



Authentication and Authorisation for Research and Collaboration

## Sitting under a broad-leaved AARC-TREE

making authentication & authorization for research collaboration even better

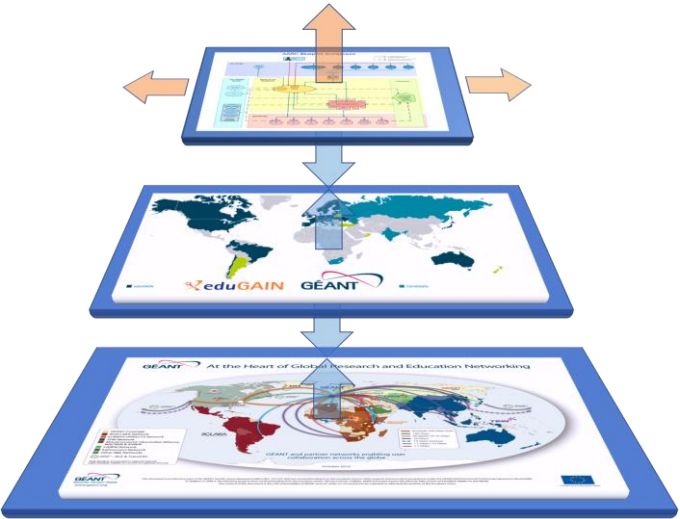
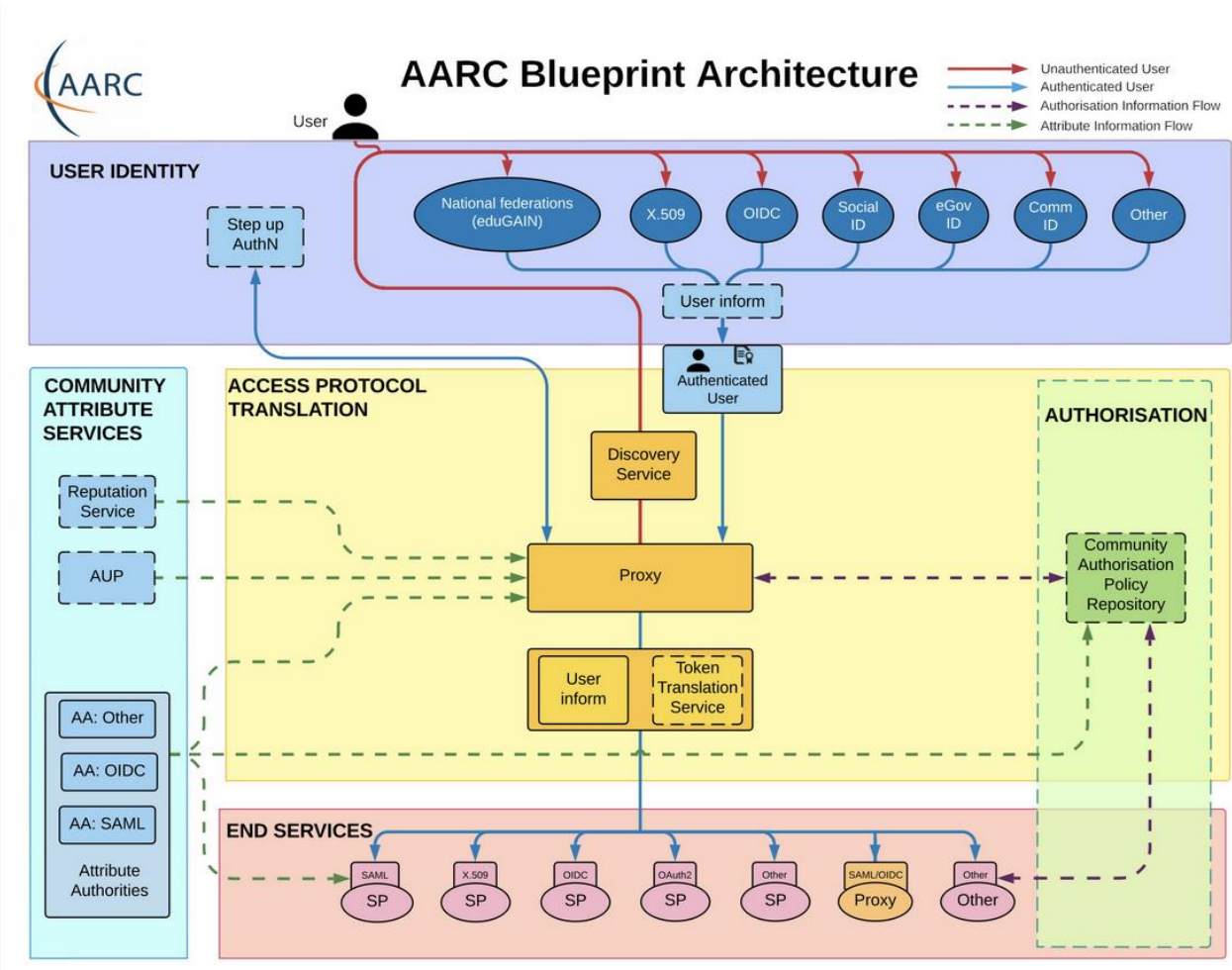
**David Groep**



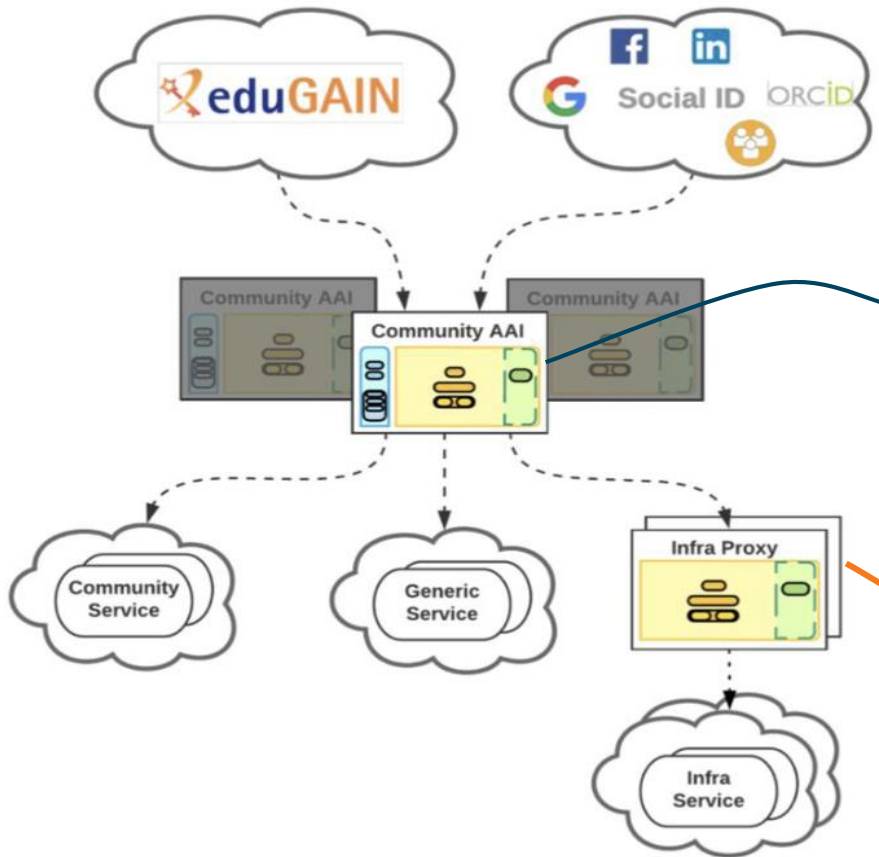
Nikhef Physics Data Processing programme and UM Dept. Advanced Computing Sciences

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

# AARC – Authentication and Authorisation for Research Collaboration



# The Community AAI and the Infrastructure Proxy: definition



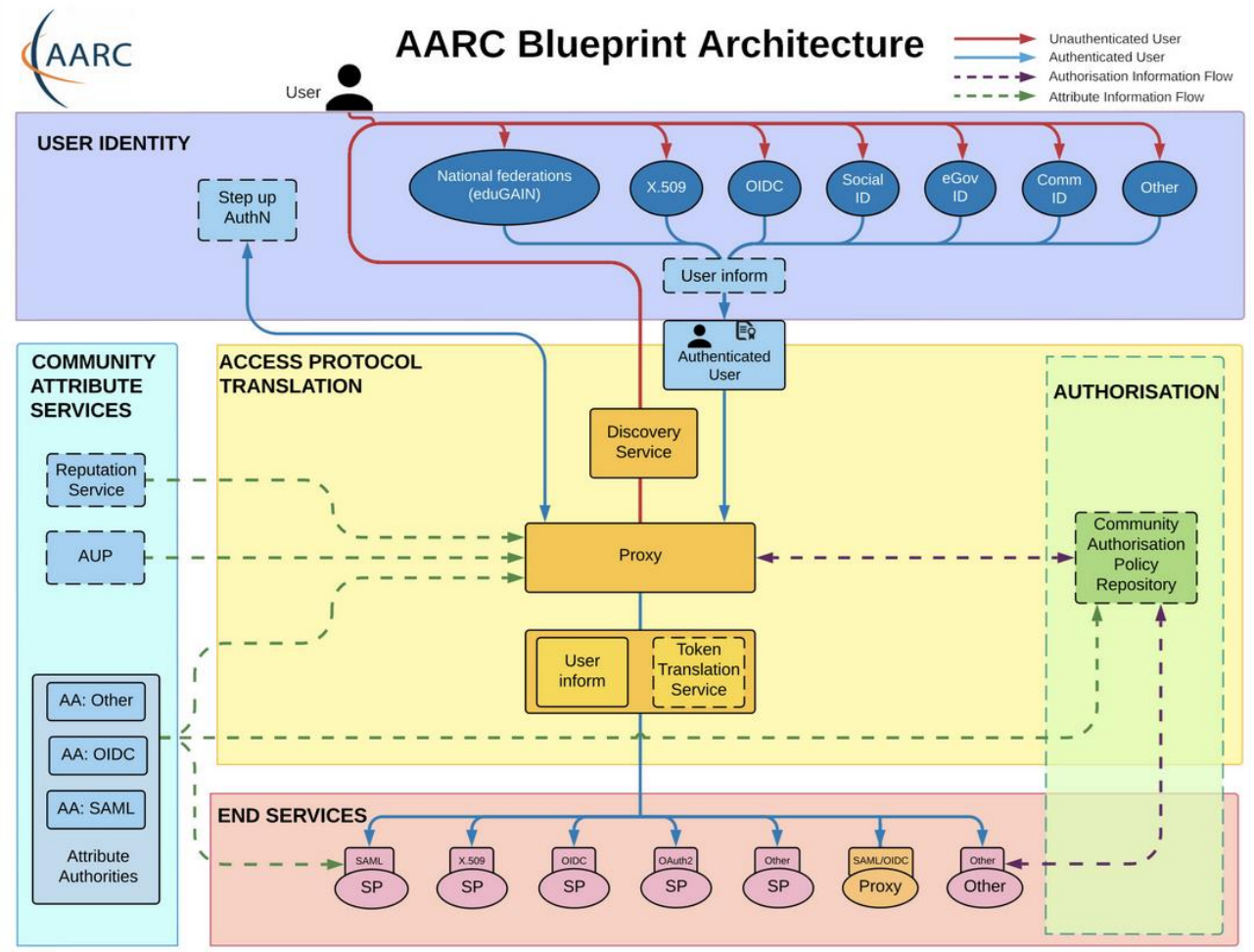
## Community AAI

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



Not sure how to begin with the AARC Blueprint Architecture? There are plenty of guidelines available but it can be a minefield at first. You probably want to start by designing the high level approach of your infrastructure based on the AARC Blueprint Architecture. There are several general topics you should consider, such as Data Protection (AARC-G042) and Federated Security Incident Response (AARC-I051). Here you can find common questions matched to the relevant Blueprint Architecture component, along with links to guidelines that can help.

**User Identity:**

- How should I integrate Social Media Identity Providers? AARC-G008
- How should users link accounts, and how does that affect Assurance? AARC-G009
- How should services indicate that they would like users to authenticate with multifactor authentication, and how should my proxy forward that information? AARC-G029

**Assurance:**

- How should assurance information of external identities be calculated? AARC-G031
- What can I say about assurance of identities from social media accounts? AARC-G041
- How is assurance impacted by account linking? AARC-G009
- How should assurance information be shared with other infrastructures? AARC-G021
- Which Assurance Profiles should I use, there are so many! AARC-I050

**Community Attribute Services:**

- How should attributes from multiple sources be aggregated? AARC-G003
- How should I express the home institute of a user? AARC-G025
- How should I express the identifier of a user? AARC-G026
- What are the best practices for running my Attribute Authorities securely? AARC-G071
- Which Acceptable Use Policy should I use to facilitate interoperability? AARC-I044
- How should I infer the affiliation of a user? AARC-G057

**Access Protocol Translation:**

- Which best practices should I follow for my Token Translation Services? AARC-G004
- How should I translate from Identity Federation information to X.509 certificates? AARC-G010

**Authorisation:**

- How should I manage authorisation information from multiple sources? AARC-G006
- How should group and role information be expressed to facilitate interoperability? AARC-G002
- How should resource capabilities be expressed? AARC-G027

**Proxies:**

- How can I ensure that my proxy is able to accurately claim that it supports best practices in Identity Federation? AARC-G015
- How should I express the home institute of a user? AARC-G025
- How should I express the identifier of a user? AARC-G026
- How should I express assurance information for users when interacting with another proxy? AARC-G021
- How can my proxy simplify the discovery process for end-users? AARC-G061
- How can my proxy route the user to the correct discovery service? AARC-G062

**End Services:**

- My service needs to act on behalf of the user – how should I handle credential delegation and impersonation? AARC-G005
- My services are not web based, how can I use identities from the proxy? AARC-G007
- How should Services hint which IDP they would like users to use? AARC-G049
- Which Security practices should I follow? AARC-G014

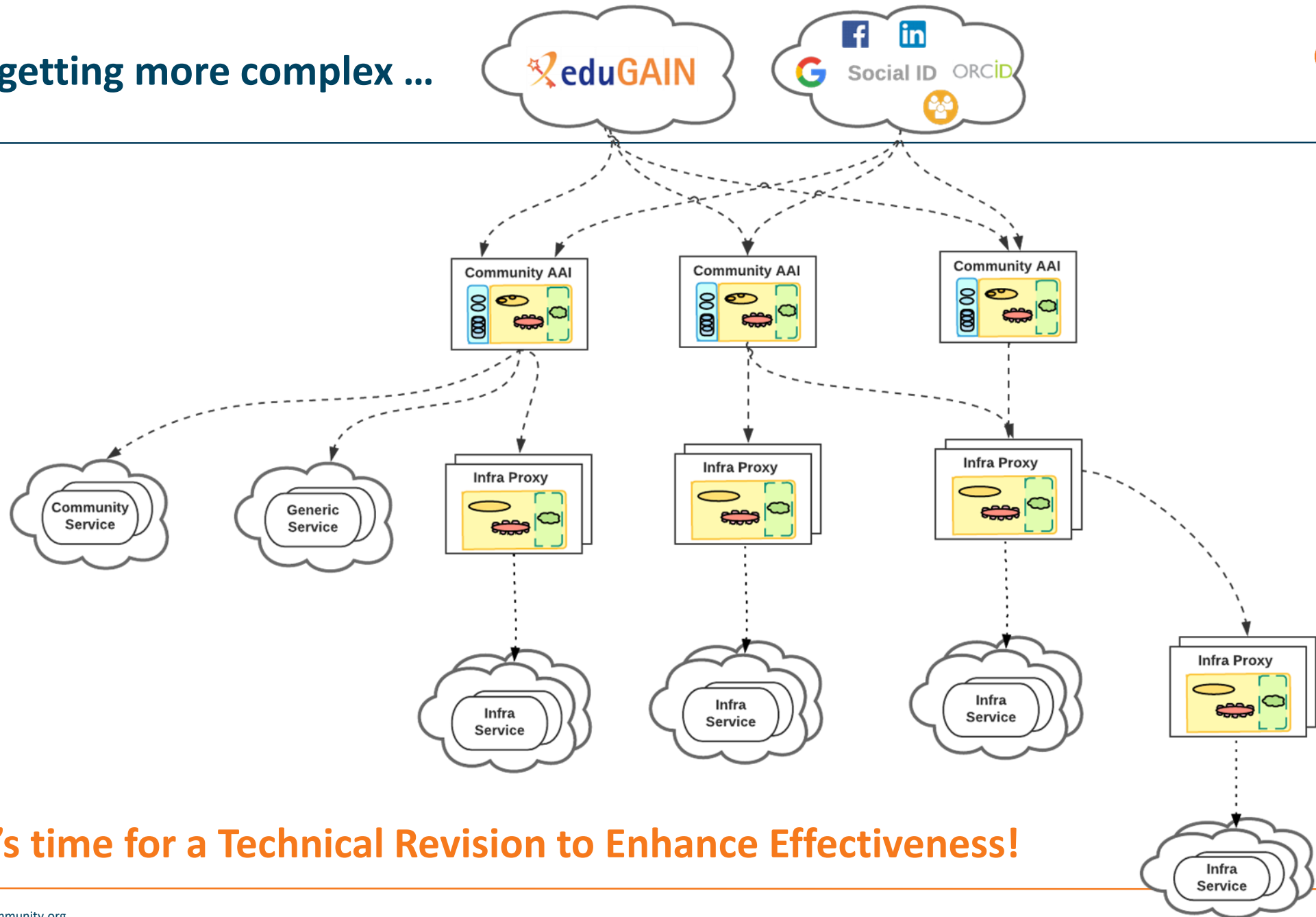
**What next? Are you looking for a kick start with your policies? Take a look at the Policy Development Toolkit which provides a set of templates.**

Personal Data	Protection Contact	Services (abide by)	processing personal data.	
Privacy Policy	Infrastructure Management (for general policy) & Services (for service specific policies)	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
		Services (abide by)	This policy defines requirements for running a service within the infrastructure.	Google Doc
		Users (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

**PDK**

Showing 1 to 9 of 9 entries

But it's getting more complex ...



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



## What will AARC TREE bring?

---

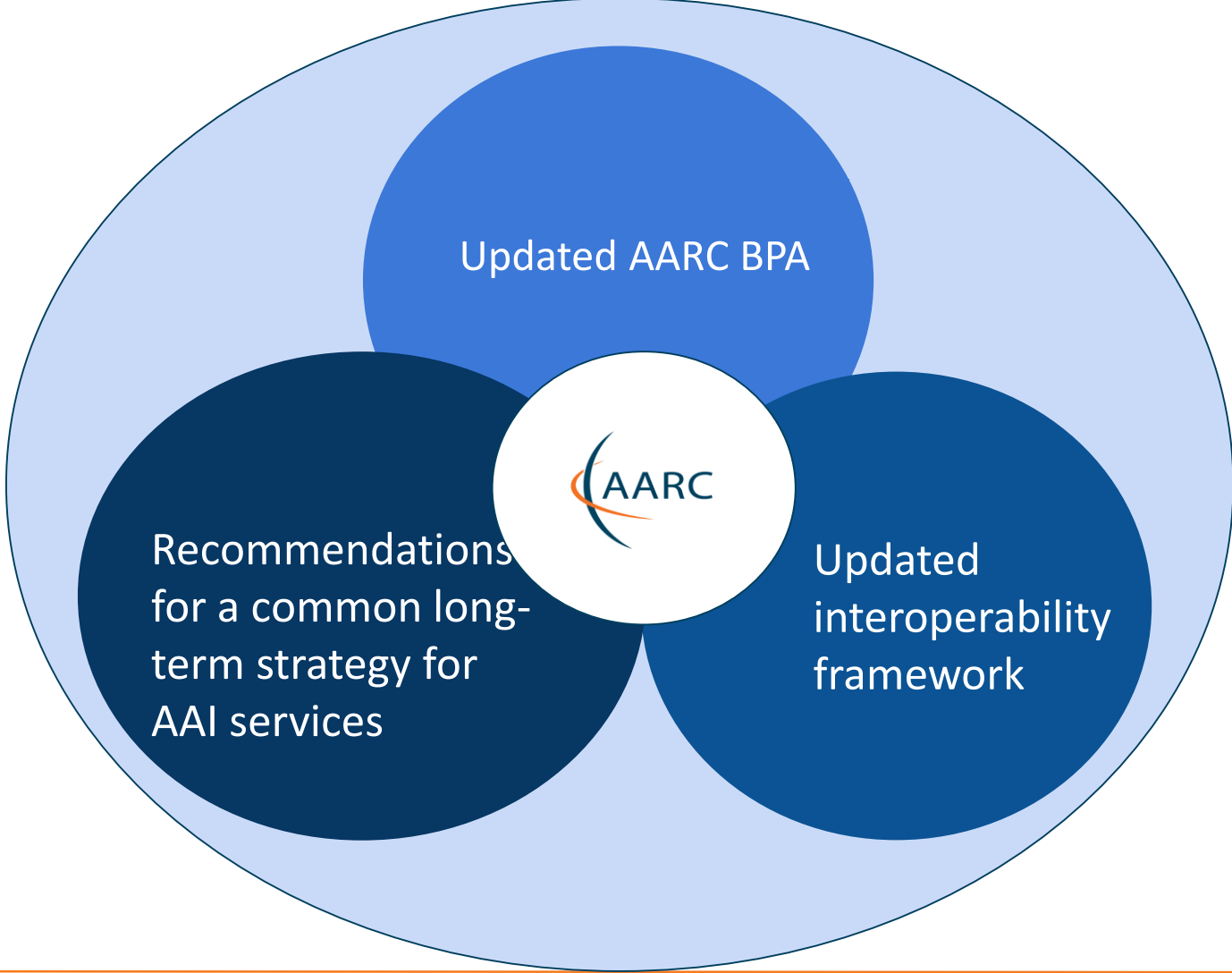
**Capture** and **analyse** new authentication and authorisation interoperability requirements (that support integration use-cases across the thematic area) and **provide** a landscape analysis of AAls services (including gaps) in the RIs represented in AARC TREE

**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@aacr-community.org](mailto:policy@aacr-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**

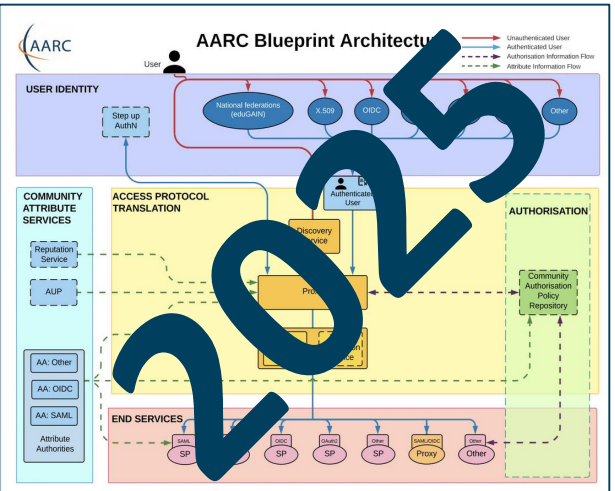
- improve scalability
- leverage emerging standards like **OpenID Federation**

**Authorisation guidelines**

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

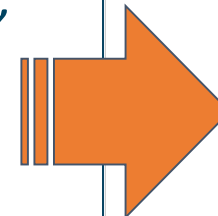
**Decentralised identities**

- 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

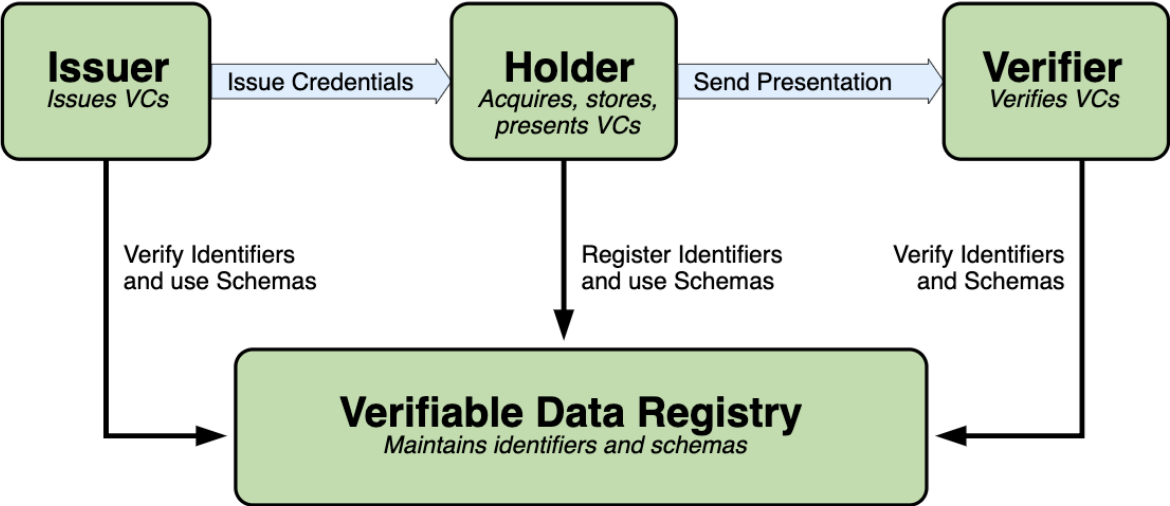
*This document defines a profile for expressing the attributes of a researcher's digital identity. The profile contains a common list of attributes and definitions based on existing standards and best practises in research & education. The attributes include identifiers, profile information, community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

<b>1 Introduction</b>	2
<b>2 Attribute profile specification</b>	2
2.1 Community Identifier	4
2.2 Display Name	5
2.3 Given Name	5
2.4 Family Name	6
2.5 Email Address	7
2.6 Affiliation within Home Organisation	8
2.7 Affiliation within Community/Research Infrastructure	10
2.8 Groups	11
2.9 Capabilities	11
2.10 Assurance	12
2.11 ORCID	13
2.12 Community username	14
2.13 Pairwise identifier	15
2.14 SSH Public key	16
2.17 Identity Type	19
2.18 Home Organisation's Country	19
2.19 Home organisation compliance with policies	20
2.20 User agreement to policies	21
2.21 Email verification status	22



# Decentralised identities

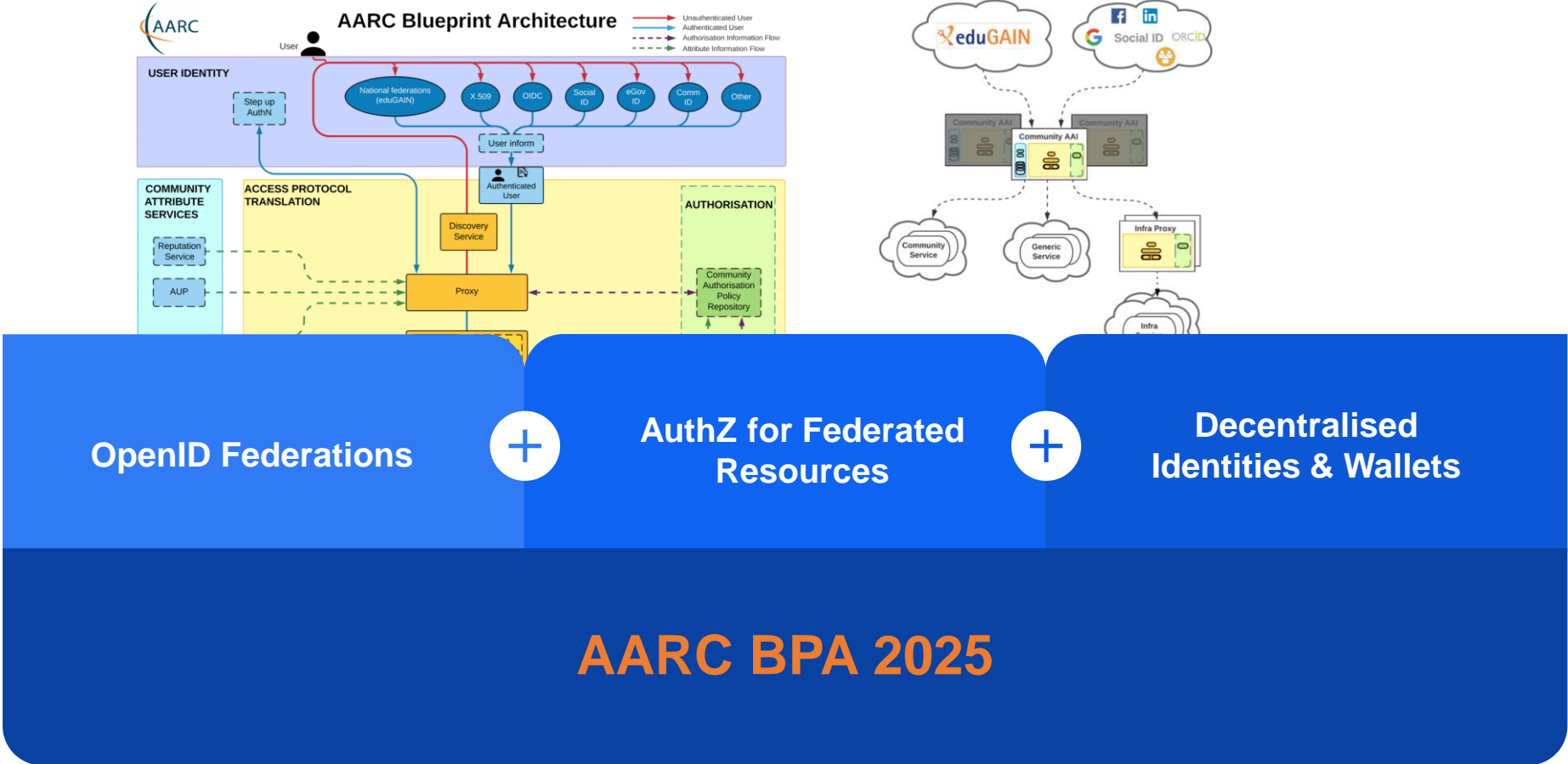
- Provide guidance on the use of decentralised identities and digital identity wallets
  - Explore Distributed Identifiers, Verifiable Credentials/Presentations & trust frameworks
- Support the EU Digital Identity Wallet (EDIW) initiative



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

# AARC Blueprint Architecture 'BPA2025'!

## AARC BPA 2019



# 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?	Audience
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abide)
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Management & Security Services (abide)
Membership Management Policy	Infrastructure Management	Research Communities (abide)
Acceptable Authentication Assurance	Infrastructure Management	Research Communities (abide)
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management & Security Services (abide)
Policy on the Processing of Personal Information	Infrastructure Management & Data Protection Contact	Research Communities (abide)
Privacy Policy	Infrastructure Management	Users (view)



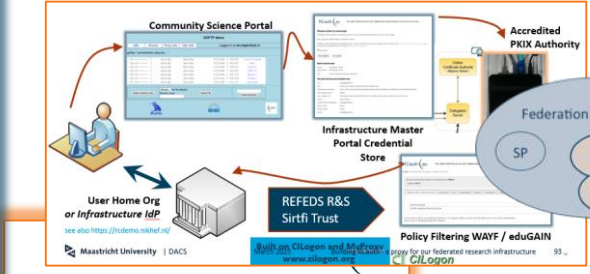
### Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)

Publication Date: 2019-03-01 (Final)  
 Authors: David Groep, Marcus Hardt, David Hüber, Christos Kanetopoulos, Mikael Lindén, Jan Nelson, Hannah Short, Uros Stevanovic  
 Internal Reference: AARC-init-LSAAI-policy-recommendations.docx  
 DOI: pending  
 Document Code: AARC-G040

© 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**  
 The AARC Pilot covering the Life Sciences AAI service, including both the proxy components and the registry service, developed in joint collaboration with EGI, EUDAT and GEANT, is a multi-staged pilot that will result in a production-equivalent service to be operated for the Life Sciences community by the pilot infrastructures. As the pilot enters its second phase, a practical policy related issue is that the LS AAI has to declare RAS and CoCo. In this document, NAI aims to provide preliminary guidance for the operators of the pilot. It must be understood that this guidance may and likely will change, in particular if and when the GEANT Data Protection Code of Conduct has been formally approved by the European Data Protection Board, and when relevant components of the Policy Development Kit and the Aligned Acceptable Use Policy for Infrastructures will be adopted.

(abide)	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



### Data Protection Impact Assessment - an initial guide for communities

Publication Date: 2018-04-30  
 Authors: Uros Stevanovic, David Groep, Jan Nelson, Stefan Pastow, Wolfgang Pemp  
 DOI: assignment deferred  
 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 data 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

**AARC-I050**  
 Comparison Guide to Identity Assurance Mappings for Infrastructures

**Self-assessment support sheet**  
 The assessment sheet supports the evaluation of the AARC-G071/ for the full description, requirements, and supporting documents.  
 • template: <https://edu.nl/88dwf>

**Assessments and review sheet**

- 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/spreadsheets/...>

**AAOPS**

## 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)

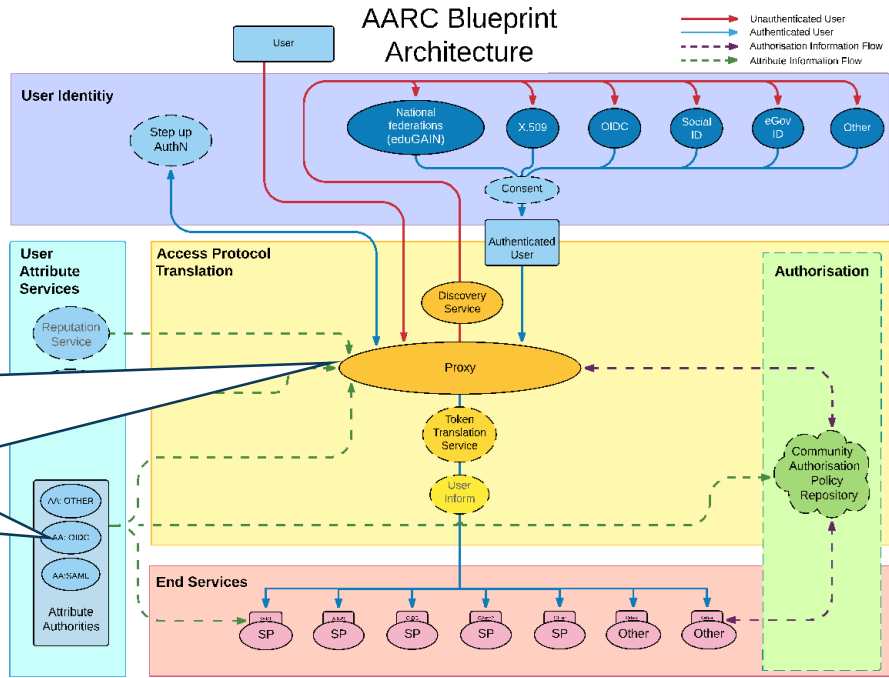
### User-centric trust alignment and policy harmonization: helping out the community (M6-M24, 26PM)

- 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).

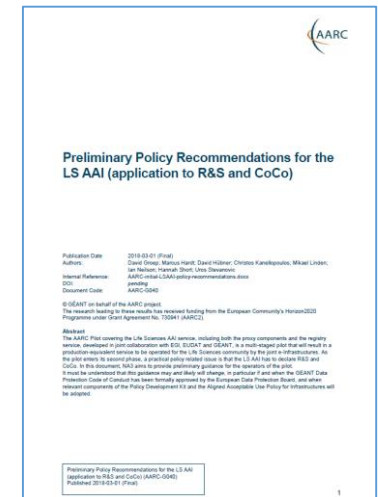
# Proxies have their own challenges as well: AUPs, T&Cs, Privacy notices, ...

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 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?



*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

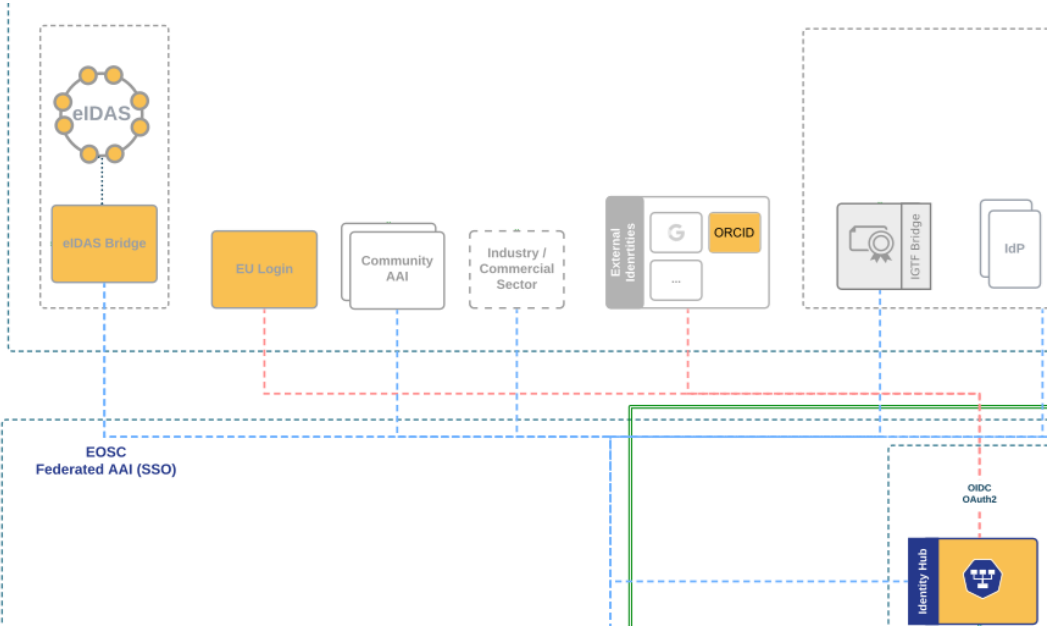
# We'll see more diverse sources of identity & assurance anyway

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 AIs 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
- Discuss 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

### Start with:

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

## Validator suite

- Including online validator service

- **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 '2<sup>nd</sup> 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>

© members of the AARC Community and the AARC TREE consortium.  
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).

