

Die Arbeitsgruppe FIM4R und ihr Impact

Peter Gietz, DAASI International

ZKI-AK-IAM
Konstanz 17.09.2025

Agenda

- Ausgangslage
- Workshops
- Publikationen
- Impact

Über DAASI International

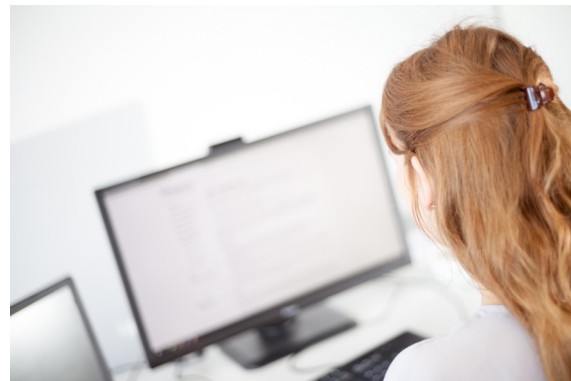
Gründung

- 2000 in Tübingen mit 4 Mitarbeiter*innen
- als Spin-Off des ZDV der Universität Tübingen
- aus DFN-Projekten zu X.500/LDAP

Stand 2025

- 26 Mitarbeiter*innen
- > 19 FTE
- > 2 Millionen Jahresumsatz

Die DAASI International ist ein erfolgreicher PoC für ein nicht skalierendes aber nachhaltiges Businessmodell auf Open-Source-Grundlage



DAASI International steht für digitale Souveränität

- Open Source für Flexibilität und digitale Souveränität
- Datenschutz für informationelle Selbstbestimmung und digitale Souveränität
- Offene Standards für Interoperabilität und Kombinationsmöglichkeiten, was ebenfalls digitale Souveränität fördert

Ausgangslage

eduGAIN und Forschungsinfrastrukturen

- Die einzelnen nationalen Forschungsföderationen waren im Entstehen und eduGAIN sorgte für die Interföderation
- Forschungsinfrastrukturen wollten Ihren Usern die Vorteile der Föderation anbieten:
 - Login mit dem Account der Heimatorganisation
 - SSO über alle Anwendungen
 - Integration bzw. weg von X.509-Userzertifikaten
- Allerdings brauchen Forschungsinfrastrukturen personenbezogene Daten (Man will wissen, wer die teuren Infrastrukturkomponenten nutzt)
- Viele IdPs behandelten Forschungsinfrastrukturen wie Wissenschaftsverlage, schicken also keine personenbezogene Daten
 - „Datenschutz“
 - „Never change a running system“

Wie bekommen Forschungsinfrastrukturen personenbezogene Daten?

- Die IdPs überzeugen, dass SPs der FIs vertrauenswürdig sind via SAML Metadata entity categories
 - „Research and Scholarship“ (R&S):
 - „Dieser SP ist gesichert der Forschungscommunity zugehörig und hat kein kommerzielles Interesse an den Daten“
 - „GÉANT Data Protection Code of Conduct V1“:
 - „Dieser SP verpflichtet sich die europäischen Datenschutzrichtlinien zu erfüllen“
 - Mittlerweile gibt es eine V2, die DSGVO-compliant ist [2]
 - „Clarin Member“:
 - Dieser SP gehört zur CLARIN Community
 - Weil eduGAIN sich langsam entwickelt hat, wurde die CLARIN SP Federation erstellt [3]
 - 3 nationale Föderationen: HAKA (FI), DFN-AAI (DE), SURFed (NL)
 - 9 CLARIN SPs
 - Ein eigener IdP für die homeless

FIM4R in a Nutshell [11]

- Federated Identity Management for Research, <https://fim4r.org>
 - Unterstützer von Forschungscommunities
 - Ziel: Föderatives IdM für Forschungscommunities besser zu machen
 - Vorsichtig Aspekte identifizieren, die hierfür am wichtigsten sind
 - Die Anforderungen der weiteren Föderationscommunity bekannt machen
 - Mit Anderen zusammenarbeiten um diese Anforderungen zu erfüllen

Workshops

Chronologie der Workshops

- June **2011**, CERN, 85 Tn. (<https://indico.cern.ch/event/129364>)
- November 2011, RAL, Oxford, ??Tn. (<https://indico.cern.ch/event/157486>)
- February **2012**, ISGC, Taipei, 50 Tn. (<https://indico.cern.ch/event/177418>)
- June 2012, MPI Psycholinguistics Nijmegen, ??Tn. (<http://www.clarin.eu/events/3501>)
- March **2013**, PSI Villigen, 47 Tn. (<http://indico.psi.ch/event/2230>)
- October 2013, CSC Helsinki, ?? Tn. (<https://refeds.org/meetings/oct13/index.html>)
- April **2014**, ESRIN, Frascati, 32 Tn. (<https://indico.cern.ch/event/301888/>)
- February **2015**, CERN, 29 Tn. (<https://indico.cern.ch/event/358127>)
- November 2015, EWTI, Wien, ?? Tn. (<https://indico.cern.ch/event/450600/>)*
- February **2017**, TIIME, Wien, ??Tn. (<https://indico.cern.ch/event/605369/>)
- September 2017, McGill University Montreal, 28 Tn. (<https://indico.cern.ch/event/647693/>)
- February **2018**, TIIME, Wien ?? Tn. (<https://indico.cern.ch/event/681873/>)
- February **2019**, TIIME, Wien, ?? Tn. (<https://indico.cern.ch/event/775478/>)
- September 2019, mini-FIM4R for Physics, Fermilab Batavia IL, USA, ?? Tn. (<https://indico.cern.ch/event/834658/>)
- December 2019, TechEx New Orleans, ?? Tn. (<https://indico.cern.ch/event/856347/>)
- February **2020**, TIIME Wien, ??Tn. (<https://indico.cern.ch/event/871628/>)
- June **2021**, Virtual Assurance Workshop, ?? Tn. (<https://indico.cern.ch/event/1038620/>)
- December **2022**, TechEx Denver (<https://indico.cern.ch/event/1202335/>)
- February **2023**, CERN (<https://indico.cern.ch/event/1224755/>)
- January 2024, TIIME Unconference, Copenhagen, ca. 45 Tn. (<https://indico.cern.ch/event/1325302/>)
- December 2024, TechEx Boston, USA (xxx)
- March 2025, TIIME Unconference, Reading, UK (<https://indico.cern.ch/event/1518035/>)

1. Workshop 2011 CERN

CERN (Bob Jones) hatte Probleme und Ideen für IAM und hat andere Forschungsinfrastrukturen zur Diskussion eingeladen. Gekommen sind:

- European Photon/Neutron facilities
- Social Science and Humanities (CLARIN)
- WLCG High Energy Physics
- Earth Sciences
- Life Sciences

1. Workshop 2011 CERN: Ergebnisse

user community	other projects	# users	chosen technology	status	IGTF
photon/neutron	EUROFEL, PanData, CRISP	10,000	Shibboleth/SAML	Umbrella prototype	no
Social Sciences and Humanities	DARIAH, CLARIN, CESSDAH, (DASISH)	hundreds now, potential for 10000+ across SSH	Shibboleth/SAML	CLARIN SP federation - will see if they can use eduGAIN	yes
WLCG	WLCG	5900 globally	X509	production	yes
earth sciences	Earth System Grid Federation, GENESI-DEC, CMIP5, Metafor, IS-ENES	5000+ for CIMP5	OpenID, X.509 and SAML	production - earth system grid	not yet but foresee for EGI integration
life sciences	ELIXIR & potentially 10 BMI ESFRI projects	millions access data via EBI website	no chosen yet	security included in BioMedBridges project workplan	no

Vgl. [1]

1. Workshop 2011 CERN: Ergebnisse

There are many common needs and hence scope for agreement

- SSO
- Easy of use for part-time users
- Focus is on data access
- Support homeless users
- Many tools and technologies deployed
- Smooth transition from existing systems

Es gab genug Gemeinsamkeiten um weiter zu machen

1. Workshop 2011 CERN: Next Steps [4]

- Identify/develop concrete use cases
- Nominate architect(s) for each community
- How we can learn from the experience and developments of our colleagues in the US?
- What about Asia & Latin America?
- Consider repeating this style of workshop With the goal of developing a roadmap we can all agree to
 - Need to work on the points shown on previous slides in between the workshops
 - we can't just talk!
 - We will keep alive the email list

Die Workshops 2 bis 4

- Immer mehr Forschungsinfrastrukturen aus immer mehr Fachdomänen stießen hinzu
- Es wurden
 - Use Cases vorgestellt
 - Eine gemeinsame Vision entwickelt
- Da Forschung international vernetzt ist, muss eine globale Lösung her
- Man beschloss ein gemeinsames Paper hierzu zu verfassen
- Es waren auch Forschungsförderer anwesend

Die erste Veröffentlichung

- Federated Identity Management for Research Collaborations [5]
 - Paper Type: Research paper
 - Date of this version: 28 August 2013
- Identity federation offers economic advantages, as well as convenience, to organisations and their users. For example, multiple institutions can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust
- A number of laboratories including national and regional research organizations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries
- Driven by these needs, representatives from a variety of research communities, have come together to discuss how to address these issues with the objective to define a common policy and trust framework for Identity Management based on existing structures, federations and technologies.
- This paper will describe the needs of the research communities, the status of the activities in the FIM domain and highlight specific use cases. The common vision for FIM across these communities will be presented as well the key stages of the roadmap and a set of recommendations intended to ensure its implementation.

Die erste Veröffentlichung: Leitlinie

- Every researcher is entitled to focus on their work and not be impeded by needless obstacles nor required to understand anything about the FIM infrastructure enabling their access to research services.

Die erste Veröffentlichung: Anforderungen

- Nach einer Einführung wird der Stand in den einzelnen Communities berichtet und gemeinsame Probleme adressiert und gemeinsame Anforderungen gelistet und priorisiert:
- Prio High:
 - User friendliness
 - Browser & non-browser federated access
 - Implementations based on open standards and sustainable with compatible licenses
 - Different Levels of Assurance with provenance
 - Authorisation under community and/or facility control
 - Attributes must be able to cross national borders

Die erste Veröffentlichung: Anforderungen

- Prio Medium
 - Bridging communities
 - Multiple technologies with translators including dynamic issue of credentials
 - Well defined semantically harmonised attributes
 - Flexible and scalable IdP attribute release policy
 - Attribute aggregation for authorisation
 - Privacy and data protection to be addressed with community-wide individual identities

Die erste Veröffentlichung: Empfehlungen

- Schließlich wurden für verschiedene Stakeholder Empfehlungen ausgesprochen:
 - Recommendations to the **research communities**:
 - A pragmatic risk analysis of the use of identity federation from the point of view of a research infrastructure provider
 - pilot studies will explore the requirements on federated identity management services in more detail (Umbrella, Elixir, CLARIN)
 - Recommendations to the **technology providers**
 - Separation of Authorization and Authentication
 - Credentials revocation
 - Attribute delegation to the research community
 - A one size fits all model for levels of security supported for a given FIM system will not scale into the future.

Die erste Veröffentlichung: Empfehlungen

- Recommendations to **funding agencies**:
 - In order to implement this common policy and trust framework for Identity Management an agreed funding model is required with an appropriate governance structure

Die erste Veröffentlichung: Impact

- Und sie wurden gehört!
 - Unter Mitwirkung von GEANT, die eduGAIN so weiter entwickeln wollten, dass es die Anforderungen der FIs erfüllt, wurde
 - Eine Studie durchgeführt: Study on AAA Platforms For Scientific Resources in Europe [12]
 - ein EU-Workshop in Brüssel veranstaltet, um der Kommission von den Nöten der FIs zu berichten [13]
 - Die EU hat im Rahmen von EINFRA ein Projekt ausgeschrieben, das genau diese Nöte adressieren sollte
 - GEANT und eine Reihe von an FIs arbeitenden Institutionen (einschl. DAASI) haben dann den entsprechenden Antrag gestellt, der zur ersten Iteration des AARC-Projekts geführt hat:
 - Authentication and Authorization for Research and Collaboration“ Phase I 2015-2017

AARC I [6]

- Defining an Authentication and Authorization framework for international research and collaboration communities
 - One Blueprint architecture
 - One set of Policies
 - One Collection of training materials
- Leveraging the eduGAIN meta-Federation
- Integrating communities into general research infrastructures like EGI and EUDAT
- AARC Blueprint Architecture: Based on a Proxy model that attaches many Community SPs to eduGAIN IdPs and generally makes life much easier

AARC I Blueprint Architecture [7]

- Defining an Authentication and Authorization framework for international research and collaboration communities
 - One Blueprint architecture
 - One set of Policies
 - One Collection of training materials
- Leveraging the eduGAIN meta-Federation
- Integrating communities into general research infrastructures like EGI and EUDAT
- AARC Blueprint Architecture: Based on a Proxy model that attaches many Community SPs to eduGAIN IdPs and generally makes life much easier

AARC I Blueprint Architecture [7]

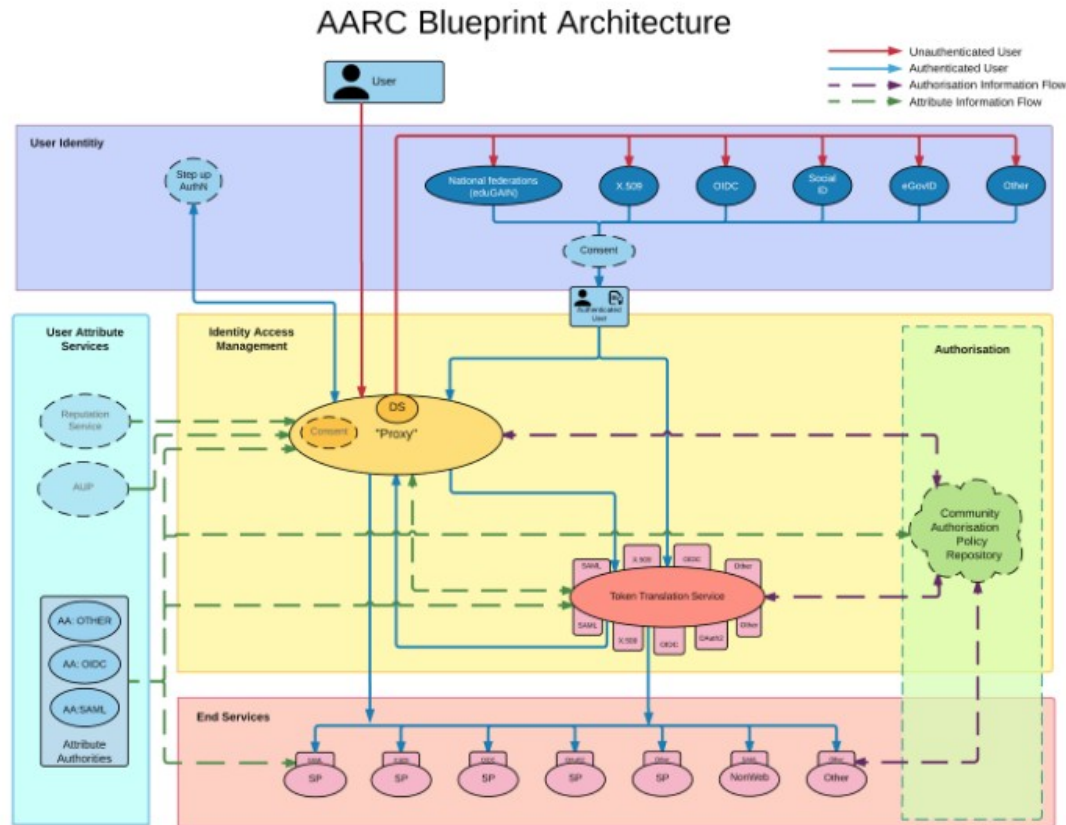
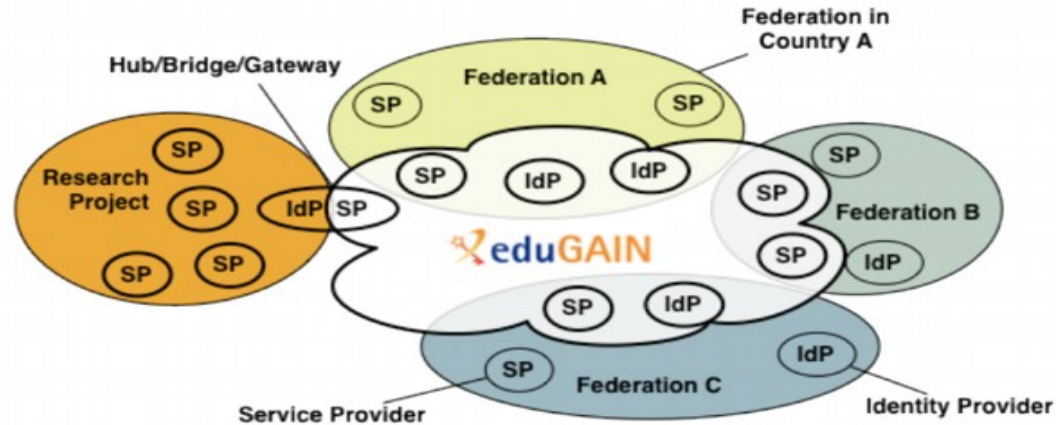


Figure 2.6: AARC Blueprint Architecture 2017

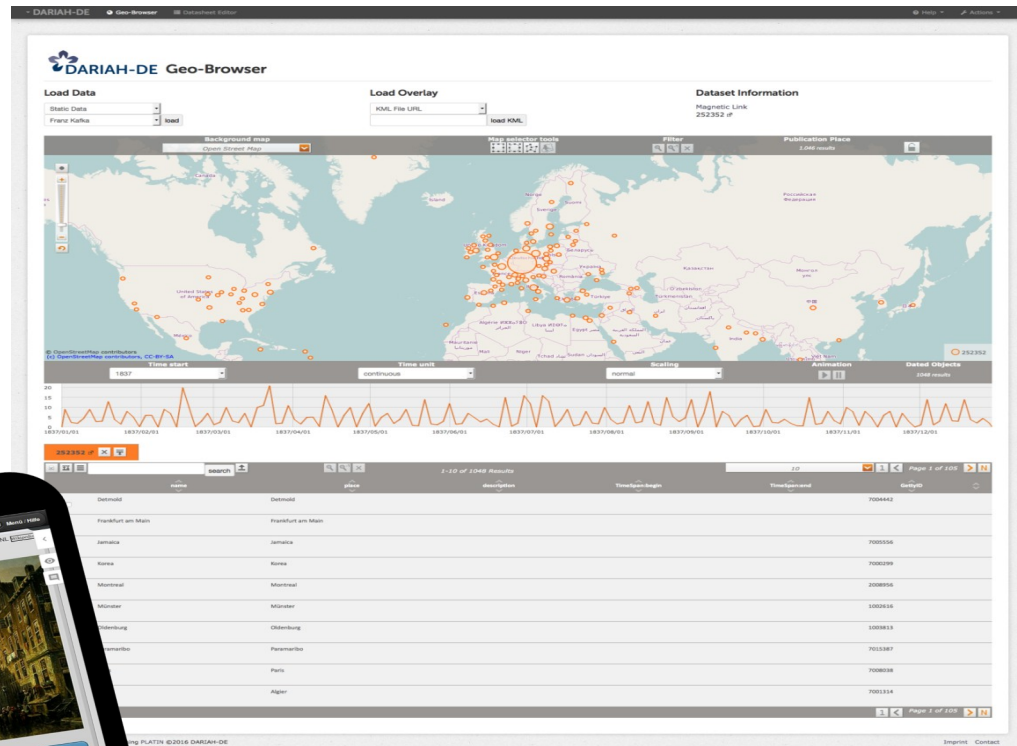
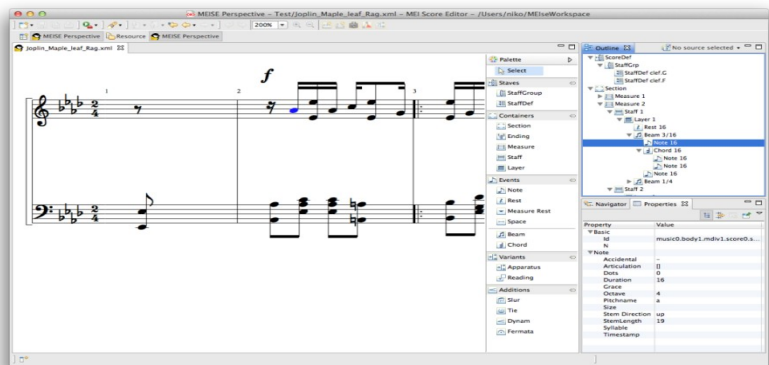
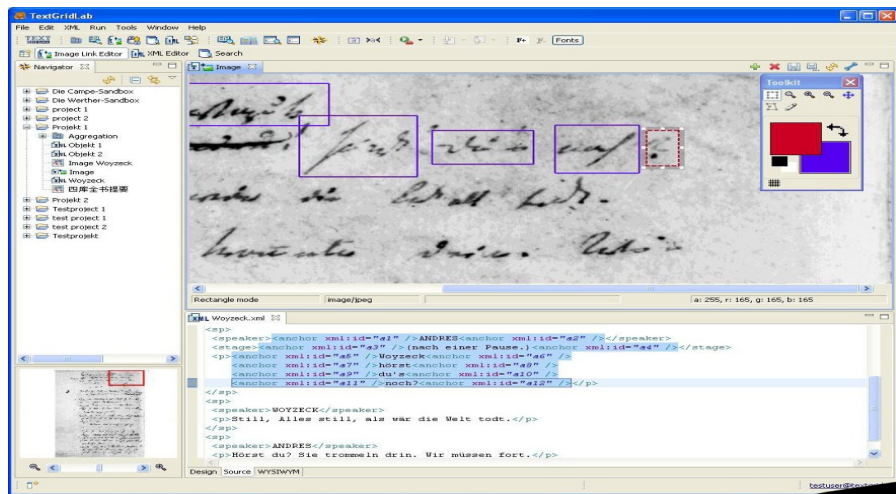
The Workshop Journey continues ...

- In den folgenden Workshops wurden weitere Status-Updates der einzelnen Communities gegeben
- Und geschaut, wie man die AARC BPA berücksichtigen kann

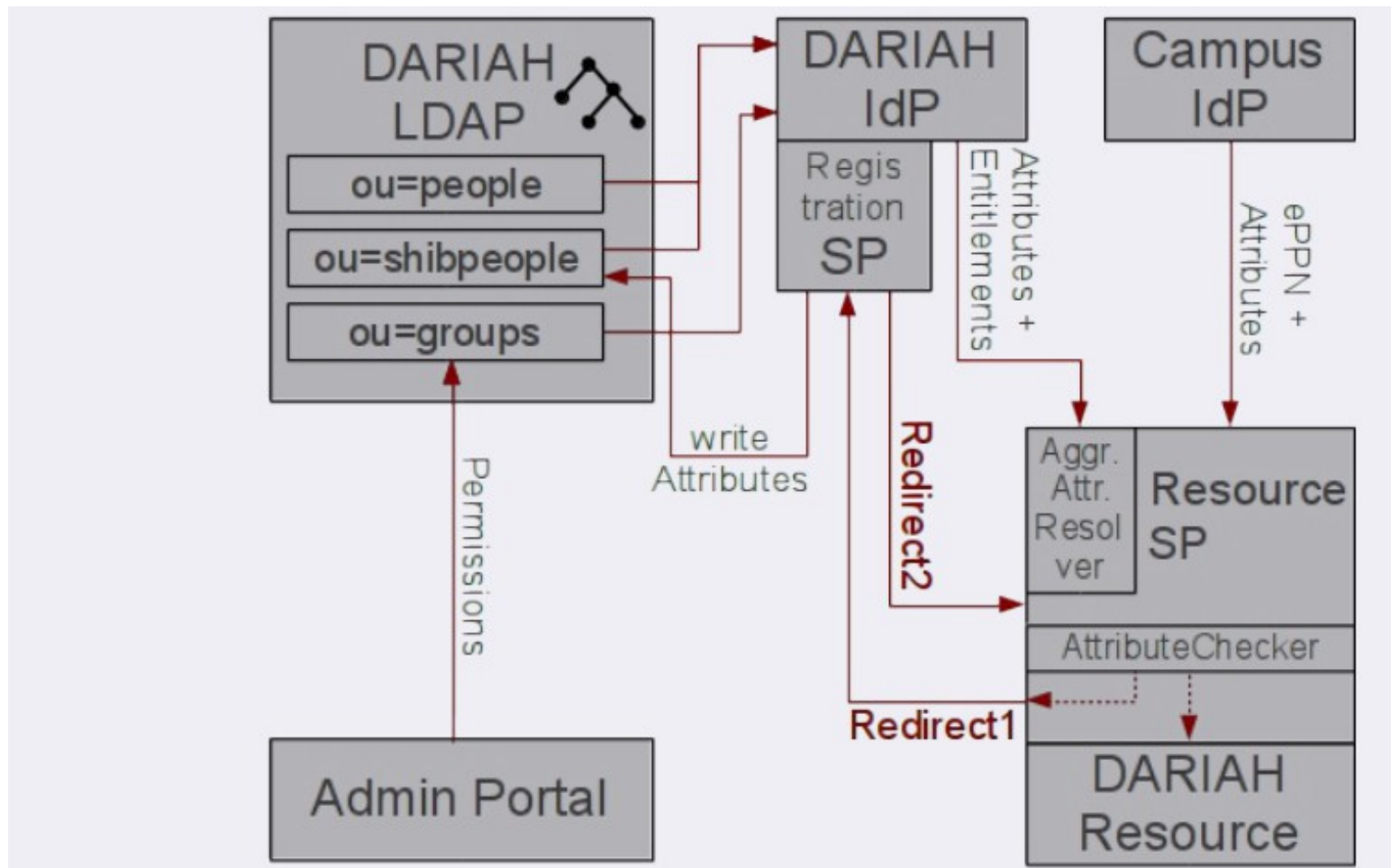


- Zum Beispiel DARIAH AAI:

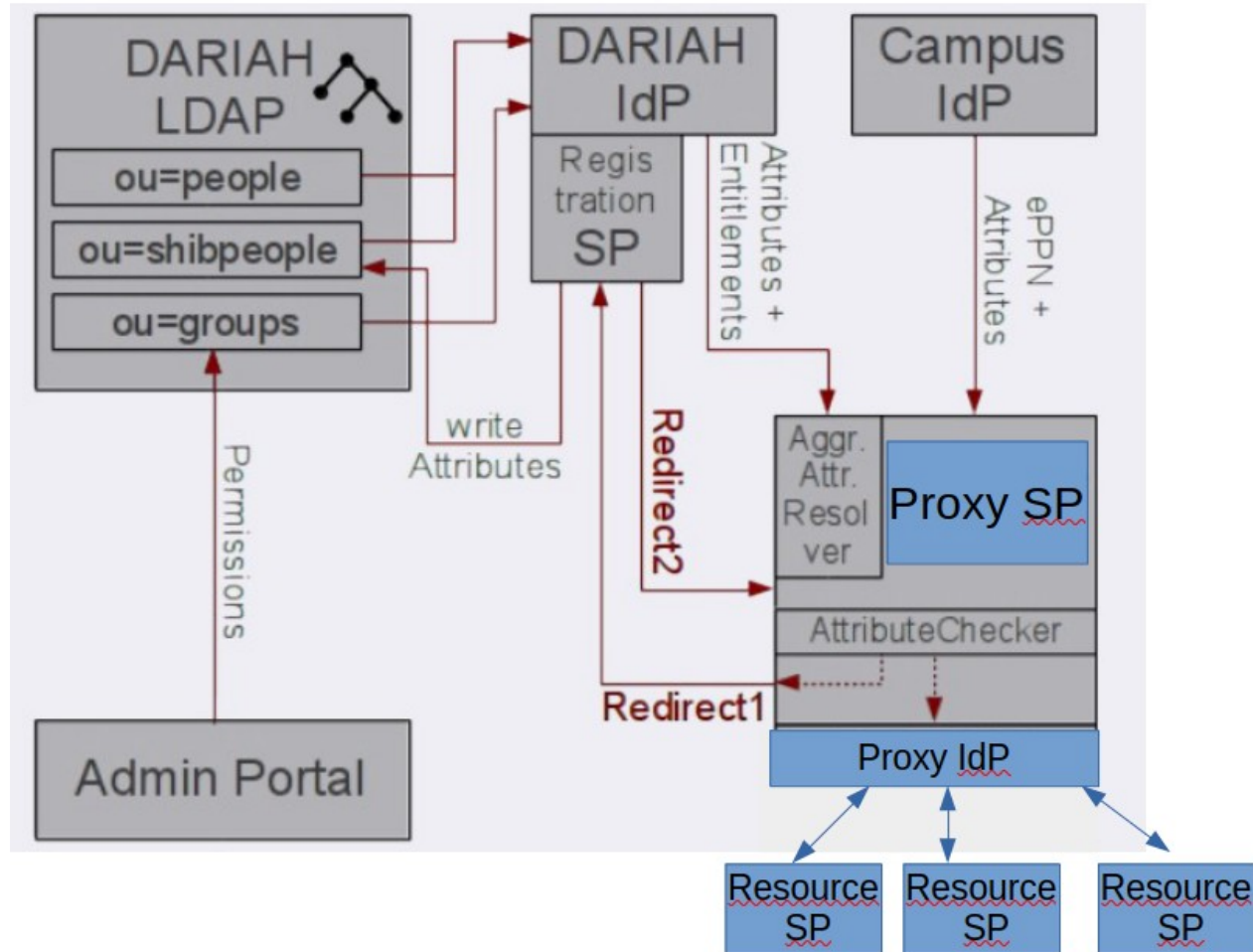
DARIAH eine Virtuelle Forschungsinfrastruktur für Geisteswissenschaften



DARIAH AAI ohne AARC BPA



DARIAH AAI mit AARC BPA



The Workshop Journey continues ...

- Im 2016-Workshop wurde das Paper evaluiert um zu sehen, was bisher erreicht werden konnte [8]:

2012 Requirements: how have we done?

- **User friendliness (high)** - *Good but varies wildly, citizen scientists partially addressed*
- **Browser & non-browser federated access (high).** – *Mostly requires web intervention*
- **Bridging communities (medium).** – *eduGAIN addresses R&E but little interaction with commercial/social*
- **Multiple technologies with translators including dynamic issue of credentials (medium).**
- **Implementations based on open standards and sustainable with compatible licenses (high).**
- **Different Levels of Assurance with provenance (high).**
- **Authorisation under community and/or facility control (high).**
- **Well defined semantically harmonised attributes(medium).** – *R&S, not so much for other attributes*
- **Flexible and scalable IdP attribute release policy(medium).** – *R&S seems to have reached happy medium*
- **Attributes must be able to cross national borders(high).** - *Good work from AARC but GDPR problematic for intergovernmental organisations*
- **Attribute aggregation for authorisation(medium).** – *Case by case basis*
- **Privacy and data protection to be addressed with community-wide individual identities(medium)**

2012 Recommendations: how have we done?

- Recommendations to the research communities
 - Conduct Risk Analysis – SCI
 - Run Pilot Studies coordinated by experts - AARC
- Recommendations to the technology providers
 - Separation of Authorization and Authentication – as per attribute delegation
 - Credentials revocation
 - Attribute delegation to the research community – partially done within the context of pilots
 - Standardise efforts in Levels of Security/Assurance – Minimal LoA, Sirtfi
- Recommendations to funding agencies
 - Fund FIM technologies that are focused on solving the described needs of the research communities – AARC/AARC2

So what do we want to do?

- Basically we have two options:
 - Create a new version of the document
 - Less work?
 - Are all original authors available?
 - Write a new document, referencing the old one
 - We could write a summary of what had happened
 - We could then formulate some new requirements and recommendations

Die zweite Veröffentlichung

- Man entschied sich eine zweite Version des Papers mit neuer Autorenschaft zu schreiben [9]:
- Federated Identity Management for Research Collaborations, Version 2, Published June 22, 2018
 - This white-paper expresses common requirements of Research Communities seeking to leverage Identity Federation for Authentication and Authorisation. Recommendations are made to Stakeholders to guide the future evolution of Federated Identity Management in a direction that better satisfies research use cases. The authors represent research communities, Research Services, Infrastructures, Identity Federations and Interfederations, with a joint motivation to ease collaboration for distributed researchers. The content has been edited collaboratively by the Federated Identity Management for Research (FIM4R) Community, with input sought at conferences and meetings in Europe, Asia and North America.

Die zweite Veröffentlichung

Contents

1	Introduction	4
1.1	About FIM4R	4
1.2	Vision	4
1.3	Structure of the Paper	4
2	The Evolution of Federated Identity Management	4
2.1	The Research Community Proxy	5
2.2	Impact of the FIM4R v1 White Paper	6
2.3	Successes	6
2.4	Outstanding Challenges	7
3	Research Community Characteristics and Status	7
4	Analysis of Common Requirements	9
4.1	Requirements Collection	9
4.2	Requirements Categories	9
4.3	FIM Ecosystem Constituents	10
4.4	Requirements Matrix	11
4.5	Analysis of Requirements	16
	Distribution of Requirements Across FIM Constituents • Relative Importance of the Requirements	
5	Recommendations	17
5.1	Governance and Coordination	18
	Increase research representation in FIM governance • Sustain operation of critical FIM services • Provide avenues for ongoing coordination	
5.2	Baseline of Research User Experience	18
	Release Research & Scholarship attributes • Provide usability essentials • Remove interoperability barriers in eduGAIN metadata processes • Admit research organisations to federation • Enable researcher mobility	
5.3	Security Incident Response Readiness	19
5.4	Harmonisation of Research Community Proxy Operations and Practices	19
	Follow the proxy model and related AARC guidelines • Re-use shared AAI and related services	
5.5	Sensitive Research User Experience	20
5.6	Mapping of Groups to Recommendations	20
6	Next Steps	20

Die zweite Veröffentlichung

B Appendix: Descriptions of Contributing Research Communities	26
B.1 Arts and Humanities	26
B.2 Climate Science	26
B.3 Earth Observation (EO)	27
B.4 European Neutron and Photon Facilities (umbrellaID)	28
B.5 Gamma-Ray Astronomy Implementation of the CTA AAI	28
B.6 Gravitational Wave Astronomy gw-astronomy.org • Laser Interferometer Gravitational Wave Observatory (LIGO) • Virgo Collaboration • Kamioka Gravitational Wave Detector (KAGRA)	30
B.7 High Energy Physics HNSciCloud	31
B.8 Ionospheric and Atmospheric Science Current Implementation of EISCAT AAI • Future requirements for EISCAT_3D AAI	32
B.9 Infectious Disease Research National Institute of Allergy and Infectious Diseases Virtual Research Organization Platform	33
B.10Life Sciences Reference Implementation AAI • Sensitive data access models are evolving	34
B.11Linguistics	36
B.12Nuclear Physics FAIR • Italian National Institute for Nuclear Physics (INFN)	37
B.13Radio Astronomy Murchison Widefield Array (MWA) • Square Kilometre Array (SKA)	38
B.14Virtual Atomic and Molecular Data Centre Technical overview • Needs and requirement for Authentication, Authorisation and Accounting	40

The Workshop Journey continues ...

- Jährlich treffen sich die Forschungsinfrastrukturen meist mehrmals, um Fortschritte zu berichten und neue Themen zu integrieren, wie etwa OIDC, OID Federation, Wallets, etc.
- Es besteht ein fruchtvoller Austausch zwischen AARC (I, II und TREE) und FIM4R
- Man trifft sich auf der TIIME Unconference und bei weiteren FIM4R-Workshops

Ein drittes Paper

- Ein weiteres Paper wurde aus der Gruppe heraus veröffentlicht:
 - FIM4R Position Paper on the Desired Evolution of EOSC Authentication and Authorisation Infrastructures - Published March 26, 2020 [10]
 - The European Open Science Cloud (EOSC) will soon enter the next phase of integration and consolidation with the establishment of a common service portal listing underpinning services that enable distributed resources in the areas of computation, data, open access, and above-the-net collaboration services. The Federated Identity Management for Research (FIM4R) community at a recent full-day workshop in Vienna and at the TIIME conference later the same week (17-20 Feb 2020) discussed its views on the evolution of the EOSC Authentication and Authorisation Infrastructure (AAI) and the conclusions are documented [here](#). These have been distributed to the whole FIM4R community, including those who were not in Vienna, with individuals given a two week comment period after which all input was incorporated. This paper is an agreed statement on behalf of the whole community.

The Workshop Journey continues ...

- We believe that the successful EOSC AAI landscape will be composed of multiple, interoperable Authentication and Authorisation Infrastructures (AAIs) protecting clusters of services. The following recommendations are intended to enable this desired outcome:
 - The EOSC AAI Framework Should Integrate with Existing Services
 - EOSC Should Incorporate Existing Services
 - Harmonise AAI Services within EOSC
 - The EOSC AAI Framework Should Prioritise User Experience
 - EOSC Should Provide Operational Support

The Workshop Journey continues: Communities [11]

Research Fields

- Arts and Humanities
- Astronomy
- Climate Science
- Earth Observation
- European Neutron and Photon Facilities
- Gravitational Wave Astronomy
- High Energy Physics
- Infectious Disease Research
- Ionospheric and Atmospheric Science
- Life Sciences
- Linguistics
- Nuclear Physics
- Virtual Atomic and Molecular Data Centre

Experiences from Research Driven Services

- HNSciCloud
- ORCID

Identity Federation Projects/Communities

- AARC2
- GÉANT-GN4
- InCommon/Internet2
- REFEDS

The Workshop Journey continues: Communities



FIM4R v 2.0



Das Team ist ziemlich stabil



Kopenhagen 2024



Montreal 2017

Die nächsten FIM4R-Workshops

- Bei der nächsten Internet2 Technology Exchange in Denver, Colorado
 - **8.-12.12.2025**
 - <https://events.internet2.edu/website/84273/home/>
- Bei der nächsten TIIME Unconference in Amsterdam
 - **9-10.2.2026**
 - <https://tiime-unconference.eu/>
 - FIM4R trifft sich am Montag den 9.2.2026

Fazit

- FIM4R ist eine einflussreiche Gruppe, die die Belange der internationalen Forschungsinfrastrukturen vertritt
- Obwohl selbst nie gefördert, wurden mittlerweile 14 Jahre lang regelmäßige Treffen abgehalten, meist mehrmals pro Jahr
 - Die meisten Präsentationen sind immer noch im Netz vorhanden
- Es gibt immer noch ein Core-Team, das regelmäßig Workshops organisiert:
 - Tom Barton, David Kelsey, Hannah Short, Maarten Kremers, Peter Gietz
- Die Veröffentlichungen hatten einen großen Impact
 - Ohne FIM4R hätte es vielleicht AARC nie gegeben!
- AARC und FIM4R befruchten sich gegenseitig

Vielen Dank für Ihre Aufmerksamkeit!

Weitere Infos: <https://FIM4R.org>

Quellen:

- [1] https://indico.cern.ch/event/129364/contributions/1348987/attachments/88562/126768/2011-06-10_-_Identity_Management_Workshop_-_User_Requirements_Summary.pdf
- [2] <https://wiki.refeds.org/download/attachments/1606455/GEANT%20Data%20Protection%20Code%20of%20Conduct%20v11%20%28version%2025%20November%202019%29%20-%20approvedchanges.pdf?version=2&modificationDate=1576070173185&api=v2>
- [3] <https://indico.cern.ch/event/129364/contributions/1348976/attachments/88548/126742/CLARIN-FedIdManagement.pdf>
- [4] https://indico.cern.ch/event/129364/contributions/1348987/attachments/88562/126767/2011-06-10_-_Identity_Management_Workshop_-_Next_Steps.pdf
- [5] <https://fim4r.org/wp-content/uploads/2017/07/CERN-OPEN-2012-006-2.pdf>
- [6] https://www.dariah.eu/wp-content/uploads/2017/03/DARIAH-CLARIN-AAI-2019_v4.pdf
- [7] <https://aarc-community.org/wp-content/uploads/2017/05/DJRA1.2-AARC-Blueprint-Architectures-1.pdf>
- [8] https://indico.cern.ch/event/605369/contributions/2440439/attachments/1415425/2166824/20161130_FIM4R_Intro.pdf
- [9] <https://zenodo.org/records/1307551>
- [10] <https://zenodo.org/records/3727546>
- [11] <https://indico.cern.ch/event/1224755/contributions/5234745/subcontributions/412100/attachments/2592157/4477060/FIM4R-17-Introduction.pdf>
- [12] <https://confluence.terena.org/spaces/aaastudy/pages/21266435/AAA+Study+Home+Page>
- [13] <https://confluence.terena.org/spaces/aaastudy/pages/21266437/AAA+Study+Workshop>