Authentication and Authorisation for Research and Collaboration

Sitting under a broad-leaved AARC-TREE

making authentication & authorization for research collaboration even better

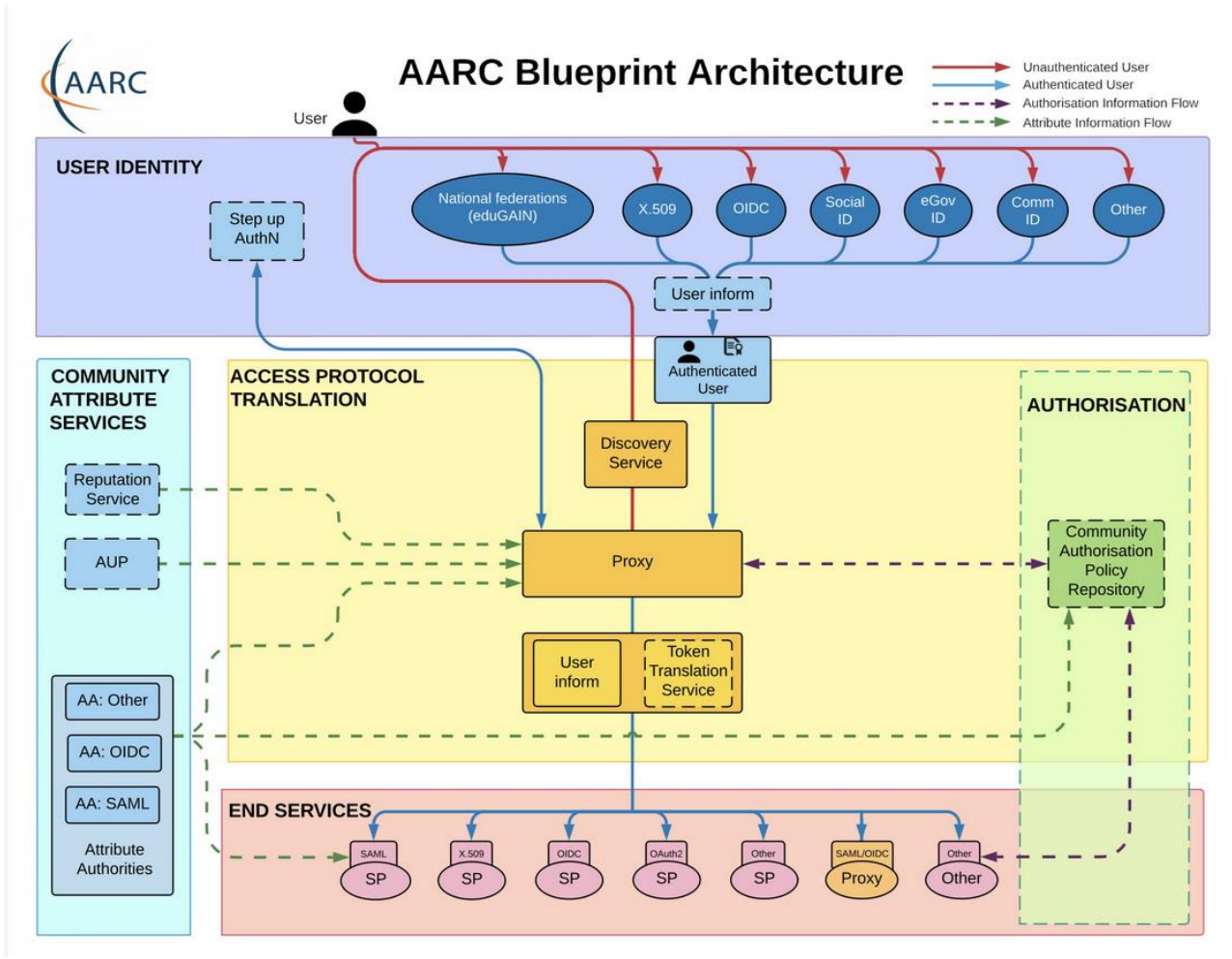
David Groep

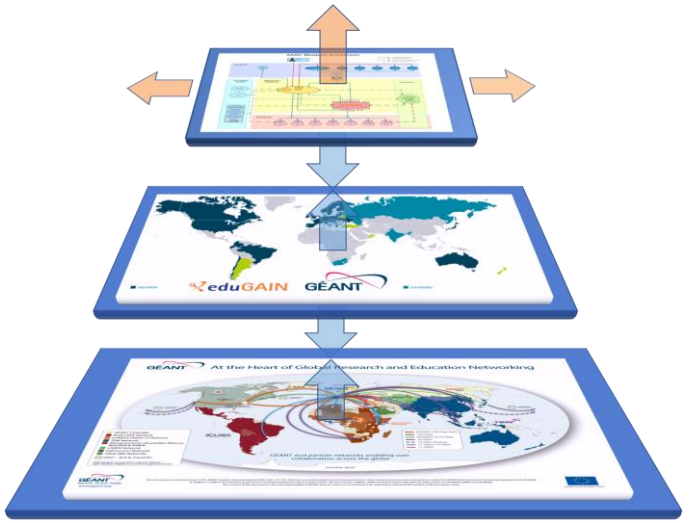
Nikhef Maastricht University

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

International Symposium on Grids and Clouds (ISGC) 2024
Taipei, March 2024

AARC – Authentication and Authorisation for Research Collaboration





FENIX RESEARCH INFRASTRUCTURE

SSHOC

LSC LIGO Scientific Collaboration

panosc photon and neutron open science cloud

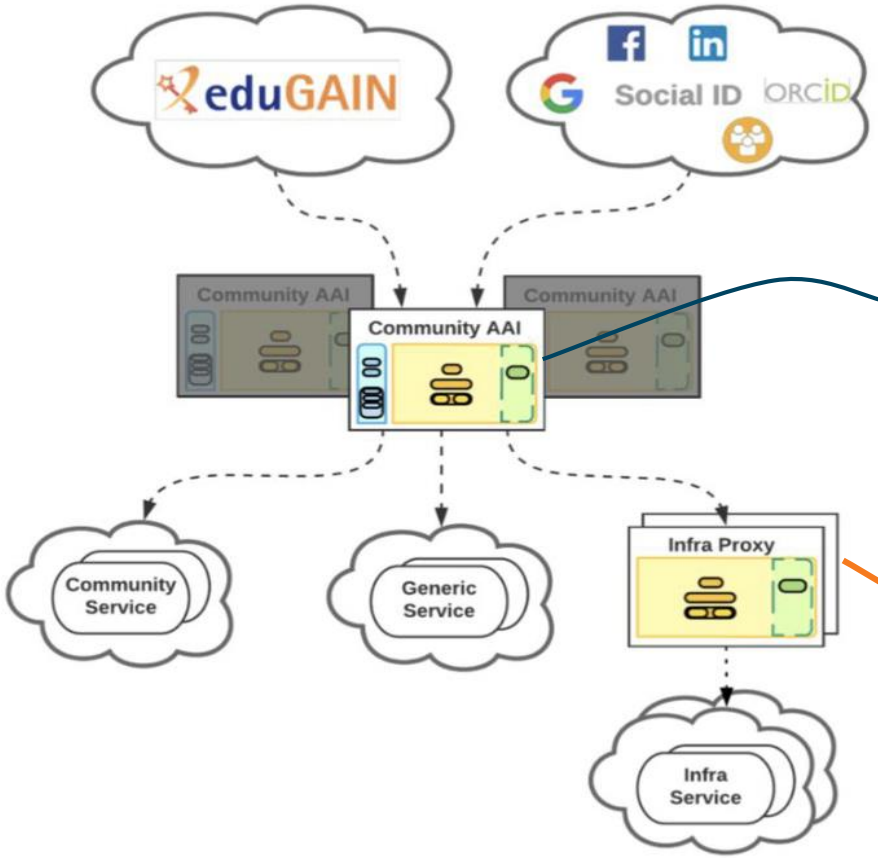
EOSC-Life

ESCAPE

neic PUHURI LUMI

DARIAH-EU Digital Research Infrastructure for the Arts and Humanities

The Community AAI and the Infrastructure Proxy: definition



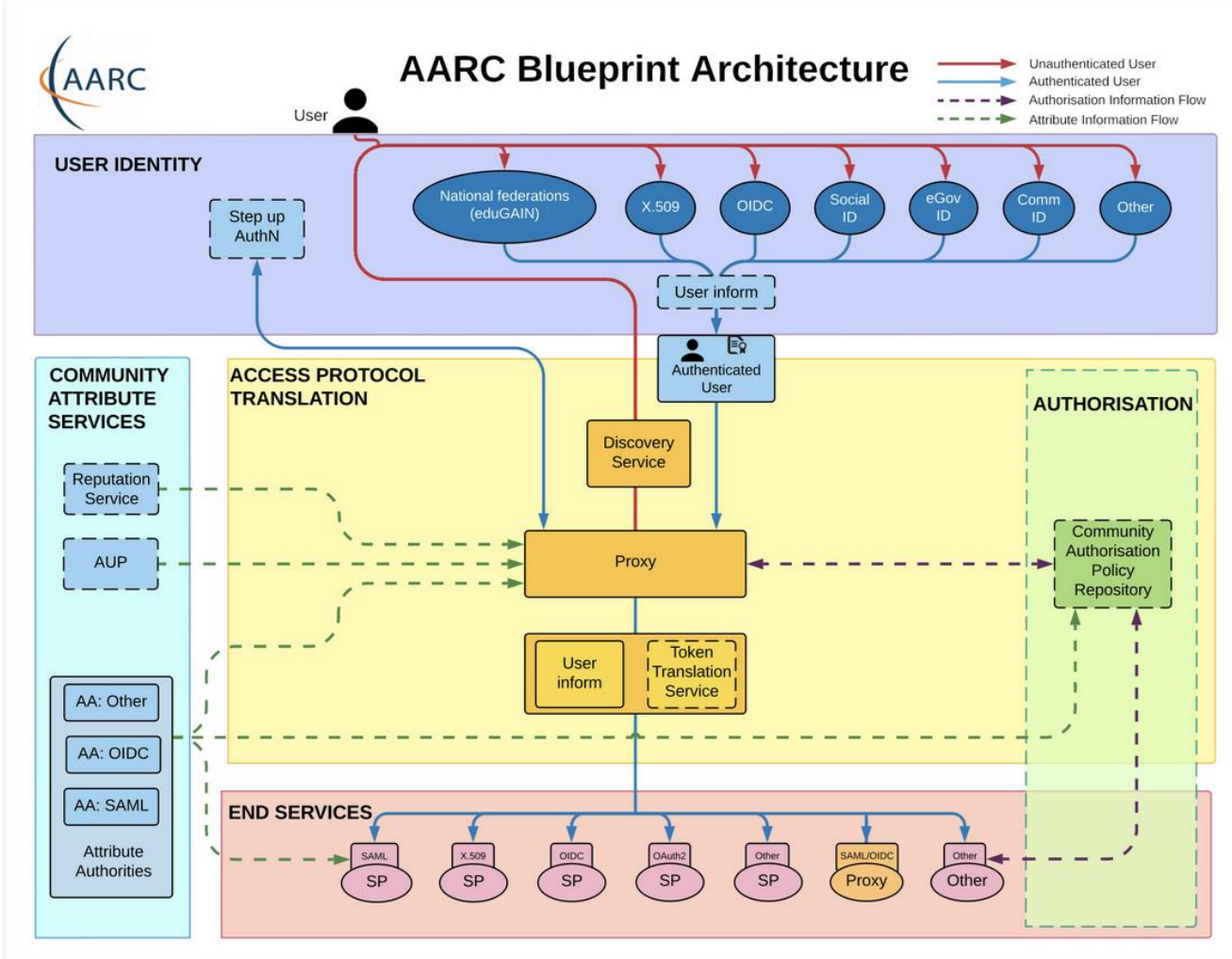
Community AAI

The purpose of the Community AAI is to streamline researchers' access to services, both those provided by their own infrastructure as well as the services provided by infrastructures that are shared with other communities.

Infrastructure Proxy

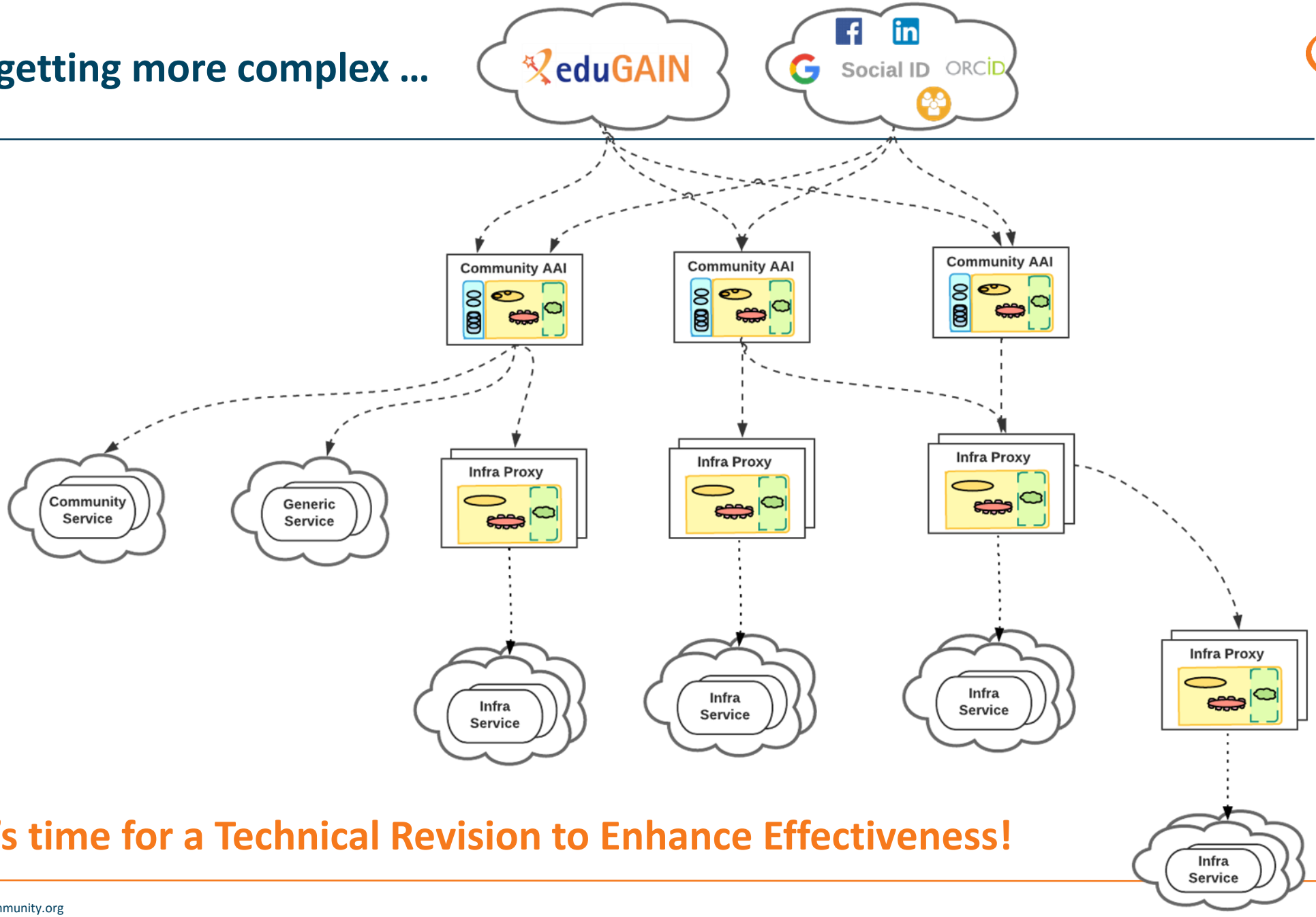
The Infrastructure Proxy, enables Infrastructures with a large number of resources, to provide them through a single integration point, where the Infrastructure can maintain centrally all the relevant Policies and business logic for making available these resources to multiple communities

Interoperability – more than just the nice colours



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

But it's getting more complex …



… it's time for a Technical Revision to Enhance Effectiveness!

What will AARC TREE bring?

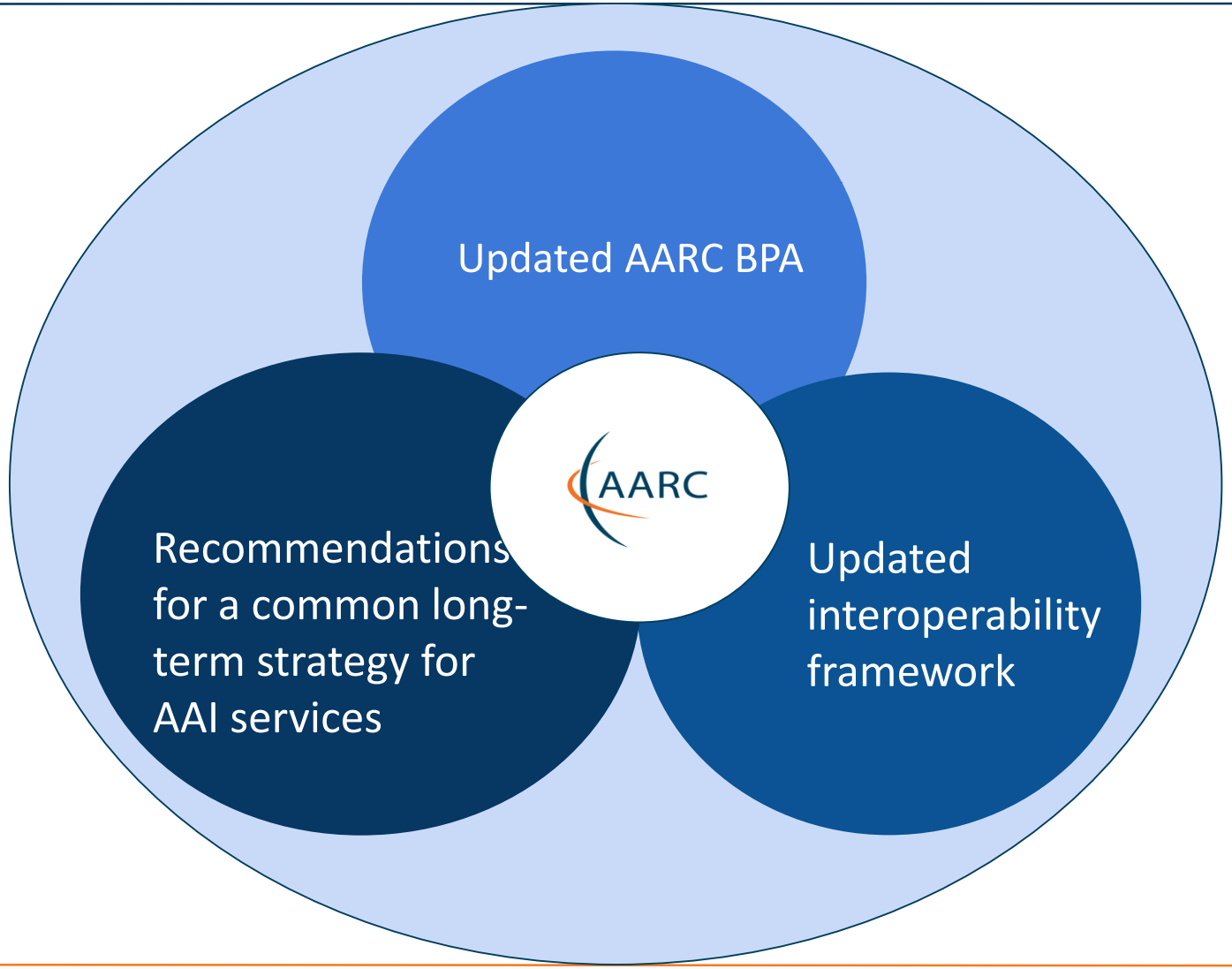
Capture and **analyse** new authentication and authorisation interoperability requirements (that support integration use-cases across the thematic area) and **provide** a landscape analysis of AAIs services (including gaps) in the RIs represented in AARC TREE

Expand the number of research communities that can implement the AARC BPA and/or the AARC guidelines, by providing a validation environment and toolkits. At the same time support existing AARC communities in adopting new guidelines

Define and **validate** new technical and policy guidelines for the AARC BPA that address RIs use-cases. This will improve the integration of RIs across thematic areas and increase the ability of RIs to support emerging needs

Bring RIs, e-Infrastructures and relevant stakeholders **together** to align strategies to integrate new technologies, better interoperate and share resources across thematic areas and produce a compendium and recommendations for different stakeholders

AARC TREE Main Facts: Expected results



The AARC TREE in the Trust and Identity Landscape

AARC Engagement Group for Infrastructures

The forum of e/r-Infras that operate an AARC BPA complaint AAI.
It's a closed group on purpose as we want to get feedback from the hands on group.
They approve the AARC guidelines.

Technical WG

- Led by Nicolas and Christos
- This is where technical guidelines are discussed
- Anybody can join the discussion: **https://lists.geant.org/sympa/info/aarc-architecture**

Policy WG

- Led by Dave and David
- Supported by EnCo and IGTF
- Anybody can join the discussion: **policy@aarc-community.org** https://lists.geant.org/sympa/info/aarc-na3

Technology

Evolve the BPA to address the more complex (and the simpler) worlds

guidelines for **harmonising expression of community user attributes**

- **reduce inconsistencies** between implementations
- improve **interoperability** & **end-user usability** across research community communities and infrastructures

Extend AARC BPA

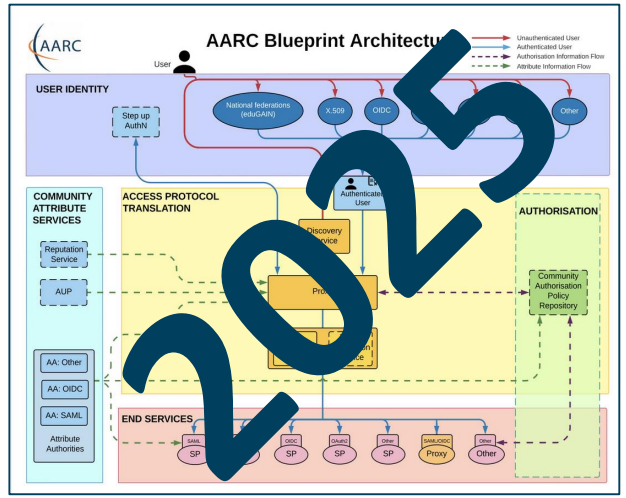
- improve **scalability**
- leverage emerging standards like **OpenID Federation**

Authorisation guidelines

- best practises to enable efficient & effective **sharing of federated resources**

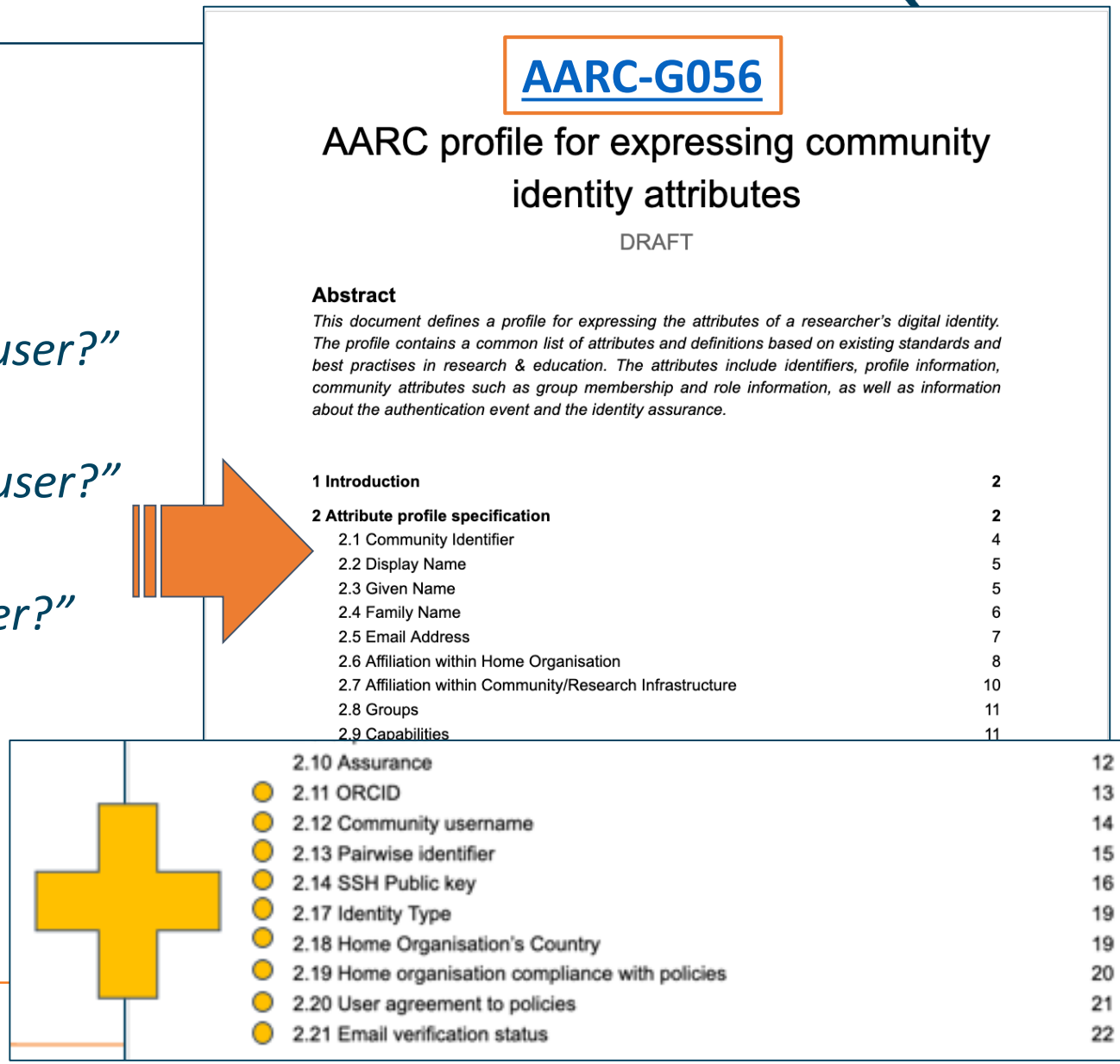
Decentralised identities

- guidance for **digital wallets** linked to BPA



How to *express* community identity attributes?

- *"How to express the **identifier** of a user?"*
  → AARC-G026
- *"How to express the **groups and roles** of a user?"*
  → AARC-G069 (was AARC-G002)
- *"How to express **resource capabilities** of a user?"*
  → AARC-G027
- *"How to express the **home institute** of a user?"*
  → AARC-G025
- *How to express user **assurance** information when interacting with another proxy?"*
  → RAF & AARC-G021



AARC-G056

AARC profile for expressing community identity attributes

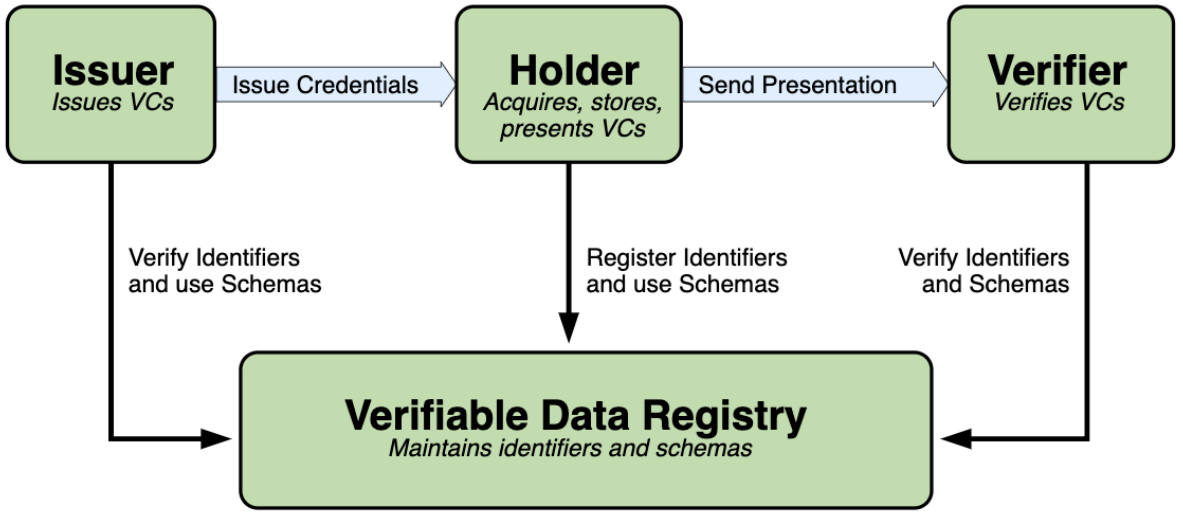
DRAFT

Abstract

This document defines a profile for expressing the attributes of a researcher's digital identity. The profile contains a common list of attributes and definitions based on existing standards and best practises in research & education. The attributes include identifiers, profile information, community attributes such as group membership and role information, as well as information about the authentication event and the identity assurance.

Decentralised identities

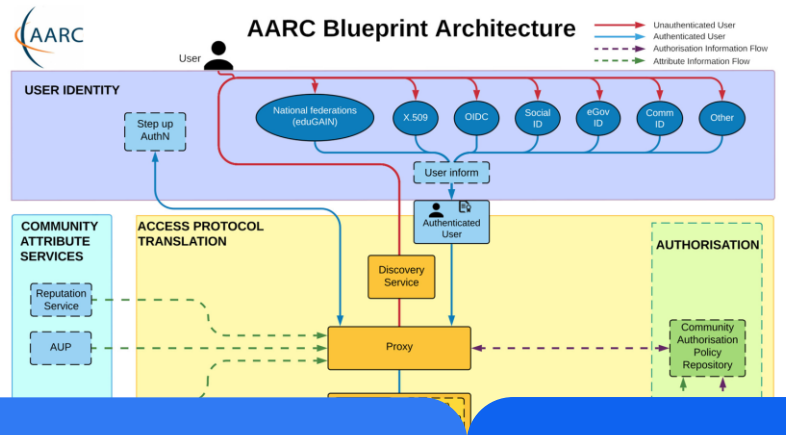
- Provide guidance on the use of decentralised identities and digital identity wallets
  - Explore Distributed Identifiers, Verifiable Credentials/Presentations & trust frameworks
- Support the EU Digital Identity Wallet (EDIW) initiative

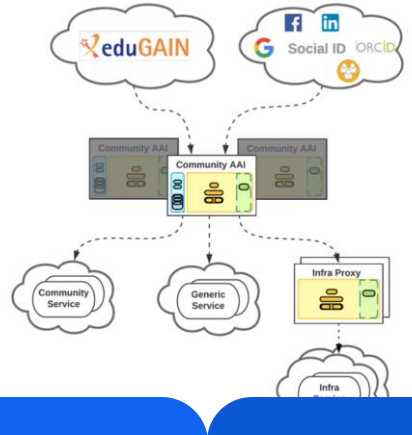


https://www.w3.org/TR/vc-data-model/

AARC Blueprint Architecture ‘BPA2025’!

AARC BPA 2019





OpenID Federations + AuthZ for Federated Resources + Decentralised Identities & Wallets

AARC BPA 2025

Policy and good practice harmonisation

An AARC beyond the Policy Development Kit?

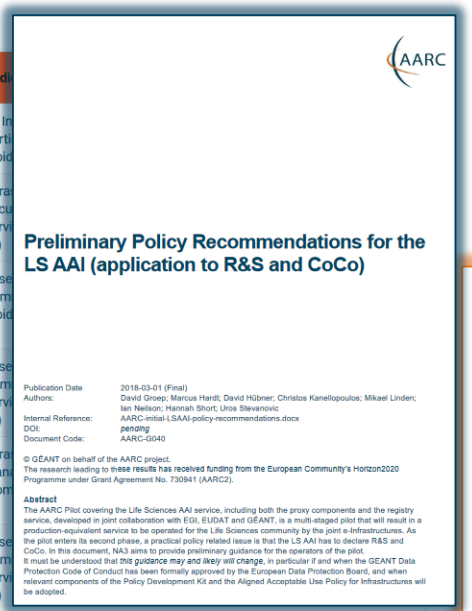
Current PDK is targeted at *large and structured* communities – and quite complex

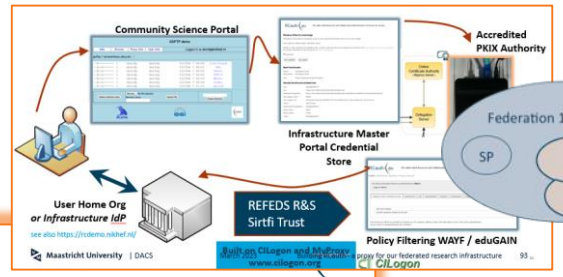
Document	Who should complete the template?	Audi		
Top Level Infrastructure Policy	Infrastructure Management	All In Parti (abid		
Incident Response Procedure	Infrastructure Management & Security Contact	Infra Secu Servi by)		
Membership Management Policy	Infrastructure Management	Rese Com (abid		
Acceptable Authentication Assurance	Infrastructure Management	Rese Com Servi by)		
Risk Assessment	Infrastructure Management, Services & Security Contact	Infra Man (com		
Policy on the Processing of Personal	Infrastructure Management & Data Contact	Rese Com Servi by)		
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

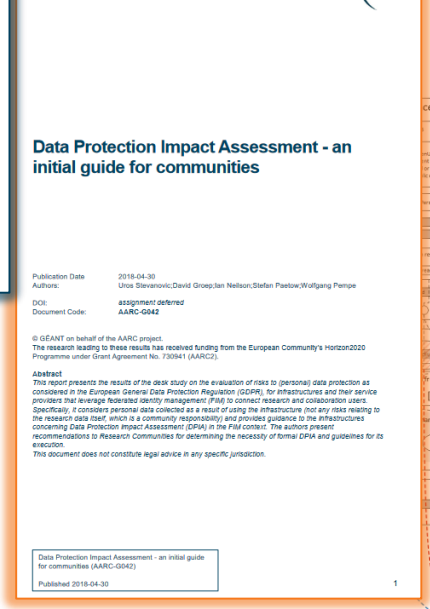
restrictions)

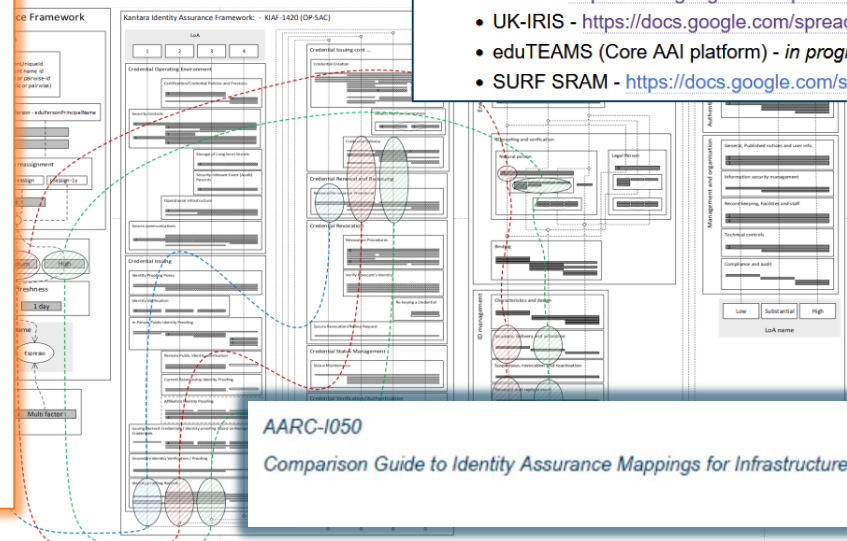
Showing 1 to 9 of 9 entries Previous Next

PDK









Self-assessment support sheet

The assessment sheet supports the evaluation of the AARC-G0 g071/ for the full description, requirements, and supporting doc

- template: https://edu.nl/88dwf

Assessments and review sheep

- WLCG - https://docs.google.com/spreadsheets/d/1z
- UK-IRIS - https://docs.google.com/spreadsheets/d/1
- eduTEAMS (Core AAI platform) - *in progress*
- SURF SRAM - https://docs.google.com/spreadsheet

AAOPS

AARC-I050

Comparison Guide to Identity Assurance Mappings for Infrastructures

Objective: support the diverse and different policies needed now

Infrastructure alignment and policy harmonisation: helping out the proxy (M1-M18, 21PM)

- Operational Trust for Community and Infrastructure BPA Proxies
- Increase acceptance of research proxies by identity providers through common baselines
- Review infrastructure models for **coordinated AUP, T&C, and privacy notices**, improving cross-infrastructure user experience (users need to click only once)

User-centric trust alignment and policy harmonization: helping out the community (M6-M24, 26PM)

- Lightweight community management policy template
- Guideline on cross-sectoral trust in novel federated access models
- Assurance in research services through (eIDAS) public identity assertion

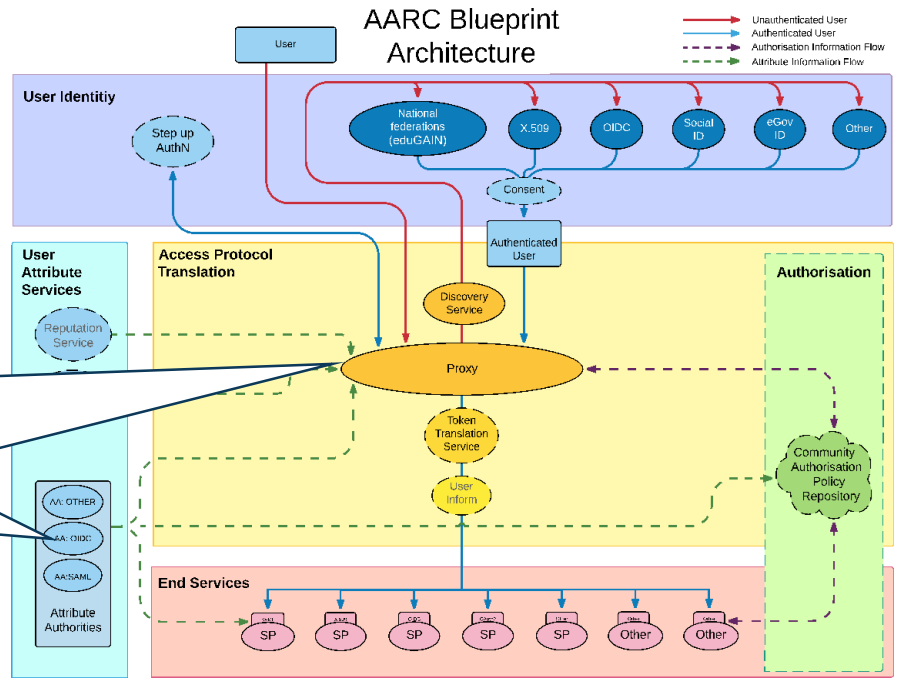
Anchored in the research user communities by **co-creation with FIM4R**, through policy workshops validating the restructured policy framework … together with the new BPA

AARC G071 is there to help, but do we 'get the trust across'?

Community membership management directories and attribute authorities

- integrity of membership
- identification, traceability
- site and service security
- network protections
- assertion integrity

> Trust marks and expression



But when proxies are proxying proxies, can we proxy the trust?

Agree to a

common baseline

… an approach that was successful previously!

… set of (one or more) guidelines that represent a widely agreed and jointly-developed ***operational trust baseline*** *for infrastructure membership management and proxy components. Supplemented by policy guidance on how to connect sectoral federations with* ***more specific*** *policies. Driven by your (FIM4R, WISE, EOSC, …) feedback, and those of current proxy operators (in AEGIS).*

See https://www.igtf.net/guidelines/aaops/ and https://aarc-community.org/guidelines/aarc-g071/

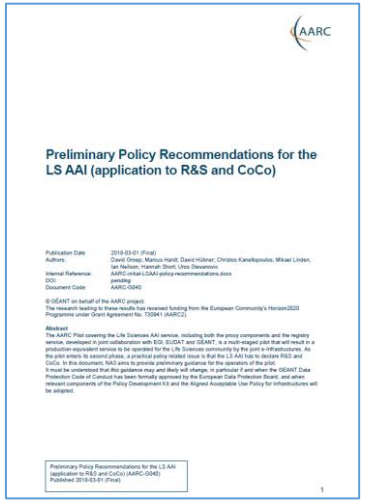
Proxies have their own challenges as well: AUPs, T&Cs, Privacy notices, …

For large ‘multi-tenant’ proxies:

- some subset users in some communities use a set of services – how to I present their Terms and Conditions, and their privacy policies, so that the users
  - only see the T&Cs and notices for services they will access
  - this does not to need to be manually configured for each community
  - is automatically updated when services join

as well as for community and dedicated proxies:

- when new (sensitive) services join, who needs to see the new T&Cs?
- can we communicate acceptance of T&Cs to services even if ‘we’ are small and ‘they’ are large?


Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)

beyond AARC-G040

What is an acceptable user experience in clicking through agreements?
What is most effective in exploiting the WISE Baseline AUP? What do *you* need?

With Fewer Clicks to More Resources!

Helping out the community – a simpler policy toolkit for communities

What we heard and observe:

> *"small to mid-sized communities do not have the resources to maintain a bespoke community management policy"*

Leaves both communities and operators of membership management services unclear about trust assurance level of members - current templates in toolkit too complex and prescriptive

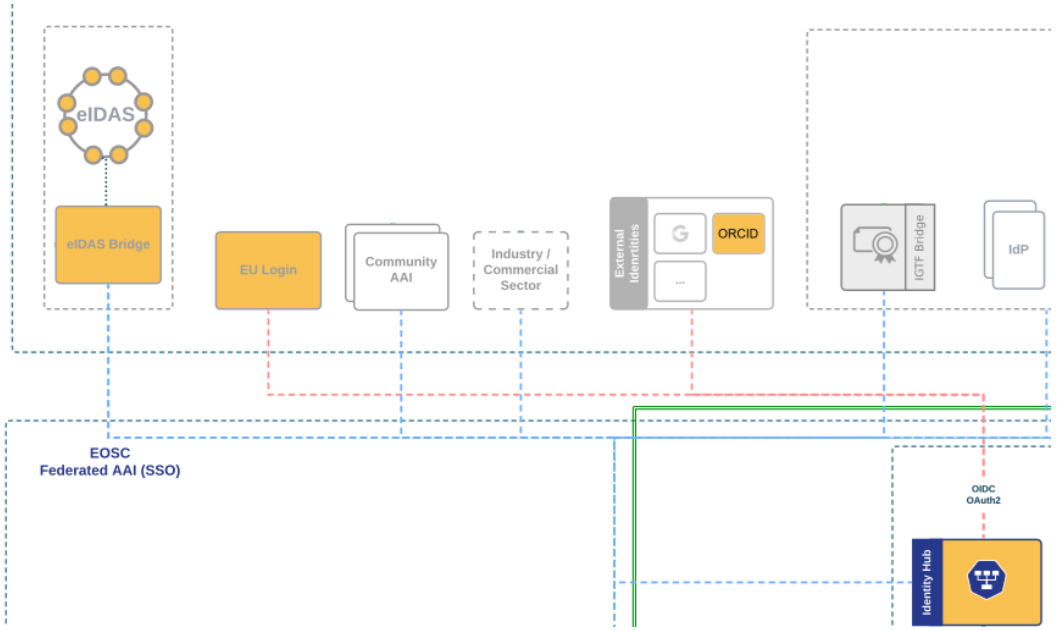
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.

- community consultation on the 'minimum viable community management' – we are here!
- template and implementation guidance (FAQ) on community lifecycle management
- how to implement the community management in the (EOSC) AAI services

We'll see more diverse sources of identity & assurance anyway

Most reliable (and most 'available') source of assurance may be the European government identity ecosystem.

- Step-up to at least substantial level can now readily be done 'at home' by users through their national eID schemes
- Joint work on eIDAS, Erasmus Student Mobility, and more makes this more accessible
- Better attainable than relying on home institutions?



… but:

- what to do with non-European users?
- how to link the identities together

All About Enabling Research – FIM4R & communities are the driving factor

Also in AARC-TREE we target a “co-creation process” with the research communities:

- support FIM4R to increase the reach of workshops in the next 2 years
- community review *and* your ideas and input on both policy and architecture
- start from the high-level requirements and broad community input

Really a global activity: we want to engage everyone in AARC TREE and beyond

Involving the user community from start to finish

Dedicated work package to collect requirements from (new) communities

Landscape analysis of AARC BPA adoption

- Conduct an AARC BPA **adoption survey** among the RIs,
  online survey accompanied by the arranged conversations with the individual RIs
- Collect information on current deployment of AARC BPA AAIs and adoption of guidelines

Result: **Landscape analysis of AARC BPA adoption (around December 2023)**

Use cases requirements & consultations

- Design and create survey (including technology and policy questions)
  based on FIM4Rv2 paper, Evolution, EOSC AAI TF requirements
- Engage FIM4R, AEGIS, EOSC AAI TF, National Ris, EU data spaces to capture requirements
- Discus with our ESFRIs to get expectations & requirements via consultations, workshops etc

Result: **Use cases requirements described in a white paper (target Q1 2025)**

Handover to Compendium

Adoption and validation

Pilots

- Validate the guidelines
- Technical feasibility
- Cross RIs

Validator suite

- Including online validator service

Start with:

- **WISE AUP and Privacy Notice across RIs**
- **OpenID Federations**

- **Validators to test implementations of guidelines**
- **Online validation service available to all**
- **Collaboration with AEGIS to test participating RIs**

Engage partners

- Get feedback
- Feasibility
- Technical correctness

Continuous cycle!

- *Collect* feedback from outside the project
- *Provide* feedback to technology and policy

Compendium and Recommendations

In the '2nd year' of climbing the tree (April 2025 - February 2026)

Publish the **compendium of AARC best practices**
and **deliver recommendations** for a common long-term strategy
for AAI services in pan-European Research Infrastructures in Europe

- based on the use case input ☺
- promotes proposed approach from architecture and policy activities
- iterate with the infrastructures at large to produce the final version

Image generated by Adobe Firefly 2 with the text prompt “image of a broad-leaved lemon tree with a person sitting below it leaning against the trunk in the sunshade”

Let’s climb the AARC TREE together!

Thanks to the AARC Community, including folk from whom I re-used graphics and material in this overview. In random order: Licia Florio, Nicolas Liampotis, Christos Kanellopoulos, Marina Adomeit, Janos Mohacsi, Ilaria Fava, Slavek Licehammer, Dave Kelsey, Ian Neilson, Marcus Hardt, Mischa Salle, Hannah Short, and Maarten Kremers.

Thank you

Any Questions?

davidg@nikhef.nl

https://aarc-community.org

The work leading to these results has received funding from the European Union and other sources.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. Grant Agreement No. 101131237 (AARC TREE).