Authentication and Authorisation for Research and Collaboration

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

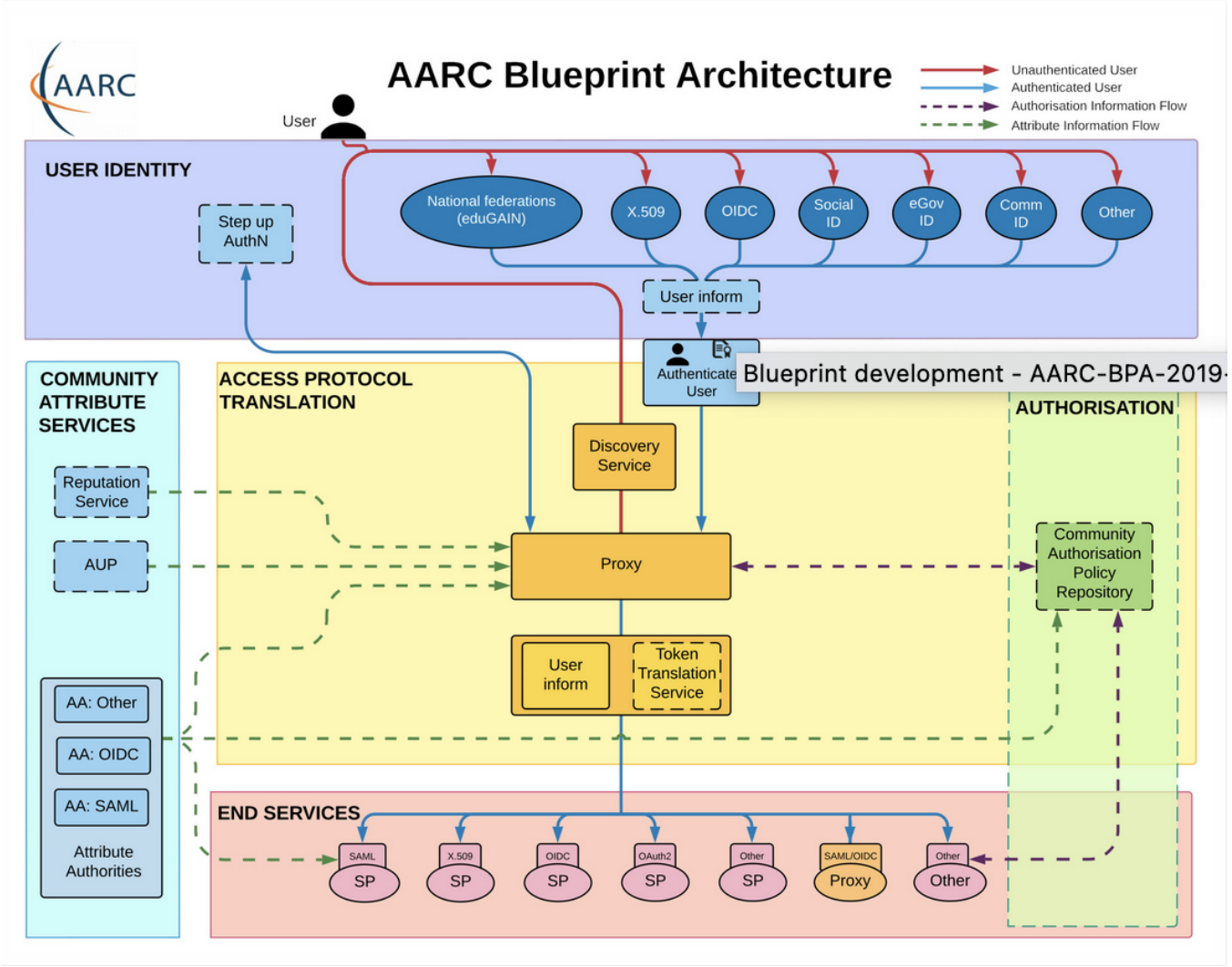
a preliminary insight in potential developments in the AARC Community

David Groep
AARC Policy Area Coordinator
Nikhef Physics Data Processing programme and UM Dept. Advanced Computing Sciences

Nikhef Maastricht University

TNC23 Workshop *Standing on the shoulders of giants*
June 2023

Arguably the best remembered picture from our AARC community



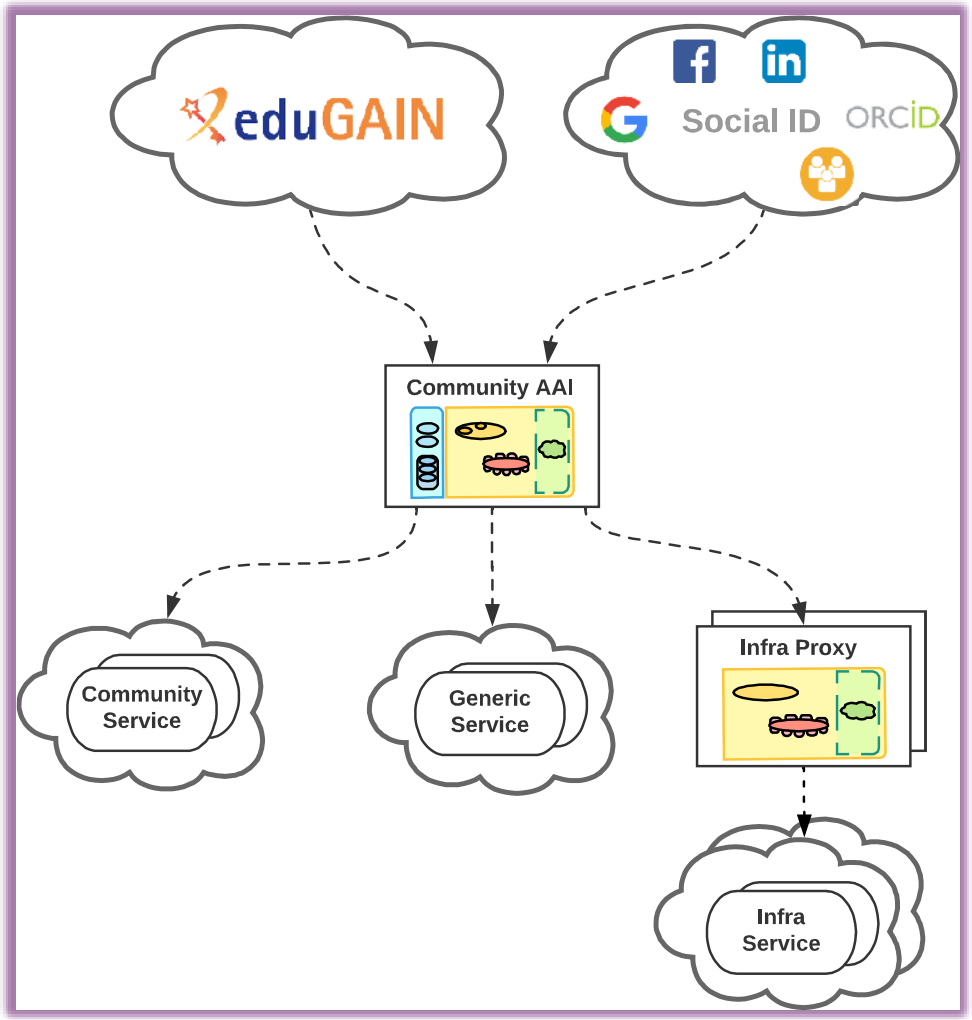
Beyond a single BPA proxy – complexities in composite infrastructure

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 ?! ☺



AARC G045 https://aarc-community.org/guidelines/aarc-g045/
and EOSC AAI Task Force report – ISBN 978-92-76-28113-9, DOI:10.2777/8702

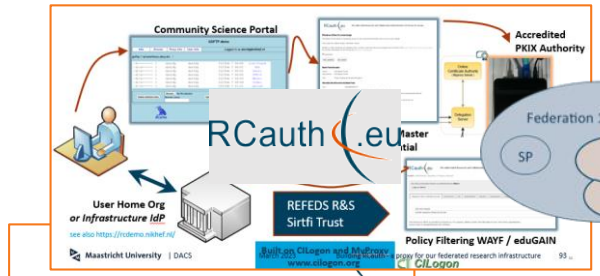
And an AARC beyond Sirtfi, RCauth, and the Policy Development Kit?

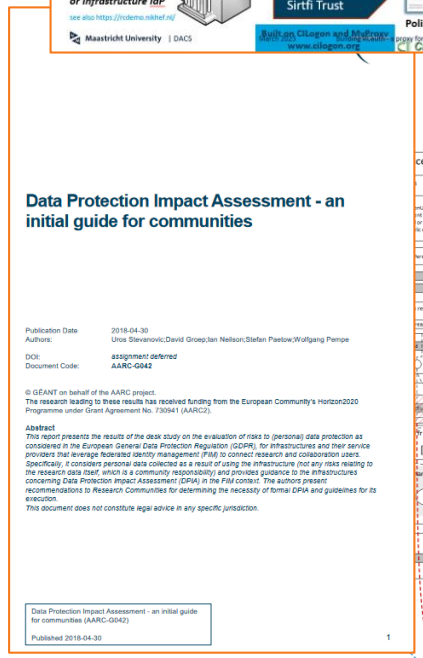
Document	Who should complete the template?	Audience	Description	Link
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together	Google Doc
Incident 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	Infrastructure Management & Data Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.	Google Doc
Privacy	Infrastructure	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	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

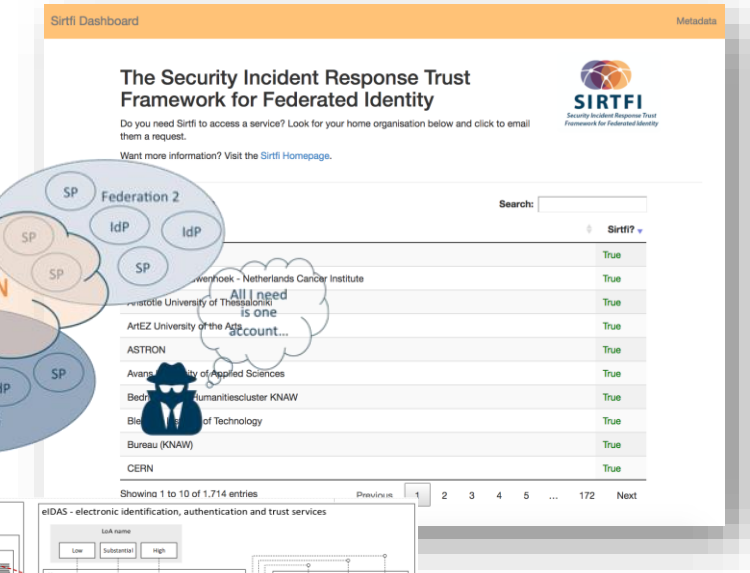
restrictions)

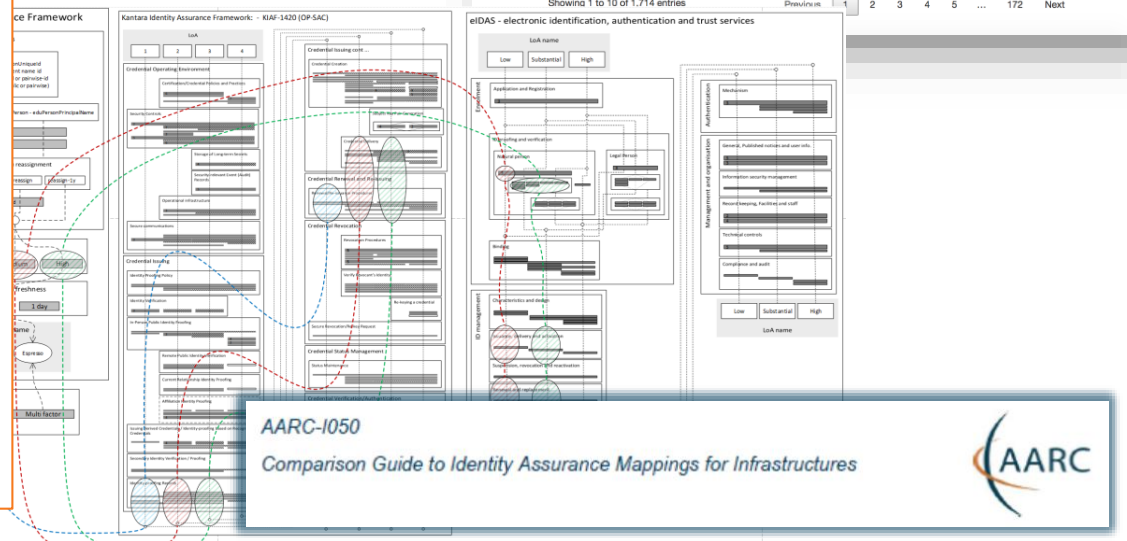
Showing 1 to 9 of 9 entries Previous Next

PDK









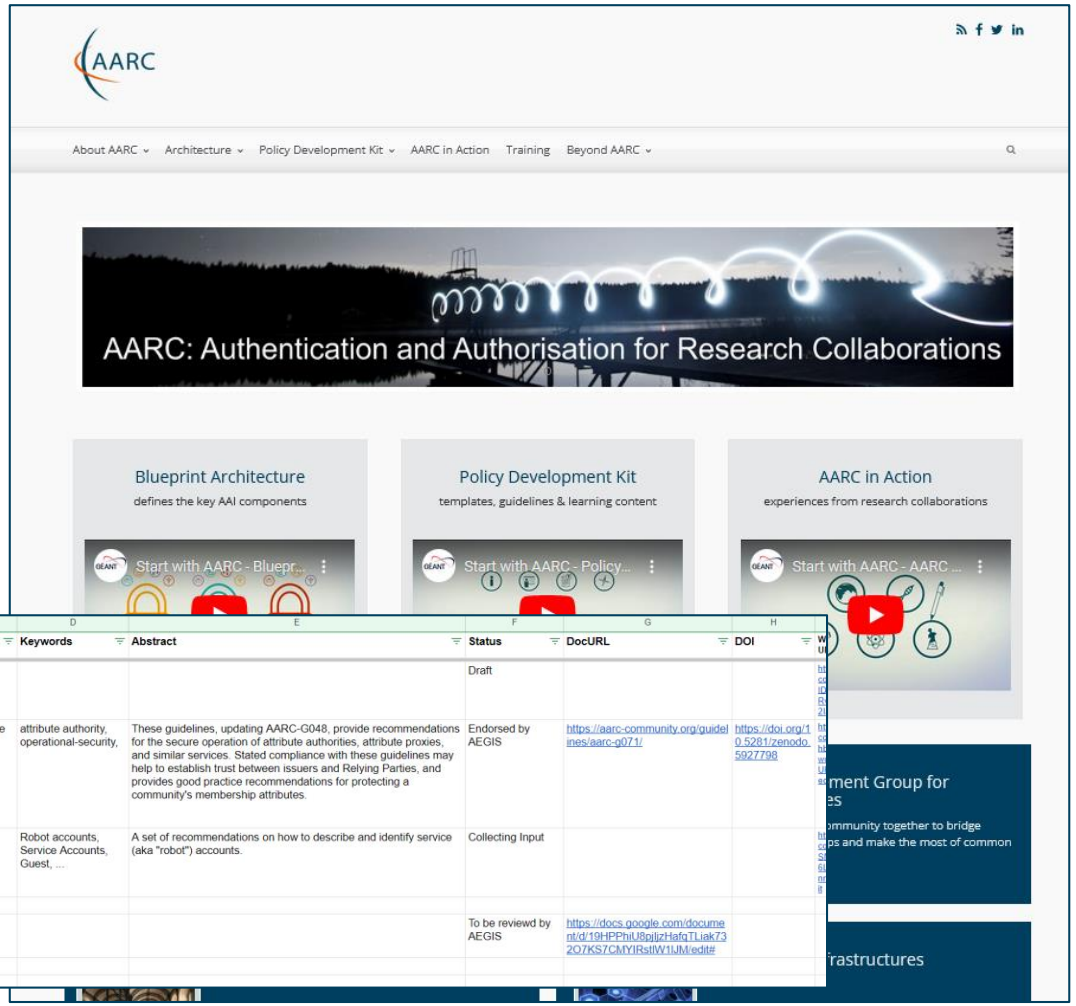
Our AARC Community

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



DocNum	Other Ic	Title	Keywords	Abstract	Status	DocURL	DOI
AARC-G070		Expression of primary group Membership			Draft		
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
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		
AARC-G079		Specification of AARC Entity Categories			To be reviewd by AEGIS	https://docs.google.com/document/d/19HPPhiU8pIjzHafqTLiak732O7KS7CMYIRsIlW1IJM/edit#	
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

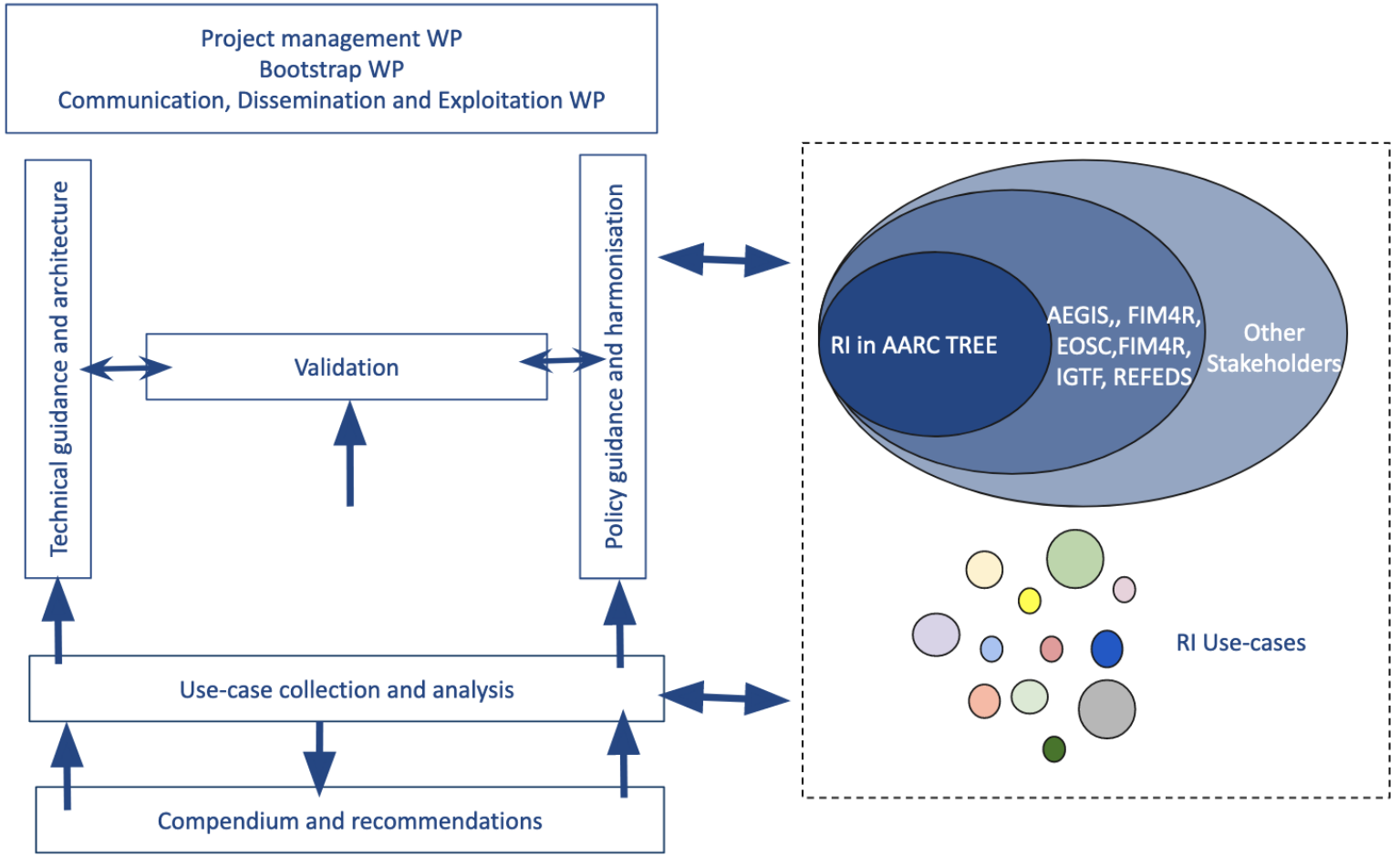
Service and resource providers:

- 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

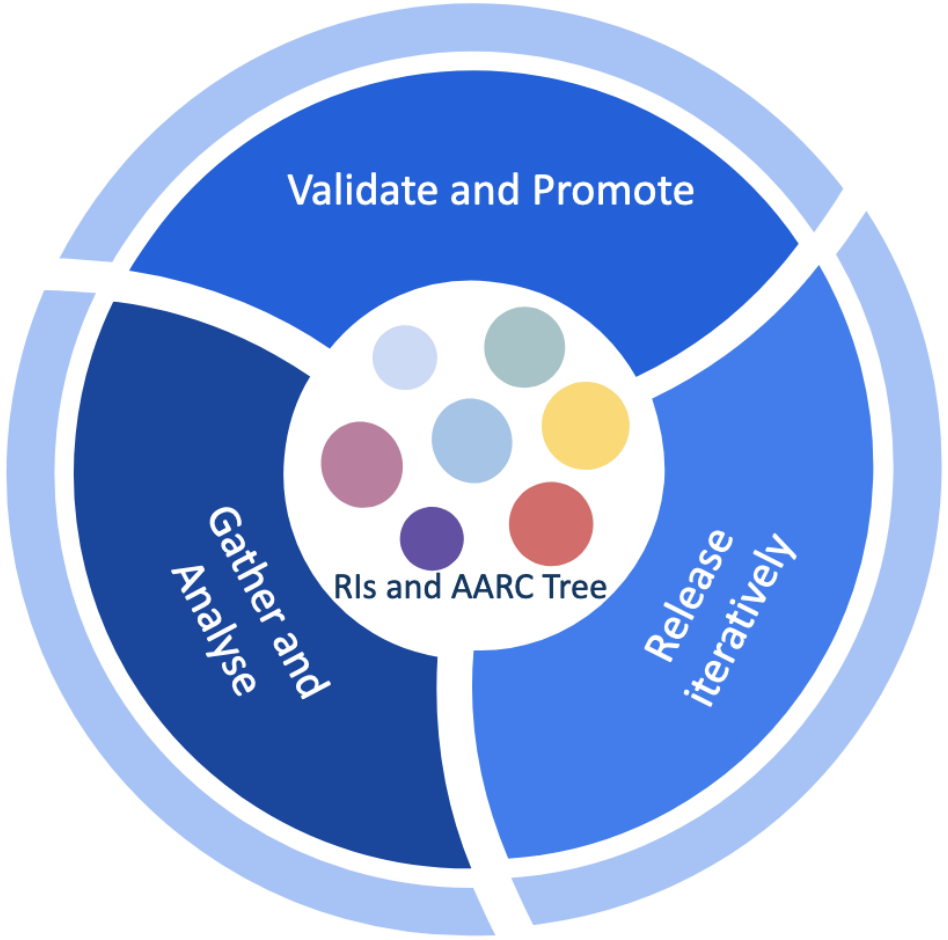
Research-infrastructure alignment and policy harmonisation

- 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')

A proven methodology



- Provide guidance based on a broad and open community process: FIM4R, EOSC, AEGIS, WISE, REFEDS, IGTF, AppInt, …
- 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?

davidg@nikhef.nl

AARC

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)

Lemon tree image: Tomwsulcer, https://commons.wikimedia.org/wiki/File:Lemon_Tree_in_Santa_Clara_California.jpg