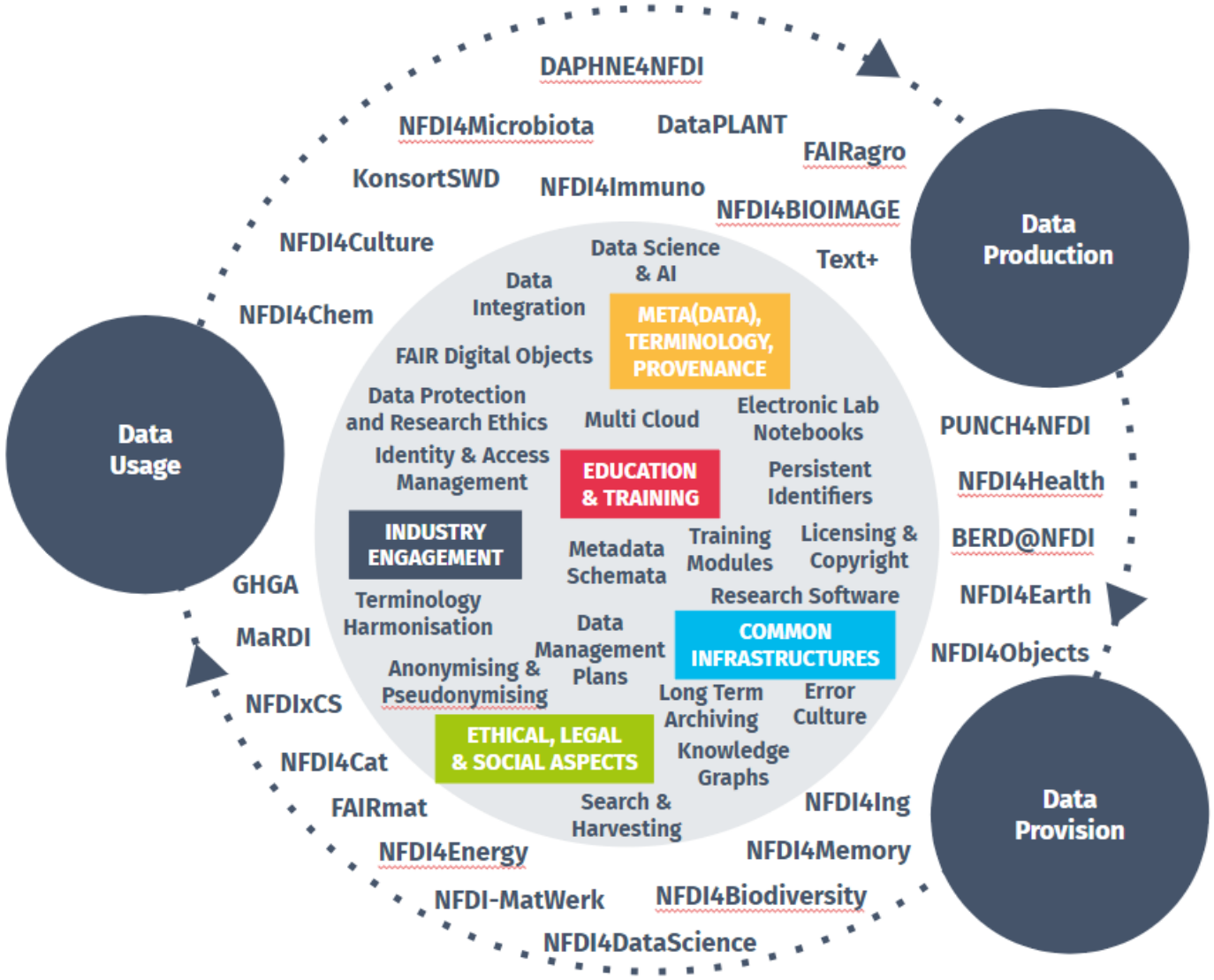
base4 nfdi Basic Services for NFDI

NFDI Basisdienst Identity & Access Management

79. DFN-Betriebstagung, 17. Oktober 2023

Thorsten Michels, RPTU
Wolfgang Pempe, DFN-Verein



base4 nfdi Funded by **DFG** as part of **NFDI**.
Grant Numbers: 521453681, 521460392, 521462155, 521463400, 521466146, 521471126, 521473512, 521474032, 521475185, 521476232

Agenda

- Kurzvorstellung NFDI
- Basisdienste und Base4NFDI
- Beteiligte
- Ausgangslage und Vorarbeiten
- Lösungsmodell, NFDI-AAI
- Verhältnis zur DFN-AAI
- Details zum Projekt

IAM4nfdi

Identity and Access Management for the German National Research Data Infrastructure

Nationale Forschungsdateninfrastruktur - NFDI

- Geht zurück auf Empfehlung des Rats für Informationsinfrastrukturen in 2016
- Förderung geplant über 10 Jahre (bewilligt: 5 Jahre)
- 1. Runde ab Oktober 2020: 9 Fachkonsortien
- 2. Runde ab Oktober 2021: 10 Fachkonsortien
- 3. Runde ab März 2023
  - 7 Fachkonsortien

    sowie
  - Base4NFDI – Verbundantrag zur Implementierung von Basisdiensten für die NFDI
- … und das Direktorat

Weitere Infos unter https://www.nfdi.de

NFDI – Sektionen und Arbeitsgruppen

- Sektionen adressieren Konsortien-übergreifende Querschnittsthemen
- Sektionen strukturieren ihre Aktivitäten in Arbeitsgruppen (Working Groups)
- Sektion **Common Infrastructures** (https://www.nfdi.de/section-infra/)
  - WG Data Integration (DI)
  - WG Data Management Planning (DMP)
  - **WG Identity and Access Management (IAM)**
  - WG Persistent Identifiers (PID)
  - WG Long-term Archival (LTA)
  - … und aktuell 5 weitere

base4 nfdi

WG Identity & Access Management (IAM)

- Konzeption einer zukünftigen IAM-Infrastruktur für die NFDI
  - Milestone 1: AAI Implementation Guidelines
  - Milestone 2: Identity Space Baseline Scheme (u.a. Attribute)
  - Milestone 3: Role and Group Management
  - Milestone 4: IAM Architecture for “one NFDI”
  - Konzept: https://doi.org/10.5281/zenodo.6421866
- Eine Untergruppe (“Kernteam”) bearbeitete dezidiert Baseline Scheme und Architecture
  - Orientiert sich an AARC Blueprint Architecture und Guidelines (https://aarc-community.org)
  - Empfehlungen zur Verwendung von Software für **Community-AAIs**
  - Aktueller Stand: https://www.nfdi-aai.de

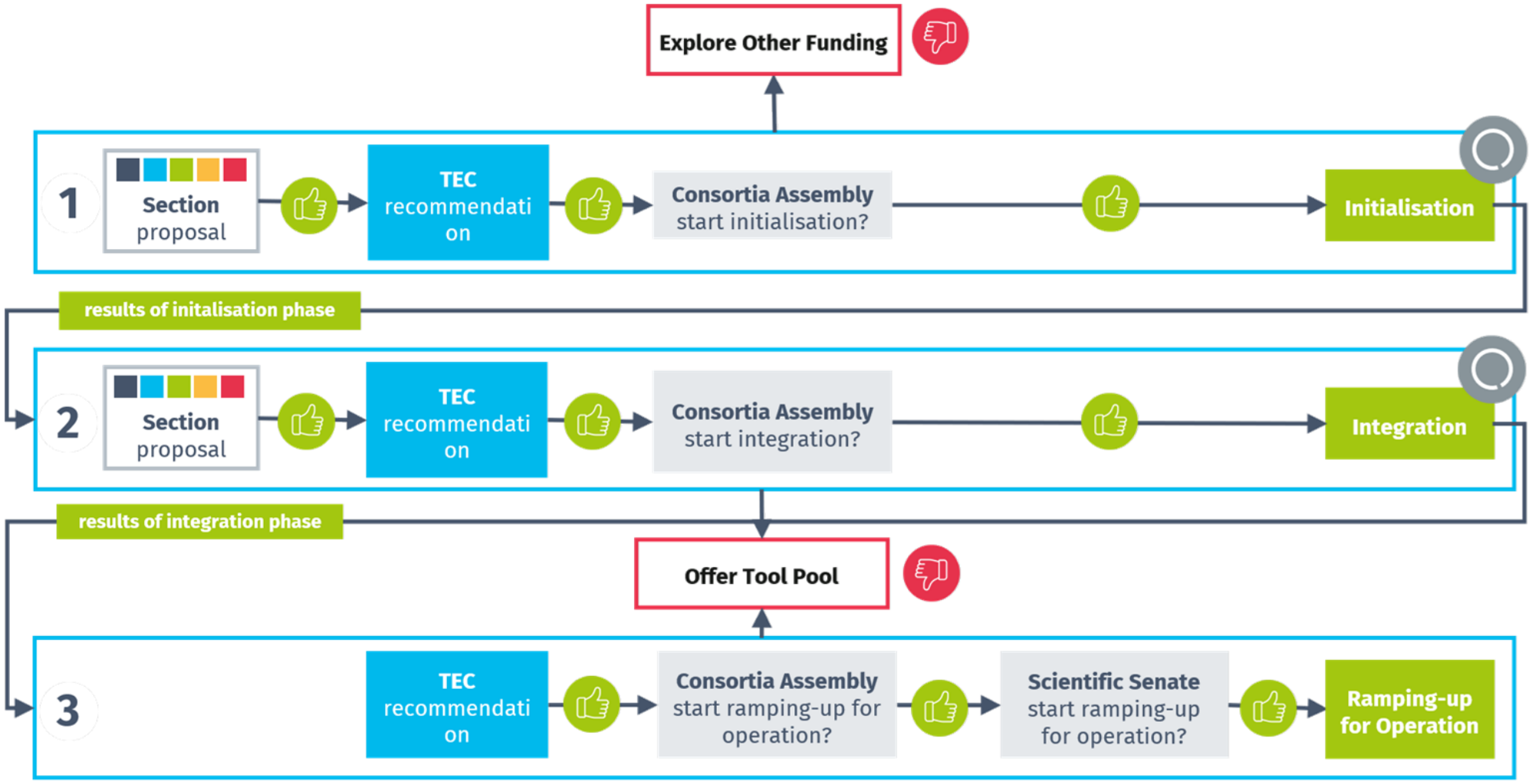
Base4NFDI – Basic Services for NFDI

- Ein Verbundvorhaben aller 26 Fachkonsortien
  - gem. Beschluss der GWK im November 2022, zusammen mit 7 Fachkonsortien der 3. Runde
  - Projektbeginn 1. März 2023, Koordinator Prof. Lars Bernhard, TU Dresden
  - https://www.base4nfdi.de
- Base4NFDI bietet „Rahmen und Inhalt“ für die Entwicklung von Basisdiensten in der NFDI
  - feste Mittel für den Rahmen, d.h. Steuerung und Organisation über u.a. Service Stewards
  - flexible Mittel für die inhaltliche Arbeit an Basisdiensten –
    hierfür ist projektinternes Antragsverfahren in drei Phasen vorgesehen, s.u.
- Antrag formuliert bereits beispielhaft drei Themenfelder für mögliche Basisdienste
  - Identity and Access Management, Persistent Identifiers, Terminology Service

Förderung von Basisdiensten: Ansatz

- die Entwicklung eines Basisdienstes ist in drei Phasen angelegt
  - Initialisation (ca. 3 FTE über 1 Jahr)
  - Integration (ca. 6 FTE über 2 Jahre)
  - Ramping Up for Operations (ca. 4 FTE über 1 bis max. 3 Jahre)
- jede Phase wird separat beantragt, begutachtet und finanziert
  - mit steigenden Anforderungen an die Unterstützung aus Sektionen und Fachkonsortien
  - Technical Expert Committee in Base4NFDI formuliert Empfehlungen zu den Anträgen
  - Entscheidung über Aufnahme in die Förderung erfolgt in Konsortialversammlung der NFDI
  - die Einreichung von Anträgen zu den ersten beiden Phasen erfolgt über die Sektionen
- abgebrochene Vorhaben wandern ggf. in „Tool Pool“ der Fachkonsortien außerhalb Base4NFDI

Förderung von Basisdiensten: Bewilligung



Stand der Vorhaben für Basisdienste

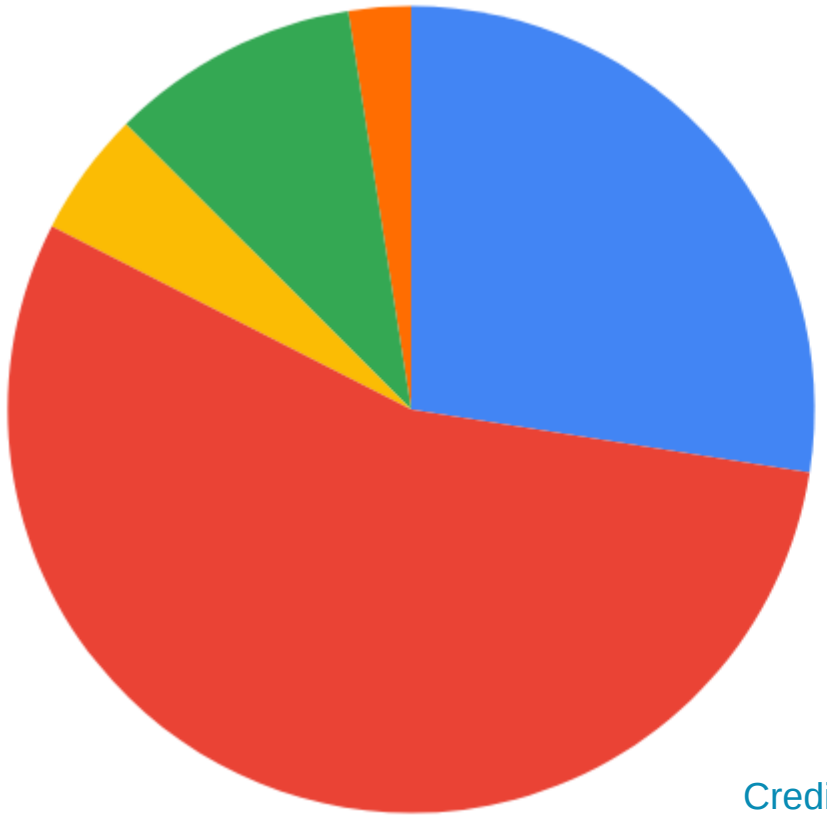
- in Initialisierungsphase aufgenommen und begonnen
  - 05/2023–01/2024 IAM4NFDI – Identity & Access Management
  - 08/2023–07/2024 TS4NFDI – Terminology Services
  - 09/2023–08/2024 PID4NFDI – Persistent Identifier Service
- eingereichte Anträge zur Aufnahme in Initialisierungsphase (Begutachtung in 10/23)
  - NFDI Research Software Marketplace „nfdi.software“
  - Jupyter4NFDI
  - Competence Training for Research Data Management „RDMTraining4all“
- erster eingereichter Antrag zur Aufnahme in Integrationsphase (Begutachtung in 10/23)
  - IAM4NFDI

Vorarbeiten Arbeitsgruppe und „Kernteam“

- Survey zur Anforderungsanalyse Ende 2021
- Architektur-Workshop Sommer 2022
- IAM Basics Workshop März 2023

Requirements Analysis

Why is your service interested in the Authentication aspects of AAI



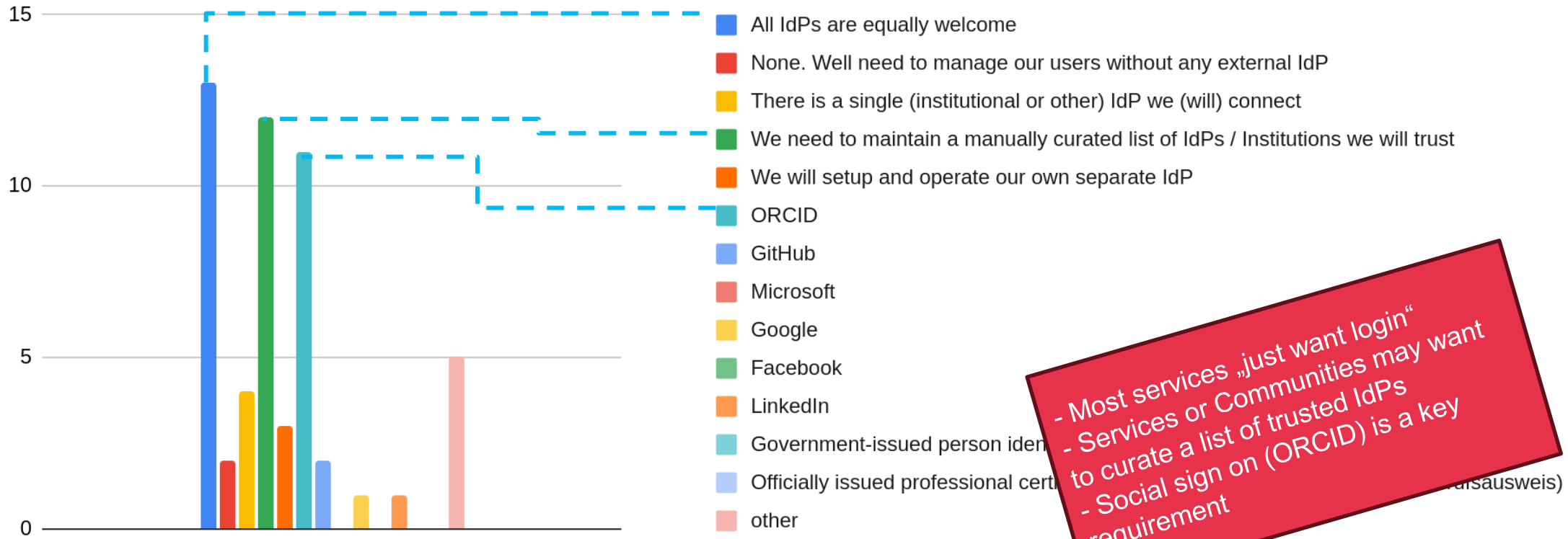
- We want to improve the user experience by avoiding yet another account on their side
- We need to enable/ensure a common user identity (namespace) across several services
- We want to avoid having to deal with password management ourselves
- We aim to minimize that users create [illegible] unconnected accounts within [illegible]
- other

- Interlinking of user assets in between services → need a shared user identifier.
- User should have the experience of a single login for all NFDI related services

Credit: Marius Politze, RWTH

Requirements Analysis

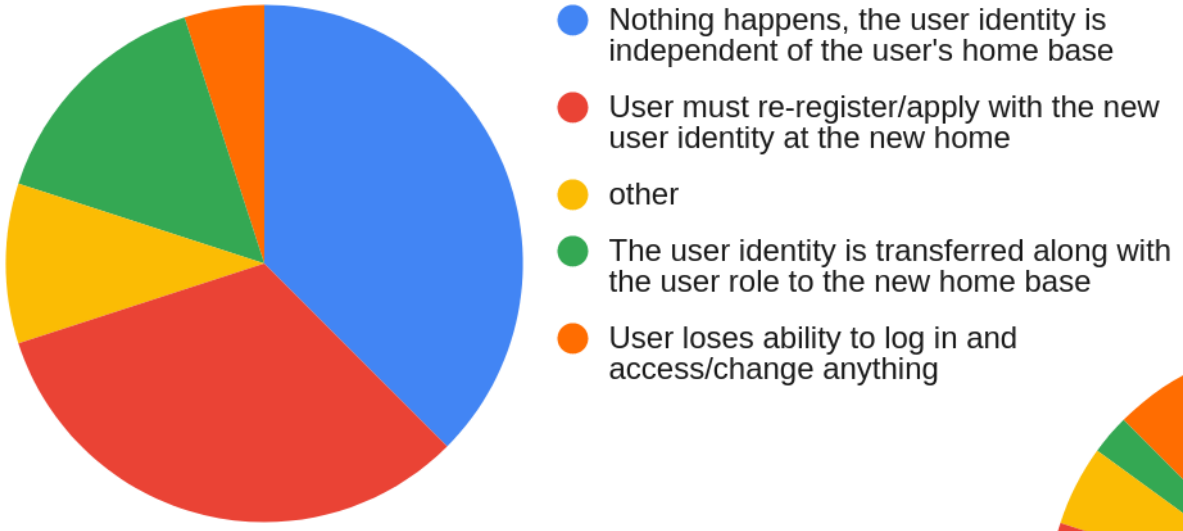
Preferred Identity provider for users

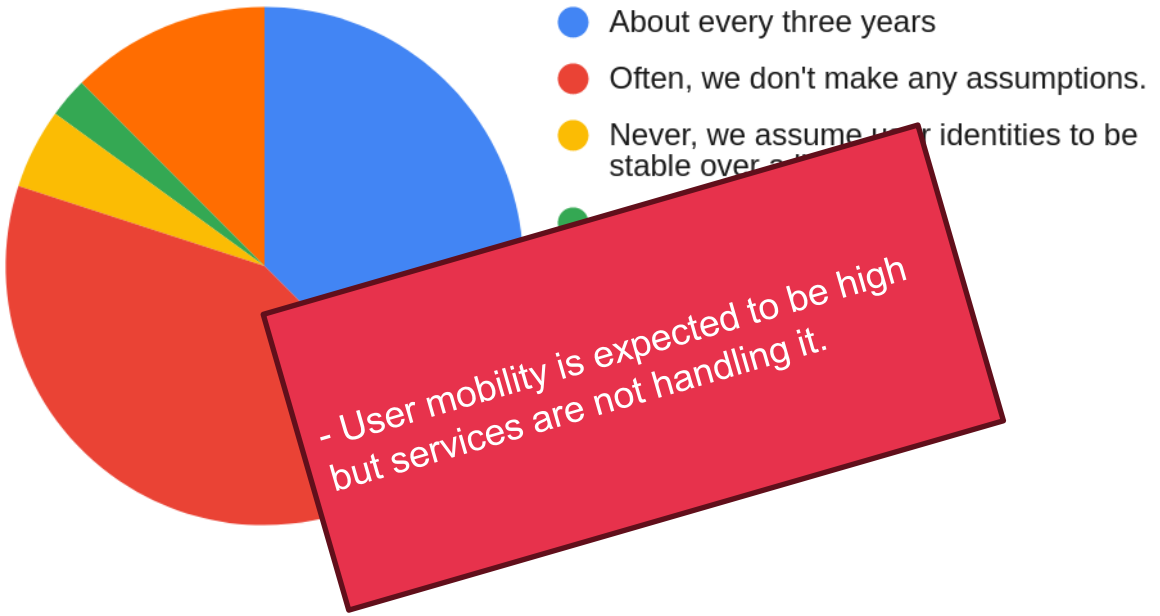


Credit: Marius Politze, RWTH

Requirements Analysis

Consequence and Frequency of user mobility

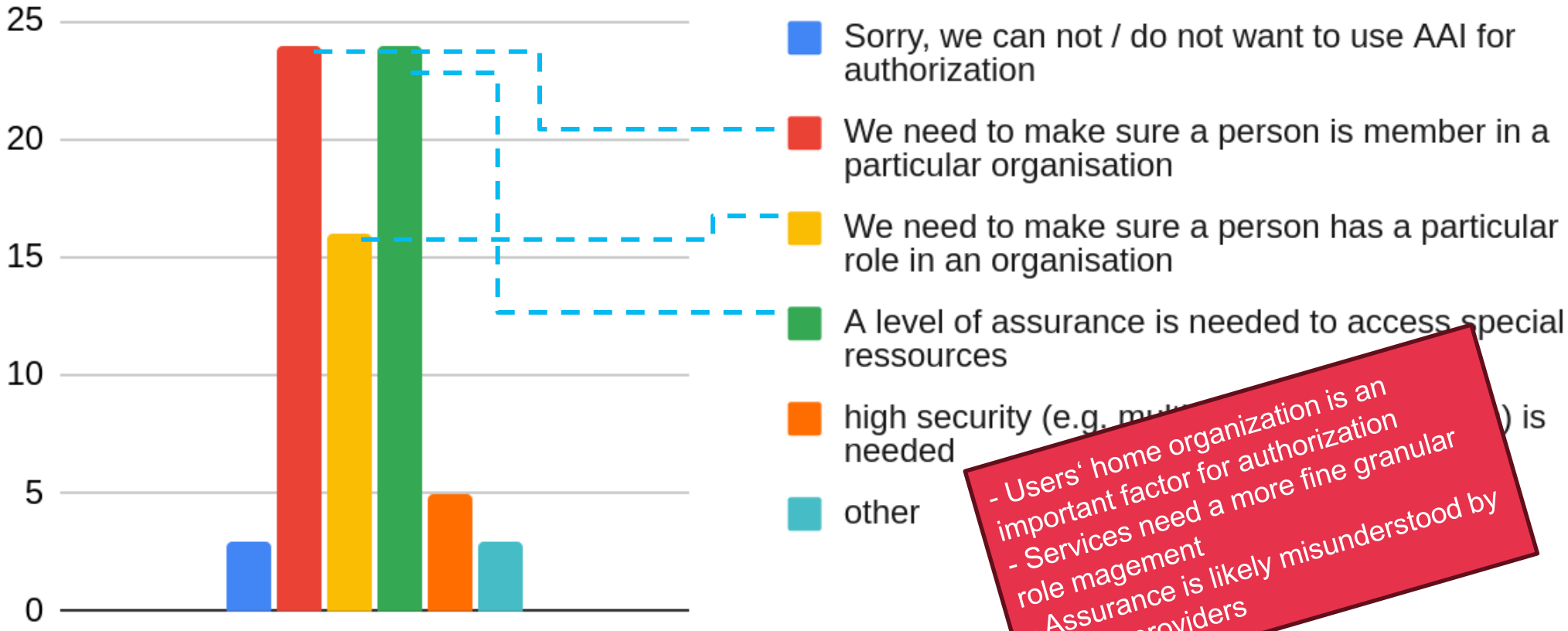




Credit: Marius Politze, RWTH

Requirements Analysis

Why is your service interested in the Authorization aspects of AAI?

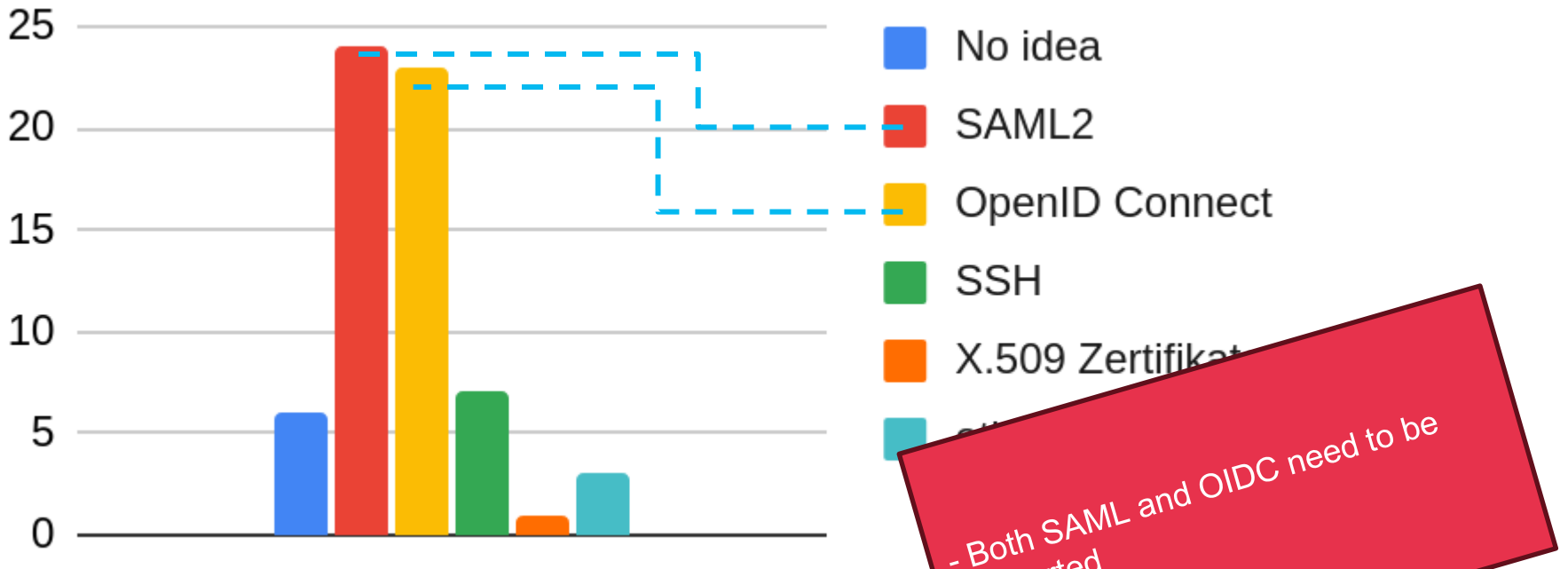


- Users‘ home organization is an important factor for authorization
- Services need a more fine granular role magement
- Assurance is likely misunderstood by service providers

Credit: Marius Politze, RWTH

Requirements Analysis

Which login standards / protocols are being used



Credit: Marius Politze, RWTH

Basisdienst IAM4NFDI

- durchläuft derzeit Initialisierungsphase, Integrationsphase beantragt
- Eckdaten Initialisierungsphase
  - RWTH und DFN als Co-Lead, weitere Partner sind GWDG, KIT, FZJ, RPTU und DAASI
  - begonnen am 1. Mai 2023, Laufzeit 9 Monate
  - Homepage Basisdienst: https://base4nfdi.de/?view=article&id=30&catid=2
- Eckdaten Integrationsphase
  - Antragspartner unverändert
  - beabsichtigter Beginn zum 1. Februar 2024, Laufzeit 24 Monate
- weiterführende Informationen einschließlich Anträge unter https://www.nfdi-aai.de

Ausgangspunkte für IAM4NFDI

- die übergreifende Behandlung des Themenfeldes „Identitäts- und Access Management (IAM)“ wurde bereits früh in der NFDI gefordert (2linkNFDI, diverse Positionspapiere, Expertengremium)
- … einerseits mit Verweis auf etablierte Strukturen, Prozesse und Regelungen
  - Identity Management in den Einrichtungen, Authentifizierung über Heimat-Identität
  - DFN-AAI einschl. internationaler Anbindung
- … andererseits begleitet vom Wunsch nach Erweiterung um zusätzliche Funktionalität, u.a.
  - Verwaltung Community-spezifischer Rechte und Rollen zur Autorisierung
  - Verwaltung von Nutzenden außerhalb teilnehmender Einrichtungen
  - Account Linking
- Ergebnisse der Anforderungsanalyse, Interoperabilität mit EOSC

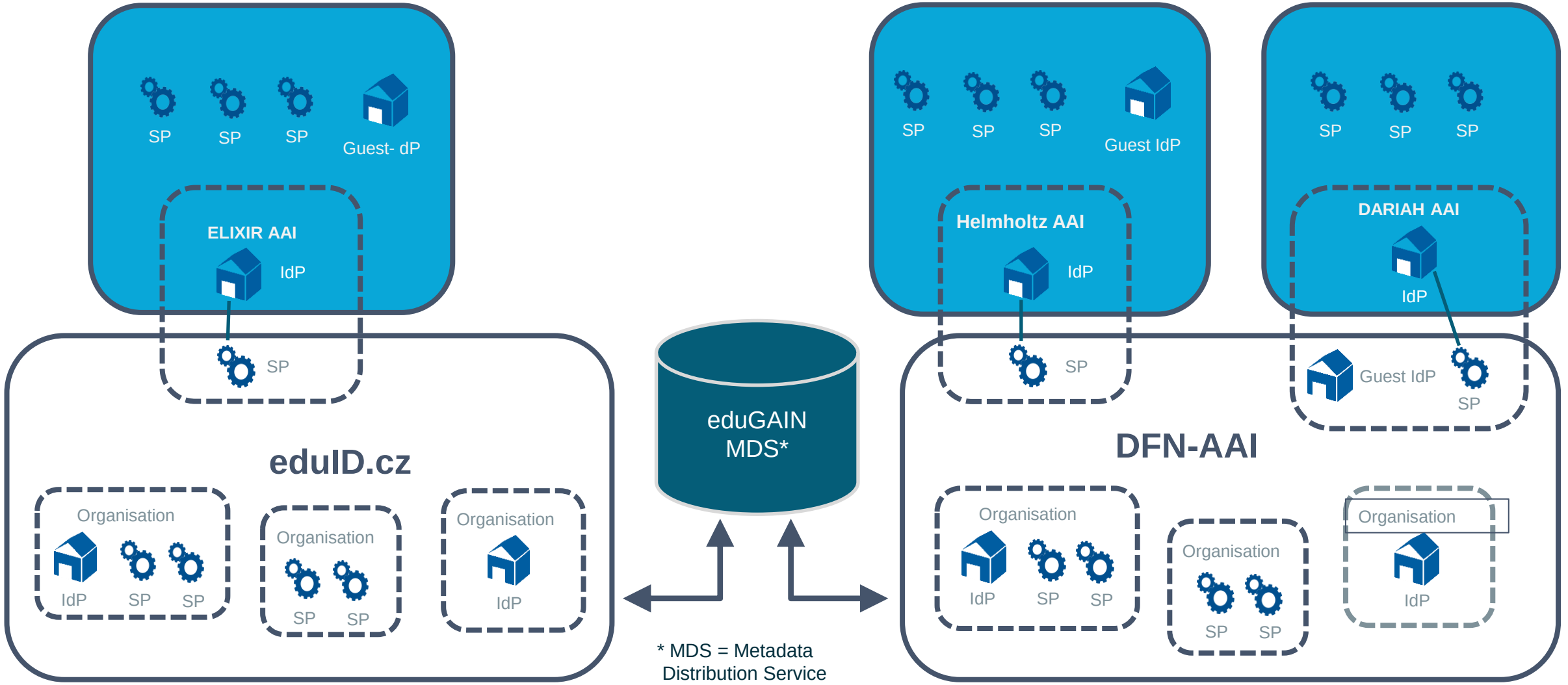
Ansatz von IAM4NFDI – Allgemein

- Notwendigkeit – und Möglichkeiten(!) – von Interoperabilität in den Vordergrund stellen
  - nichts neu erfinden, was es schon gibt und was schon läuft
  - wann immer möglich auf Vorhandenes aufbauen
- Vermittlung des Status Quo hat höchste Priorität in der Initialisierungsphase
  - allgemeine AAI-Architektur
  - Infrastruktur-Komponenten
  - Attribut-Profile
  - Policy Framework
- Erkenntnis nach Diskussionen und aus Bedarfserhebung
  - technisch fehlen (lediglich…?) Community-spezifische Komponenten

AAI-Architektur

- AAI: Authentifizierungs- und Autorisierungs-Infrastruktur
- NFDI-AAI und Community-AAIs (siehe unten) sind kein Ersatz und keine Parallelstruktur zur DFN-AAI.
- Die NFDI-AAI wird die Strukturen der DFN-AAI, vor allem die Metadatenverwaltung, mitbenutzen.

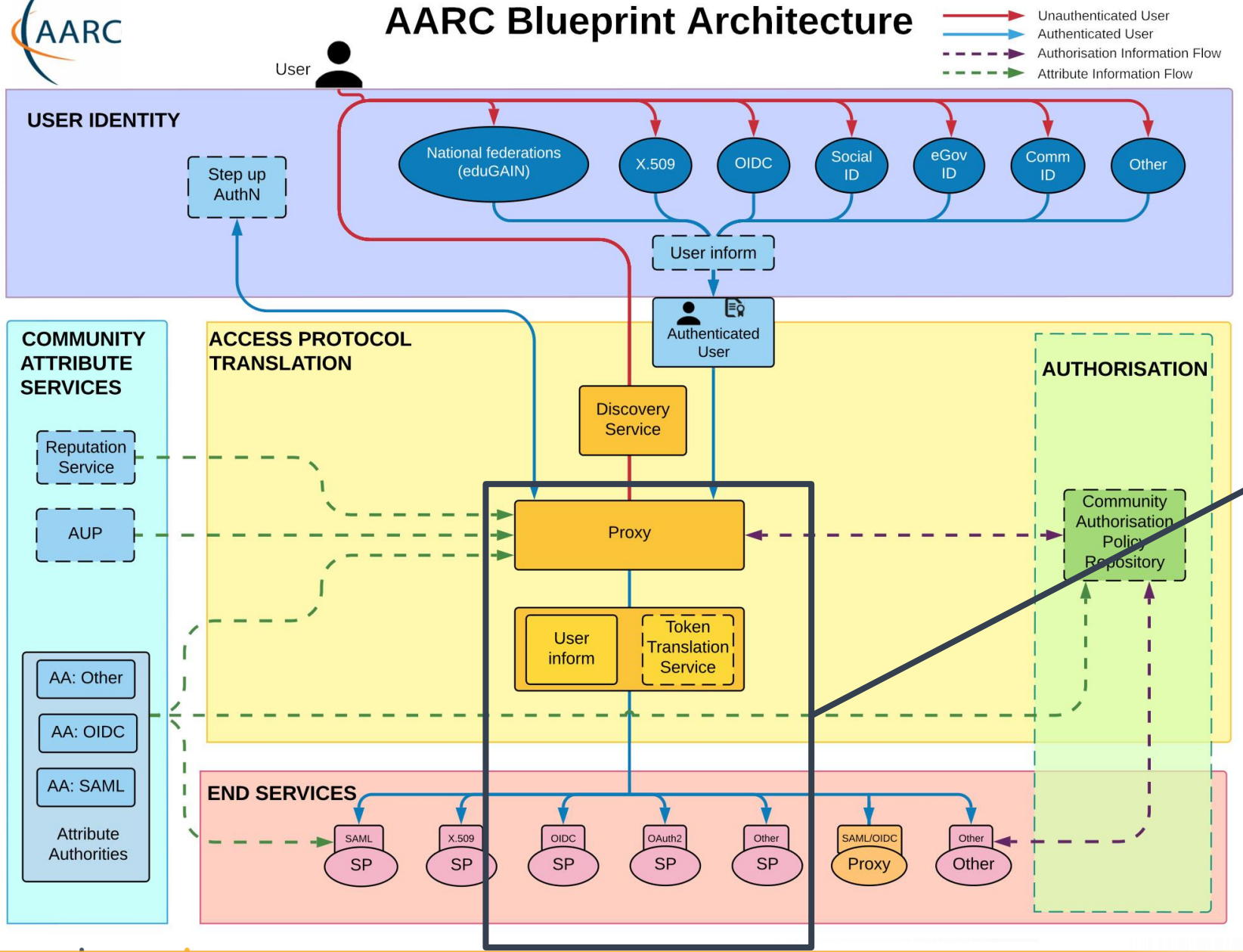
Föderationen und Community AAIs

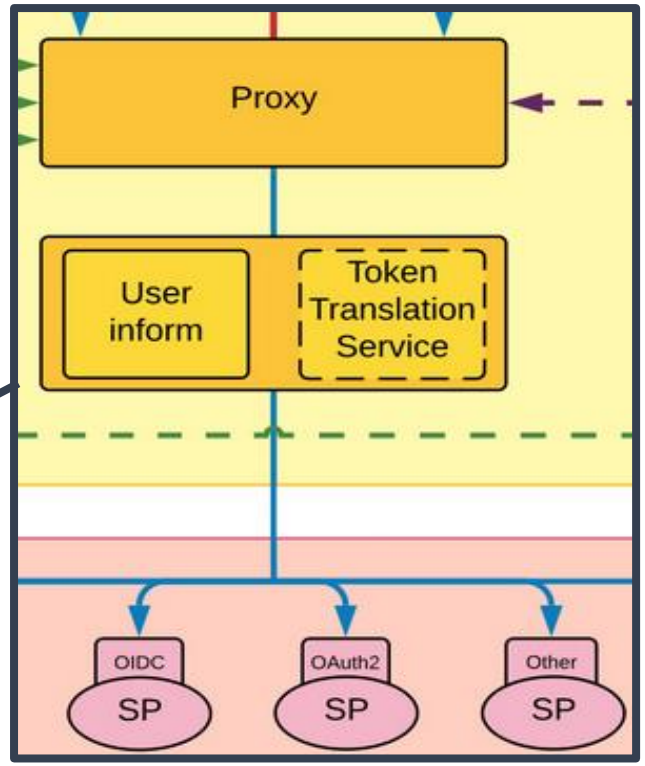


Ansatz von IAM4NFDI – Community-AAIs

- ergänzen bestehende AAI-Landschaft um Community-spezifische Funktionalität
  - „Community“ entspricht Fachkonsortium in NFDI bzw. Teilgruppen eines Fachkonsortiums
- die Community-AAIs in der NFDI bilden zusammen die NFDI-AAI
- technische Implementierung von Community-AAIs
  - es existieren bereits verschiedene Lösungen, z.T. auch von Communities genutzt
  - aber (bzw. deshalb) kein one-size-fits-all absehbar
- daraus Idee für Basisdienst Community-AAI as a Service (CAAIaaS)
  - bestehende Lösungen weiter entwickeln, anpassen und als Dienste für Fachkonsortien anbieten
- AARC Blueprint Architecture (BPA) als Grundlage für Community AAIs

AARC Blueprint Architecture





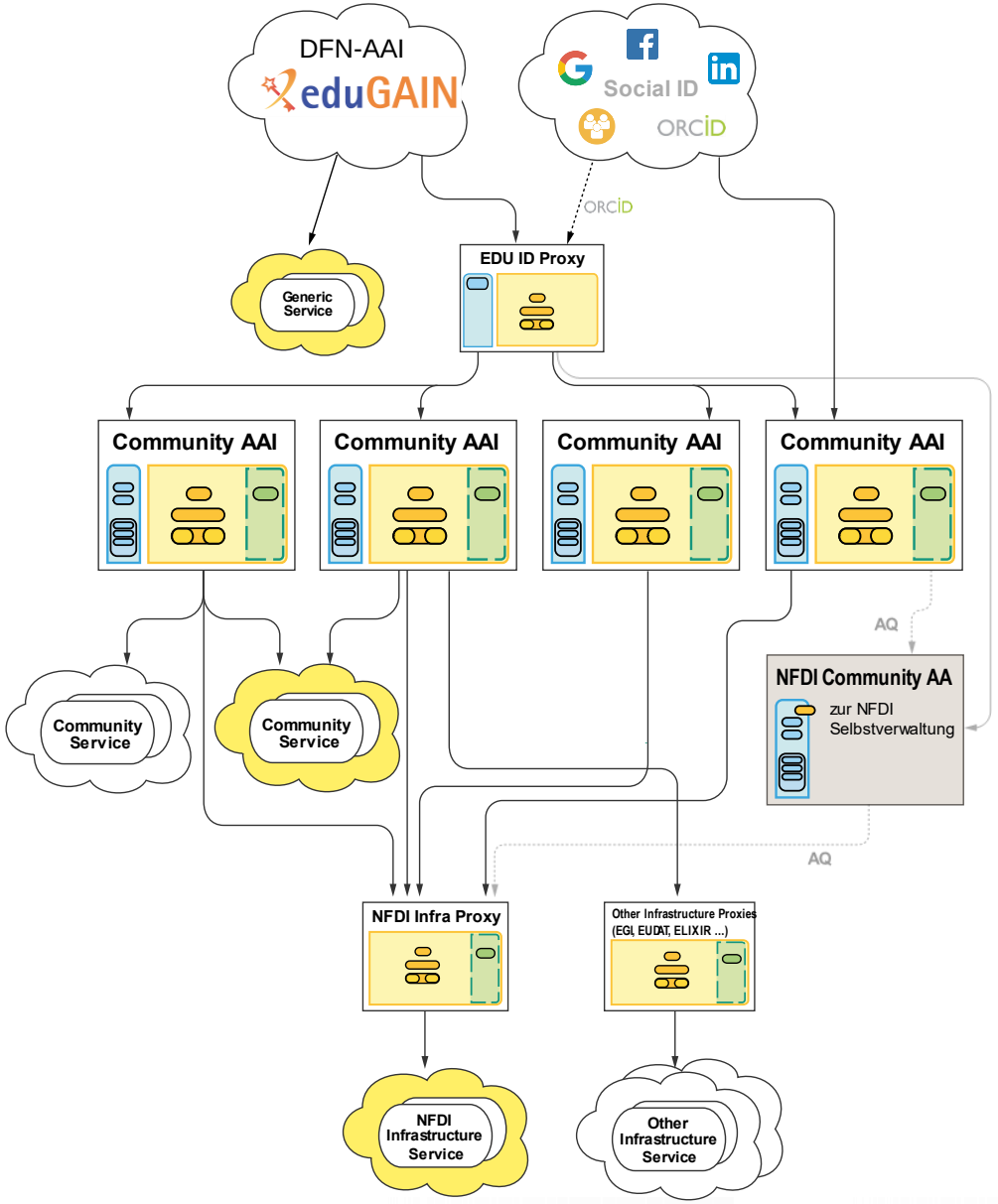
https://aarc-community.org/architecture/

AARC Blueprint Architecture (BPA)

- Fünf Komponenten, die zur Implementierung von föderierten IAM-Lösungen für (internationale) Forschungsverbünde kombiniert werden können:
  - **User Identity:** Authentifizierung über AAI, Soziale Netzwerke, ORCID, etc.
  - **Community Attribute Services:** Rechte, Rollen, VO-Management (Virtuelle Organisation)
  - **Access Protocol Translation:** IdP-/SP-Proxy, Token Translation, ...
  - **Authorisation:** Autorisierung, Verwaltung des Zugriffs auf Dienste/Ressourcen
  - **End-services:** die eigentlichen Dienste und Ressourcen

- https://aarc-project.eu/architecture/

Architektur NFDI-AAI



NFDI-AAI (1)
Community-AAIs: as-a-Service-Angebot für NFDI-Konsortien

- AcademicID (GWDG)
  - https://docs.gwdg.de/doku.php?id=de:services:general_services:academicid:start
- RegApp (KIT/SCC)
  - https://www.scc.kit.edu/dienste/regapp.php
- Unity (FZJ)
  - https://unity-idm.eu
- Didmos (DAASI International)
  - https://daasi.de/en/federated-identity-and-access-management/iam-solutions/didmos/
- Weiterführende Informationen unter https://www.nfdi-aai.de/community-aai-software/

NFDI AAI (2)

Service-Integration auf drei Ebenen

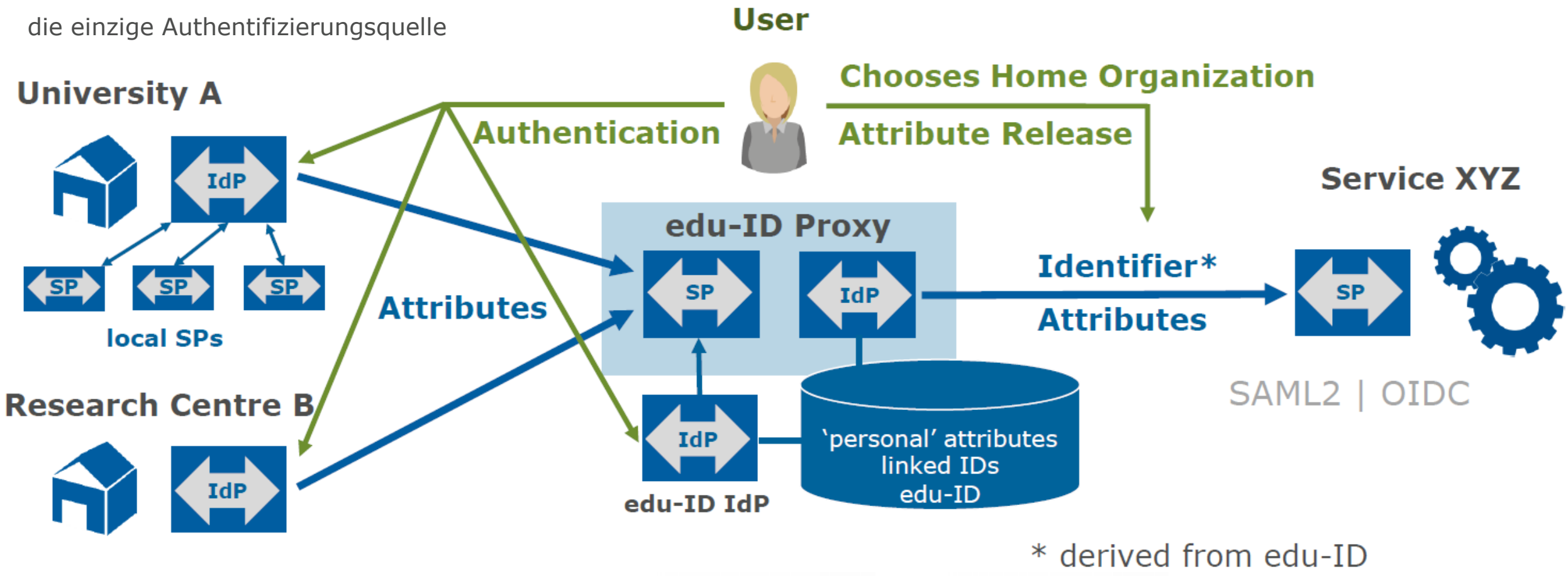
- Generic services → Föderation (DFN-AAI)
  - Ressourcen, die auch außerhalb der NFDI genutzt werden
- Community services → Community AAI
  - Community- bzw. fachspezifische Ressourcen
- Infrastructure services → Infrastruktur Proxy (nächste Folie)
  - Ressourcen, die Community- bzw. Konsortien-übergreifend genutzt werden

NFDI-AAI (3) – weitere Komponenten

- Infrastruktur-Proxy:
  - Zur Anbindung von Diensten, die sich an mehrere Communities richten
    → Einfacheres Einbinden von Benutzern aus mehreren Identitätsquellen (eduGAIN, ORCID, „Soziale Netzwerke“)
  - Gibt Attribute aus dem VO-Management weiter, z.B. Mitgliedschaften.
  - Kann in Ausnahmefällen Autorisierungsentscheidungen für einen Dienst treffen, wenn der nicht in der Lage ist, Benutzer ohne passende Attribute abzulehnen.
  - Identity Linking zwischen Community-AAIs und/oder anderen Identitätsquellen.
- NFDI Attribute Authority
  - Zur Verwaltung von NFDI-internen Rechten z.B. außerhalb oder oberhalb von Communities.
- edu-ID Proxy
  - Permanente, unveränderliche digitale Identität über von edu-ID abgeleitete Identifier
  - Aggregation/Verlinkung von Daten aus unterschiedlichen Quellen wie Heimat-IdP und ORCID
  - Zentraler Homeless-/Gast-IdP

edu-ID Proxy

Für “Homeless Users” ist der edu-ID IdP
die einzige Authentifizierungsquelle



Attribut-Profile

- Community-AAIs stellen den Diensten einen genormten Satz von Attributen zur Verfügung.
- Dafür müssen die Home-IdPs Standardattribute freigeben:
  - Heimateinrichtung
  - User Identifier
  - Personennamen
  - E-Mail-Adresse
  - Affiliation
  - Assurance
- Dieses Attributprofil wird abgedeckt durch die REFEDS Personalized Access Entity Category: https://refeds.org/category/personalized
- Die Community-AAIs bauen daraus SAML-Attribute und OIDC-Claims, z.B. voPersonID bzw. voperson_id.
- Details: https://www.nfdi-aai.de/documents/policies-v0.9/04_IAP.pdf

NFDI-AAI Policy Dokumente

„Spielregeln“ der NFDI-AAI, orientieren sich an AARC Policy Development Kit

- Top Level Infrastructure Policy
- Virtual Organisation Membership Management Policy
  - VO Lifecycle Management – *a checklist*
  - Service Access Policy Template - *optional*
- Policy on the Processing of Personal Data
- Security Incident Response Procedure
- Infrastructure Attribute Profiles
- Acceptable Use Policy Template –> Dienstanbieter, Virtuelle Organisationen
- Privacy Policy Template –> SP-Komponenten, Virtuelle Organisationen
- (Verzeichnis der Verarbeitungstätigkeiten)

Arbeitspakete IAM4NFDI (1)

- WP1: Policy, Governance, and Legal Aspects (Leitung: DFN, RWTH)
  - Datenschutzfragen, Policy-Framework, Schaffung der Basis für eine IAM-Governance-Struktur
- WP2: AAI Architecture and Implementation (Leitung: KIT)
  - Schaffung der technischen Grundlagen für die NFDI-AAI und den Betrieb der Community AAIs
- WP3: Incubator (Leitung: RWTH)
  - Entwicklung und Implementierung spezifischer technischer Lösungen insbesondere zur Integration von Ressourcen in Community AAI Implementierungen

Arbeitspakete IAM4NFDI (2)

- WP4: Operations (Leitung: GWDG, DAASI)
  - Nachhaltiger und stabiler Betrieb der Infrastruktur-Komponenten, insbesondere der Community-AAI-Implementierungen

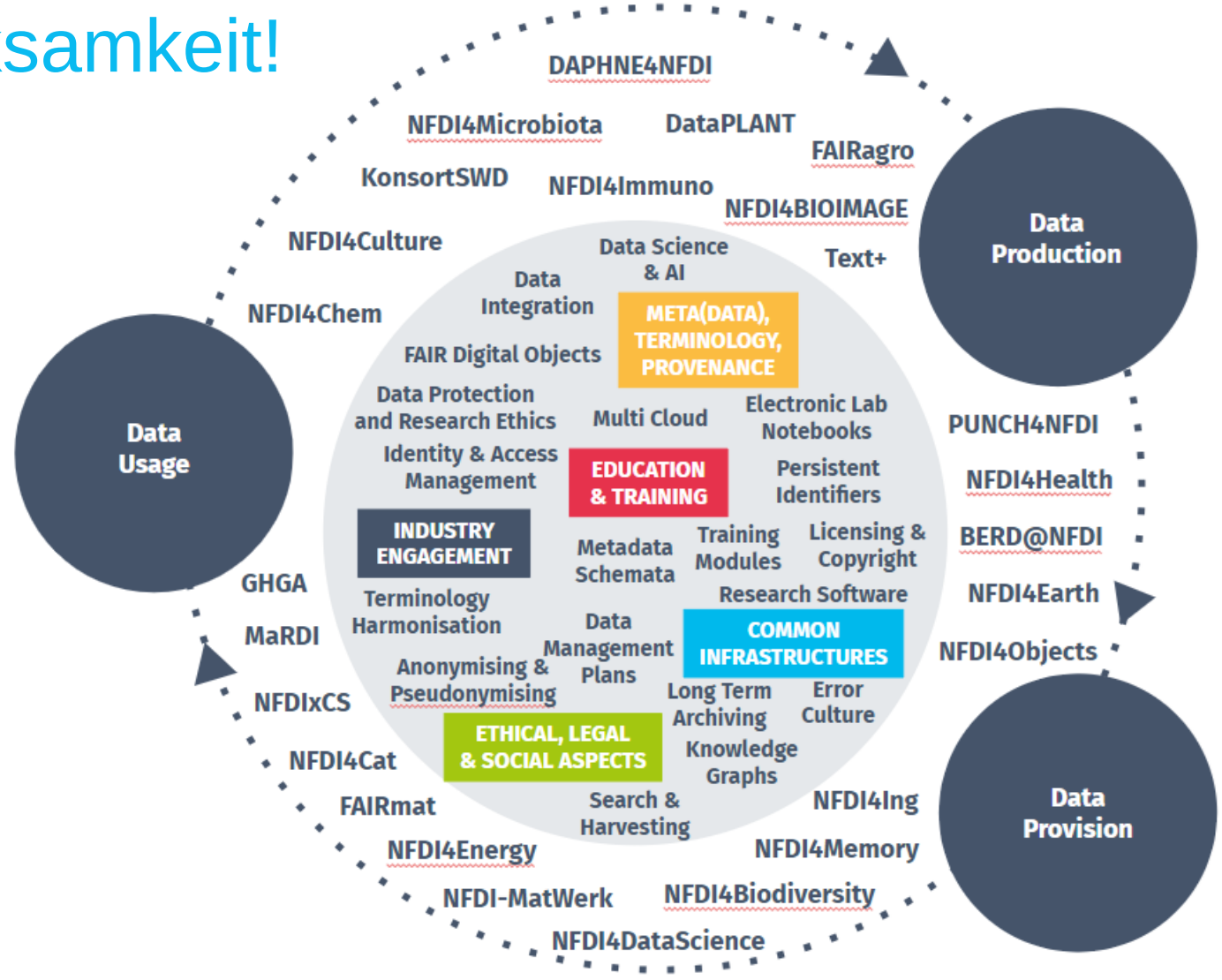
- WP5: Dissemination, Training, and Community Engagement (Leitung: RPTU)
  - Organisation von Informations- und Trainings-Events für die Zielgruppen, Erstellung von Dokumentation und Sammeln von Feedback

Stand der Dinge

- Test- und Demoinstanzen der vier CAAI-Lösungen aufsetzen.
- RDMO-Software als Beispieldienst an die vier CAAIs anbinden.
- Zwei Workshops (NFDI und AAI) und zwei Infoshares (Projekt IAM4NFDI) veranstaltet
- Policies erstellen und genehmigen lassen → Governance-Struktur
- Abstimmung Inkubator-Projekte
- Vernetzung und Kooperationen:
  ZKI AK IAM, ZKI Herbsttagung, DFN-BT, FIM4R-Workshop, FIDM-Ländertreffen, EOSC Task Force AAI Architecture, …

Vielen Dank für die Aufmerksamkeit!

Gibt es Fragen?



Kontakt:

Thorsten Michels, michels@rptu.de

Wolfgang Pempe, pempe@dfn.de

Projektteam: aai-kernteam@lists.kit.edu

base4nfdi

Funded by **DFG** as part of **NFDI**.

Grant Numbers: 521453681, 521460392, 521462155, 521463400, 521466146, 521471126, 521473512, 521474032, 521475185, 521476232