



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 Physics Data Processing programme and UM Dept. Advanced Computing Sciences

IGTF EUGridPMA+ 63 AARC meeting

Geneva, February 2025

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 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)
- **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')

Generalised consolidated Security Operational Baseline from PDK+EOSC + relation to G071



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

Consider federation models, Wallet VCs, and assurance step-up via gov eID VCs together?

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

Overview of main policy activities (and AARC TREE project interactions)

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

WP3 Use Case Analysis

WP5 Compendium

We did AARC G083 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

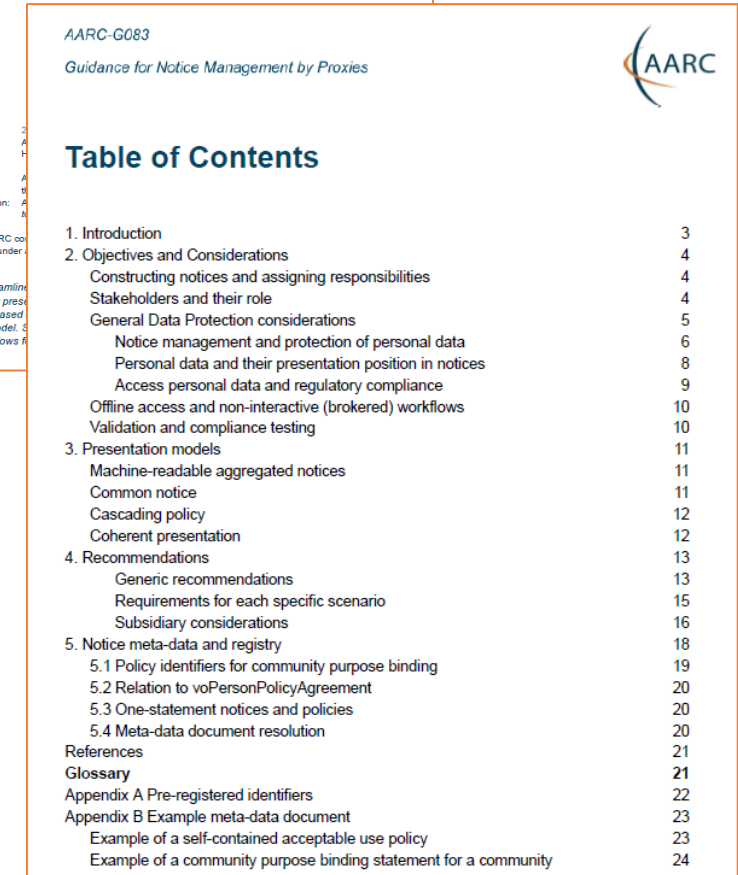
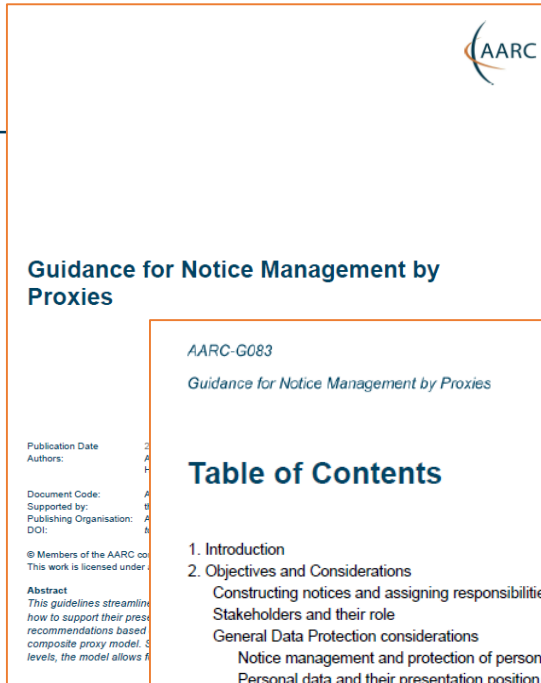


Table of Contents	
1. Introduction	3
2. Objectives and Considerations	4
Constructing notices and assigning responsibilities	4
Stakeholders and their role	4
General Data Protection considerations	5
Notice management and protection of personal data	6
Personal data and their presentation position in notices	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 {
  "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 betref
network en computers bij Nikhef. Iedere gebruiker van
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"
}

```

Framing the requirements for proxies ('G082')

AARC-I082

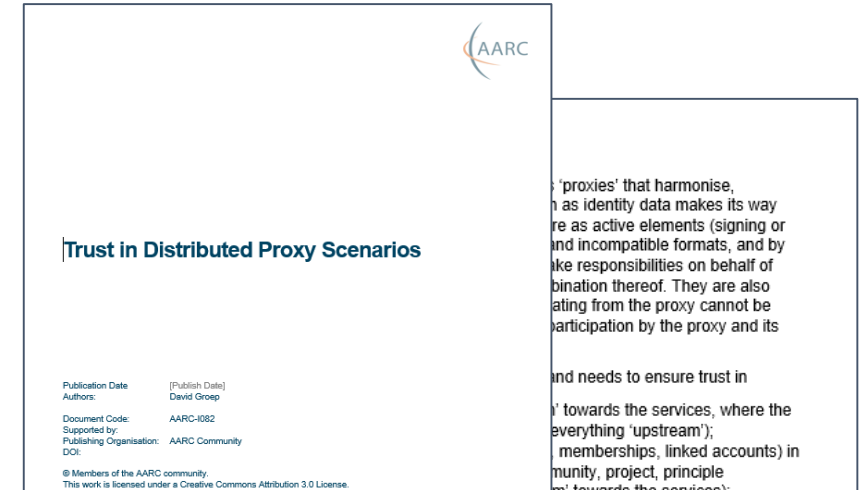
Trust in Distributed Proxy Scenarios



Table of Contents

1. Introduction.....	2
2. Context and related guidelines.....	4
2.1. Security Operational Baseline.....	4
2.2. AAOPS proxy operations.....	4
2.3. Sirtfi and incident response.....	4
3. Composite proxies and challenges.....	4
4. User experience.....	5
4.1. Owning consent.....	5
4.2. Transitive trust for services through chained proxies.....	5
5. Operational models for proxies.....	5
6. Recommendations.....	5

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



'proxies' that harmonise, as identity data makes its way through as active elements (signing or signing and incompatible formats, and by taking responsibilities on behalf of the user on behalf of the combination thereof. They are also acting on behalf of the proxy and its participation by the proxy and its

and needs to ensure trust in the chain of trust towards the services, where the proxy acts as 'everything upstream'; the proxy acts as a membership, linked accounts) in the community, project, principle and 'upstream' 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, SURFconnect and eduGAIN are shown as examples) that introduce further indirections in the chain of trust between service and user.

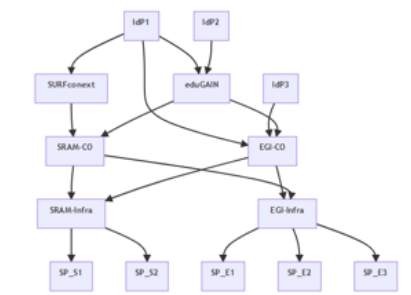


Figure 1. Mesh of proxies linking authentication sources (top) to service providers (bottom). Community proxies and infrastructure proxies are cross-connected to multiple infrastructure proxies. More complex scenarios with composite proxies are possible. Source: Maarten Krommes (SURF), <https://eugridpma.org/minutes/59>

Trust framework for proxies and Snctfi research services

guidelines & good practice for BPA proxies - interaction with research services

- Define the structure for the new PDK, with policies, procedure templates, and guidelines
- Discuss proxy transparency ... should middle things be transparent or not. Or how?
- Transitive trust
- ...



Could this constitute a new 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

- 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

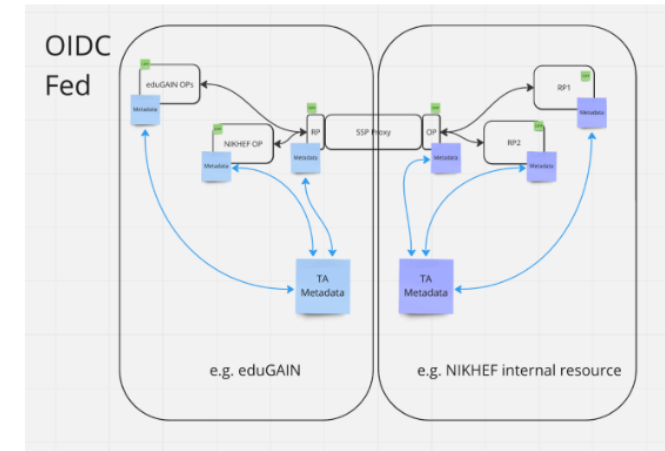
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide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

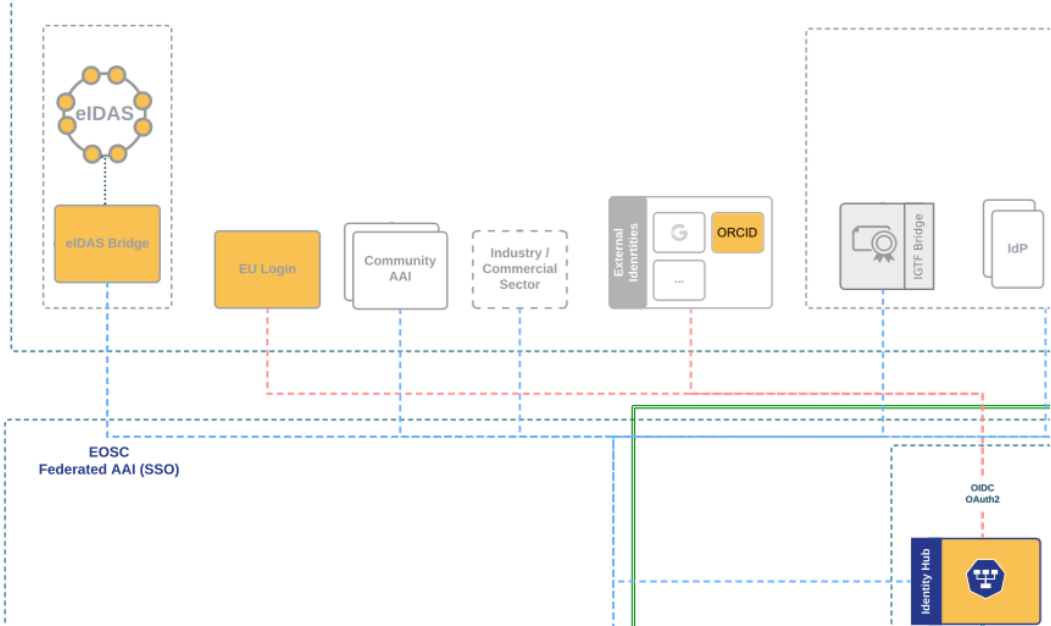
We'll see more diverse sources of identity & assurance anyway

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



Deliverables



	Deliverable name	Short description	#WP	Lead	Type	Due
M2.1	Guidance for notice management by proxies	<i>Guideline submitted to AEGIS ('G040+')</i>				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	<i>Report submitted to AEGIS</i>				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!

	AARC										
	STFC	Nikhef	NDN	EGI	CERN	GRNET	KIT	SURF	GEANT		SUM
Work item	PM	PM	PM	PM	PM	PM	PM	PM	PM	PM	PM
Research Infra Alignment (Nikhef)											21
Operational Trust for Proxies	★★	★★	★	★★						★★	★★★★
‘Snctfi’ R&E Baseline & 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>

© 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).

