AARC

Authentication and Authorisation for Research and Collaboration

Of AARC TREEs and colourful pictures
Enhanced effectiveness for AARC in FIM for Research
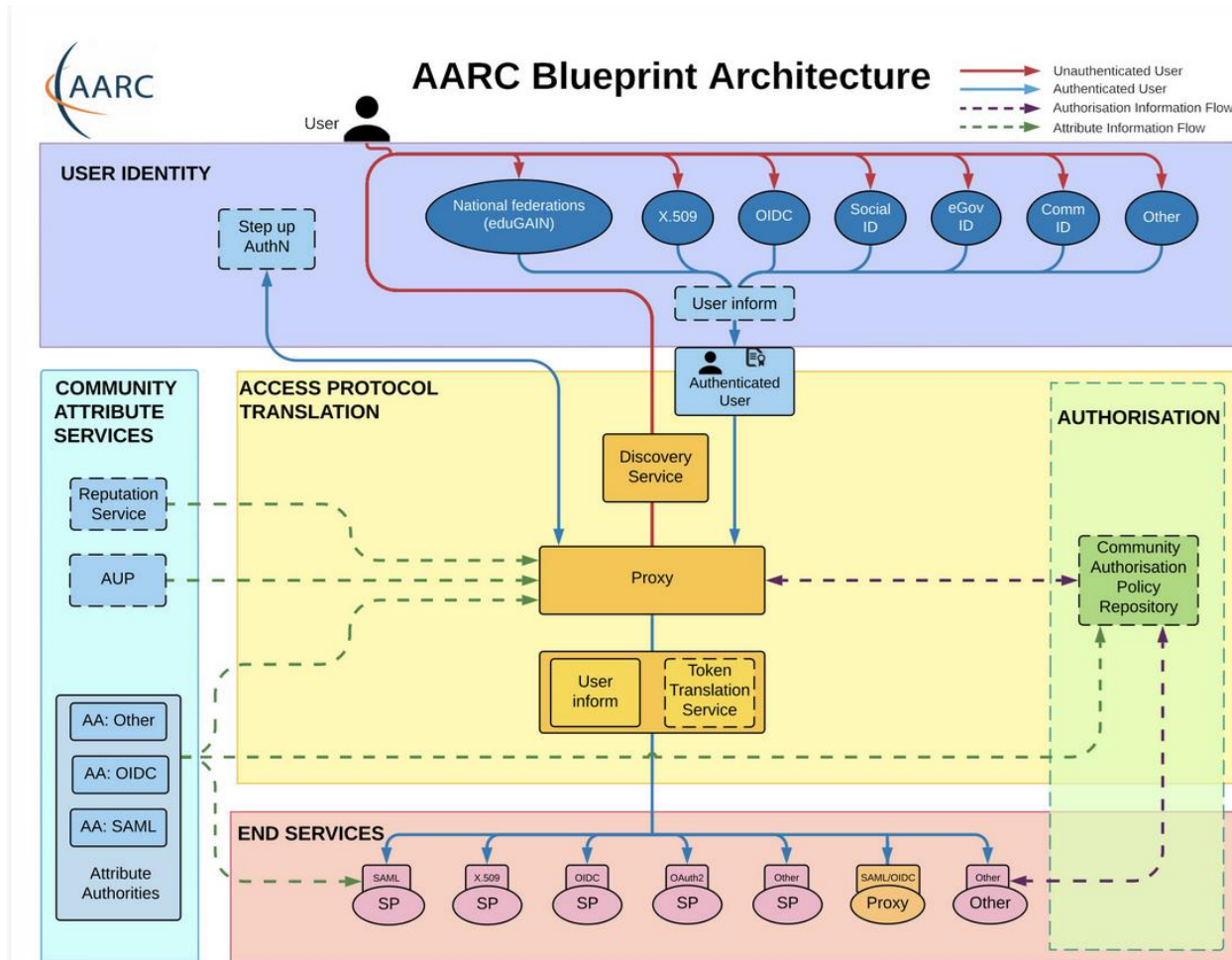
David Groep
Nikhef & Maastricht University
for the AARC TREE Collaboration

Nikhef   Maastricht University

FIM4R at Internet2 TechEx
December 2024

AARC Blueprint Architecture: many communities and collaboration, and full of fancy colourful pictures and stuff
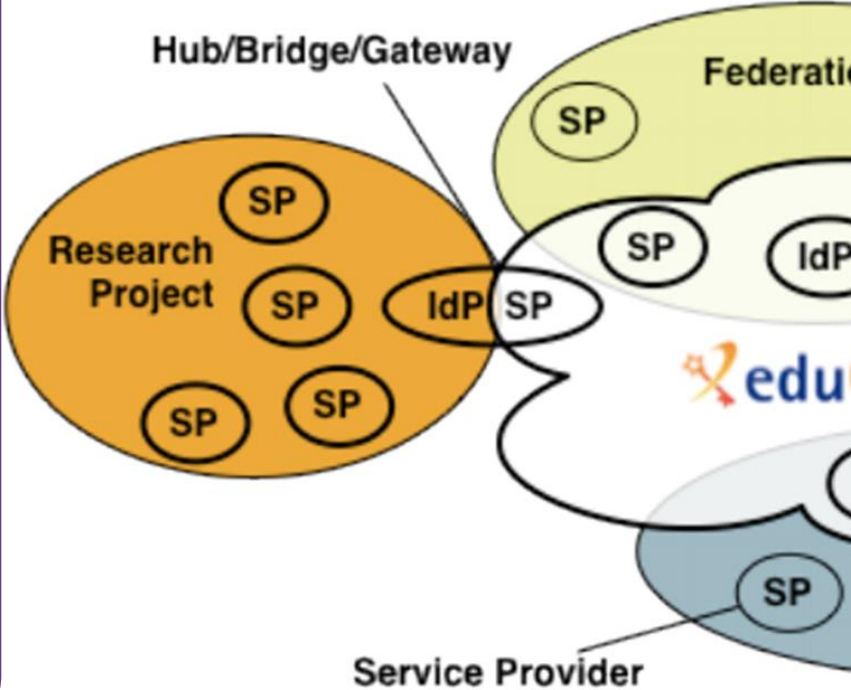
What is the AARC BPA?

The Authentication and Authorization For Research and Collaborations **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 AAIs.
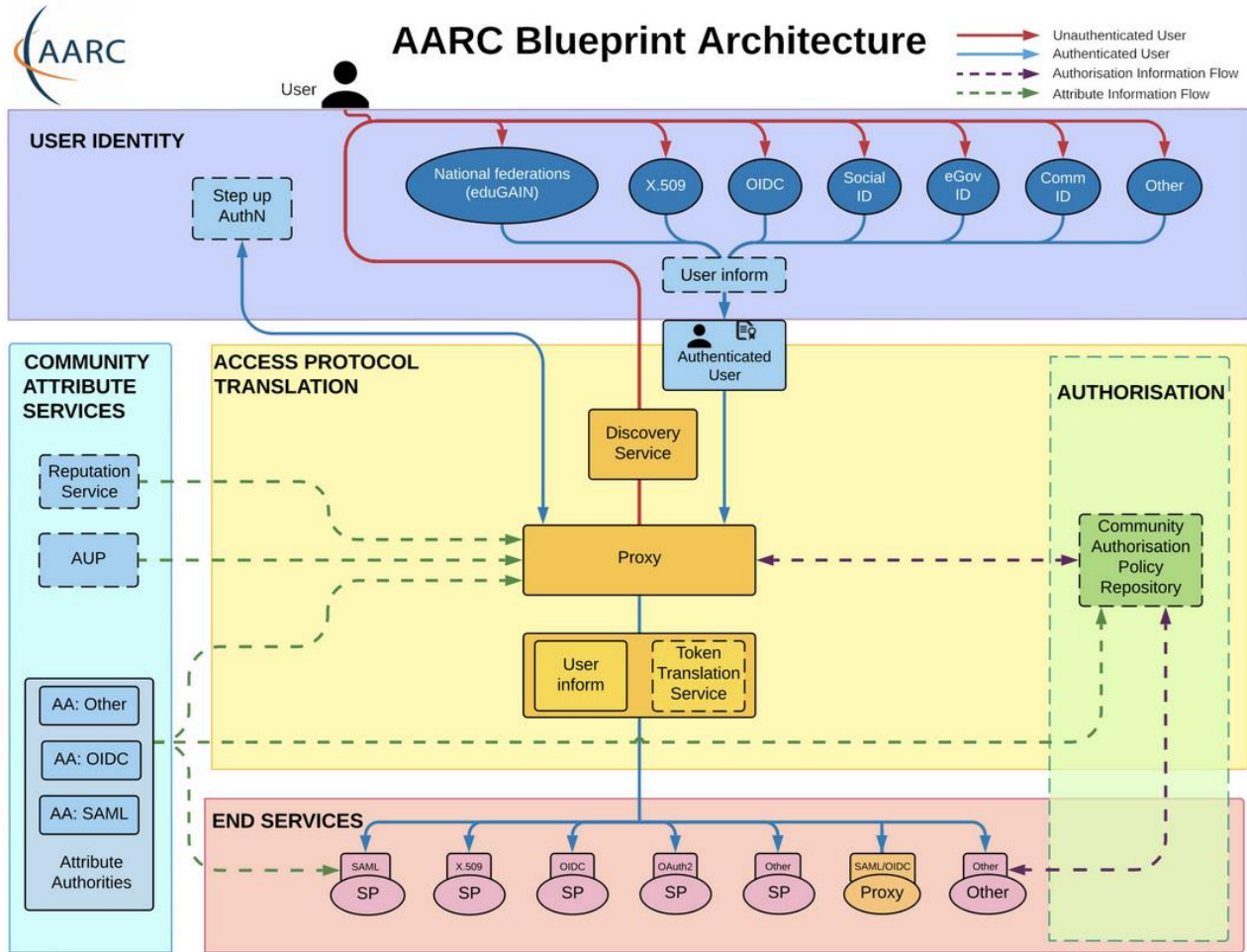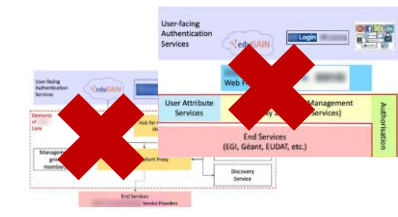
The AARC BPA: the IdP-SP proxy to enable federated access for research

o Access services using **identities from users' Home Organizations**, but **hide complexity** of multiple IdPs, federations, AA technologies

o **One persistent identity** across all the community's services through **account linking**

o **Access** services **based on role(s)** users have **in the collaboration**.

o For both **web** and **non-web** resources

o Integration of **guest identity solutions**

o **Support for stronger authentication assurance** mechanisms

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

Authentication and Authorization for Research Collaboration – https://aarc-community.org/

Of AARC TREEs and colourful pictures

Interoperability – more than just the nice colours

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

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
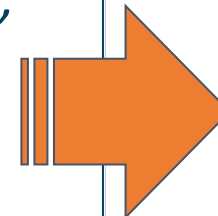
AARC-G056

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.

Of AARC TREEs and colourful pictures

The Community AAI and the Infrastructure Proxy – structuring elements
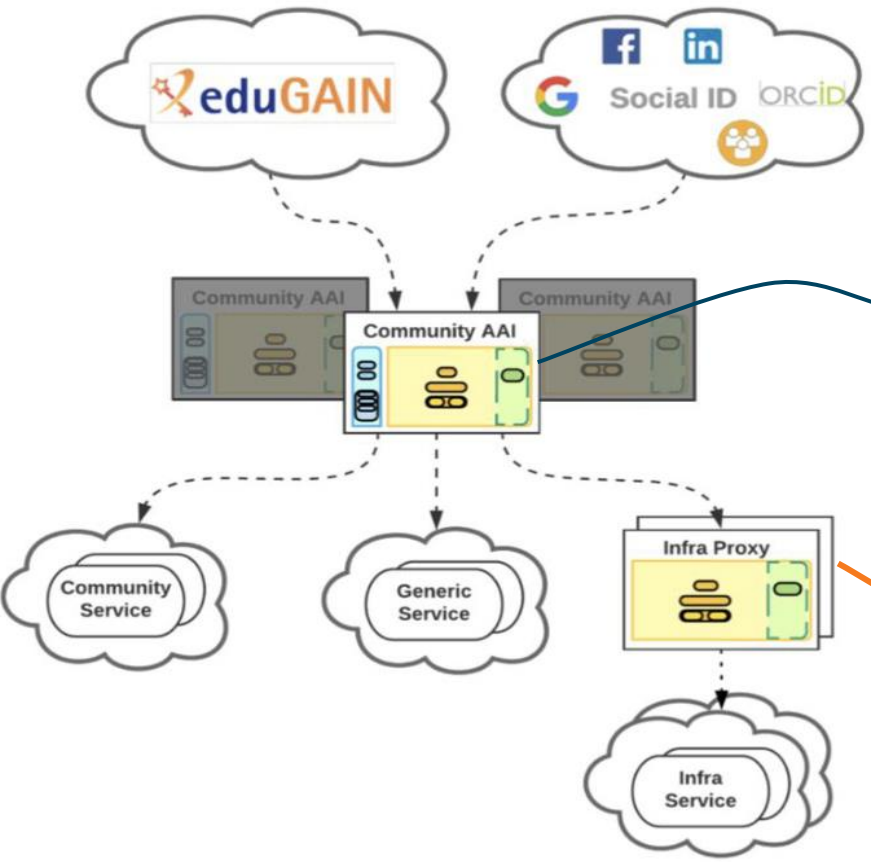
Community AAI

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 Technical Revision to Enhance Effectiveness

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

Recommendations for a common long-term strategy for AAI services

Updated AARC BPA

Updated interoperability framework

Bring RIs, e-Infrastructures and relevant stakeholders **together**

Of AARC TREEs and colourful pictures
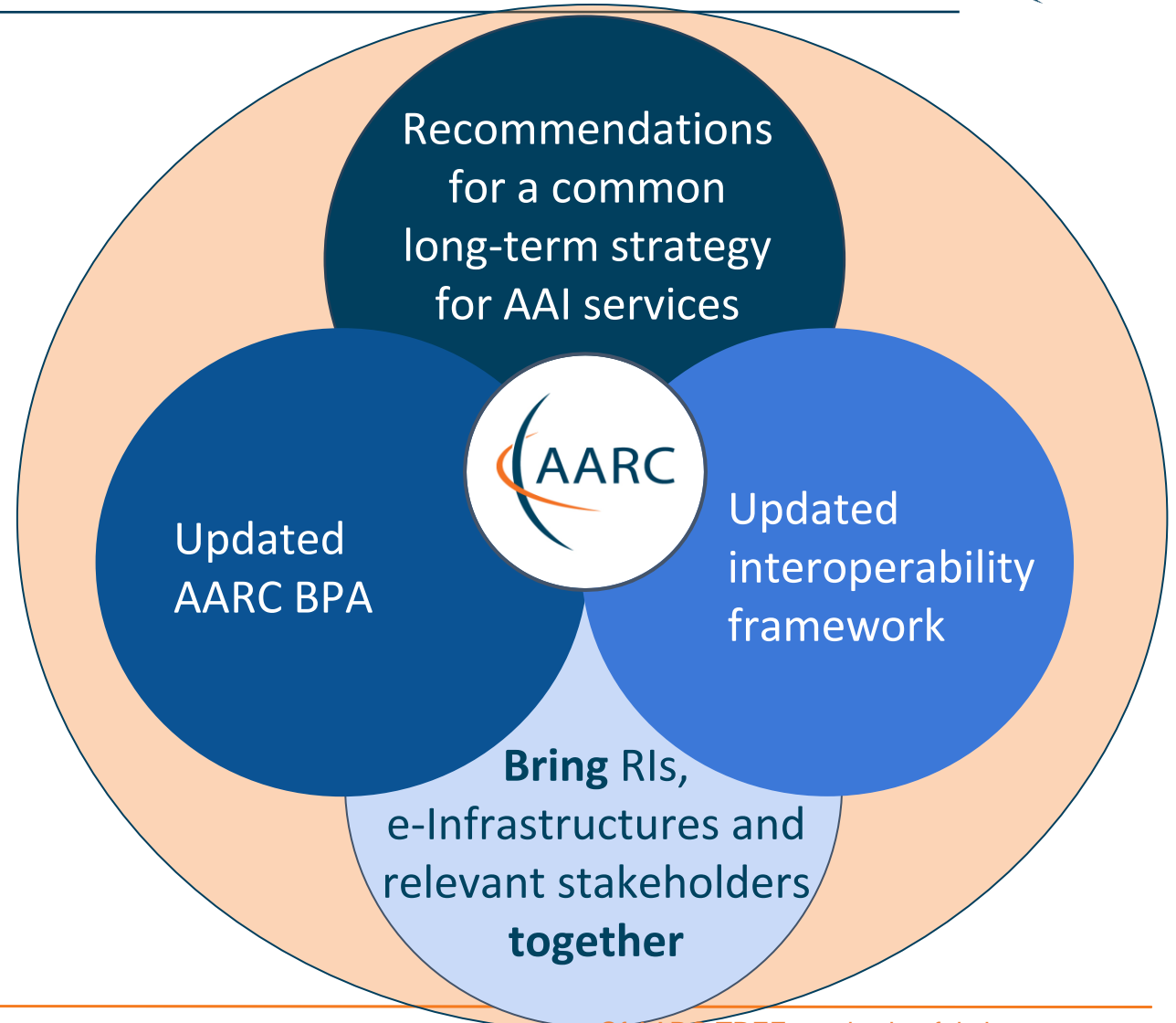
Our federated world is growing more complex
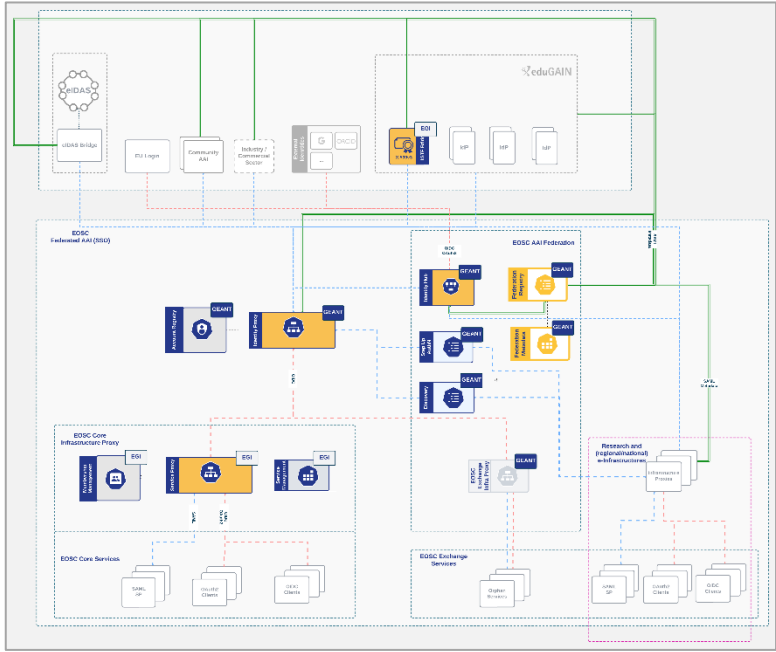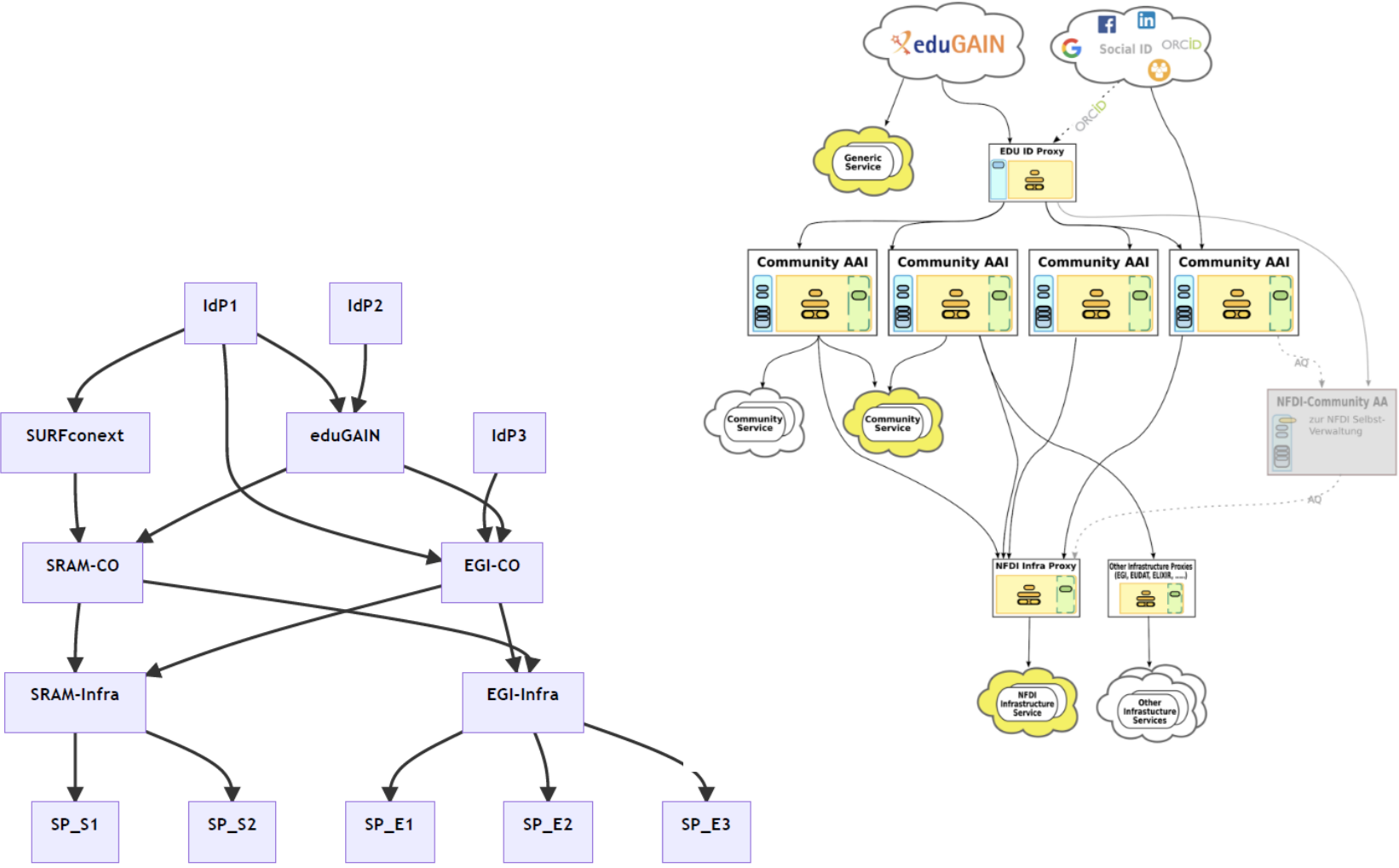
Images: SURF SSRAM and EGI by Maarten Kremers, NDFI AAI (Marcus Hardt), EOSC AAI for the EOSC Core and Exchange Federation for the EOSC European Node by Christos Kanellopoulos, Nicolas Liampotis, David Groep (June 2023 version)

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 ado...

- due in December 2024

...llection and Analysis

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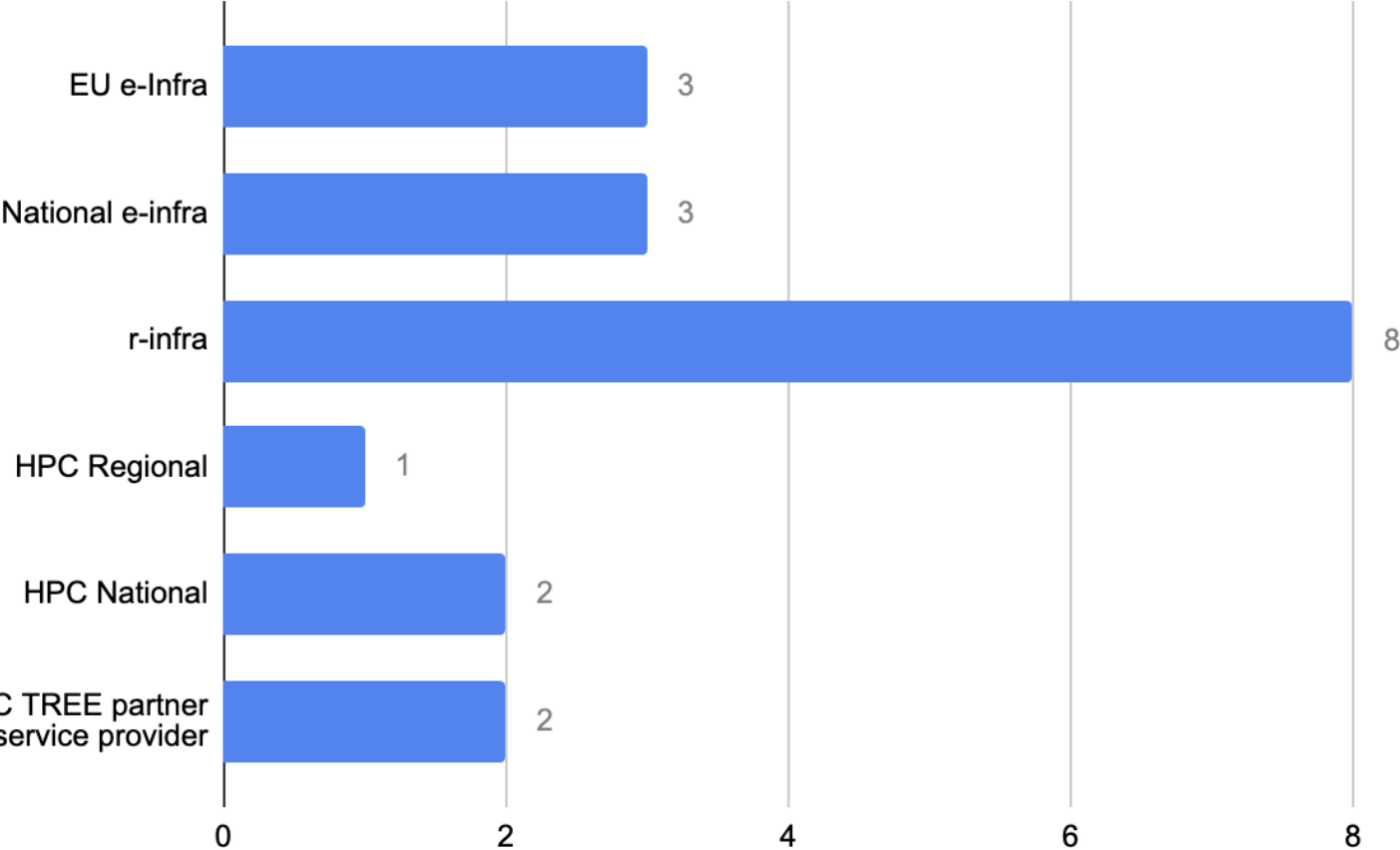
We think that this group should not be considered in the survey - we found institutional SP proxies to be too bespoke

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
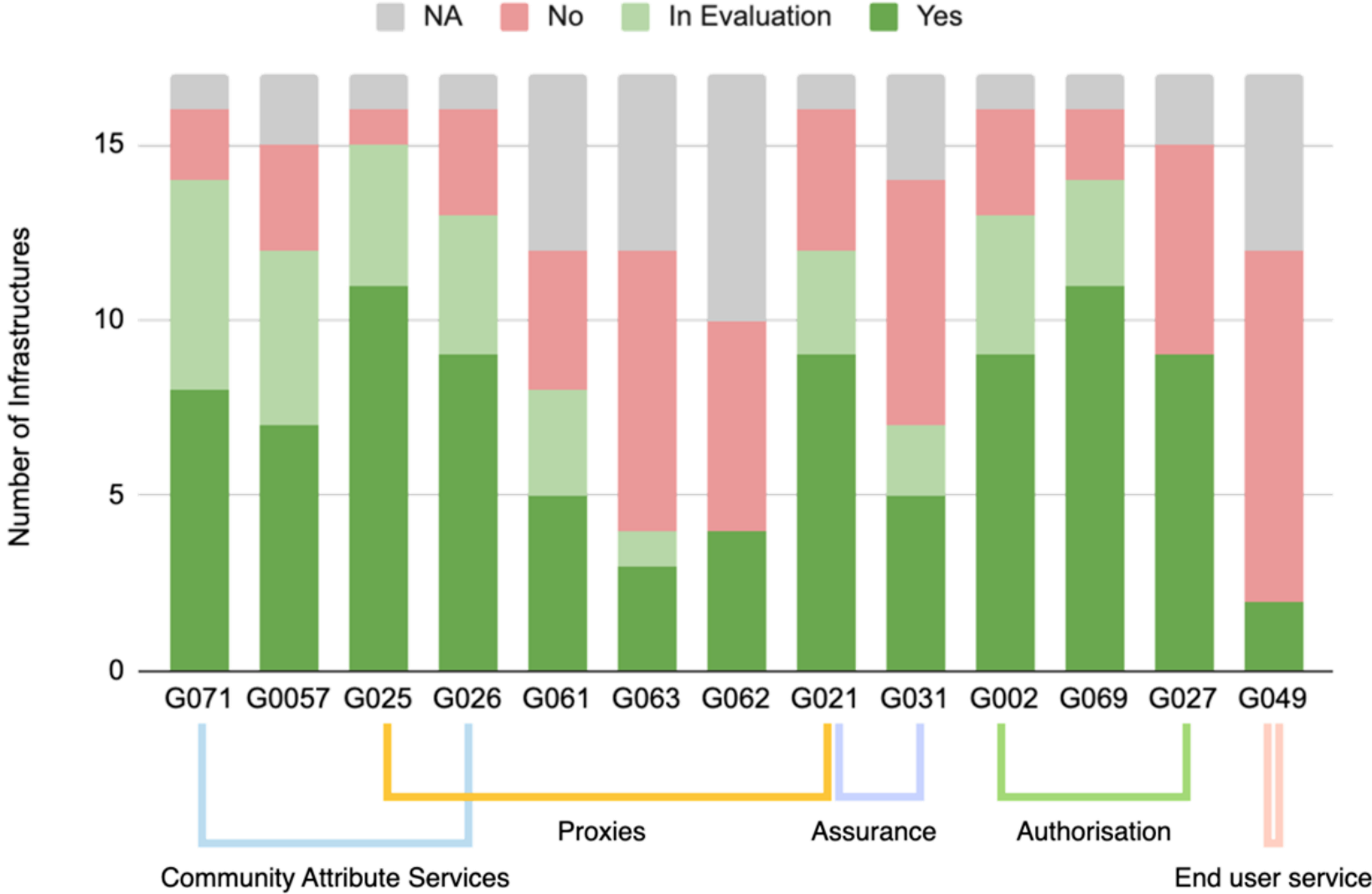
So how to evolve the guidelines?

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 interoperatability
- Policy development kit
- Trust mechanisms and federation

Validation and adoption

A common suite of architecture and policy guidelines

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

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.

Abstract
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.

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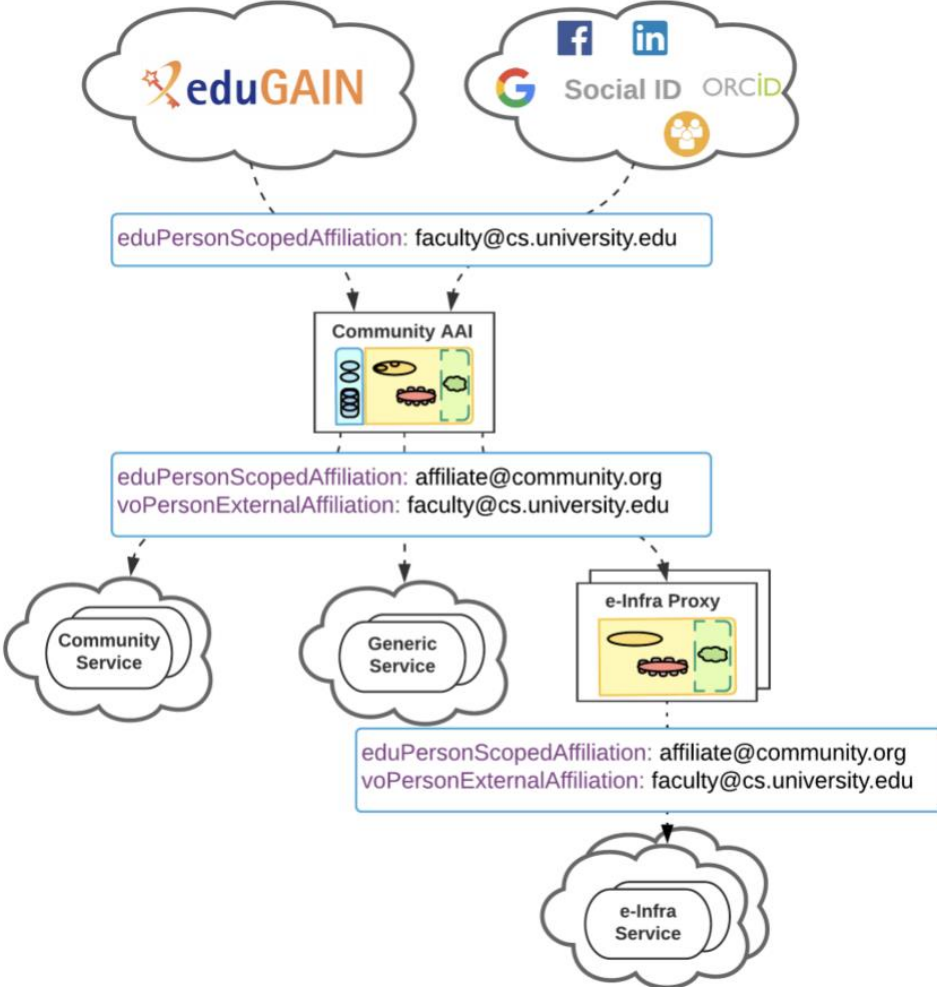
AARC-I058 Methods for Establishing Trust between OAuth 2.0 Proxies

- *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
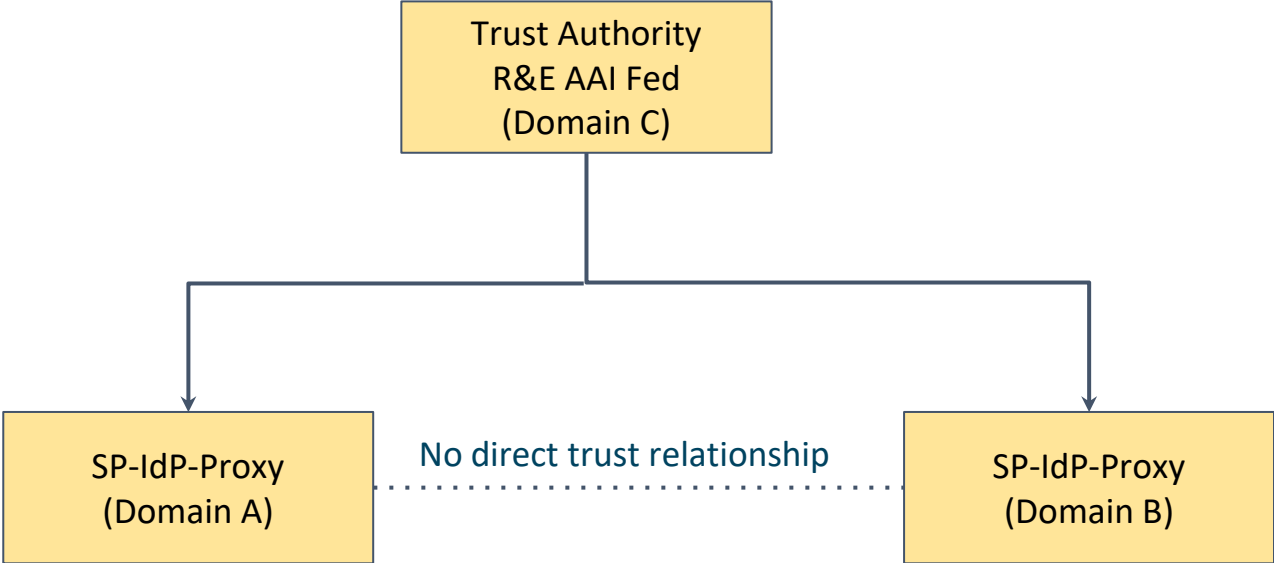
Comparing federation approaches in AARC-I058

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)
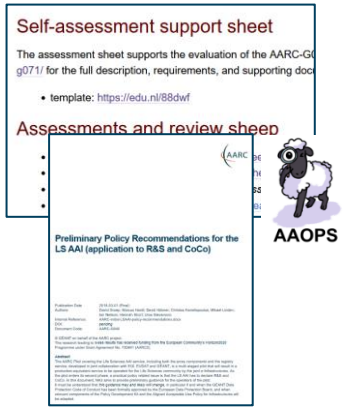
User-centric trust alignment and policy harmonization: helping out the community

- Lightweight community management policy template

- Guideline on cross-sectoral trust in novel federated access models

- Assurance in research services through (eIDAS) public identity assertion
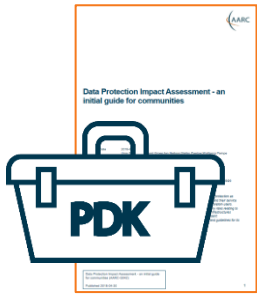
How to establish secure operation for your (AARC BPA) proxy?

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

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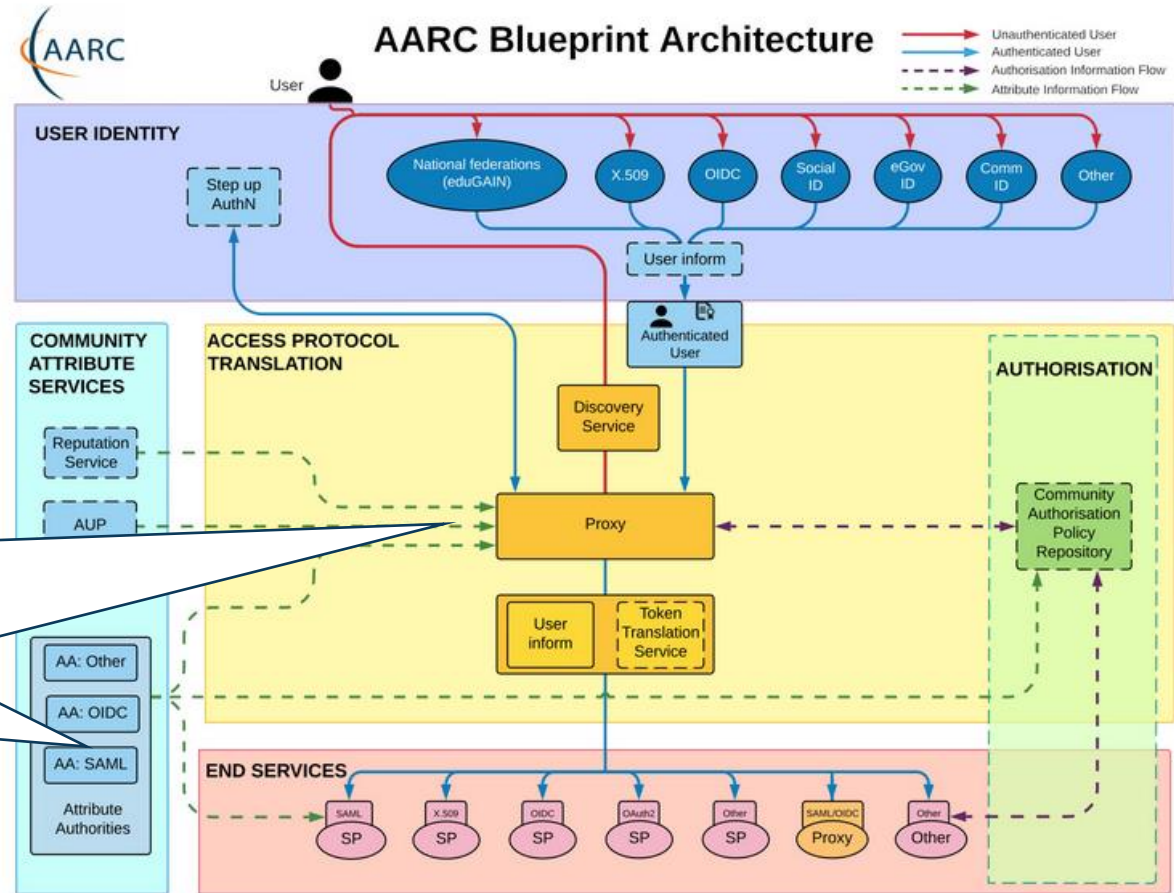
Guidelines for Secure Operation of Attribute Authorities
and other issuers of access-granting statements
(AARC-I048, in collaboration with IGTF AAOPS)

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 to 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?
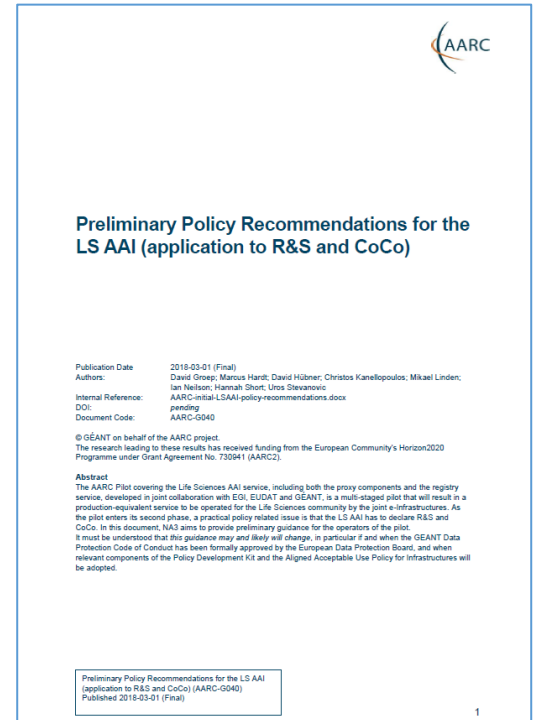
beyond AARC-G040

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'

Document thumbnail (right side):

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

Publication Date: 2018-03-01 (Final)
Authors: David Groep; Marcus Hardt; David Hübner; Christos Kanellopoulos; Mikael Linden; Ian Neilson; Hannah Short; Uros Stevanovic
Internal Reference: AARC-initial-LSAAI-policy-recommendations.docx
DOI: pending
Document Code: AARC-G040

© GÉANT 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 GÉANT, is a multi-staged pilot that will result in a production-equivalent service to be operated for the Life Sciences community by the joint e-infrastructures. As the pilot enters its second phase, a practical policy related issue is that the LS AAI has to declare R&S and CoCo. In this document, NA3 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 GÉANT 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.

Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo) (AARC-G040) Published 2018-03-01 (Final)

1

AARC G082 Notice Management by Proxies

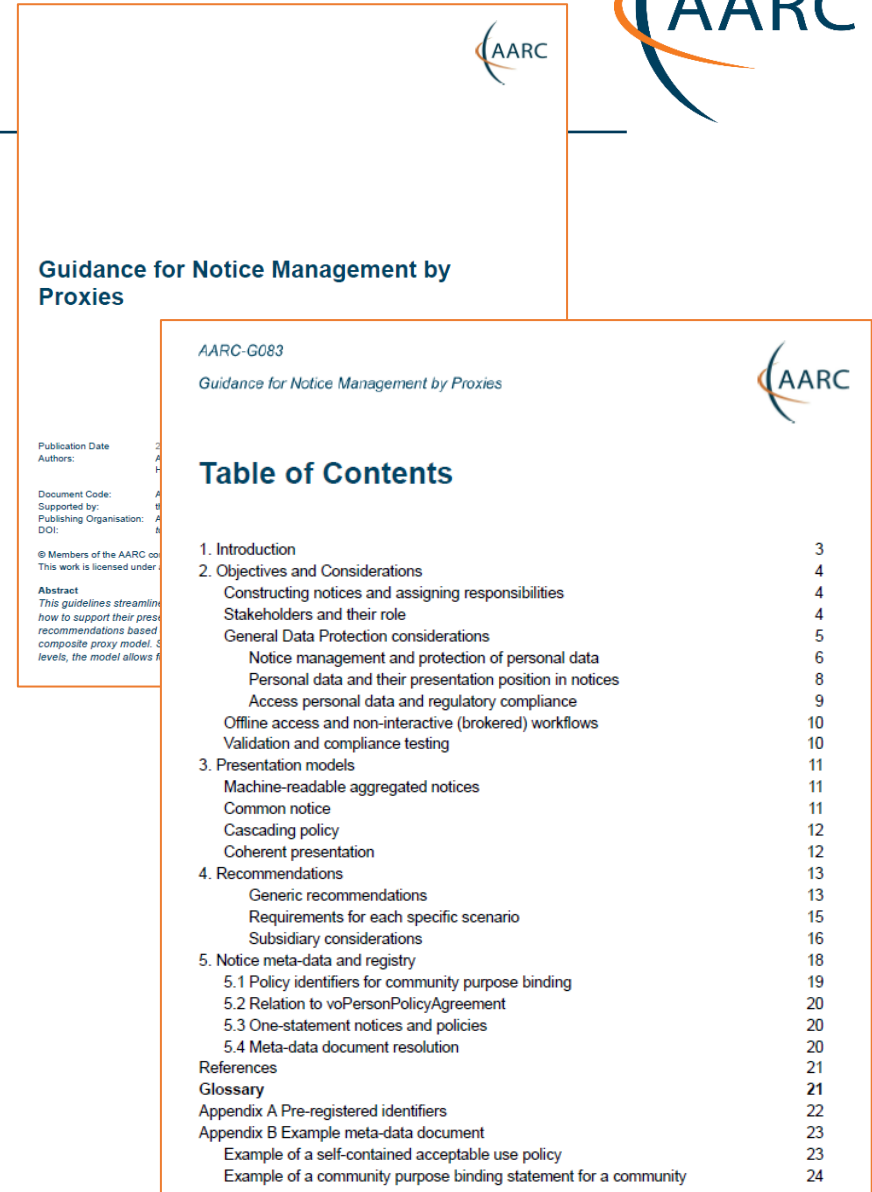**Four presentation models**. In order of preference

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

Guidance for Notice Management by Proxies

AARC-G083
Guidance for Notice Management by Proxies

Publication Date
Authors:

Document Code:
Supported by:
Publishing Organisation:
DOI:

© Members of the AARC co
This work is licensed under

Abstract
*This guidelines streamline
how to support their prese
recommendations based
composite proxy model. S
levels, the model allows f*

Table of Contents

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

```
{
  "id": "urn:doi:10.60953/68611c23-ccc7-4199-96fe-74a
  "aut": "https://www.nikhef.nl/",
  "aut_name": "Nikhef",
  "valid_from": 1649023200,
  "ttl": 604800,
  "contacts": [
    "helldesk@nikhef.nl",
    "information-security@nikhef.nl"
  ],
  "security_contacts": [
    "abuse@nikhef.nl"
  ],
  "privacy_contacts": [
    "privacy@nikhef.nl"
  ],
  "policy_class": "acceptable-use",
  "notice_refresh_period": 34214400,
  "includes_policy_uris": [
    "https://documents.egi.eu/document/2623"
  ],
  "policy_uri": "https://www.nikhef.nl/aup/",
  "description#nl_NL": "Deze Gebruiksvoorwaarden betr
netwerk en computers bij Nikhef. Iedere gebruiker va
wordt geacht op hoogte te zijn van deze voorwaarden e
  "description": "This Acceptable Use Policy governs
networking and computer services; all users of these services are expected to
understand and comply to these rules."
}
```

```
{
  "id": "https://operations-portal.egi.eu/vo/view/voname/xenon.biggrid.nl",
  "aut": "https://xenonexperiment.org/",
  "aut_name": "Xenon-nT collaboration",
  "valid_from": 1311890400,
  "ttl": 31557600,
  "contacts": [
    "grid.support@nikhef.nl",
  ],
  "security_contacts": [
    "vo-xenon-admins@biggrid.nl"
  ],
  "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"
}
```
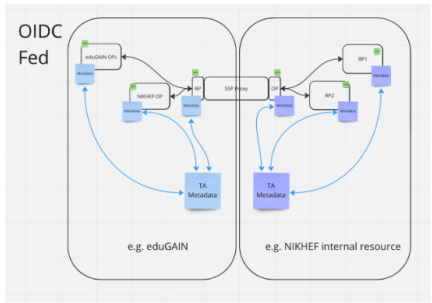
"small to mid-sized communities do not have the resources to maintain a bespoke community management policy"

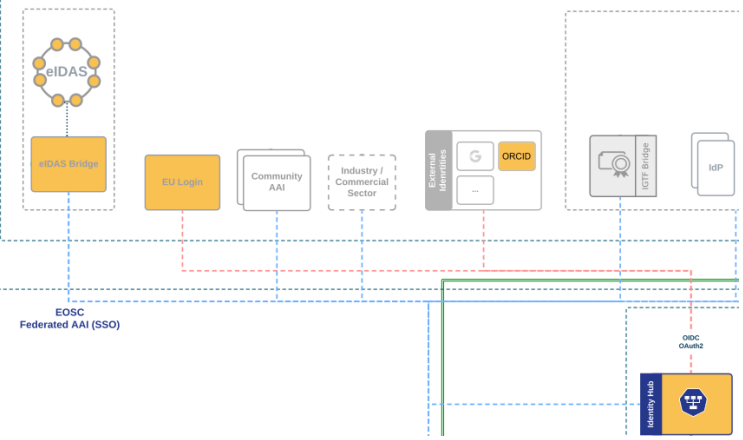this leaves communities *and SP operators* unclear about trust assurance level of members

Today's BPA proxy links attributes **as well as** trust

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
another (+ augment of claims), but also bridging trust between both "domains"
In OIDC federation, you can chain metadata statements not by publishing to a [...]
hierarchies, trust anchors who can sign intermediates . multiple signatures on th[...]

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.

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 ?
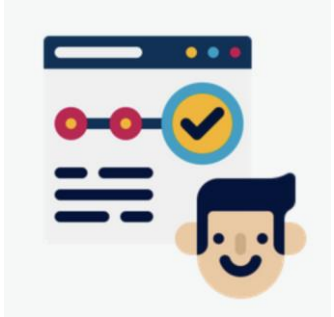
Use Cases Collection and Analysis

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
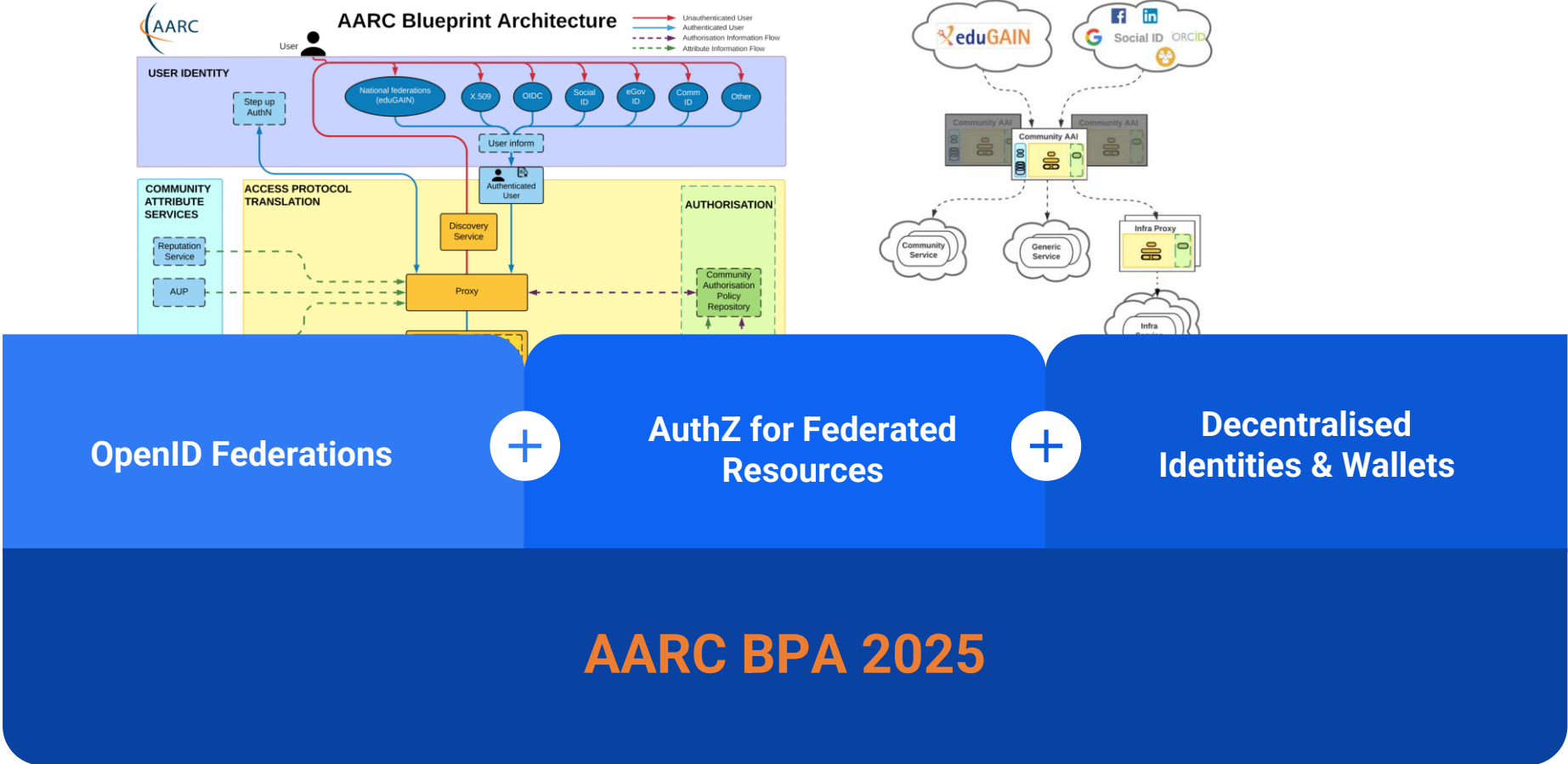
Compendium & Recommendations

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

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

AARC BPA 2025

AARC Community - open for all

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@aarc-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