



Authentication and Authorisation for Research and Collaboration

## Of AARC TREEs and colourful pictures

Enhanced effectiveness for AARC in FIM for Research

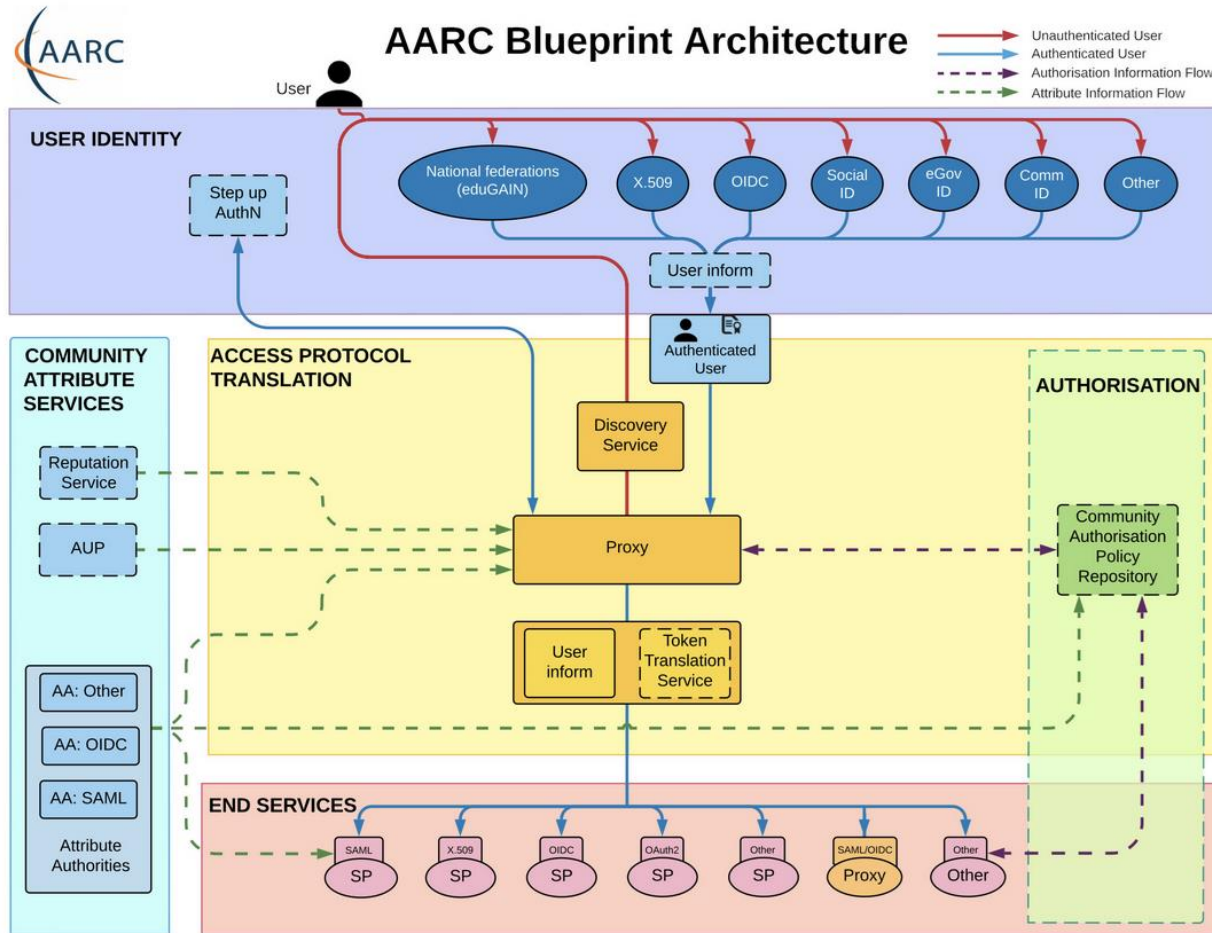
**David Groep**

Nikhef & Maastricht University  
*for the AARC TREE Collaboration*



FIM4R at Internet2 TechEx  
*December 2024*

# AARC Blueprint Architecture: many communities and collaboration, and full of fancy colourful pictures and stuff



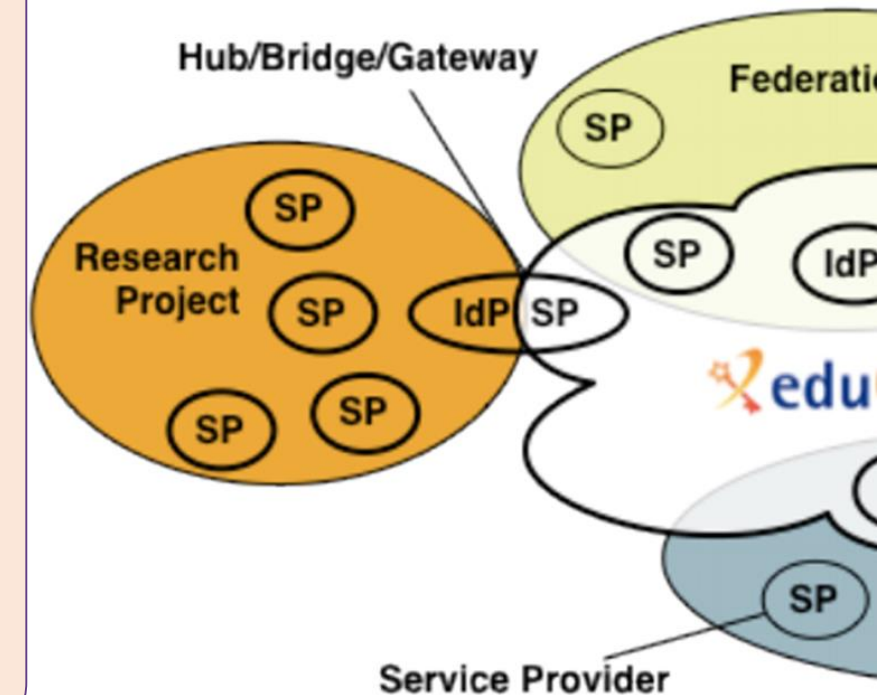
## What is the AARC BPA?

---

The **A**uthentication and **A**uthorization For **R**esearch and **C**ollaborations **BluePrint Architecture** provides a set of building blocks for software architects and technical decision makers who are designing and implementing access management solutions for international research collaborations. By design the AARC BPA is **technology agnostic** and provides an **architectural design** for those the deploy AAls.

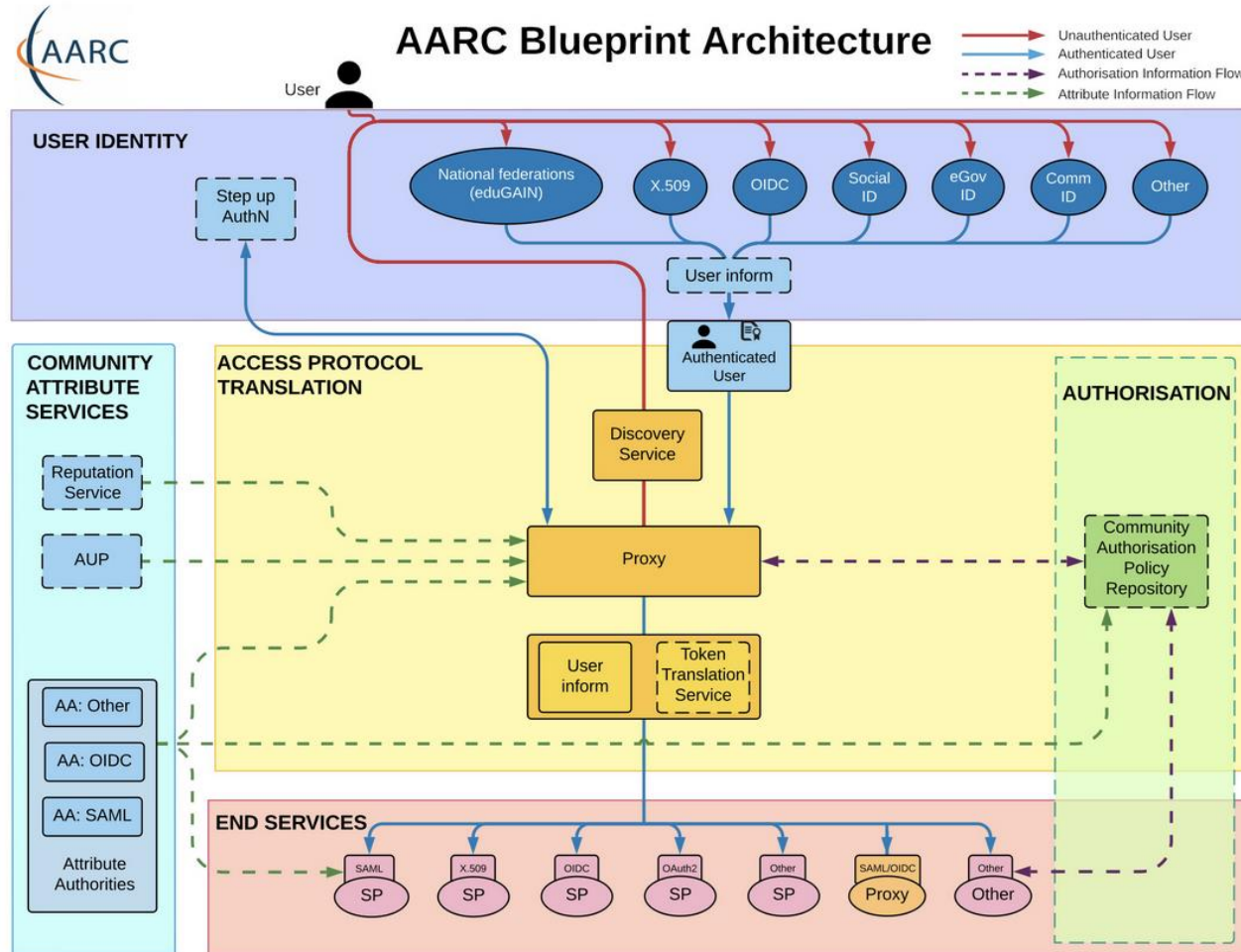
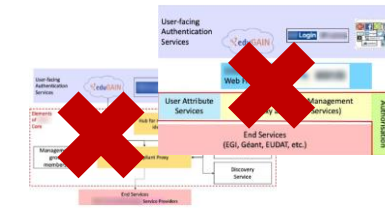
# The AARC BPA: the IdP-SP proxy to enable federated access for research

- Access services using **identities from users' Home Organizations**, but **hide complexity** of multiple IdPs, federations, AA technologies
- **One persistent identity** across all the community's services through **account linking**
- **Access** services **based on role(s)** users have in the collaboration.
- For both **web** and **non-web** resources
- Integration of **guest identity solutions**
- **Support for stronger authentication assurance** mechanisms



Graphics: Ann Harding and Lukas Hammerle (SWITCH) – from a long time ago now!

# 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

**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

**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

**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

**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

**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.
		Services (abide by)	This policy defines requirements for running a service within the infrastructure.
		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.

Showing 1 to 9 of 9 entries



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

Of AARC TREES and colourful pictures



# Example: 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

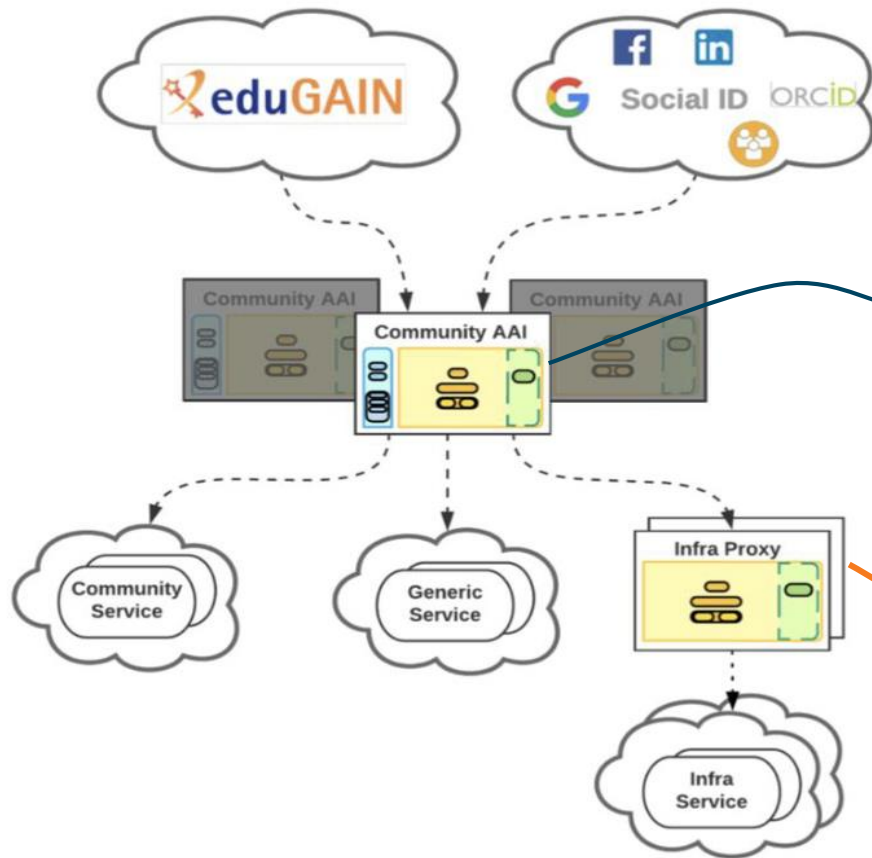
#### Abstract

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.

1 Introduction	2
2 Attribute profile specification	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



# The Community AAI and the Infrastructure Proxy – structuring elements



## 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

# AARC TREE: new EU funding to enhance the impact of AARC



AARC ▾

Architecture

Policy

Guidelines

AARC TREE



## AARC TREE Project

New funding for our community

[Read more](#)



## AARC TREE Project Main Facts

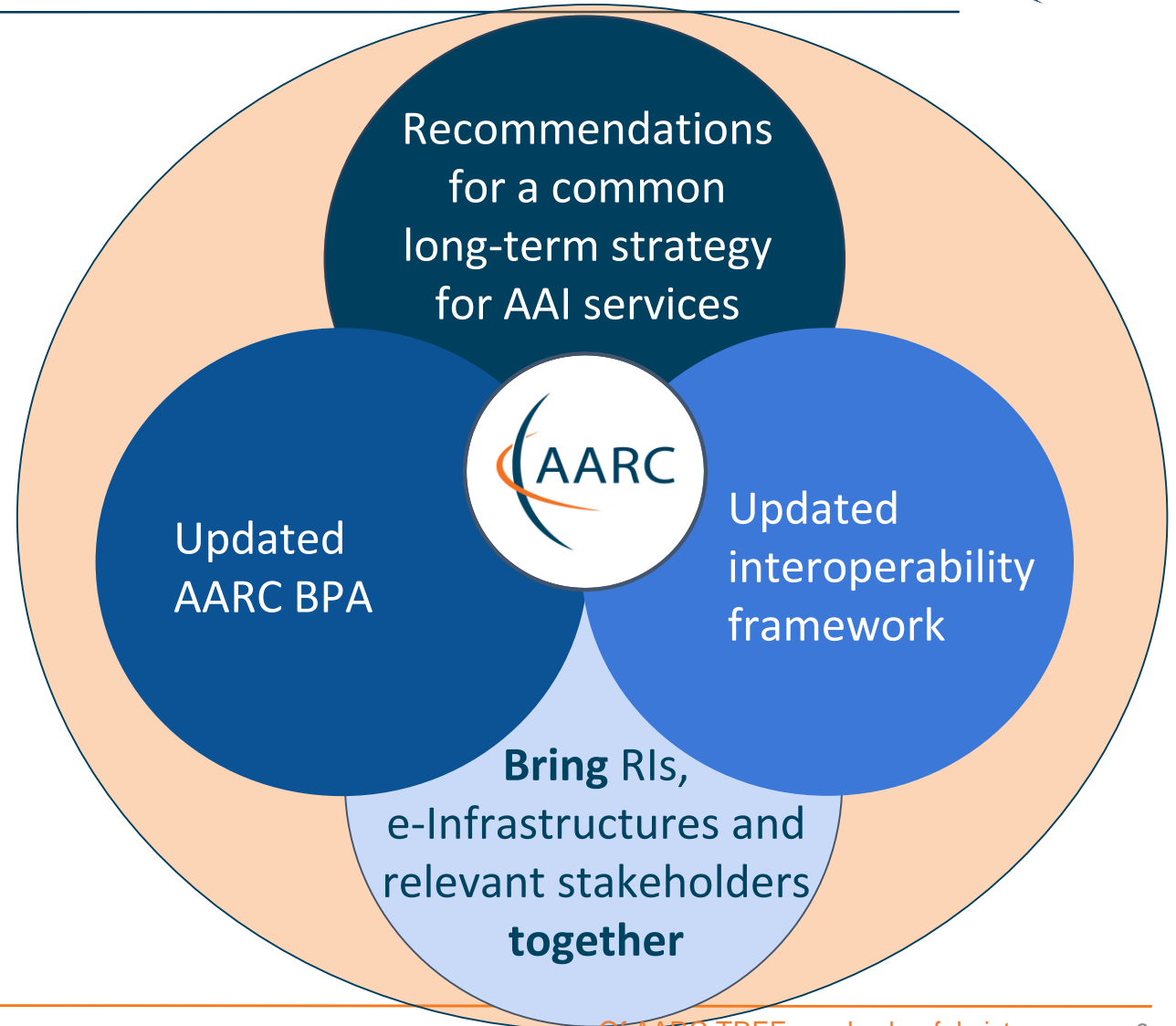
Start date: March 2024

Duration: 24 M

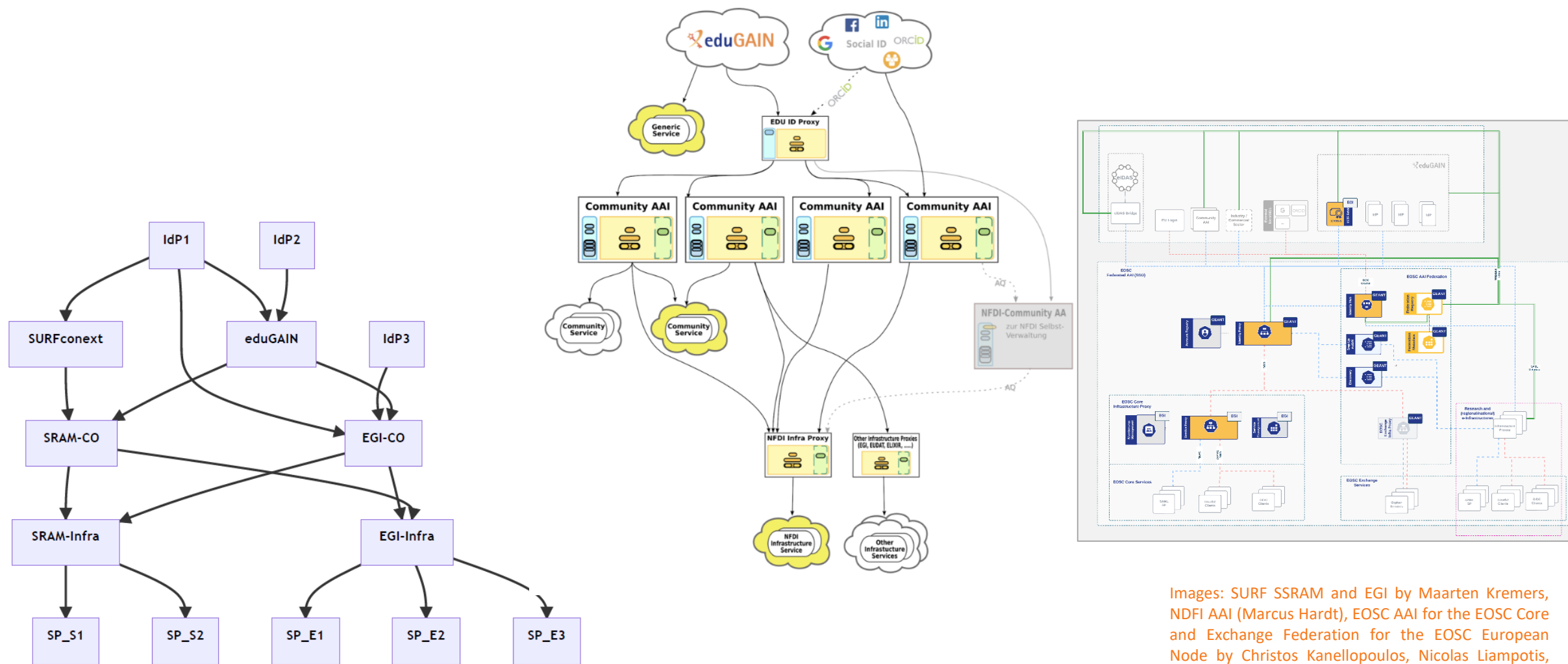
22 Partners

NDN (Licia 😊) is the coordinator

**We want to make AARC3  
a global activity to engage  
everyone interested  
in the evolution of AARC BPA**



# Our federated world is growing more complex



Images: SURF SSRAM and EGI by Maarten Kremers, NFDI AAI (Marcus Hardt), EOSC AAI for the EOSC Core and Exchange Federation for the EOSC European Node by Christos Kanellopoulos, Nicolas Liampotis, David Groep (June 2023 version)

## AARC TREE main goal is to increase the (global) impact

---

### **Landscape analysis of AARC BPA adoption**

- due in December 2024

### **Use-Case Collection and Analysis**

- due in February 2025

**Survey of the RIs and eInfras in AARC TREE and beyond - The survey focused only on the AARC Guidelines that are endorsed by AEGIS**

# AARC TREE main goal is to increase the (global) impact

## Landscape analysis of AARC BPA adoption

- due in December 2024

## Collection and Analysis

February 2025

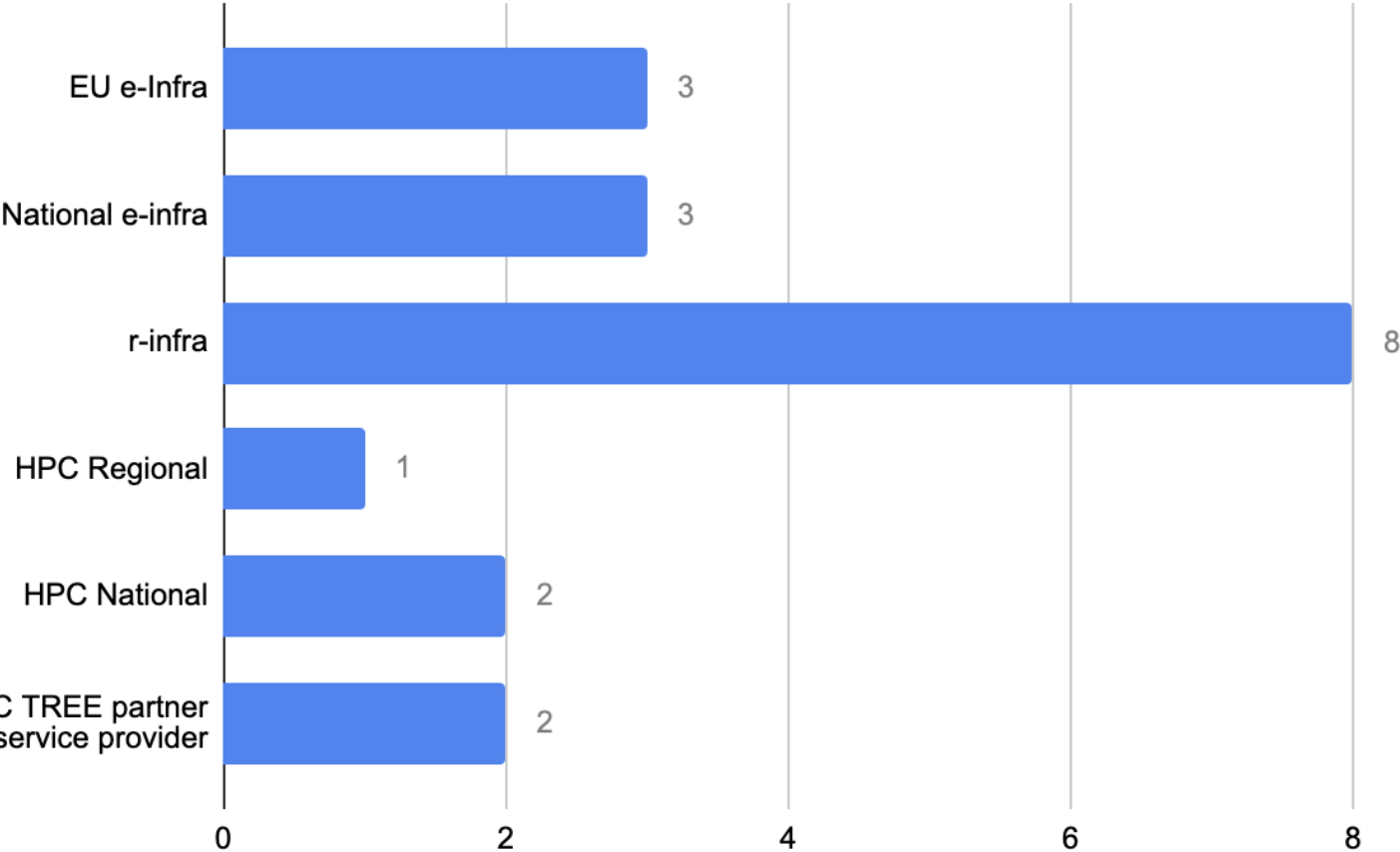
If you have not been  
contacted and you  
feel you should  
provide your inputs  
please get in touch!!!

## Survey of the RIs and eInfras in AARC TREE and beyond

[marina@sunet.se](mailto:marina@sunet.se) [mohacsi.janos@kifu.gov.hu](mailto:mohacsi.janos@kifu.gov.hu)

# Where are AARC guidelines used today ...

- ... and what can we learn from current implementations to ease it for new communities?



We think that this group should not be considered in the survey - we found institutional SP proxies to be too bespoke



## Survey findings

---

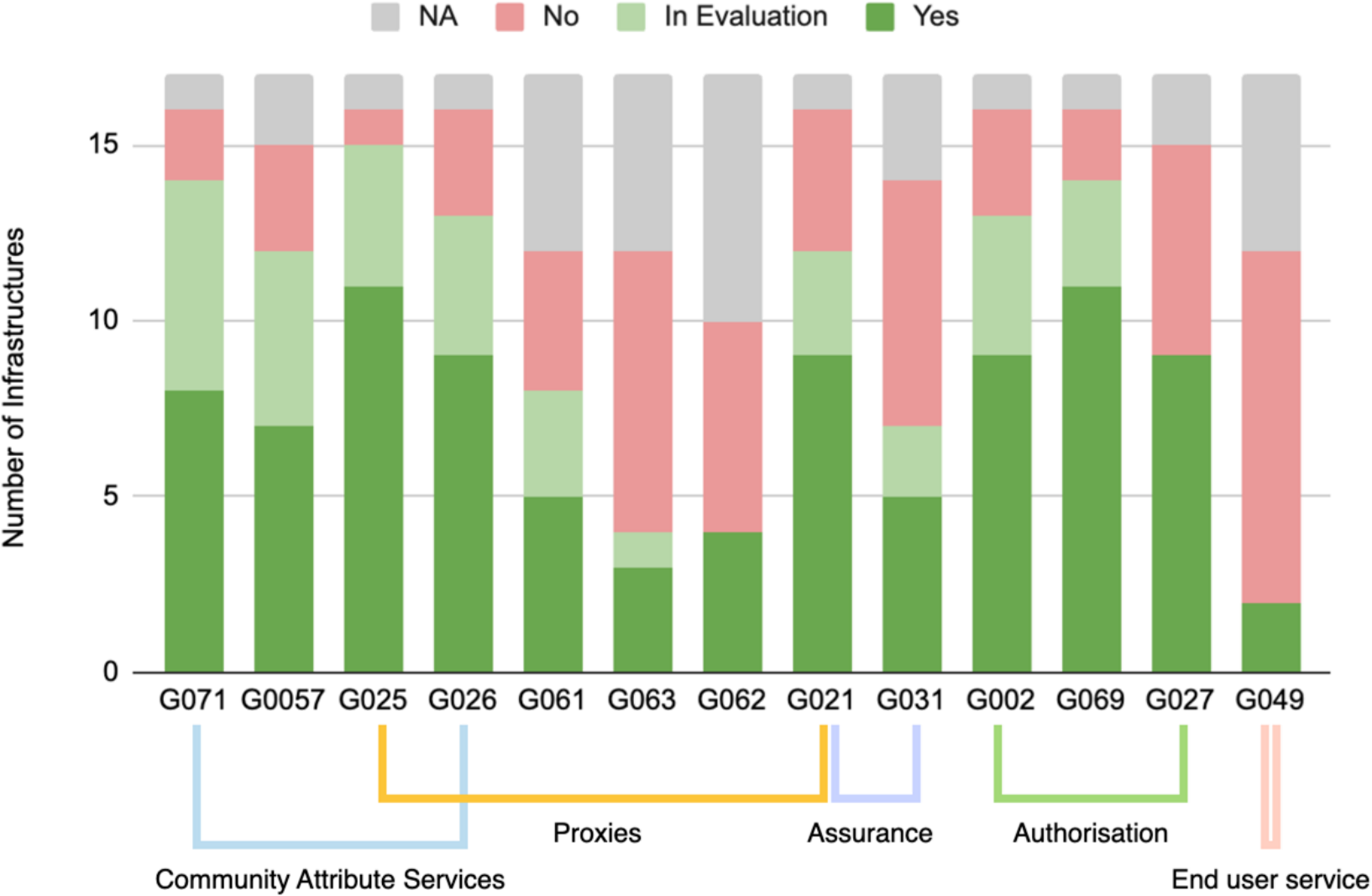
Most implemented guidelines are in the area of Community Attribute Services and Authorisation

G061 and G062 guidelines which are about implementation of the *discovery services* and *signaling about the end-user service* seem to be not prioritised or relevant

Guidelines that overlap with Community Attribute Services and Assurance are well adopted

Least adopted guideline is the one in the End user service area that is related to *IdP hinting* for discovery services

# Adoption of Guidelines among interviewed Research and e-Infrastructures



## So how to evolve the guidelines?

---

Use the experience of the RI and e-Infrastructures that have deployed most of the guidelines to support the adoption for others

People often do not know where to start from - Too many guidelines and not always clear how to deploy them. We need to **identify the must use guidelines**

Not all guidelines are fully tested in operational environments. Exploring if those that roll out the guidelines can provide some how-to ('validation')

# AARC BPA Guidelines – evolving interoperability with new guidance



## Architecture

- Protocols and profiles
- Attribute specs and transport
- Communications and interfaces

## Policy

- ISM interoperability
- Policy development kit
- Trust mechanisms and federation

## Validation and adoption

# A common suite of architecture and policy guidelines



[Home page](#) > [Guidelines](#)

## Guidelines

The **AARC Guidelines** complement the **AARC Blueprint Architecture** (BPA) and the **policy best practices** recommended by the AARC project.

The guidelines can apply to any topic that helps to advance Federated Identity Management for research and collaboration.

The AARC Guidelines help communities and infrastructures to implement and operate an AAI for research and collaboration more effectively and in an interoperable way.



[Architecture](#) [Policy](#) [Targeted](#) [Endorsed by AEGIS](#)

### **AARC-G083 Guidance for Notice Management by Proxies**

03/11/2024

### **AARC-G071 Guidelines for Secure Operation of Attribute Authorities**

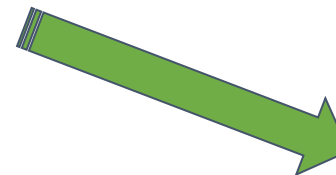
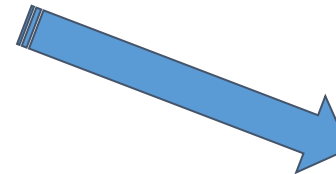
11/04/2022

### **AARC-I051 Guide to Federated Security Incident Response for Research Collaboration**



# Development: interoperable Attribute Profile beyond Personalised (G056)

- Purpose: **Defines how AARC-compliant AAI services express the attributes of a subject's digital identity.**
- Builds upon the [REFEDS Personalized Access entity category](#)
  - Attributes include: Organisation, user identifier, name, email address, affiliation, and assurance.
- Adds community-related attributes such as group memberships, roles, and resource capabilities.



<b>Abstract</b>	
<i>This document defines a profile for expressing the attributes of a subject's digital identity, as released by AARC-compliant AAI services. The profile contains a common list of attributes and definitions based on existing standards and best practices in research and education. These attributes include identifiers, profile information, community attributes such as group membership and role information, as well as information about the identity assurance.</i>	
<b>1 Introduction</b>	<b>3</b>
<b>2 Versioning</b>	<b>3</b>
2.1 Version Numbering Scheme	3
2.2 Backward Compatibility	3
2.3 Current Version	3
<b>3 Attribute profile specification</b>	<b>4</b>
3.1 Subject Identifiers	5
3.1.1 Public Subject Identifier	6
3.1.2 Pairwise Subject Identifier	7
3.2 Name	9
3.2.1 Display Name	9
3.2.2 Given Name	10
3.2.3 Family Name	12
3.3 Email	13
3.3.1 Email Address	13
3.4 Organisation	15
3.4.1 Organisation Display Name	15
3.4.2 Organisation Domain	16
3.5 Affiliation	18
3.5.1 Affiliation within Home Organisation	18
3.6 Assurance	21
3.7 Group and Role information	22
3.8 Resource Capabilities	24
3.9 AARC Profile Version	25
<b>4 References</b>	<b>27</b>
Annex A	29

# AARC-G056 enables workflows across infrastructures

- if you get the attributes, in the right place, *and* know what they mean



Distinguishes between the following profiles

- **Core** - Considered essential for basic functionality.
- **Extended** - Its inclusion provides additional information about the subject but is not mandatory.

but also discussed their rendering in SAML, OIDC, SCIM, and whether it should be voPerson-based, or add/replace with sub claims and subject-id

- discussions you can help shape!

Attribute Category	Attribute Name	Profile (Core or Extended)
Subject Identifier	Public Subject Identifier	Core
	Pairwise Subject Identifier	Core
Name	Display Name	Core
	Given Name	Core
	Family Name	Core
Email	Email Address	Core
Organisation	Organisation Display Name	Core
	Organisation Domain	Core
	Organisation's Country	Extended
	Organisation Compliance with Policies	Extended
Affiliation	Affiliation within Home Organisation	Core
	Affiliation within Community/Research Infrastructure	Extended
Assurance	Assurance	Core
Group and Role information	Group and Role information	Core
Resource Capabilities	Resource Capabilities	Core
External Subject Identifiers	External Subject Identifiers	Extended
	ORCID	Extended
SSH Public keys	SSH Public keys	Extended
Certificates	Certificate Subject DNs	Extended
	Certificate Issuer DNs	Extended
Subject Type	Subject Type	Extended
Subject Status	Subject Status	Extended
Agreement to Policies	Agreement to Policies	Extended
Authenticating Authorities	Authenticating Authorities	Extended

<https://github.com/aarc-community/architecture-guidelines/issues/15>

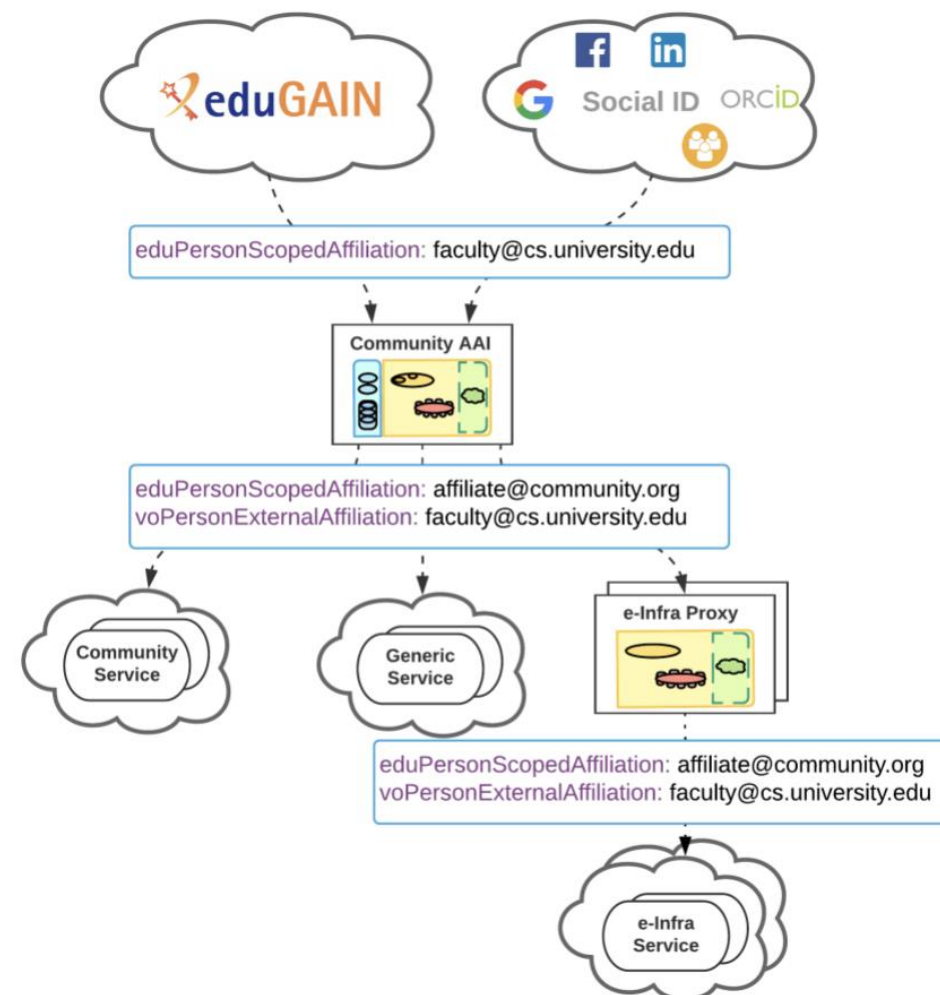
# Authorisation and affiliation in community use cases

## Problem

- How to communicate affiliation of a user with the community

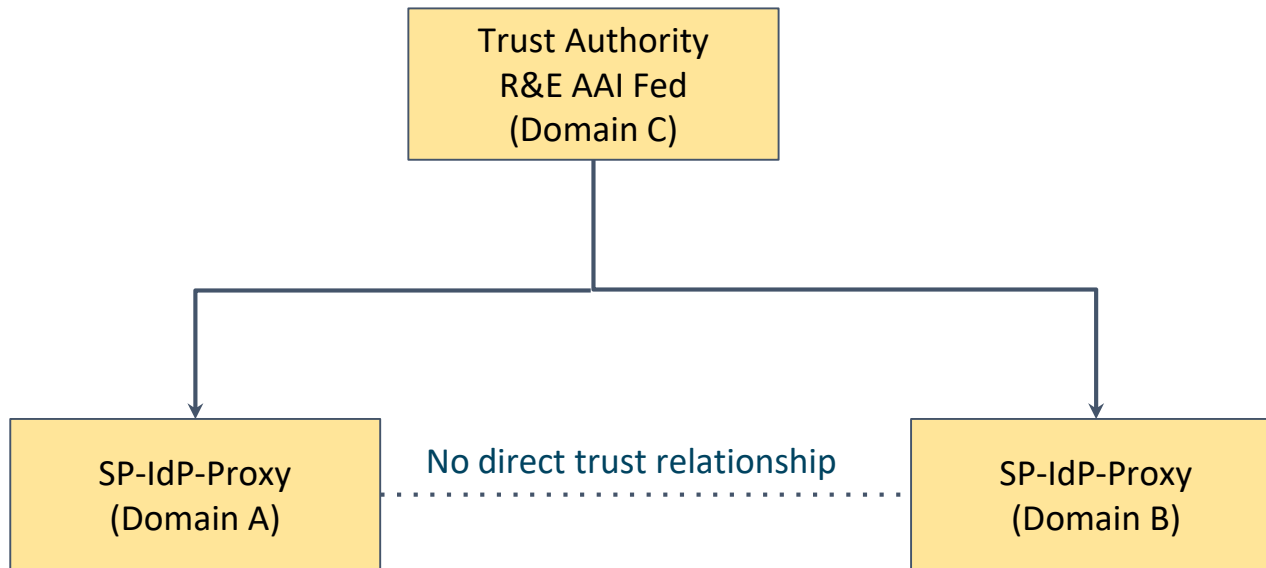
## Guidelines

- [AARC-G025 - Guidelines for expressing affiliation information](#)
- [AARC-G057 - Inferring and constructing voPersonExternalAffiliation](#)



# AARC-I058 Methods for Establishing Trust between OAuth 2.0 Proxies

- *Informational guideline rather than a normative one: encourage alignment!*
- How to establish trust across proxies in different domains? OpenID Federation or ...



<https://docs.google.com/document/d/18bvC63O3wti8nw5lhgUbBVMtDG9ggqpe5ad8Om9voBo/edit>

# Comparing federation approaches in AARC-I058

Metric \ Approach	1 Shared list of entity IDs	2 Shared list of entity statements	3 Shared list of entity statements via extended listing	4 Targeted entity statement resolution	5 Shared list of entity IDs with OID-Fed metadata	6 OID-Fed entity discovery
Metadata format	OIDC / OAuth2, no federation metadata (e.g. security contact info)	OID-Fed	OID-Fed	OID-Fed	OID-Fed	OID-Fed
Publish/update metadata	non-standard	non-standard	non-standard	non-standard	OID-Fed well-known endpoint	OID-Fed well-known endpoint
Retrieve metadata	OIDC Discovery	Custom resolve endpoint for aggregated response	OID-Fed extended_list	OID-Fed resolve endpoint	OID-Fed well-known endpoint	OID-Fed (resolve trust chain & metadata)
Support for federation policies	Distributing Trust Mark specific lists	Trust Marks	Trust Marks	Trust Marks	Trust Mark specific lists / Trust Marks signed by list providers	Full flexibility: Trust Marks, metadata policies

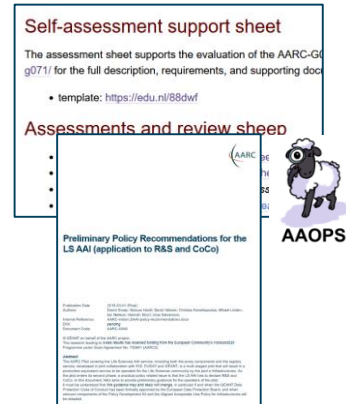


# Policy and good practice underpinning the AARC Blueprint BPA



## Infrastructure alignment and policy harmonisation: helping out the proxy

- **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

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



# How to establish secure operation for your (AARC BPA) proxy?

## The Challenge

- How to securely operate proxies, attribute authorities and issuers of statements for entities?

## Guideline

- [AARC-G071 Guidelines for Secure Operation of Attribute Authorities](#)

## Summary

- Operational security processes and procedures
- Requirements on traceability, auditability, and logging
- Requirements on the secure operation
- Requirements on securing the interactions



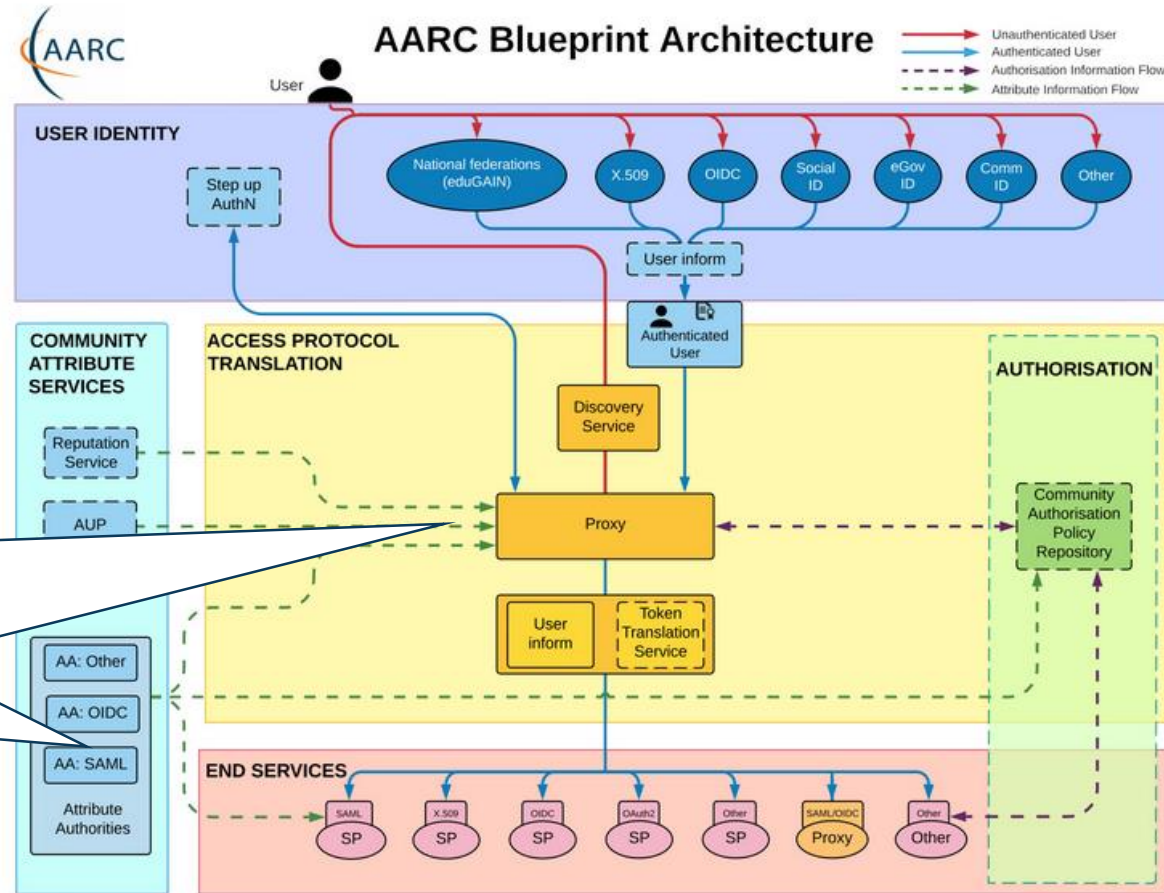
### Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities

Publication Date	2022-04-11
Authors:	Members of the IGTF and the AARC Community; David Groep; Ian Collier, Tom Dack; Jens Jensen; David Kelsey; Maarten Kremers; Ian Neilson; Stefan Paetow; Hannah Short; Mischa Sallé; Uros Stevanovic
With feedback from	Marina Adomeit; Sander Apweiler; Jim Basney; Christos Kanellopoulos; Johannes Reetz
AARC Document Code:	<b>AARC-G071</b>
Supported by:	<i>This guideline is a joint work of the International Global Trust Federation IGTF, the AARC community, and global partners. The research leading to these results has received funding from the European Community's Horizon2020 Programme by way of the AARC2 project (Grant Agreement No. 730941), EOSC-hub (Grant Agreement 777536), as part of the GÉANT 2020 Framework Partnership Agreement (FPA) under Grant Agreement No. 856726 (GN4-3), as well as from other sources</i>
Publishing Organisations:	IGTF and AARC Community
DOI:	<a href="https://doi.org/10.5281/zenodo.5927799">https://doi.org/10.5281/zenodo.5927799</a>

# Operational security focus in the BPA: beyond just the IdPs

## Community membership management directories and attribute authorities

- integrity of membership
- identification, naming and traceability
- site and service security
- protection on the network
- assertion integrity



Guidelines for Secure Operation of Attribute Authorities  
and other issuers of access-granting statements  
(AARC-I048, in collaboration with IGTF AAOPS)

# Deployment guidance included ...

## 4.2. Attribute Management and Attribute Release

### AMR-1

The Community must define and document the semantics, lifecycle, data protection, and release policy of attributes stored or asserted by the AA.

The community should follow the guidance from relevant policy documents. In particular, the Policy Development Kit has recommendations on Community Membership Management. It is recommended to use standardised attributes where possible, e.g. from eduPerson [EPSC] or SCHAC [SCHAC], and their semantics must be respected.

If Communities make modifications to the attribute set, their semantics, or release policies, it is recommended that they inform both their relying parties as well as the AA Operator thereof, since the AA operator may have implemented checks for schema consistency. The Community is ultimately responsible for the values and semantics of the attributes.

### AMR-2

The AA Operator must implement the community definitions as defined and documented, for all the AAs it operates.

By implementing these requirements, the AA operator will support the chain of trust between Community and the RPs. An AA Operator must only host those communities for which it can implement the requirements.

### AMR-3

It is recommended that the AA Operator provide a capability for the community to

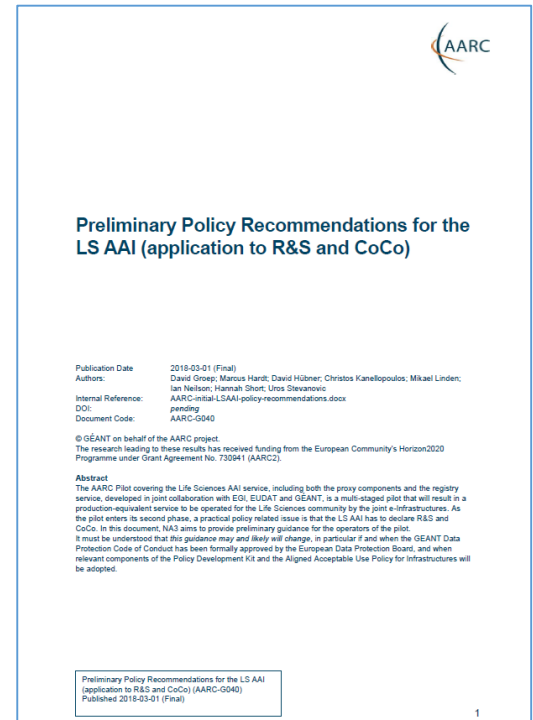
# Proxies have more challenges as well: AUPs, T&Cs, Privacy notices, ...

## For large 'multi-tenant' proxies

- some subset users in some communities use a set of services – how to present their Terms and Conditions and their privacy policies, so that 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

## For community and dedicated proxies

- when new (sensitive) services join, who needs to see the new T&Cs?
- can we communicate existing acceptance of T&Cs to downstream services?



*beyond AARC-G040*

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

**‘with fewer clicks to more resources’**



# AARC G082 Notice Management by Proxies

## Four presentation models. In order of preference



1. machine-readable aggregated notice
2. common notice (single common authority domain)
3. cascading notices (assume responsibility for underlings)
4. coherent presentation (you show what you need, but not more)

## Generic recommendations

- use the WISE Baseline AUP composition model, record what and when user confirmed acceptance, and be able to confirm this downstream

**plus a machine-actionable model to construct notices based on a hierarchy of proxies**

- sufficient to build you a comprehensive WISE Baseline AUP
- and a set of privacy notices (for those GDPR encumbered)
- plus a namespace inspired by RFC6711's LoA registry

	
<b>Guidance for Notice Management by Proxies</b>	
AARC-G083 Guidance for Notice Management by Proxies	
	
<b>Table of Contents</b>	
1. Introduction	3
2. Objectives and Considerations	4
Constructing notices and assigning responsibilities	4
Stakeholders and their role	4
General Data Protection considerations	5
Notice management and protection of personal data	6
Personal data and their presentation position in notices	8
Access personal data and regulatory compliance	9
Offline access and non-interactive (brokered) workflows	10
Validation and compliance testing	10
3. Presentation models	11
Machine-readable aggregated notices	11
Common notice	11
Cascading policy	12
Coherent presentation	12
4. Recommendations	13
Generic recommendations	13
Requirements for each specific scenario	15
Subsidiary considerations	16
5. Notice meta-data and registry	18
5.1 Policy identifiers for community purpose binding	19
5.2 Relation to voPersonPolicyAgreement	20
5.3 One-statement notices and policies	20
5.4 Meta-data document resolution	20
References	21
Glossary	21
Appendix A Pre-registered identifiers	22
Appendix B Example meta-data document	23
Example of a self-contained acceptable use policy	23
Example of a community purpose binding statement for a community	24

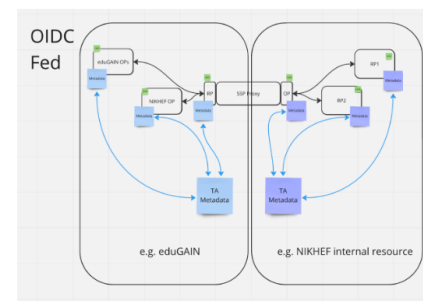
# Automatically constructing notices? Will that work? We can at least try!

```
{
  "id": "urn:doi:10.60953/68611c23-ccc7-4199-96fe-74a {
  "id": "https://operations-portal.egi.eu/vo/view/voname/xenon.biggrid.nl",
  "aut": "https://www.nikhef.nl/",
  "aut_name": "Nikhef",
  "aut": "https://xenonexperiment.org/",
  "valid_from": 1649023200,
  "aut_name": "Xenon-nT collaboration",
  "ttl": 604800,
  "valid_from": 1311890400,
  "contacts": [
    "ttl": 31557600,
    "contacts": [
      "helldesk@nikhef.nl",
      "grid.support@nikhef.nl",
      "information-security@nikhef.nl"
    ],
    "security_contacts": [
      "abuse@nikhef.nl"
    ],
    "privacy_contacts": [
      "vo-xenon-admins@biggrid.nl"
    ],
    "policy_class": "acceptable-use",
    "policy_uri": "https://www.nikhef.nl/aup/",
    "notice_refresh_period": 34214400,
    "includes_policy_uris": [
      "https://documents.egi.eu/document/2623"
    ],
    "description#nl_NL": "Deze Gebruiksvoorwaarden betreffen het gebruik van het netwerk en computers bij Nikhef. Iedere gebruiker van deze services wordt geacht op hoogte te zijn van deze voorwaarden en is verantwoordelijk voor het begrijpen van deze voorwaarden en het ervoor zorgen dat deze worden gevolgd."
  ],
  "policy_uri": "https://www.nikhef.nl/aup/",
  "description": "This Acceptable Use Policy governs the use of the networking and computer services; all users of these services are expected to understand and comply to these rules."
}
  "policy_class": "purpose",
  "augments_policy_uris": [
    "https://wise-community.org/wise-baseline-aup/v1/"
  ],
  "policy_uri": "https://operations-portal.egi.eu/vo/view/voname/xenon.biggrid.nl",
  "description": "detector construction and experiment analysis for the search of dark matter using Xenon detectors"
}
```

# Next: helping out the community: policy toolkit for communities & trust

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

this leaves communities *and SP operators* unclear about trust assurance level of members



David Groep:  
Raise of hands  
Who knows about

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

What was the problem that triggered this session?

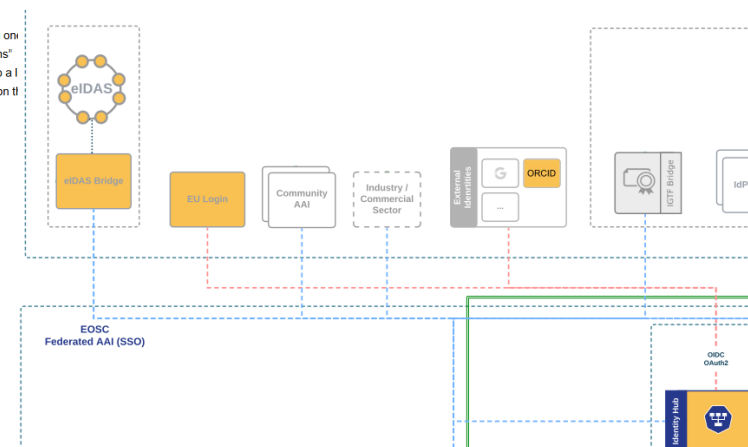
Proxies are wonderful, they can be opaque and expose things to the outside world.

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 on another (+ augment of claims), but also bridging trust between both “domains”

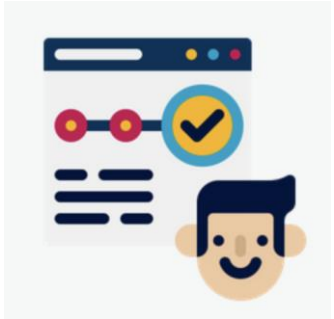
In OIDC federation, you can chain metadata statements not by publishing to a I hierarchies, trust anchors who can sign intermediates . multiple signatures on ti



And what about assurance: we’ll have more, and maybe more reliable, sources of assurance in the near term?

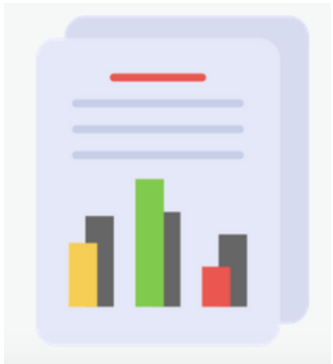
# Right now in AARC TREE:

## *Time to engage ?*



### Use Cases Collection and Analysis

with the large ESFRI RIs, clusters, FIM4R communities, and EOSC national nodes to validate BPA effectiveness and act as a flywheel to increase its application

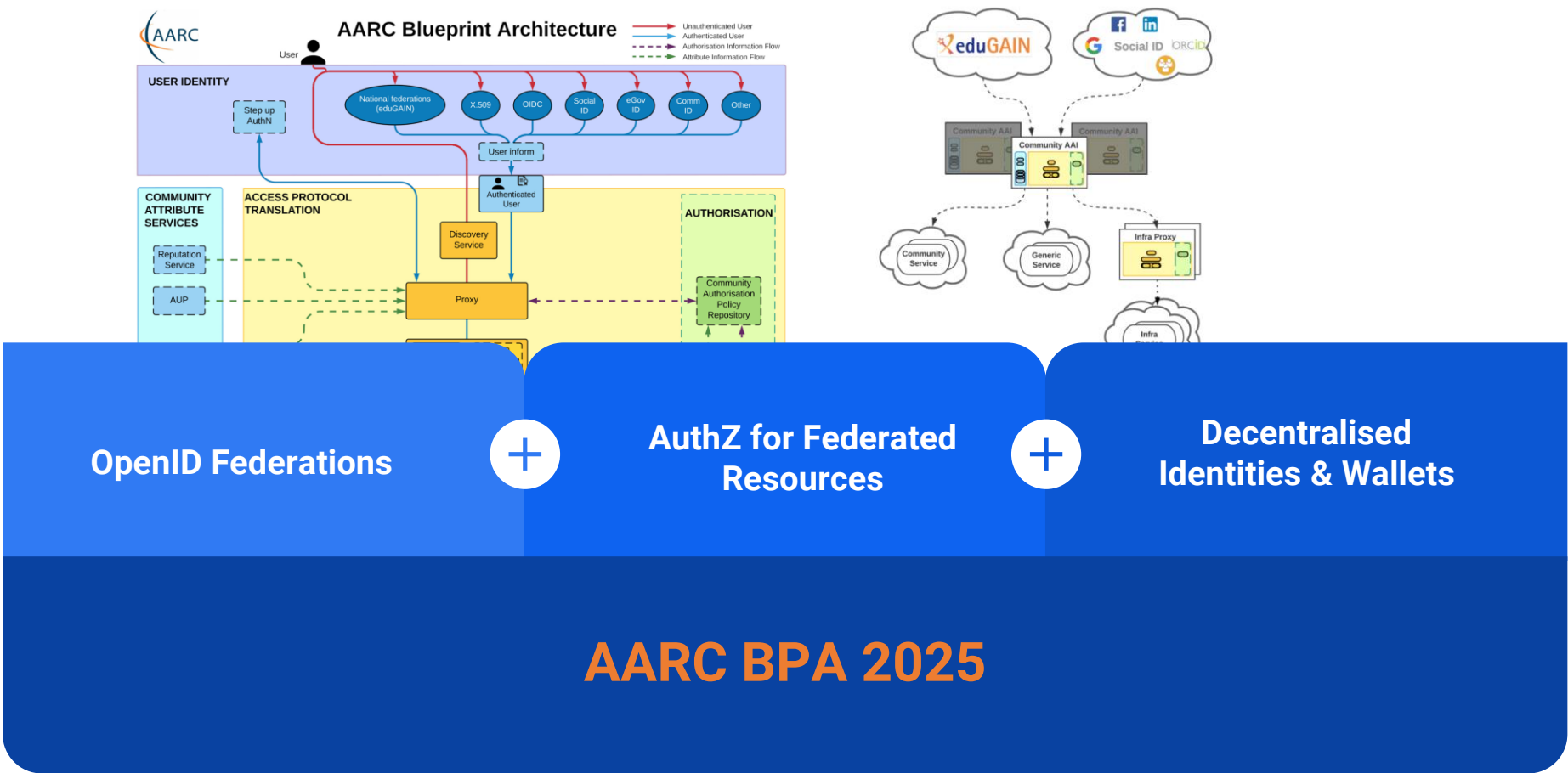


### Compendium & Recommendations

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

# AARC Blueprint Architecture 'BPA2025'

## AARC BPA 2019



## AARC BPA 2025



## 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
- 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@aacrc-community.org](mailto:policy@aacrc-community.org)  
<https://lists.geant.org/sympa/info/aarc-na3>

Thanks to the AARC Community, including folk from whom we 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, Catharina Vaendel, Arnout Terpstra, and Maarten Kremers.

# Thank you

## Any Questions?



<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).

