich
 - (z.B. incident response, password management, ...)
 - Geht jemand wegen “password management” zur Rechtsabteilung?
 2. **Policy Framework**
 - Beschreibung innerhalb eines geordneten Rahmens
 3. **DSGVO Konformität** so einfach wie möglich machen

Policies [2/2]

- Welche Policies
 - ... **müssen** von Euch abgesegnet (befolgt) werden
 - NFDI Top Level Policy (TLP)
 - VO Membership Management Policy (VOMMP)
 - Security Incident Response Proecedure (SIRP)
 - Policy on Processing of Personal Data (PPPD)
 - Infrastructure Attribute Policy (IAP)
 - VO Lifecycle Policy (VOLP): Checkliste, guter Einstieg in Policies
 - ... **können** von Euch selbst gemacht werden
 - Community AAI Acceptable Use Policy (CAAI-AUP)
 - **VO Acceptable Use Policy (VO-AUP)**
 - Service Acceptable Use Policy (SAUP)
 - Service Access Policy (SAP)
 - ***-Privacy Policy (*-PP)**
 - ... welche Vorlagen **sollte** ich mir anschauen?
 - **Alle**, aber es gibt keine Überraschungen
 - Template Verfahrnsverzeichnis

NFDI Policies

Alle Policies und Templates finden sich auf unserer Policy website

complies with policy

defines policy	Infrastructure Management	Infrastructure Security Contact	VO Management	Service Provider	SP-IdP Proxy	Identity Provider	User
Infrastructure Management	Top Level Infrastructure Policy						
	SIRP						
	PPPD						
	VO LP			IAP			CAAI AUP
	VOMMP						
VO Management			VO PP				VO AUP
SP-IdP Proxy (CAAI)					Proxy PP		
Service Provider			SAP	SPP	SAP		SAUP

Key:

Existing Policy (Modifications are not encouraged)
Optional Policy (Template available)
Existing Policy (Few Additions necessary)
Required Policy (Template available)

<https://doc.nfdi-aai.de/policies>

Questions?

