Authentication and Authorisation for Research and Collaboration

Trust Policy Harmonisation and Interoperability

WP2: Aligning proxy good practices, easily accessible to users

David Groep
AARC TREE WP2 Lead

Nikhef Maastricht University

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

AARC TREE kick-off meeting
Utrecht, March 2024

An AARC beyond the Policy Development Kit?

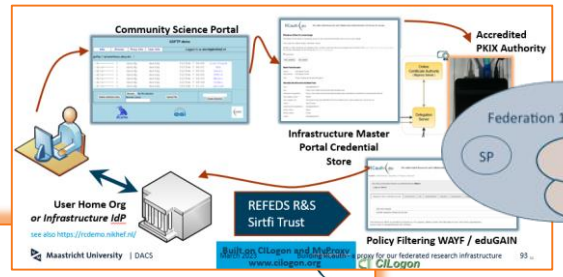
Current PDK is targeted at *large and structured* communities – and quite complex

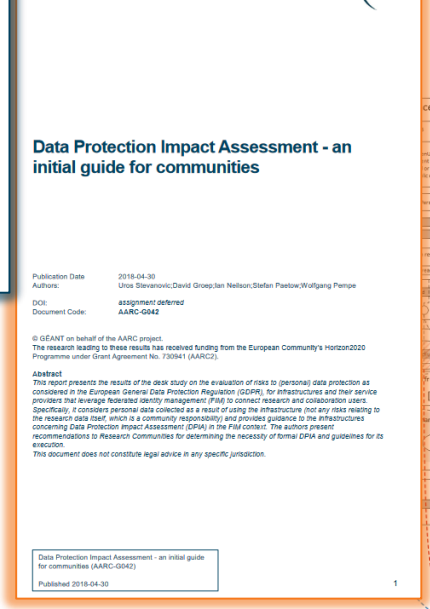
Document	Who should complete the template?	Audi		
Top Level Infrastructure Policy	Infrastructure Management	All In Parti (abid		
Incident Response Procedure	Infrastructure Management & Security Contact	Infra Secu Servi by)		
Membership Management Policy	Infrastructure Management	Rese Com (abid		
Acceptable Authentication Assurance	Infrastructure Management	Rese Com Servi by)		
Risk Assessment	Infrastructure Management, Services & Security Contact	Infra Man (com		
Policy on the Processing of Personal	Infrastructure Management & Data Contact	Rese Com Servi by)		
Priva	Infra	Users (view)	This can be used to document the data collected and processed by the Infrastructure and its participants. Each service in the infrastructure, as well as the infrastructure itself, should complete the template.	Google Doc
		(abide	This policy defines requirements for running a service within the Infrastructure.	Google Doc
		(abide by)	This is a template for the acceptable use policy that users must accept to use the Research Infrastructure. It should be augmented by the Research Community.	Google Doc

restrictions)

Showing 1 to 9 of 9 entries Previous Next

PDK





Self-assessment support sheet

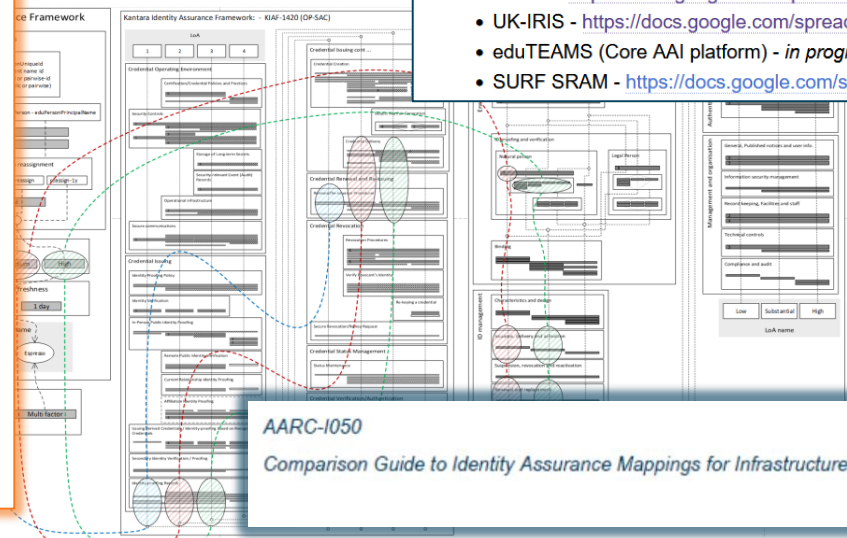
The assessment sheet supports the evaluation of the AARC-G0 g071/ for the full description, requirements, and supporting doc

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

Assessments and review sheep

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

AAOPS



AARC-I050

Comparison Guide to Identity Assurance Mappings for Infrastructures

Objective: support the diverse and different policies needed now

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

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

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

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

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

Effort in AARC TREE to address issues and explore policy needs

- AARC-TREE policy topics are devised (and effort assigned to each), with results defined in terms of how (policy) guidelines **support proxy use cases and communities**
- **Participatory model**, with FIM4R, AEGIS, and community proxy operators
- What is needed for operational trust in terms of, *e.g.*, '**baseline requirements**' policy and guidelines?

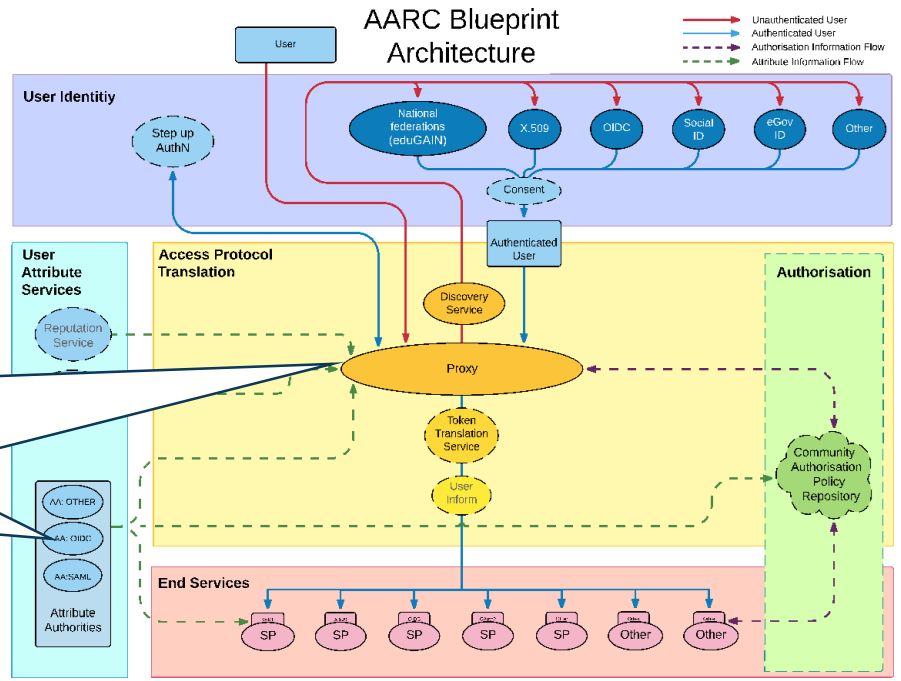
Let's look at some we identified when writing AARC-TREE …

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!

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

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

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

Sctfi

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

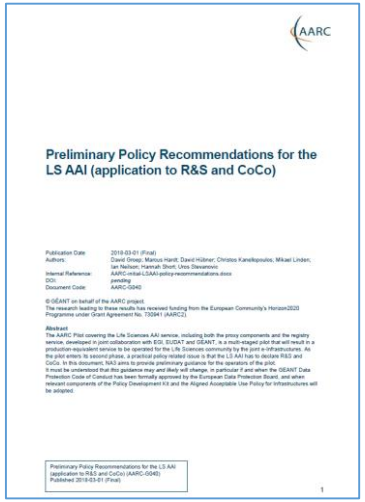
Proxies have their own challenges as well: AUPs, T&Cs, Privacy notices, …

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 to need to be manually configured for each community
  - is automatically updated when services join

as well as for community and dedicated proxies:

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


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

beyond AARC-G040

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

With Fewer Clicks to More Resources!

Helping out the community – a simpler policy toolkit for communities

What we heard and observe:

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

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

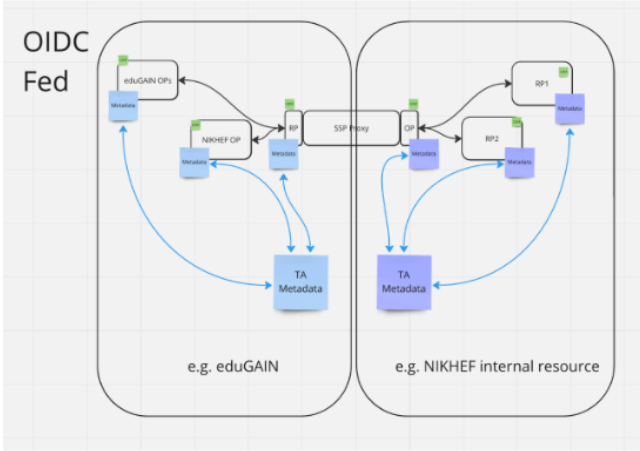
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide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

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

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
- 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 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

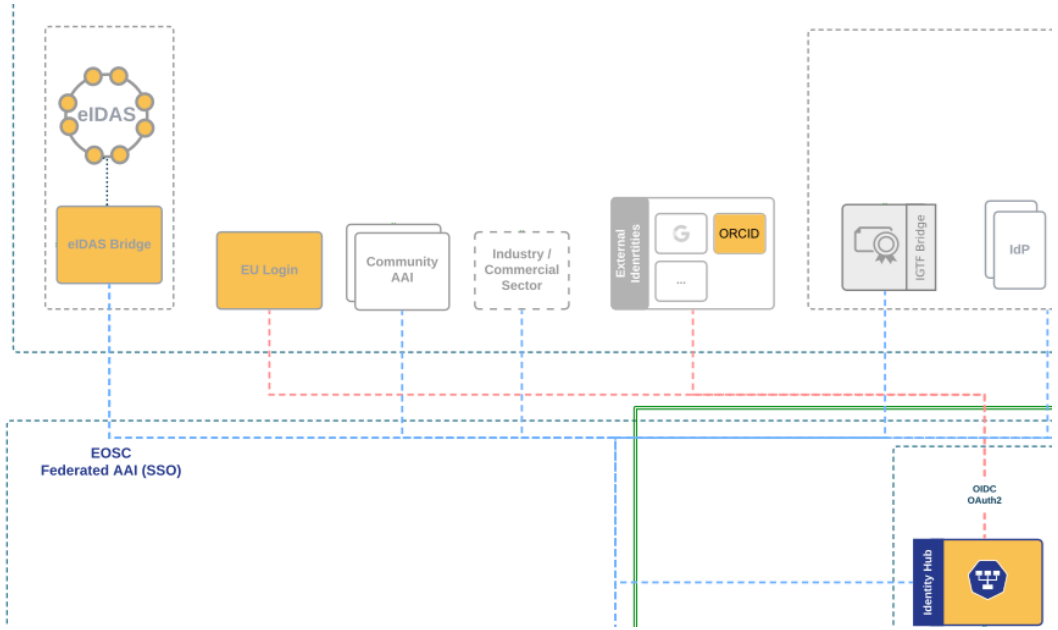
We'll see more diverse sources of identity & assurance anyway

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 the driving factor

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

- we have resources to help FIM4R run a couple of workshops in the next 2 years
- we need community review *and* your ideas and input on both policy and architecture
- start from the high-level requirements and broad community input

really must be a cross-WP activity, engaging everyone in AARC-TREE

Task descriptions allows us to be really supporting to research & infra's!

- The **Operational Trust framework for Community and Infrastructure BPA Proxies** (effort required 9 PM) provides the mechanisms by which Research Infrastructures can engage with the global identity federations by demonstrating their trust baseline and data protection. We will provide the trust- and information security guidelines for both the infrastructure 'membership management' and 'proxy' (aggregator) components in the Architecture beyond the current 'Sirtfi' baseline, created together with the current infrastructure proxies and sectoral provider federations and the research infrastructures(using FIM4R and the WISE information security community forums). The guidelines will become part of the revised Policy Development Kit. The result is a lower barrier to the integration of new research infrastructures and the incumbent (ESFRI) cluster proxies in eduGAIN and EOSC federations.
- Besides the BPA proxy *itself* being a trusted party in federations, the responsible infrastructures themselves also need a framework to ensure their *proxied services* are properly handling data - so that they can participate in federation with confidence. The evolution and implementation of **'Snctfi' Scalable Negotiator for a Community Trust Framework in Federated Infrastructures** (effort required: 4PM) increases acceptance of research infrastructure proxies. This eases the flow of identity and attributes from eduGAIN, leading to a more ef

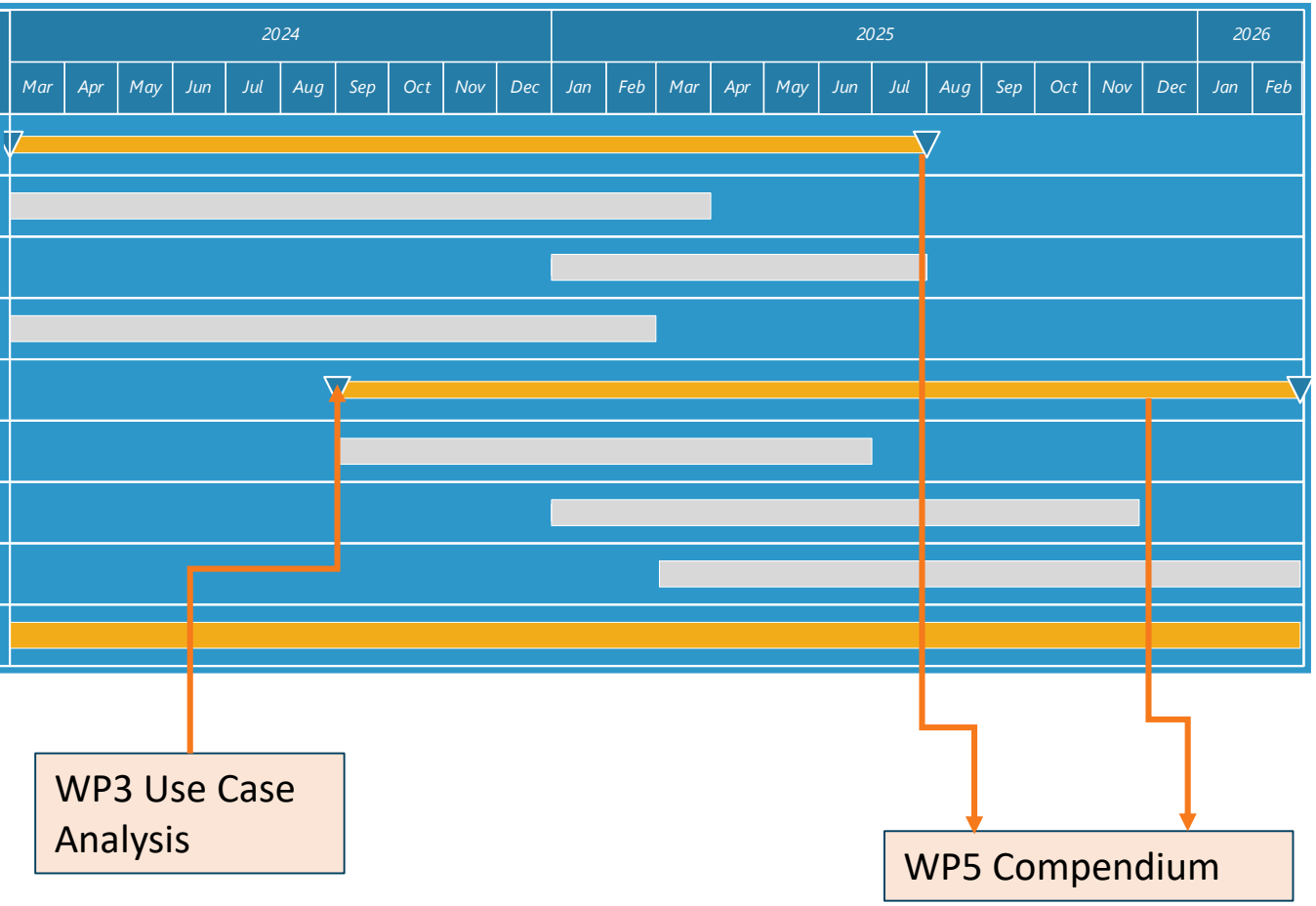
- Users increasingly have to wade through consent and information screens while on the other hand, the proxies struggle with how to present information from large numbers of distinct services in a coherent and the required 'understandable manner' to the user. We will **review infrastructure models for coordinated presentation and aggregation of 'acceptable use policies' and privacy notices**, improving cross-infrastructure user experience (effort required: 8PM). This will result in recommendations on aligning presentations by proxies and presented to AEGIS for adoption by the proxy operators. The expected outcome is increased adoption of the 'WISE Baseline AUP', good-practice privacy notices, and fewer user clicks when accessing research resources.

- Augment the Policy Development Kit with **lightweight community policy templates** (required effort: 6 PM) to enable federated access management for small to mid-sized research groups to research infrastructures. Not having the resources or expertise to maintain their own complex policy suite, we support them through templates and implementation guidance (FAQs) on community structuring, and integration with research infrastructure community AAIs across thematic areas. Analysis of the community *minimum viable policy* is based on the FIM4R requirements and the policies will ease access to services that require identity assurance and traceability of resource use.
- New **guidelines on cross-sectoral trust in novel federated access models** (effort required: 8 PM) support communities that leverage modern ('OpenID Connect Federation' and token-based) federated technologies, using protocols originally devised for just bilateral ('login with big tech') trust. These guidelines enable increased trust i
compromise and cyberattacks for
widely-varying implementation o
peers, and inconsistencies. The gu
identity privacy vs. functional req
validity, scoping, validation, and p

- Increased **assurance in research services through eID identity assertions** (effort required: 8 PM) has proven hard to obtain from home identity providers in the R&E sector. It is more readily available in the European government identity ecosystem, and we will provide an assessment of its applicability for users of research infrastructures dealing with sensitive data through the proxies in the revised AARC BPA model. Step-up to at least a substantial level could then be done at "home" through the user's national eID scheme. If suitability is confirmed, guidelines will be provided via AEGIS.
- To ensure anchoring of user-oriented policies in the research communities, they are developed via a **co-creation process through the FIM4R research communities** forum**,** reviewing the restructured policy development kit and proxy trust framework, together with the new AARC Blueprint Architecture (required effort: 4 PM). This ensures the cross-sectoral use of recommended best practices as well as the global adoption of the European model in collaborating infrastructures. Through joint workshops with WP3 (use cases), we ensure the stakeholder community (research and e-Infrastructures, ESFRI clusters, and nationally-structuring research communities) closes the trust and policy gaps using the joint policy development kit also for large structured communities across the thematic areas represented in FIM4R.

But *when, oh when*?

ID	Task Name	Start	Effort	Partners
1	**Research Infrastructure Alignment & Policy**	**2024-03-01**	**21 PM**	**Nikhef**
2	Operational Trust Frameworks	2024-03-01	9 PM	RAL, Nikhef, NorduNET, EGI, GEANT
3	Service Provider Baselining & Acceptance	2025-01-01	4 PM	RAL, Nikhef, CERN, SURF
4	Coordinated AUPs, T&Cs and Privacy Notices	2024-03-01	8 PM	RAL, Nikhef, EGI, GRNET, KIT, MU GEANT
5	**User-Centric Trust Alignment & Harmonisation**	**2024-09-02**	**26 PM**	**RAL**
6	Lightweight Community Structures	2024-09-02	5 PM	EGI, CERN, KIT, SURF, GEANT
7	cross-sectoral trust in novel federated access models	2025-01-01	9 PM	RAL, Nikhef, EGI, GRNET, KIT, KIFU
8	assurance in research services through eID identity assertions	2025-03-03	8 PM	NorduNET, EGI, SURF, MU, GEANT
9	Co-creation with FIM4R (with WP3+)	2024-03-01	4 PM	RAL, Nikhef, NorduNET



Deliverables

	Deliverable name	Short description	#WP	Lead	Type	Due
M2.1	Guidance for notice management by proxies	*Guideline submitted to AEGIS*				M10
D2.1	**Trust framework for proxies and Snctfi research services**	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	*Report submitted to AEGIS*				M18
D2.2	**AARC Policy Development Kit Revision**	Evolved suite of guidelines and templates for research and infrastructure communities	WP2	Nikhef	R	M24

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

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

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!

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

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).