



Authentication and Authorisation for Research and Collaboration

## A TREE of Trust Policy Harmonisation & Interoperability

Aligning proxy good practices, easily accessible to users

**David Groep**

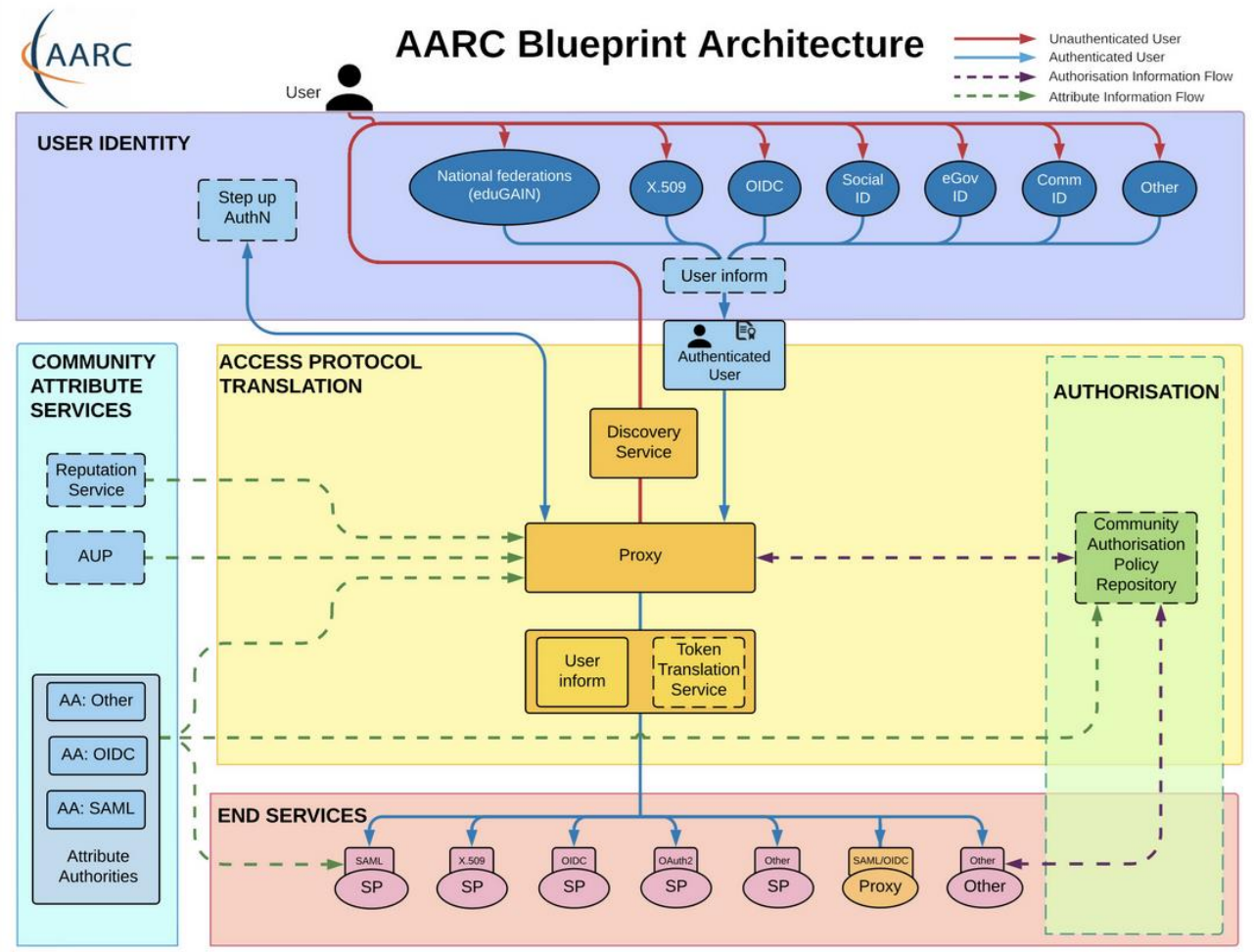
AARC TREE WP2 Lead



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

EUGridPMA61, IGTF, GN5-1, and AARC Policy Community meeting  
Abingdon, UK, May 2024

# 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

**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

**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

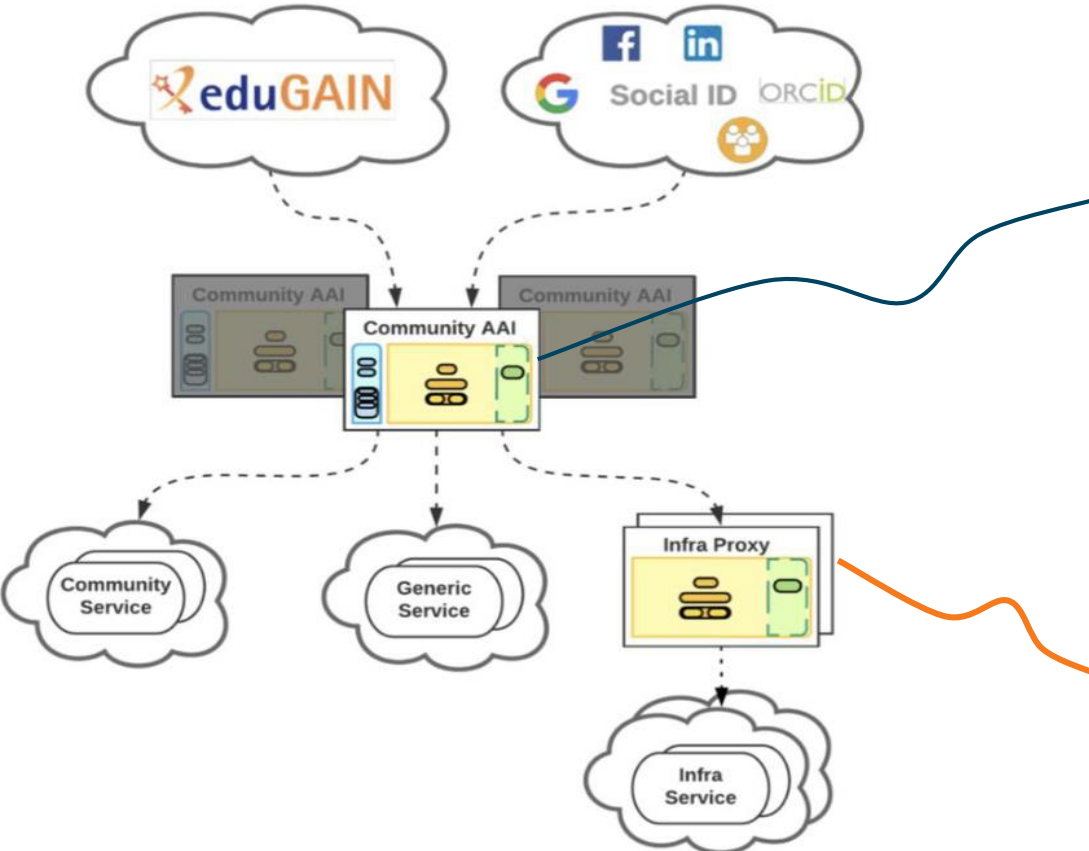
**What next? Are you looking for a kick start with your policies? Take a look at the Policy Development Toolkit which provides a set of templates.**

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.

**PDK**

Showing 1 to 9 of 9 entries

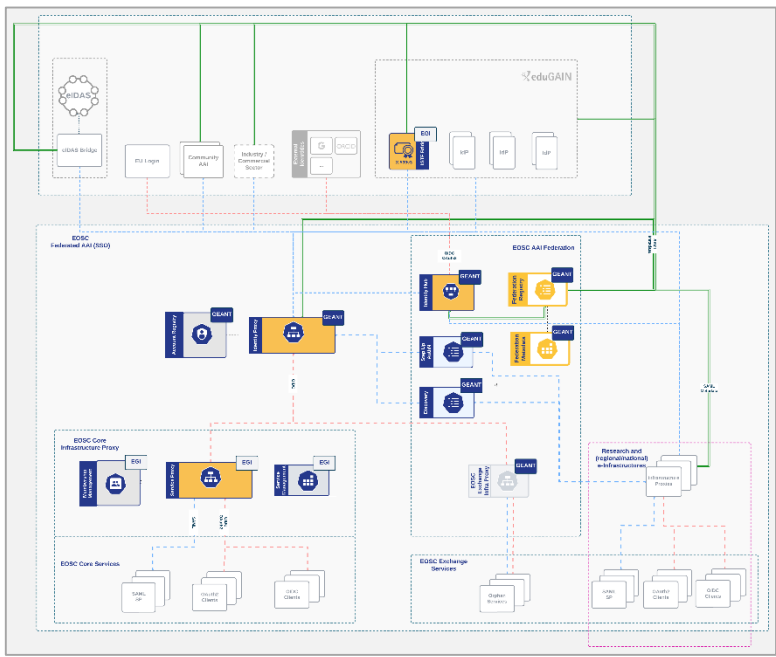
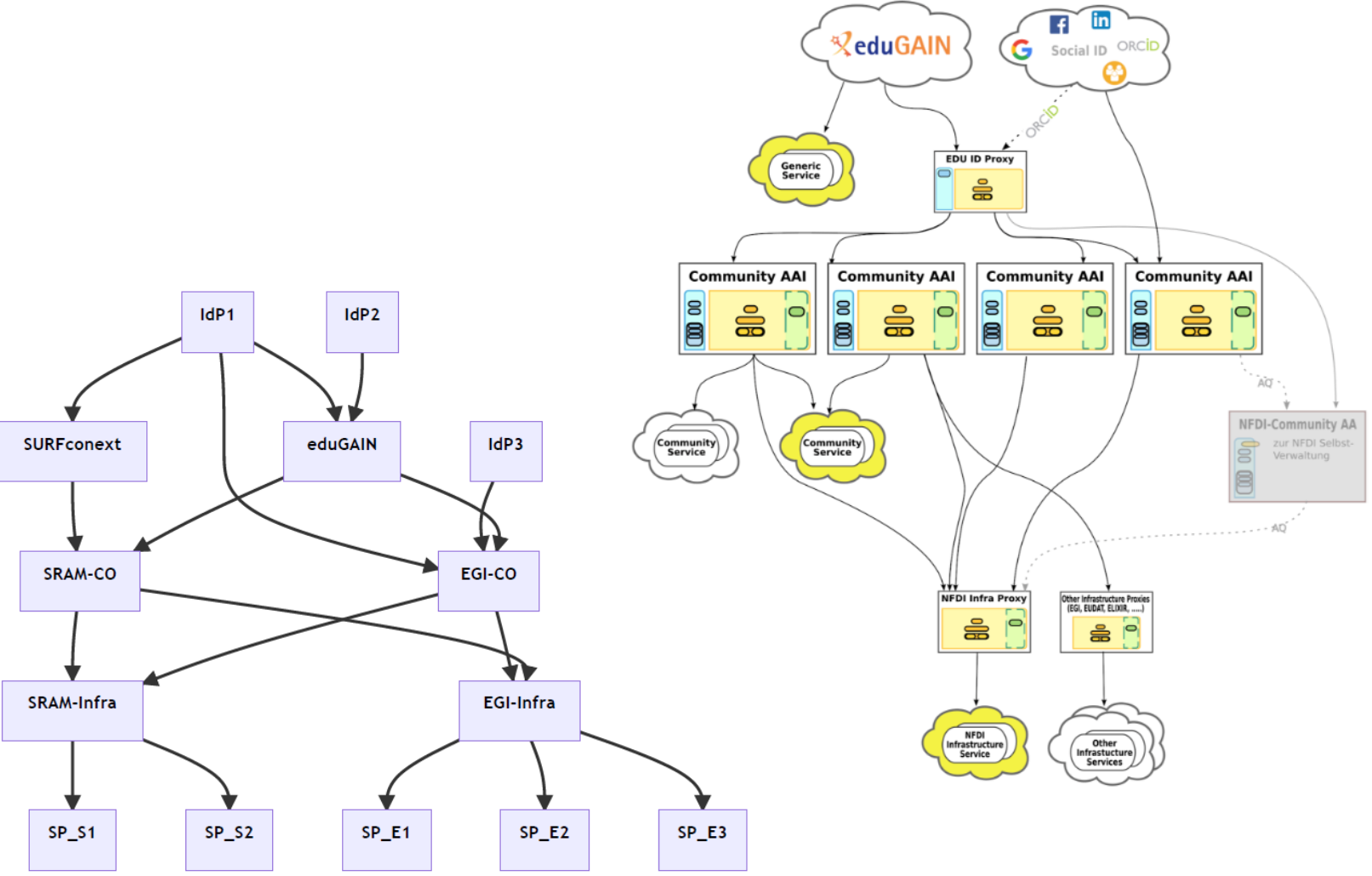
# The Community AAI and the Infrastructure Proxy – structuring elements



**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.

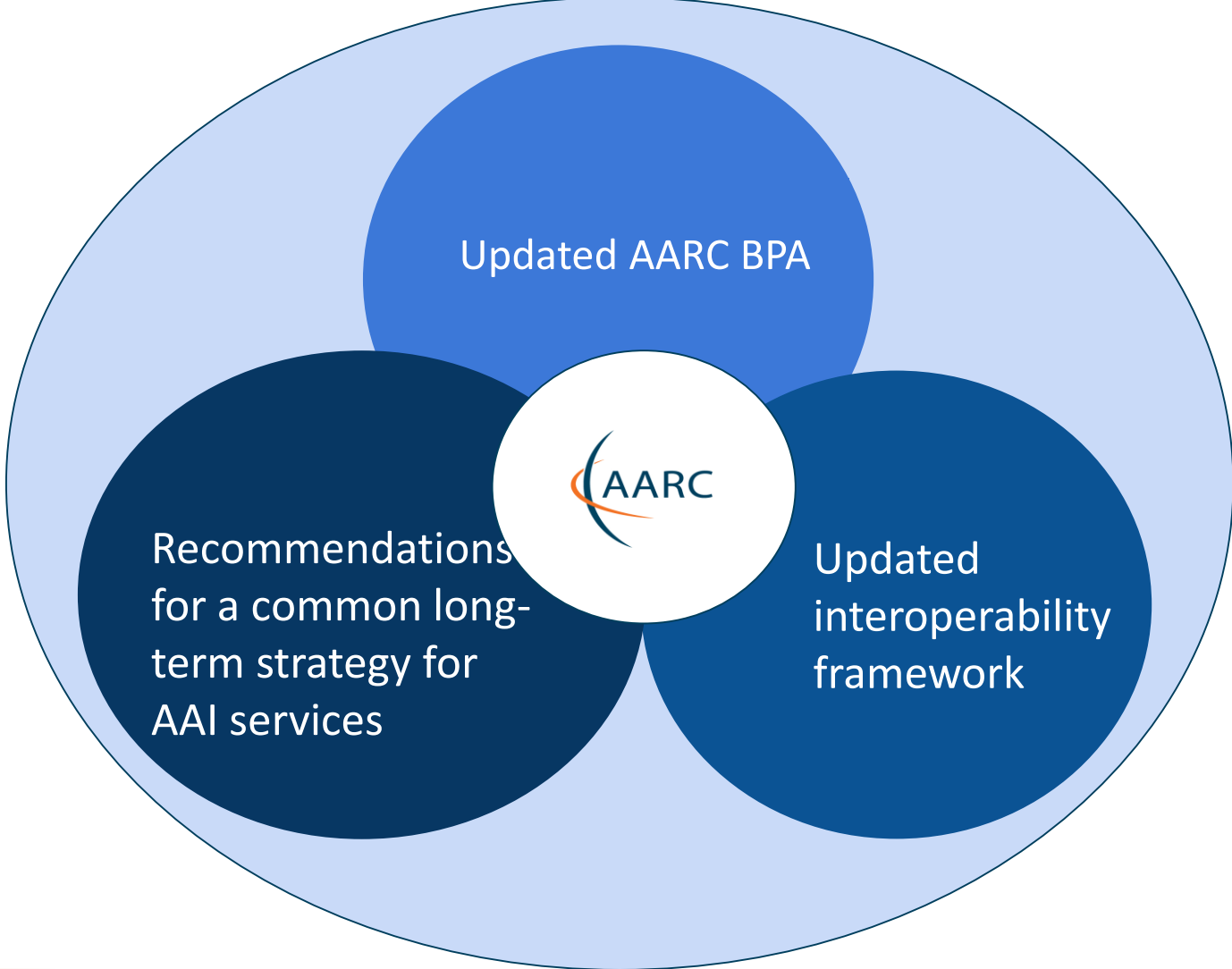
**Infrastructure Proxy**  
 The Infrastructure Proxy, enables Infrastructures with a large number of resources, to provide them through a single integration point, where the Infrastructure can maintain centrally all the relevant Policies and business logic for making available these resources to multiple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

# 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: technical evolution for enhanced effectiveness!



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

## Guidelines for **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**

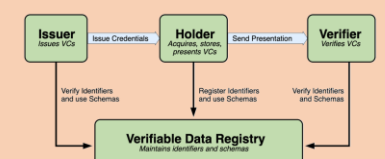
## Authorisation guidelines

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



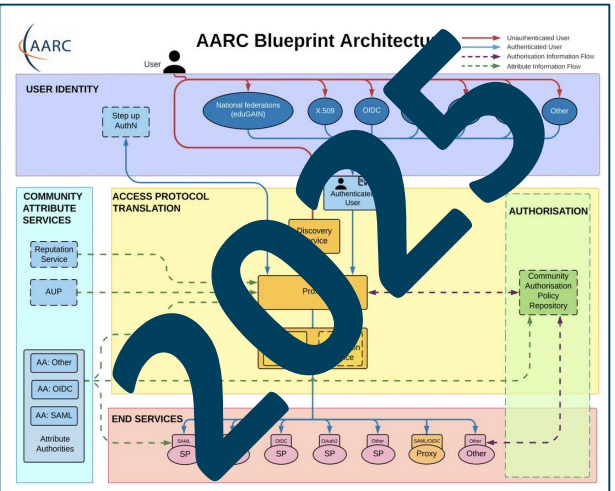
## Decentralised identities

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



```

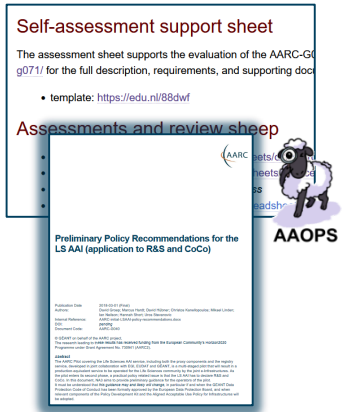
    graph TD
      Issuer[Issuer  
Issue VCs] -- Issue Credentials --> Holder[Holder  
Accounts, stores, presents VCs]
      Holder -- Send Presentation --> Verifier[Verifier  
Verifies VCs]
      Verifier -- Verify Identifiers and Schemas --> VDR[Verifiable Data Registry  
Maintains identifiers and schemas]
      VDR -- Verify Identifiers and use Schemas --> Issuer
      VDR -- Register identifiers and use Schemas --> Holder
  
```



# Policy and good practice underpinning the AARC Blueprint BPA

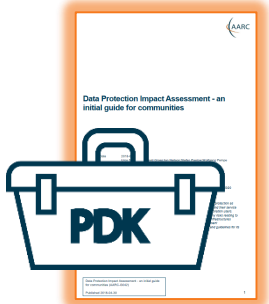
## Infrastructure alignment and policy harmonisation: helping out the proxy

- **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



Anchored in the researcher user communities by **co-creation with FIM4R**

# 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)

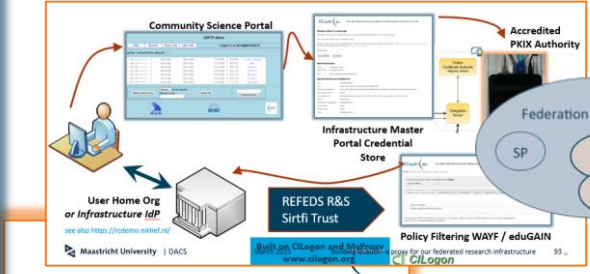


### Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)

Publication Date: 2019-03-01 (Final)  
 Authors: David Groep, Marcus Hardt, David Hüber, Christos Kanelloupolous, Mikael Lindén, Jan Nelsson, 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.



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

Publication Date: 2018-04-30  
 Authors: Uros Stevanovic, David Groep, Jan Nelsson, 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

### The Security Incident Response Trust Framework for Federated Identity

Do you need Sirtfi to access a service? Look for your home organisation below and click to email them a request.  
 Want more information? Visit the [Sirtfi Homepage](#).

### 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 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/spreadsheets/...>

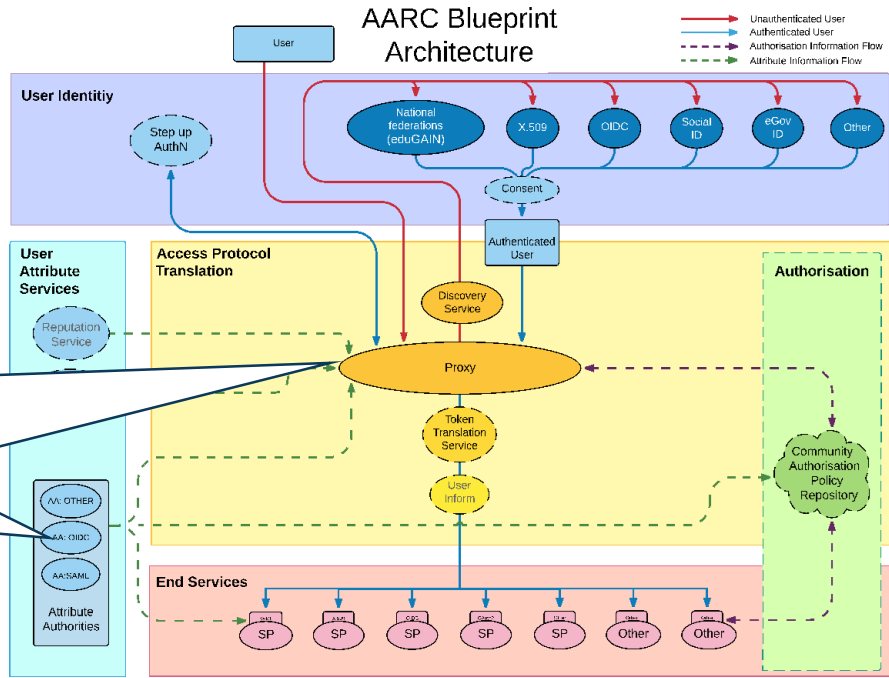
AAOPS



# 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* – that was successful before!


**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/88d4vf>

**Assessments and review sheep**

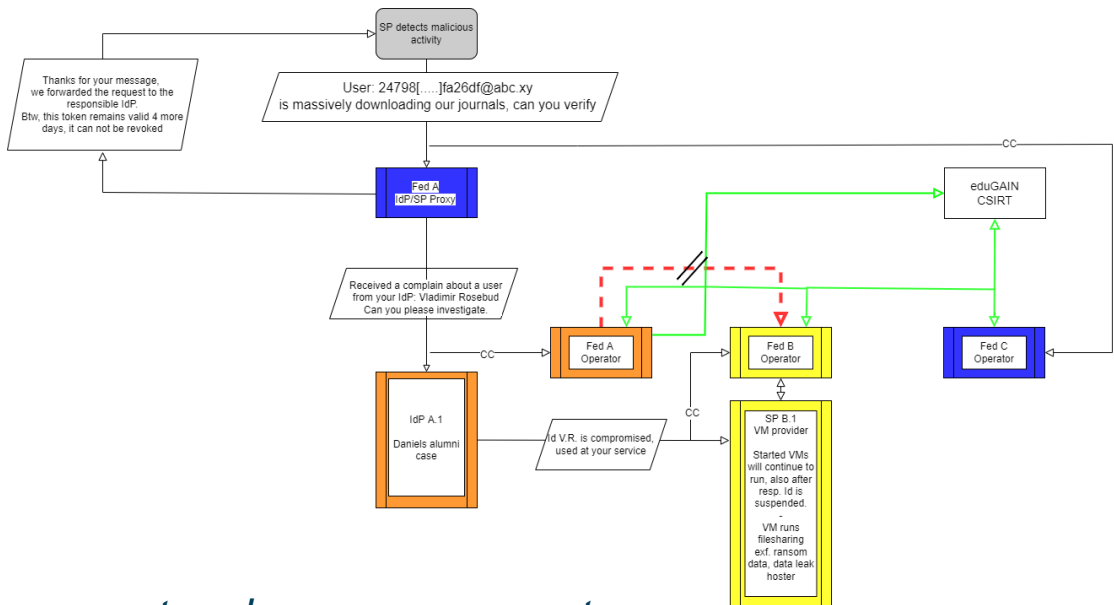
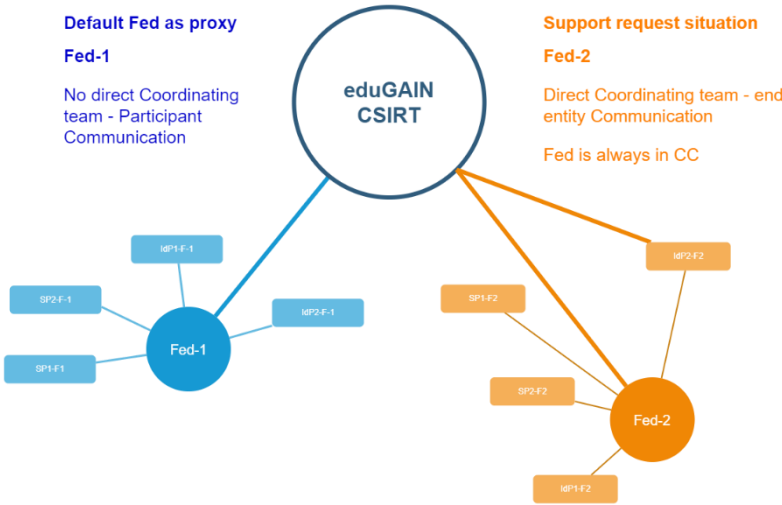
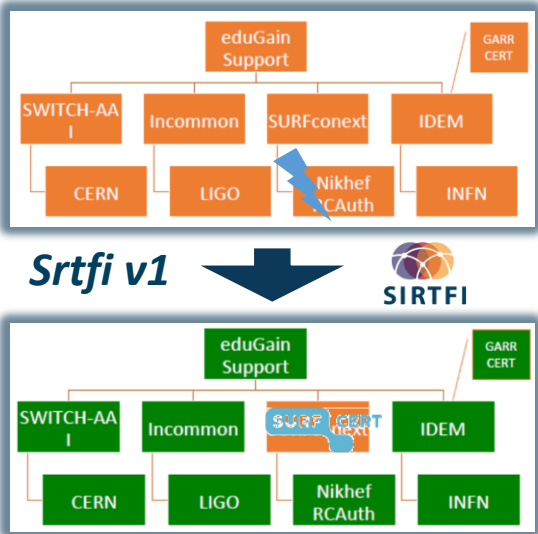
- WILCG - <https://docs.google.com/spreadsheets/d/1...>
- UK-IRIS - <https://docs.google.com/spreadsheets/d/1...>
- eduTEAMS (Core AAI platform) - *in progress*
- SURF SRAM - <https://docs.google.com/spreadsheets/d/1...>



... set of (one or more) guidelines that represent a widely agreed and jointly-developed **operational trust baseline** for infrastructure membership management and proxy components.

Now, feedback is needed of the current proxy operators (in AEGIS) and extend the baseline with guidance.

# Response and traceability across IdP-SP Proxies and the limits of Sirtfi



Guidelines for a joint **operational trust baseline** for membership management and proxy components, supplemented by policy guidance for sectoral federations with more specific policies where needed

- ‘How can we **convey the trust in what is in and behind the proxy?**’
- ‘How to provide **timely traceability** between services and identities through the proxy?’

Based on requirements from FIM4R, WISE, and the proxy operators in AEGIS.



joint work with GN5-1 EnCo and eduGAIN CSIRT



# Can we build on a trusted baseline and expectations to increase acceptance of research infrastructure proxies with R&E identity providers

---

Even though affiliation is the most relevant attribute from home IdPs, ...

- still need assurance statements and REFEDS Assurance Framework attribute freshness
- unless 'well hidden', proxies are met with scepticism by IdPs to release personalised to R&S
- do Entity Categories 'traverse' proxies? and can proxy ops rely on their 'downstreams'?

a common **baseline** that proxies can endorse and manage for their connected services helps



**review and enhance effectiveness of Snctfi 'revamped'**

*the set of guidelines that describe a (self-) accessible baseline for a set of service providers behind an AARC BPA Proxy*

and thereby encourage trust in the proxies *and* their connected services

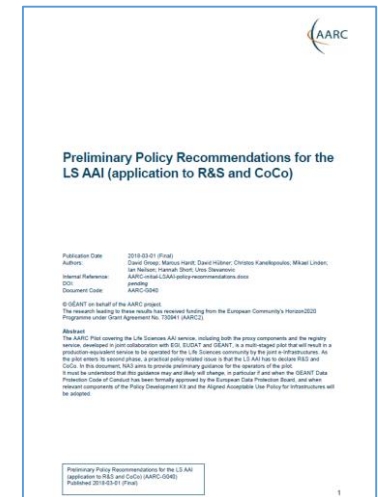
# Proxies have their own challenges as well: AUPs, T&Cs, Privacy notices, ...

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

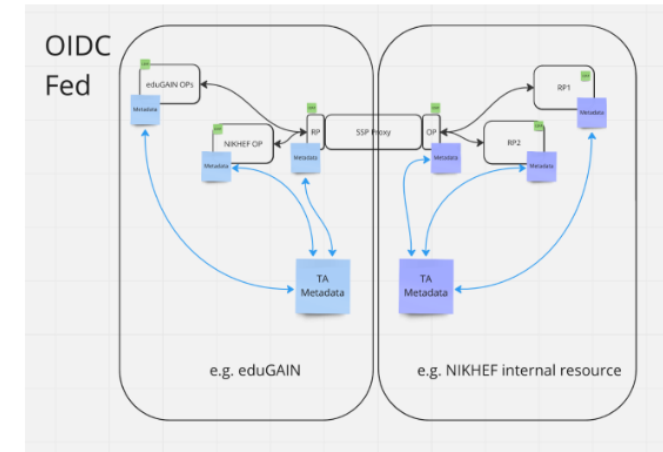
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide 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

# New trust models – what is the role of the proxy in OIDCFed?

In today's BPA proxy links both sides by being opaque, **both** for attributes **as well as** for trust

- does it *have* to be that way?
- separate claims/attribute transformation from trust bridging?
- can OIDCfed structure convey trust transparently? Should it?
- can we then be more flexible? or will it just confuse everyone?
- easier to bridge trust *across sectors* this way?  
e.g. linking .edu, .gov, and private sector federations?



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 one for format to another (+ augment of claims), but also bridging trust between both "domains"

In OIDC federation, you can chain metadata statements not by publishing to a list, but building hierarchies, trust anchors who can sign intermediates . multiple signatures on the same

See also ACAMP at TechEx23 and TIIME

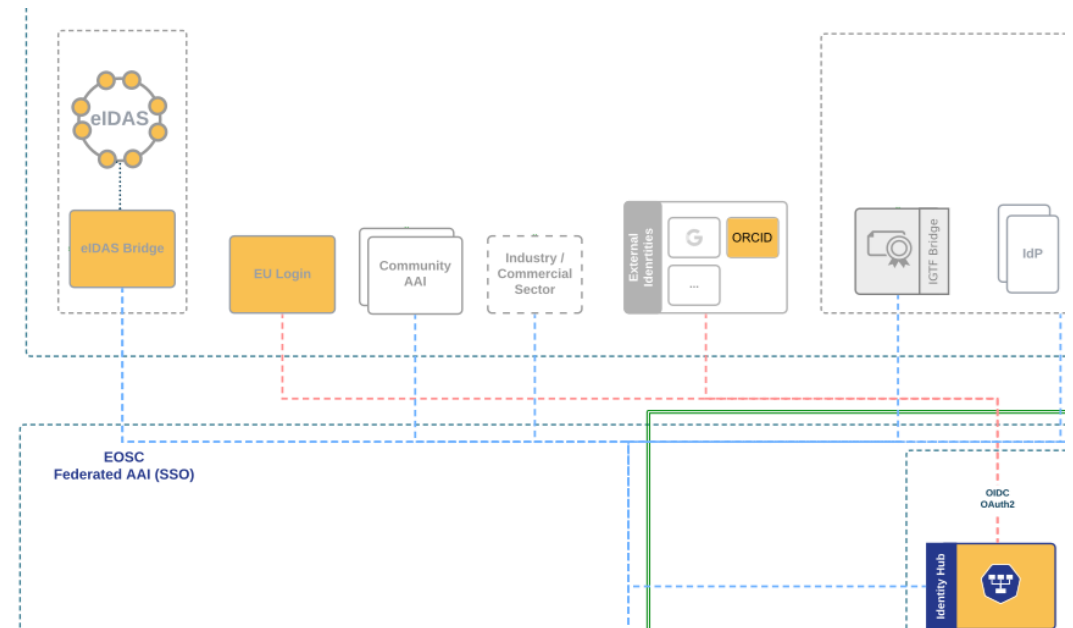
# We'll see more diverse sources of identity & assurance anyway

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 a key factor

---

Also in AARC-TREE we target a “co-creation process”

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

whatever we build must be *usable and available* by researcher communities first of all, and align to interoperability standard and open, collaborative research goals

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



# Deliverables



	Deliverable name	Short description	#WP	Lead	Type	Due
M2.1	Guidance for notice management by proxies	<i>Guideline submitted to AEGIS</i>				M10
D2.1	<b>Trust framework for proxies and Snctfi research services</b>	Trust framework, guidelines and best practice for BPA proxies and interaction with research services	WP2	RAL	R	M15
M2.2	eID assurance model suitability assessed	<i>Report submitted to AEGIS</i>				M18
D2.2	<b>AARC Policy Development Kit Revision</b>	Evolved suite of guidelines and templates for research and infrastructure communities	WP2	Nikhef	R	M24

## One AARC (Policy) Tree ...



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

**But: do you really want two trunks??**

## 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 2024)**

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

## Compendium and Recommendations

---

**Key result in the '2<sup>nd</sup> year' (April 2025 - February 2026) is the **Compendium****

**'compendium of AARC best practices' with recommendations** for a common long-term strategy for AAI services in pan-European Research Infrastructures in Europe

- based on the use case input and researcher requirements
- promotes coherent and interoperable architecture and policy
- **iterate and validate** with the infrastructures at large

*describe the road that collaborative research infrastructure AAI will take!*

## Welcome under the AARC (Policy) Tree

---



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

**Let's collect some good practices & share!**

# 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's Horizon research and innovation programme 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).



# But when, oh when?

ID	Task Name	Start	Effort	Partners	2024												2025												2026	
					Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb		
1	<b>Research Infrastructure Alignment &amp; Policy</b>	2024-03-01	21 PM	Nikhef	[Yellow bar spanning from Mar 2024 to Jul 2025]																									
2	Operational Trust Frameworks	2024-03-01	9 PM	RAL, Nikhef, NorduNET, EGI, GEANT	[Grey bar spanning from Mar 2024 to May 2024]																									
3	Service Provider Baseline & Acceptance	2025-01-01	4 PM	RAL, Nikhef, CERN, SURF	[Grey bar spanning from Jan 2025 to Jun 2025]																									
4	Coordinated AUPs, T&Cs and Privacy Notices	2024-03-01	8 PM	RAL, Nikhef, EGI, GRNET, KIT, MU GEANT	[Grey bar spanning from Mar 2024 to May 2024]																									
5	<b>User-Centric Trust Alignment &amp; Harmonisation</b>	2024-09-02	26 PM	RAL	[Yellow bar spanning from Sep 2024 to Feb 2026]																									
6	Lightweight Community Structures	2024-09-02	5 PM	EGI, CERN, KIT, SURF, GEANT	[Grey bar spanning from Sep 2024 to Jun 2025]																									
7	cross-sectoral trust in novel federated access models	2025-01-01	9 PM	RAL, Nikhef, EGI, GRNET, KIT, KIFU	[Grey bar spanning from Jan 2025 to Jun 2025]																									
8	assurance in research services through eID identity assertions	2025-03-03	8 PM	NorduNET, EGI, SURF, MU, GEANT	[Grey bar spanning from Mar 2025 to Jun 2025]																									
9	Co-creation with FIM4R (with WP3+)	2024-03-01	4 PM	RAL, Nikhef, NorduNET	[Yellow bar spanning from Mar 2024 to Feb 2026]																									

WP3 Use Case Analysis

WP5 Compendium

# A (very) distributed activity – let’s go and ensure a joint coherent output!

	AARC										
	STFC	Nikhef	NDN	EGI	CERN	GRNET	KIT	SURF	GEANT		SUM
Work item	PM	PM	PM	PM	PM	PM	PM	PM	PM	PM	PM
<b>Research Infra Alignment (Nikhef)</b>											<b>21</b>
Operational Trust for Proxies	★ ★	★ ★	★	★ ★						★ ★	★ ★ ★
‘Snctfi’ R&E Baseline & Integration	★	★			★			★			★
Models for Cross-Infra AUP & Privacy Notices	★	★		★		★	★		★ ★	★	★ ★ ★
<b>User-centric Trust Alignment (RAL)</b>											<b>26</b>
Lightweight Community Management Policy				★	★		★	★		★	★ ★
Guideline for Novel Federation Models	★	★ ★		★		★ ★	★ ★			★	★ ★ ★
Assurance in Research through eID			★	★				★ ★	★ ★	★ ★	★ ★ ★
FIM4R Policy Evolution	★ ★	★	★								★
											<b>47</b>