



Authentication and Authorisation for Research and Collaboration

and all that I can see is just another ... AARC TREE!

a preliminary insight in potential developments in the AARC Community

David Groep

AARC Policy Area Coordinator

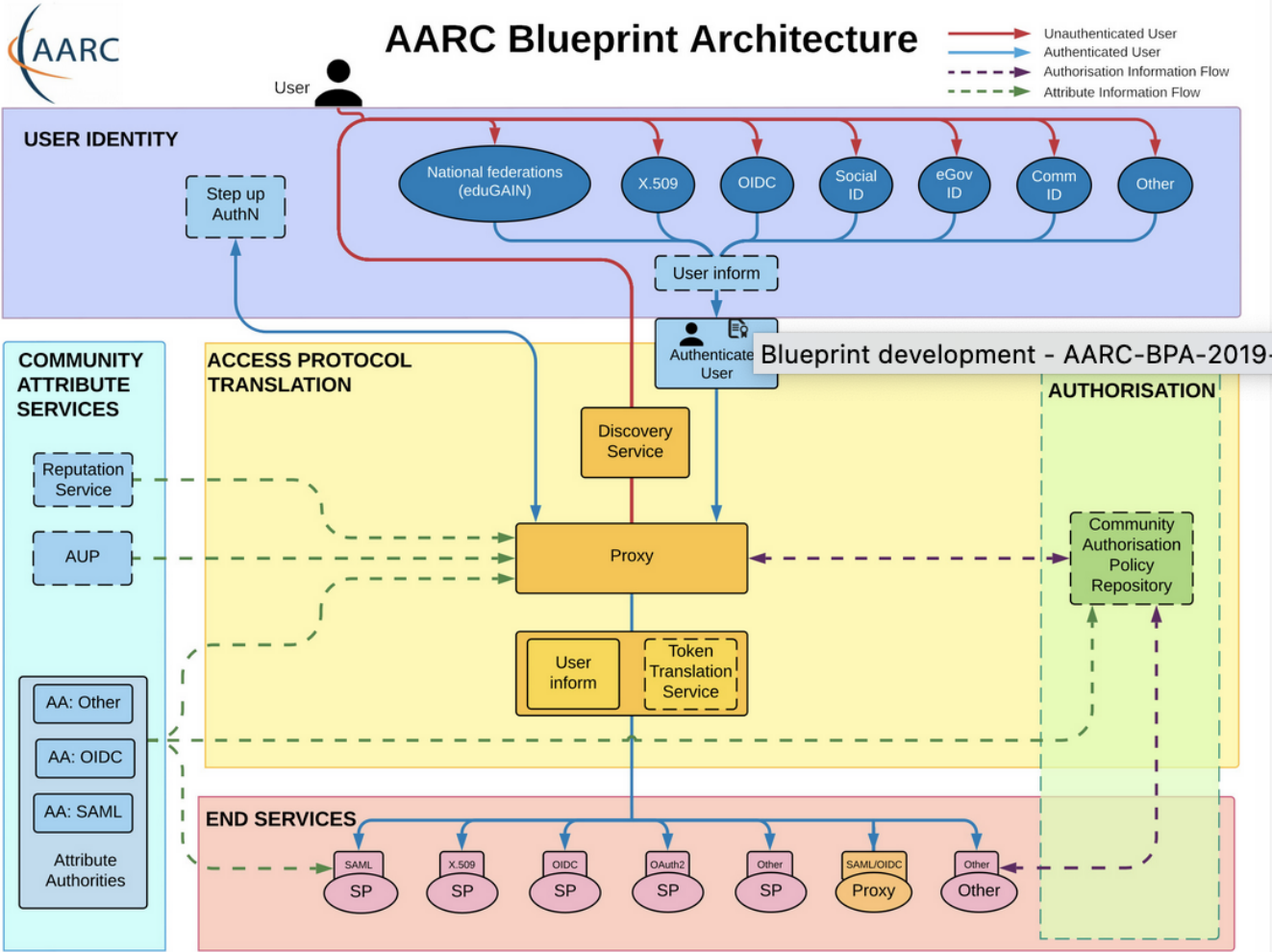
Nikhef Physics Data Processing programme and UM Dept. Advanced Computing Sciences



TNC23 Workshop *Standing on the shoulders of giants*

June 2023

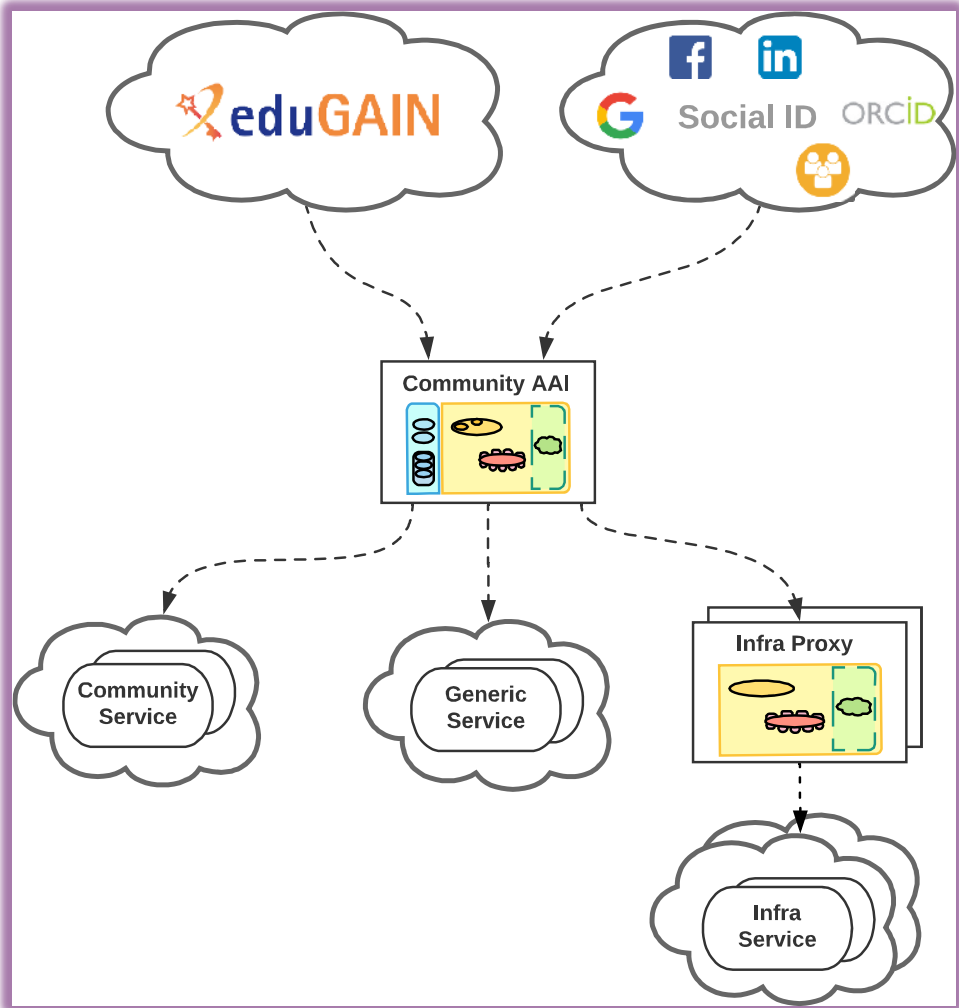
Arguably the best remembered picture from our AARC community



Beyond a single BPA proxy – complexities in composite infrastructure

EOSC AAI was one of the triggers to extend the BPA but is and will not be the only one!

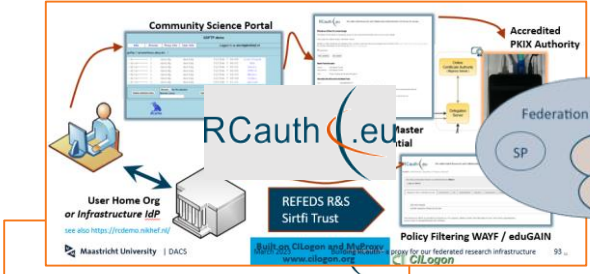
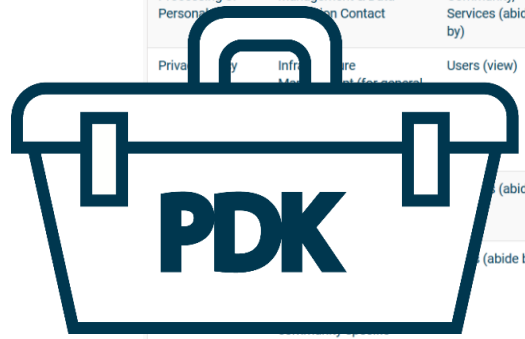
- 2019 “BPA Reloaded” (AARC-G045) lead us to composite proxy architectures
- and as we see the need grow for multiple instances of community and e-Infra proxies to work together, we end up with ...
 ... a federation of proxies ?! 😊



And an AARC beyond Sirtfi, RCauth, and the Policy Development Kit?

Document	Who should complete the template?	Audience	Description	Link
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together	Google Doc
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template procedure provides a step-by-step breakdown of actions to take following a security incident.	Google Doc
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.	Google Doc
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.	Google Doc
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.	Google Doc
Policy on the Processing of Personal Data	Infrastructure Management & Data Security Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.	Google Doc
Privacy Policy	Infrastructure Management	Users (view)	This can be used to document the data collected and processed by the Infrastructure and its participants. Each service in the infrastructure, as well as the infrastructure itself, should complete the template.	Google Doc
		(abide by)	This policy defines requirements for running a service within the Infrastructure.	Google Doc
		(abide by)	This is a template for the acceptable use policy that users must accept to use the Research Infrastructure. It should be augmented by the Research Community.	Google Doc

Showing 1 to 9 of 9 entries



Data Protection Impact Assessment - an initial guide for communities

Publication Date: 2018-04-30
 Authors: Ulrik Stenroos, David Grosjean, Neilson Stefan, Pawlow Wolfgang, Pempke
 DOI: assignment defined
 Document Code: AARC-G042

© GEANT on behalf of the AARC project.
 The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract
 This report presents the results of the case study on the evaluation of risks to personal data protection as considered in the European General Data Protection Regulation (GDPR), for infrastructures and their service providers that leverage federated identity management (FIM) to connect research and collaboration users. Specifically, it considers personal data collected as a result of using the infrastructure, not any risks relating to the research data itself, which is a community responsibility, and provides guidance to the infrastructures concerning Data Protection Impact Assessment (DPIA) in the final context. The authors present recommendations to Research Communities for determining the necessity of formal DPIA and guidelines for its execution. This document does not constitute legal advice in any specific jurisdiction.

Data Protection Impact Assessment - an initial guide for communities (AARC-G042)
 Published 2018-04-30

The screenshot shows the Sirtfi Dashboard with the title 'The Security Incident Response Trust Framework for Federated Identity'. It includes a search bar and a list of participating organizations with a 'Sirtfi?' checkbox for each. The list includes:

- University of Twente
- University of Groningen
- University of Amsterdam
- University of Leiden
- University of Utrecht
- University of Maastricht
- University of Eindhoven
- University of Radboud
- University of Wageningen
- University of Groningen
- University of Leiden
- University of Utrecht
- University of Maastricht
- University of Eindhoven
- University of Radboud
- University of Wageningen

 The dashboard also shows 'Showing 1 to 10 of 1,714 entries' and navigation buttons for 'Previous' and 'Next'.

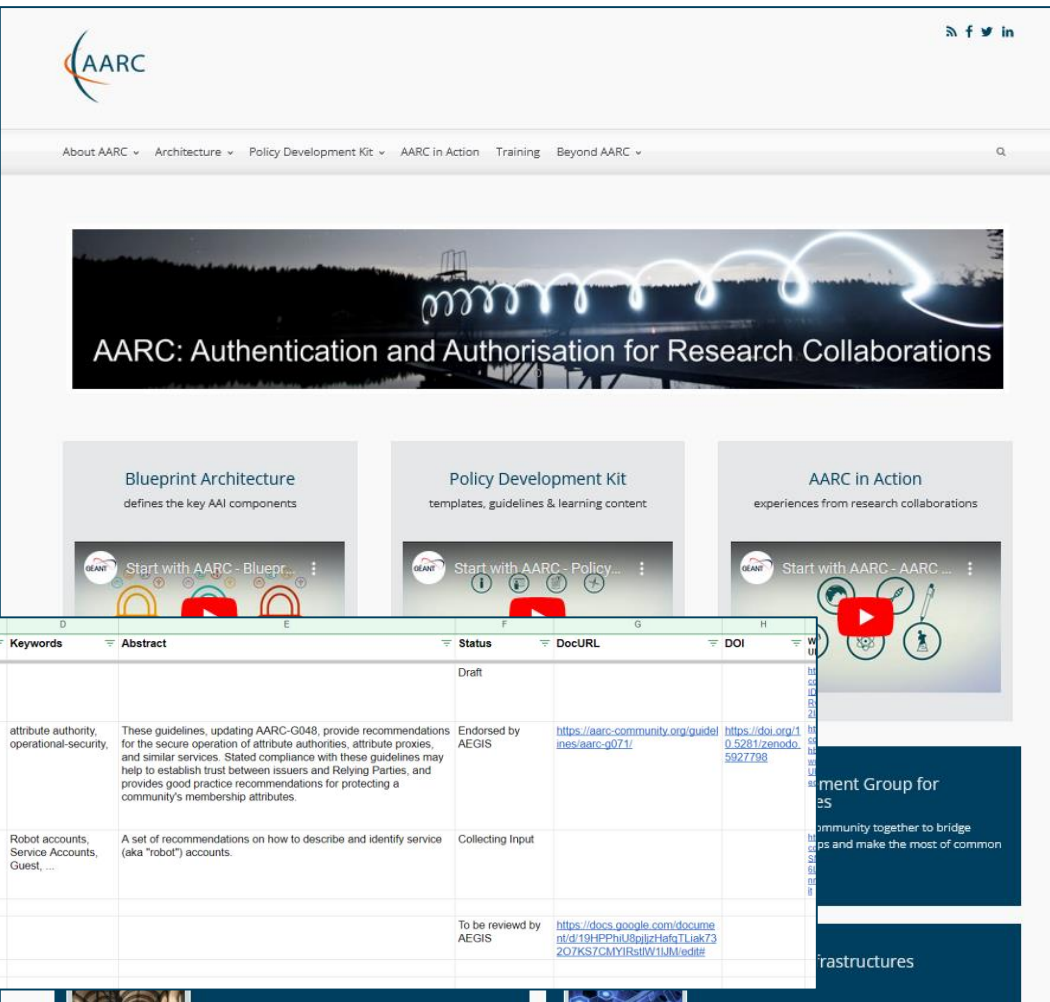
The screenshot shows the 'AARC-I050 Comparison Guide to Identity Assurance Mappings for Infrastructures'. It features a complex flowchart with various boxes and arrows, representing different identity assurance mappings. The title 'AARC-I050' is prominently displayed at the top. The diagram includes sections for 'Identity Assurance Framework', 'Kantara Identity Assurance Framework - IMAF-1420 (DP-SAC)', and 'eIDAS - electronic identification, authentication and trust services'. The AARC logo is visible in the bottom right corner.

Our AARC Community

Work on structuring AAI is far from over – and the **AARC community & AEGIS** provide the framework:

- **architecture** guidelines: primary group membership, service account information, entity categories, composite BPA proxy models
- **policy** developments: ‘AAOPS’, trust federation ‘across proxies’, assurance, and community formation in the Policy Development Kit

Today supported by a range of (inter)national infrastructures and projects (like ‘GN51 EnCo’ & ‘EOSC’) **Using WISE, IGTF, REFEDS, as open venues to convene and work**



	A	B	C	D	E	F	G	H	I
	DocNum	Other Id	Title	Keywords	Abstract	Status	DocURL	DOI	W
70	AARC-G070		Expression of primary group Membership			Draft			
71	AARC-G071		Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements	attribute authority, operational-security,	These guidelines, updating AARC-G048, provide recommendations for the secure operation of attribute authorities, attribute proxies, and similar services. Stated compliance with these guidelines may help to establish trust between issuers and Relying Parties, and provides good practice recommendations for protecting a community's membership attributes.	Endorsed by AEGIS	https://aarc-community.org/guidelines/aarc-g071/	https://doi.org/10.5281/zenodo.5927798	
72	AARC-G072		Guidelines for expressing service account information	Robot accounts, Service Accounts, Guest, ...	A set of recommendations on how to describe and identify service (aka "robot") accounts.	Collecting Input			
74	AARC-G079		Specification of AARC Entity Categories			To be reviewed by AEGIS	https://docs.google.com/document/d/19tEPPhu39qjz7afzT1akZ32Q7KS7cMYRstW1UJnUedite		
75	AARC-G080		AARC Blueprint Architecture 2022+						

So what are we facing now?!

- meta-federations of research infrastructures and horizontal providers
- interoperability with broader provider base, and not limited to *just* EU Wallets or SSI
- need better uptake and integration of the BPA, and in more Research Infrastructures
- a need for assurance (in FIM4R and beyond),
without a ubiquitous source in R&E ... but with govt. eID capabilities for some
- plus all the things we just heard about before!

It's time to enhance the effectiveness of the AARC BPA and PDK

leverage AARC's structuring effect to ease interoperation across thematic areas, and increase impact of the BPA in new communities (within and outside of EOSC)

Who should sit under the AARC TREE ... and who do we need on board

Research Infrastructures and e-Infrastructures, both national and international facilities

- providers of resources and services for research communities, ERICs, ESFRIs, and other (data) sources

Research Communities

- scientific communities, collaborations and individual researchers, (so including our mid-sized groups)

EU and global initiatives

- International Data Spaces Association (IDSA), GAIA-X, EU ID Wallets, FIM for Research (FIM4R), &c

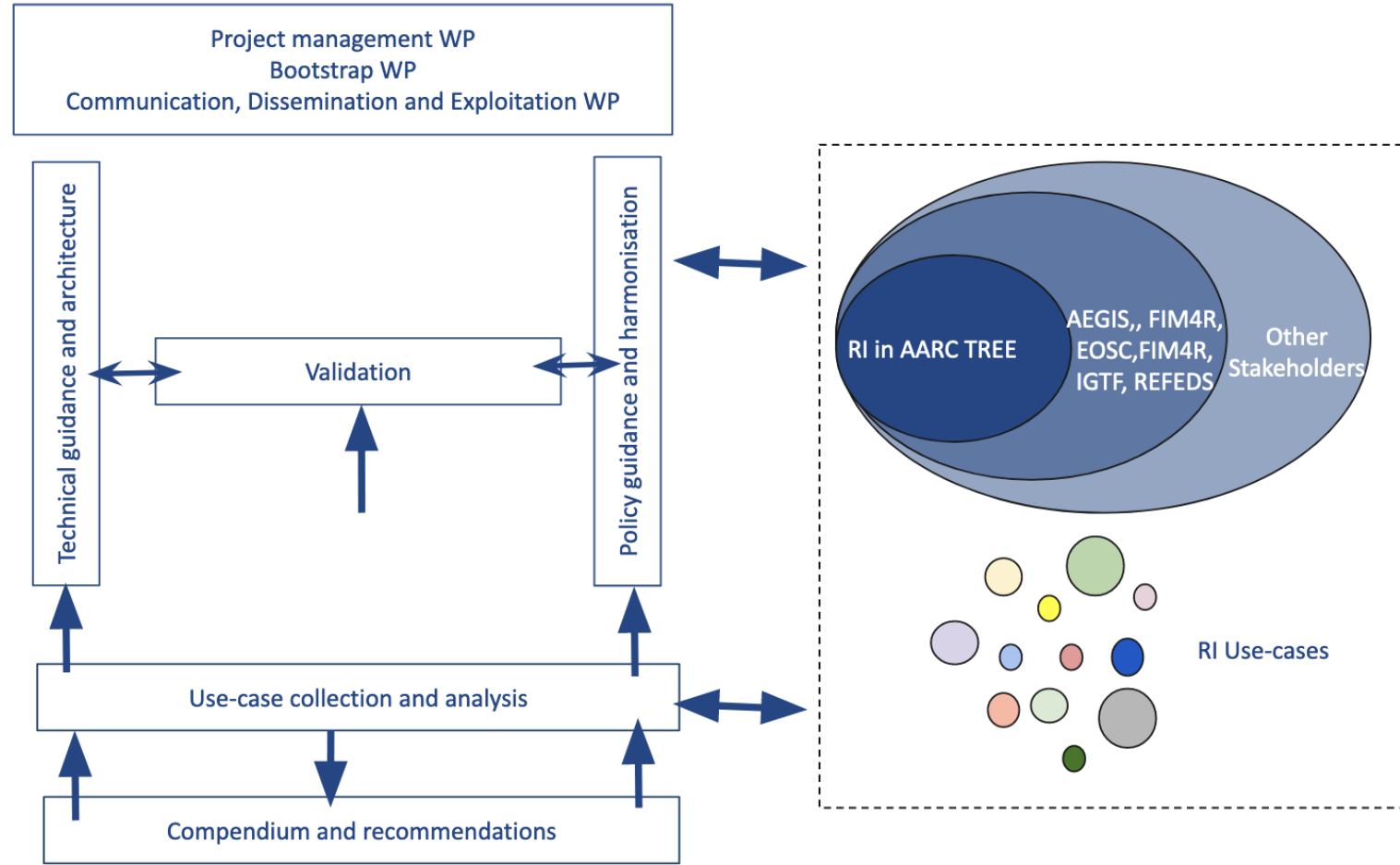
Service and resource providers:

- AAI and other providers interested in offering their services and resources to researchers

EOSC Ecosystem

- EOSC related initiatives like EOSC Association Task Forces and other EOSC projects

Growing an AARC TREE



sprouting an evolved architecture

Evolution of the AARC Blueprint Architecture

- including a more prominent role for OpenID Connect federation
- federated authorization mechanisms

Harmonisation of community user attributes

- application integration across different protocols

OpenID Connect Federations

- deployment profile of the specification
- addressing the challenges we face now in the heterogeneous EOSC AAI ecosystem

Authorisation for Federated Resources

- authorization policy interoperability

Decentralised Identities

- EU Digital Identity Wallet, distributed Identifiers, verifiable creds & presentations, decentralised storage

and evolved AARC policy development

Research-infrastructure alignment and policy harmonisation

- Operational Trust for Community and Infrastructure BPA Proxies
- Snctfi - increasing acceptance of research infrastructure proxies with R&E identity providers and sources of authentication
- Review infrastructure models for **coordinated AUP, T&C, and privacy notices**, improving cross-infrastructure user experience

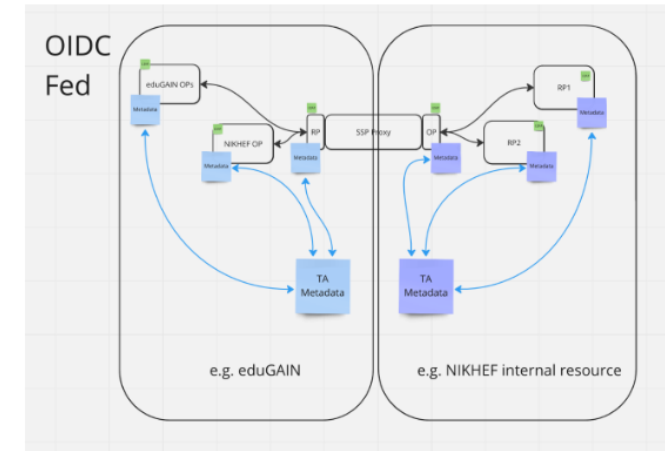
User-centric trust alignment and policy harmonisation

- Lightweight community management policy template
- Guideline on cross-sectoral trust in novel federated access models
- Assurance in research services through (eIDAS) public identity assertion
- FIM4R policy workshop series on validation of the restructured policy framework (together with the new 'BPA')

Just one of the many topics to try ...

In today's BPA, the proxy links both sides by being opaque, both for attributes as well as for trust

- does it have to be that way?
- separate claims/attribute transformation from trust bridging?
- can OIDCfed structures convey trust transparently?
- can we do more that way? or would it just confuse everyone?
- easier to bridge trust across sectors this way?
edu, gov, and private?



David Groep:

Raise of hands

Who knows about

- Proxy: most in the room
- OIDCfederation: few in the room
- Bridge PKI (public key infra): 1

What was the problem that triggered this session?

Proxies are wonderful, they can be opaque and expose things to the outside world..

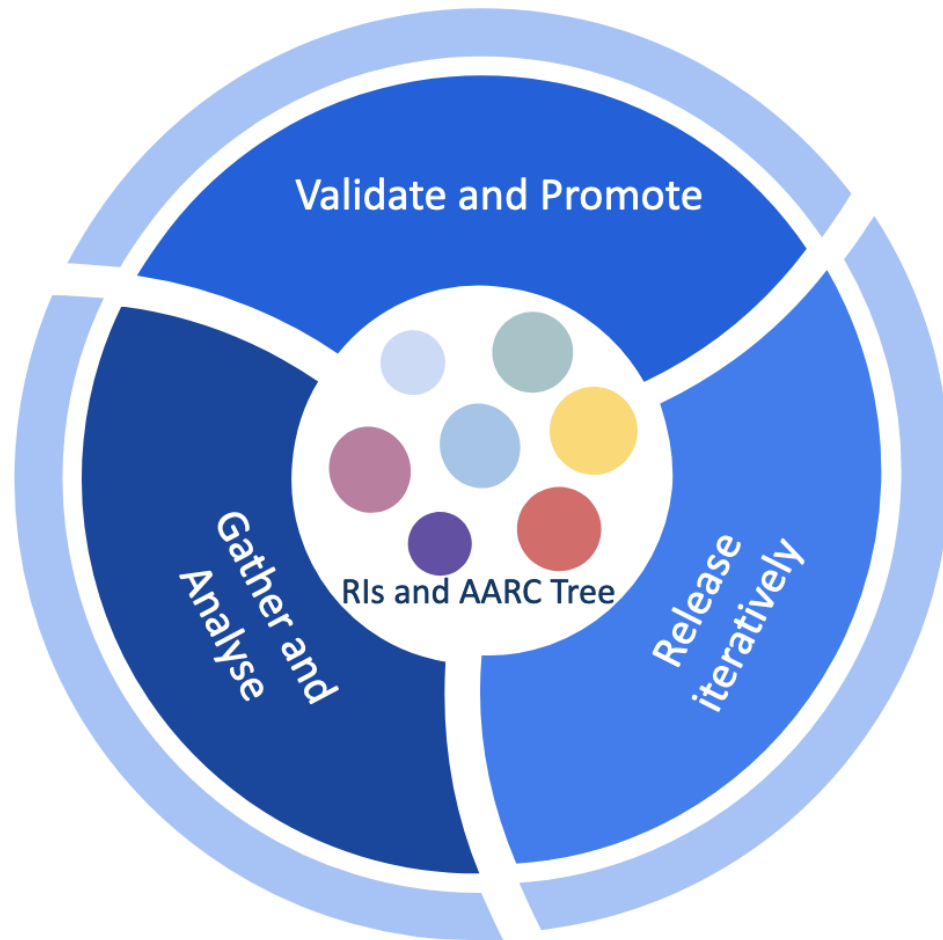
Proxy into eduGAIN using SAML, token translation, attribute transformation, augmentation
Membership services?

OIDC world, to amalgamate a set of RPs

Essentially overloading the proxy with two roles, technical role of translating one for format to another (+ augment of claims), but also bridging trust between both "domains"

In OIDC federation, you can chain metadata statements not by publishing to a list, but building hierarchies, trust anchors who can sign intermediates . multiple signatures on the same

A proven methodology



- Provide guidance based on a broad and open community process: FIM4R, EOSC, AEGIS, WISE, REFEDS, IGTF, ApplInt, ...
- Experts gather in open, dedicated teams
- Iterative stakeholder engagement
- practical validation in use cases of the research and e-infras, e.g. through AEGIS

We need our collaborators and stakeholders ... and thus: you!

Use Cases Collection and Analysis

- with the large ESFRI RIs, clusters, and national nodes to validate BPA effectiveness and act as a flywheel to increase its application

followed by adoption and validation

Compendium & Recommendations

- have the validators and use cases have a broader impact by promoting them as ‘community good practice’ examples – and telling the world about it.

The ‘Compendium’ model helped us before 😊



just some of the RIs that are looking for a BPA with enhanced effectiveness

What would be the presents under a (funded) AARC Tree?

- **Updated AARC Blueprint architecture** for emerging technologies and services in pan-European research infrastructures
 - Up-to-date guidance on implementing the architecture of their Authentication and Authorisation Infrastructure service components, incorporating new requirements, use cases and new technologies.
- Recommendations for a **common long-term strategy for AAI services and best practices**
 - AARC TREE best practices and recommendations with new technical approaches and collaboration in its implementation across scientific domains
- Updated **interoperability framework**
 - Framework to harmonise AAI policies to empower identity providers, service providers and user communities to identify interoperable policies for the open science vision.



Thank you

Any Questions?

dauidg@nikhef.nl



<https://aarc-community.org>

Any and all information in this document SHOULD NOT be construed as an endorsement of any particular organisation or plan. All information subject to change without notice. Information presented here MUST NOT be quoted out of context. (RFC 2119)