Nationale Forschungsdaten Infrastruktur

Concept for Setting up a Working Group in the NFDI Section “Common Infrastructures”

Name of the working group
Identity and Access Management

Acronym
infra-iam

Contact (persons)
DFN-Verein
Wolfgang Pempe
pempe@dfn.de

RWTH Aachen University
Marius Politze
politze@itc.rwth-aachen.de

Authors
Wolfgang Pempe
Marius Politze

1.0

29.03.2022

Abstract

The Working Group Identity and Access Management (IAM) aims to consolidate processes, policies and architectures in order to facilitate the management of digital identities and federated access to resources within and across the NFDI consortia.

The working group therefore follows the three main objectives:
Conceptional work including the evaluation and creation of blueprints, especially the AARC BPA, to establish an AAI for the "one NFDI" as well as concepts for the integration of existing tools and resources in this infrastructure
Connecting NFDI AAI and the NFDI consortia with relevant initiatives on state, national and international levels.
Consulting to support communities and resource providers to connect to the “one NFDI AAI”.

Over the course of the next two years, the working group will follow milestones to (1) provide short term AAI guidelines that allow service providers within the NFDI to connect their services to existing AAI infrastructures, (2) Build a baseline scheme for an identity space to exchange informational attributes about identities, (3) establish role and group management services and finally (4) provide an IAM architecture for the "one NFDI".

Motivation and Objectives

Identity and Access Management (IAM) deals with the processes, policies and technologies for managing digital identities and their access rights to specific resources. The function of IAM is to ensure that the correct user - either a human or a machine user - has the correct access rights to a specific resource at the right time.

One of the main objectives of the NFDI Section Common Infrastructures is the creation of a multi-cloud-based basic infrastructure, enabling unified access to data, software, and compute resources as well as sovereign data exchange and collaborative work. In order to achieve this goal, 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 the NFDI resources as easily as possible, yet in a secure manner. Interoperability is therefore a central requirement, not only within the NFDI but also regarding access to and exchange with external infrastructures like the European Open Science Cloud (EOSC, [EOSC_AAI]), NHR [NHR] and the GAIA-X ecosystem (FAIR Data Spaces, [FAIR-DS]). In order to manage the complex relationships between identity sources, virtual organizations, access management solutions, and any kind of resources, a decentralized, federated Identity and Access Management is required.

The technical and organizational framework for a federated IAM is a so-called Authentication and Authorization Infrastructure (AAI). An AAI is traditionally realized within the framework of national identity federations which are usually operated by the respective national research and education network (NREN) acting not only as generic infrastructure providers but also in particular as 'trust anchors'. The German NREN DFN has been operating the national identity federation DFN-AAI since 2007, one of the largest federations worldwide. Through its modular

architecture and participation in the international interfederation eduGAIN, the DFN-AAI enables international, cross-federation, and cross-community usage scenarios. As for research community AAIs, the AARC[1] Blueprint Architecture (BPA, [AARC_BPA]) has established itself as a best practice solution over the last years in several research communities and projects. According to this pattern, community AAIs operated by one or more research infrastructures connect with an existing national identity federation via a well-defined interface, an SP-IdP-Proxy, which acts as a Service Provider (SP) towards the Identity Providers (IdPs) of the Home Organizations registered in the national identity federation participating in eduGAIN (cf. figure 1). Those proxies are often also connected to additional Identity Providers (IdPs) with a different trust level like Social Sign-on Systems, such as ORCiD.

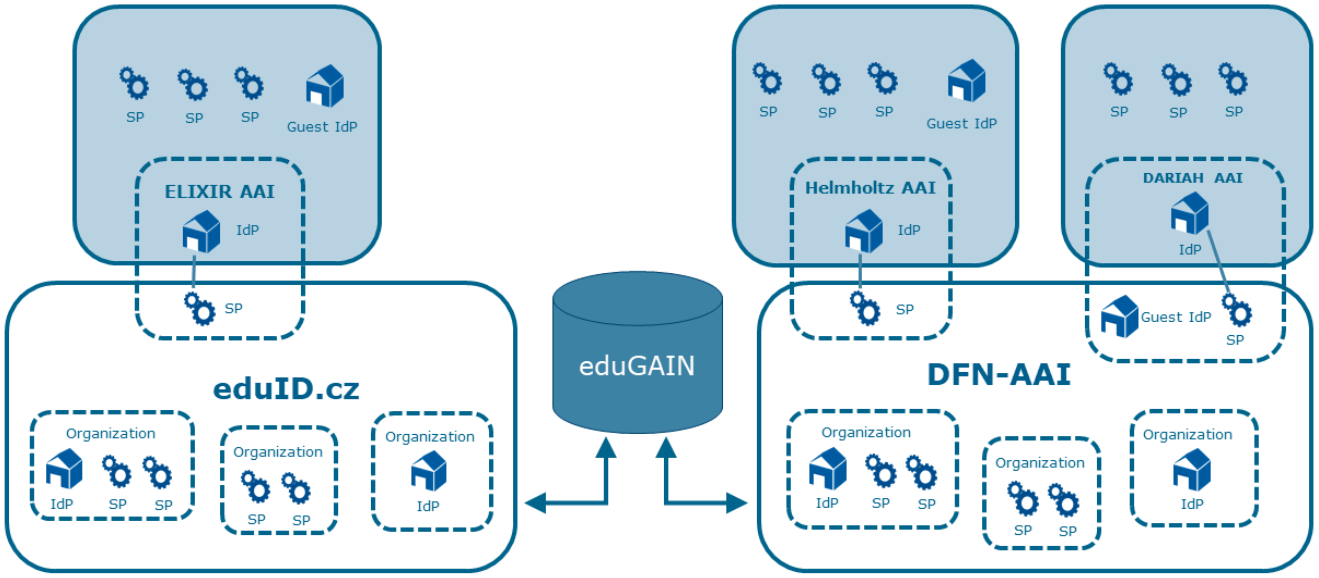

Figure 1: National Identity Federations as Connectors between Home Organizations, Services and Community AAIs.

Therefore, the main objectives of the Working Group IAM are:

- Conception
  - Research on how to implement the AARC BPA for the NFDI, central vs. decentral approaches and components
  - Research on how to integrate already existing IAM solutions and components in an overarching architecture
  - Support a Basic Services Consortium in developing not only a sustainable and interoperable IAM architecture but also the related IAM processes including the management of so-called guest users
- Connecting
  - Close cooperation and exchange with relevant initiatives and infrastructures (see section Collaboration Plan)
  - Gather IAM-related requirements from the NFDI consortia
  - Act as point of contact for a Basic Services Consortium concerning all IAM-related topics
- Consulting

[1] For more information on and the impact of the Authentication and Authorisation for Research and Collaboration project (AARC) please refer to https://aarc-project.eu/about/

- Act as a competence center for IAM/AAI matters within NFDI
- Preventing the formation of non-interoperable silos
- Support the establishment of sustainable IAM governance structures

Work Plan

Based on the above main objectives, the Working Group IAM will provide the nucleus for the NFDI consortia to lay the basis for the vision of "one NFDI" by harmonizing the IAM infrastructures.

Milestone 1 (QX 2022): AAI Implementation Guidelines

Initially the working group will compile a proposal of practical but preliminary guidelines for the implementation of AAI mechanisms in services of the NFDI. The proposal should contain comprehensive recommendations and an initial collection of best practice implementations that can be reused by the individual services in the consortium. Additionally the proposal should include a vision on how NFDI consortia can operate distributed services in compliance with GDPR.

Milestone 2 (QX 2022): Identity Space Baseline Scheme

Identity information is provided by various sources (Universites, Research Organization, Social Sign on Systems, ...). In order to build an identity space across these sources it is required to agree on a common set of baseline standards such as the upcoming AARC schema, and extend it with further information from other schemas, such as eduPerson [eduPerson], schema for academia [schac] and levels of assurance, such as the REFEDS Assurance Framework [raf]. While the academic identity providers like the ones from DFN-AAI have widely agreed on such, information from social sign-on providers need to be mapped to the identity space. The same applies in particular to identity sources that enable institution-independent and lifelong identification of researchers like the well-established ORCID system. The Working Group will work towards providing such a mapping in order to form a common identity space.

Milestone 3 (QX 2023): Role and Group Management

The NFDI consortia pose different requirements on central and distributed facilities for group and access management. The working group aims to propose guidelines for the implementation of Role and Group management mechanisms in a distributed environment that can be adopted by the different NFDI consortia. A set of shared interfaces will ensure interoperability among these solutions.

Milestone 4 (QX 2023): IAM Architecture for "one NFDI"

Putting the previous together, the working group will propose an IAM architecture for the NFDI in accordance with the requirements of the NFDI consortia, the AARC BPA [AARC_BPA] and international initiatives like EOSC and Gaia-X.

Collaboration Plan

The working group will collaborate with various institutions and organizations in the field of AAI and IAM to ensure that the proposed infrastructure is compliant with existing and future developments in these contexts.

The working group will therefore directly cooperate with different Task Areas from the existing and future NFDI consortia. Currently the following collaboration areas were identified but are subject to change once more NFDI consortia are established (especially including a future consortium covering base services):

- NFDI4Ing: Task Area Base Services
- NFDI-MatWerk: Task Area Materials Data Infrastructure
- NFDI4Culture: Task Area Governance and Administration
- Punch4NFDI: Task Area Identity and Access Management
- Text+: Task Area Infrastructure/Operations
- DataPLANT: TA Infrastructure and services

In the national and international context these organizations are

- AEGIS [AEGIS]
- DFN-Verein [DFN]
- EOSC Task Force AAI Architecture [EOSC_TF_AAI]
- EOSC Future Interoperability Framework (Task 3.1) and AAI (Task 7.3)
- FAIR-DS [FAIR-DS]
- Nationales Hochleistungsrechnen (NHR) [NHR]
- State Initiatives: IDM.NRW [IDM_NRW], bwIDM [BW_IDM], RARP [RARP], AcademicID [ACADEMICID]
- ZKI (Arbeitskreis IAM) [ZKI_AK_IAM]

Initial Membership List

DFN-Verein, 2linkNFDI, NFDI4Ing
Wolfgang Pempe
pempe@dfn.de

RWTH Aachen, NFDI4Ing; NFDI-MatWerk
Marius Politze
politze@itc.rwth-aachen.de

Karlsruhe Institute of Technology, Punch4NFDI; NFDI4Earth; NFDI4Ing; NFDI-MatWerk

Marcus Hardt, Michael Simon
hardt@kit.edu, simon@kit.edu

Universität Paderborn, NFDI4Culture
Daniel Jettka
daniel.jettka@uni-paderborn.de

ZKI, TU Kaiserslautern
Thorsten Michels
michels@rhrk.uni-kl.de

Forschungszentrum Jülich, PUNCH4NFDI
Sander Apweiler
sa.apweiler@fz-juelich.de

Technische Universität Dresden, NFDI4Chem
Michael Klix
michael.klix@tu-dresden.de

Leibniz Institut für Pflanzenbiochemie, NFDI4Chem
Steffen Neumann
sneumann@ipb-halle.de

DAASI International GmbH
David Hübner
david.huebner@daasi.de

DAASI International GmbH
Peter Gietz
p.gietz@daasi.de

Gesellschaft für wissenschaftliche Datenverarbeitung Göttingen, Text+, NFDI4Biodiversity
Christof Pohl
christof.pohl@gwdg.de

Technische Universität Darmstadt, NFDI4Ing
Waltraud Büttner
waltraud.buettner@tu-darmstadt.de

RWTH Aachen, IDM.nrw
Aylin Gündogan
guendogan@itc.rwth-aachen.de

HLRS, University of Stuttgart, NFDI4Cat
Jochen Buchholz
buchholz@hlrs.de

HLRS, University of Stuttgart, NFDI4Cat

Miroslav Puskaric
miroslav.puskaric@hlrs.de

HLRS, University of Stuttgart, NFDI4Cat
Volodymyr Kushnarenko
volodymyr.kushnarenko@hlrs.de

IPK Gatersleben, FAIRAgro
Daniel Arend
arendd@ipk-gatersleben.de

References

[ACADEMICID] https://docs.gwdg.de/doku.php?id=de:services:general_services:academicid:start
[AARC_BPA] https://aarc-project.eu/architecture/
[AEGIS] https://aarc-project.eu/about/aegis/
[BW_IDM] https://www.bwidm.de
[DFN] https://dfn.de/
[eduPerson] https://wiki.refeds.org/display/STAN/eduPerson
[EOSC_AAI] https://data.europa.eu/doi/10.2777/8702
[EOSC_TF_AAI] https://www.eosc.eu/advisory-groups/aai-architecture
[FAIR-DS] https://www.nfdi.de/fair-data-spaces/
[IDM_NRW] https://idm.dh.nrw/
[RARP] https://rarp.rlp.net/
[NHR] https://www.nhr-gs.de
[ZKI_AK_IAM] https://www.zki.de/ueber-den-zki/arbeitskreise/identity-und-access-management/