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

IGTF EUGridPMA+62 AARC meeting
Amsterdam, September 2024

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

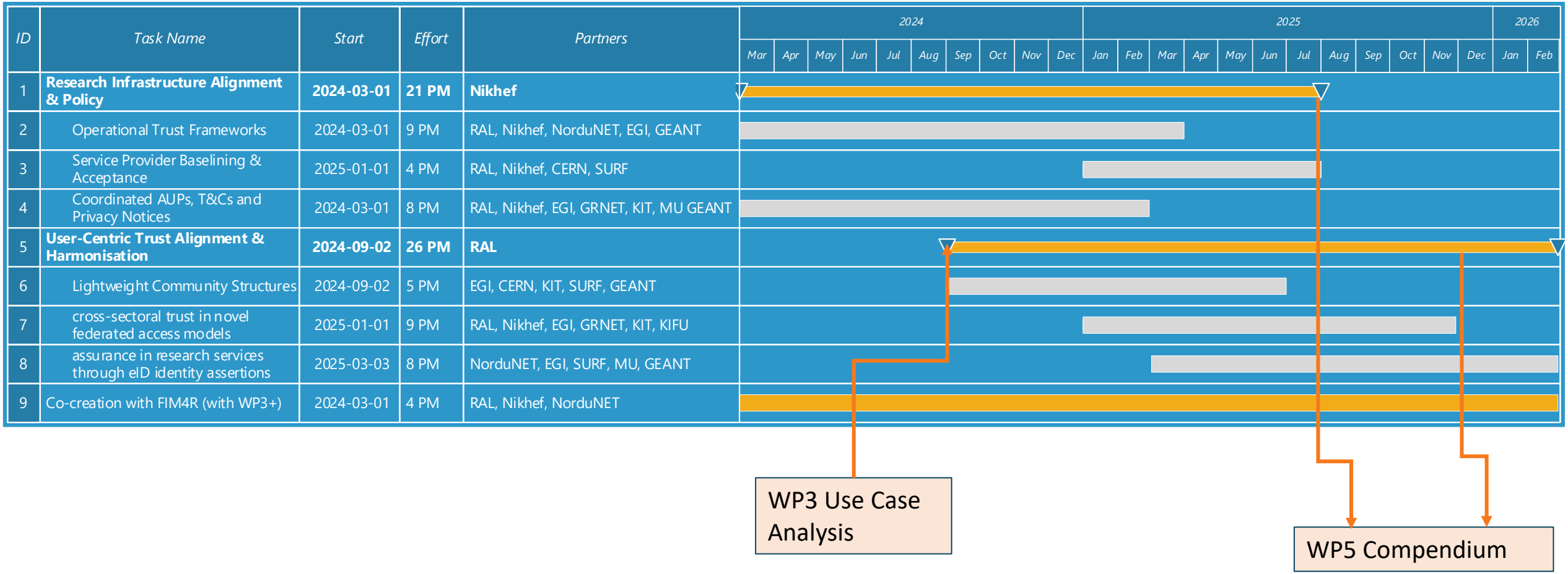
Effort in AARC TREE to address issues and explore policy needs

- 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 …

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



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

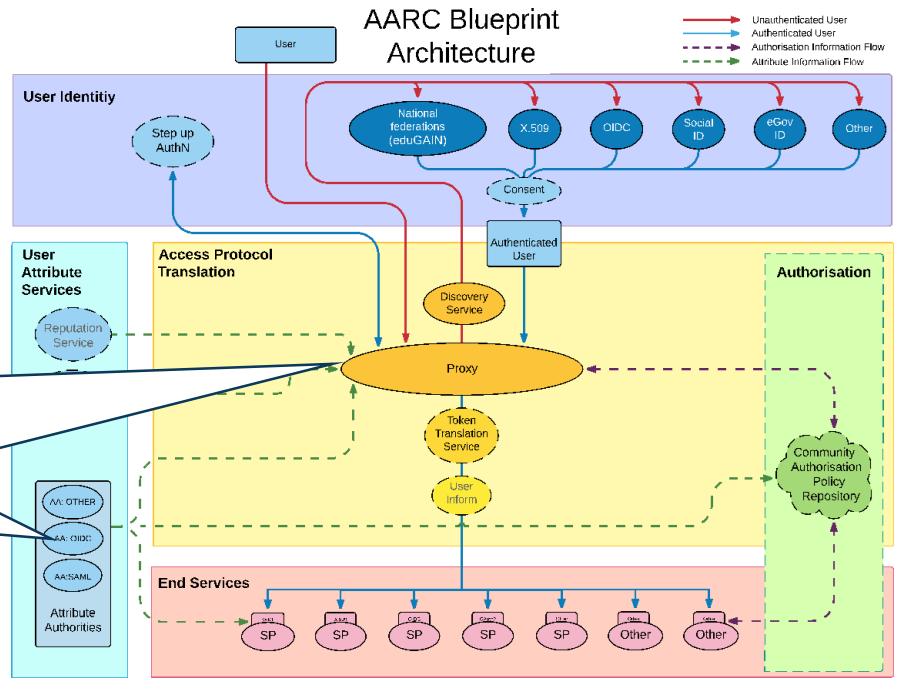
and thereby encourage trust in the proxies *and* their connected services

Evolving AARC G071 to a Baseline: 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/

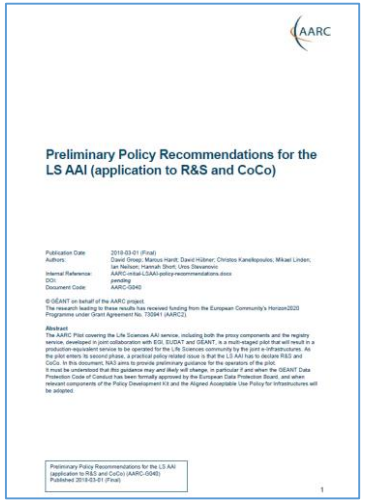
Proxies, AUPs, T&Cs, Privacy notices, … managing notice management

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!

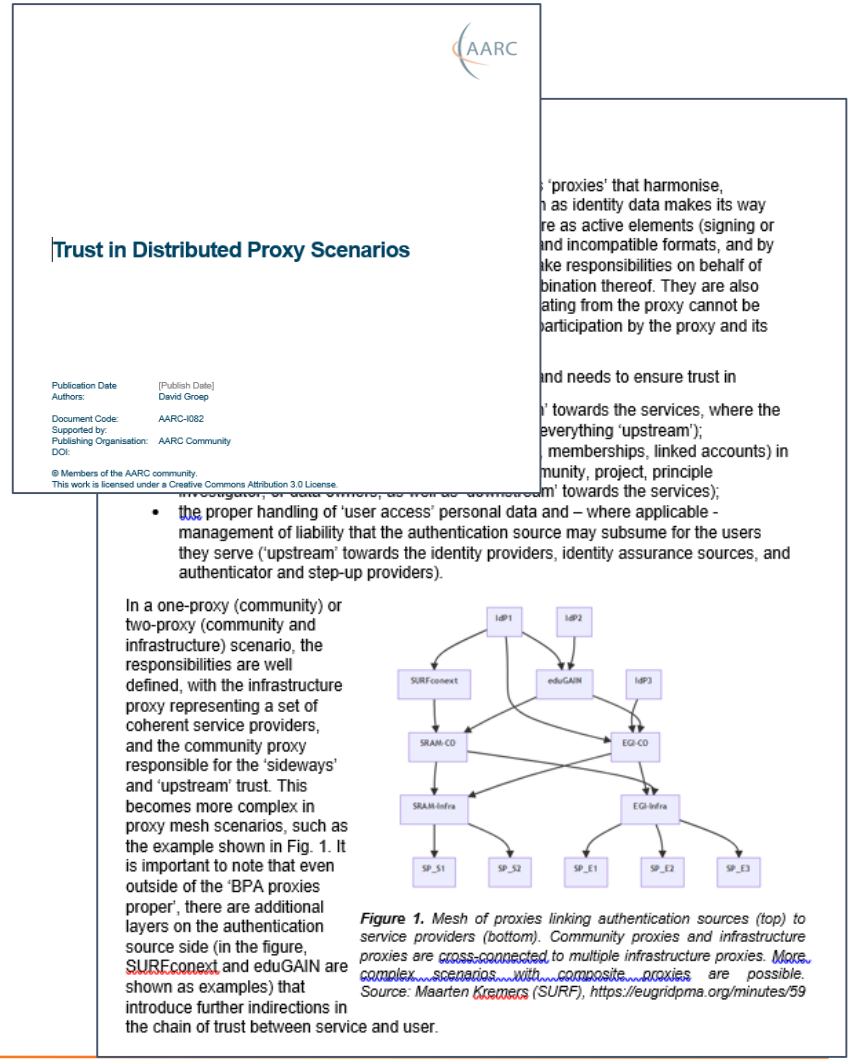
Framing the requirements for proxies ('G082')

AARC-I082

Trust in Distributed Proxy Scenarios

Table of Contents

https://drive.google.com/drive/folders/1DOi77I0Tfu04AUVWKiaDDMhfLIF5yMxD



AARC

Trust in Distributed Proxy Scenarios

Publication Date [Publish Date]
Authors: David Groep

Document Code: AARC-I082
Supported by:
Publishing Organisation: AARC Community
DOI:

'proxies' that harmonise,
as identity data makes its way
re as active elements (signing or
nd incompatible formats, and by
ke responsibilities on behalf of
bination thereof. They are also
ating from the proxy cannot be
articipation by the proxy and its

nd needs to ensure trust in

' towards the services, where the
everything 'upstream');
memberships, linked accounts) in
munity, project, principle
m' towards the services);

- the proper handling of 'user access' personal data and – where applicable - management of liability that the authentication source may subsume for the users they serve ('upstream' towards the identity providers, identity assurance sources, and authenticator and step-up providers).

In a one-proxy (community) or two-proxy (community and infrastructure) scenario, the responsibilities are well defined, with the infrastructure proxy representing a set of coherent service providers, and the community proxy responsible for the 'sideways' and 'upstream' trust. This becomes more complex in proxy mesh scenarios, such as the example shown in Fig. 1. It is important to note that even outside of the 'BPA proxies proper', there are additional layers on the authentication source side (in the figure, SURFconext and eduGAIN are shown as examples) that introduce further indirections in the chain of trust between service and user.

Figure 1. *Mesh of proxies linking authentication sources (top) to service providers (bottom). Community proxies and infrastructure proxies are cross-connected to multiple infrastructure proxies. More complex scenarios with composite proxies are possible. Source: Maarten Kremers (SURF), https://eugridpma.org/minutes/59*

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

T2: Evolving community policy support

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

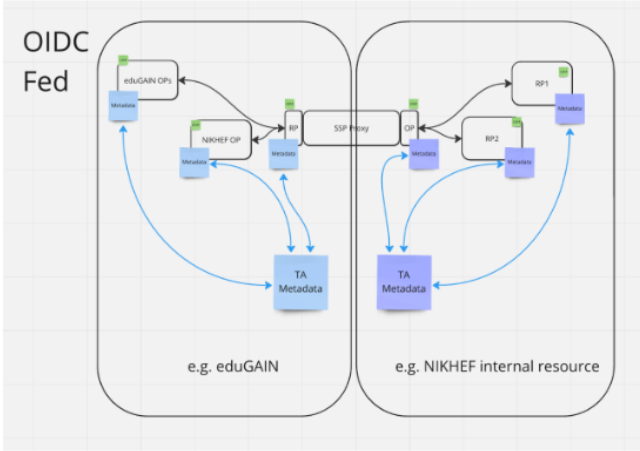
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide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

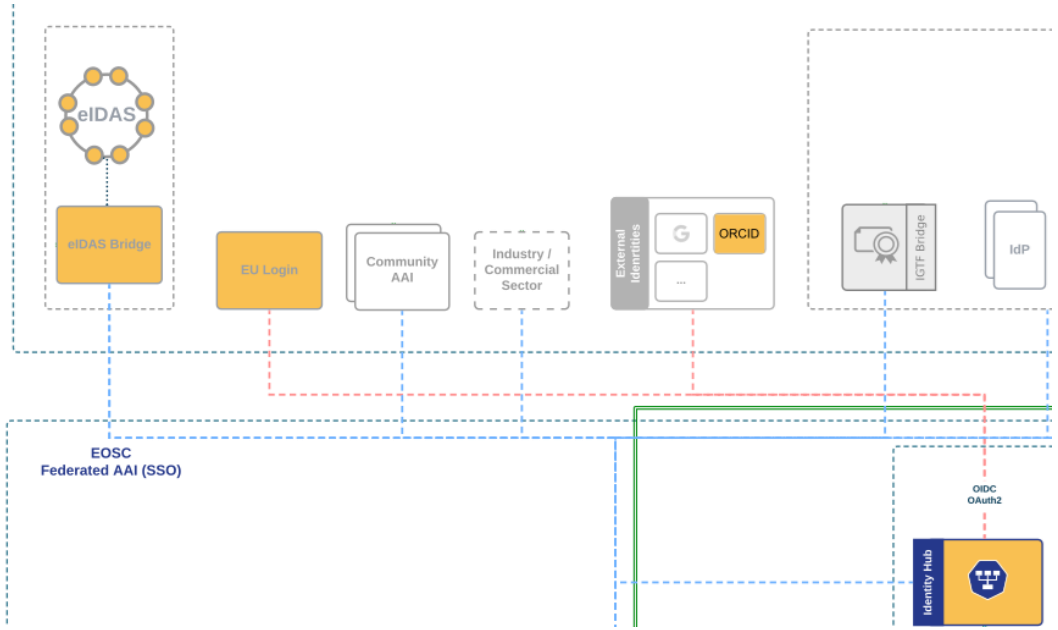
We'll see more diverse sources of identity & assurance anyway

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



Deliverables

	Deliverable name	Short description	#WP	Lead	Type	Due
M2.1	Guidance for notice management by proxies	*Guideline submitted to AEGIS ('G040+')*				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 ('G082')	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

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).