Authentication and Authorisation for Research and Collaboration

AARC TREE – Policy and good practice harmonisation

WP2

David Groep[†], Dave Kelsey[‡]
AARC TREE WP2 Leads

[†]Nikhef and Maastricht University
[‡]Rutherford Laboratory (STFC-UKRI)

AARC TREE project meeting
Reading, UK, April 2, 2025

AARC beyond incumbent practices and policies?

Current Policy Development Kit 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 Person	Infrastructure Management & Data Contact	Rese Com Servi by)		
Priva	Infr	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)			

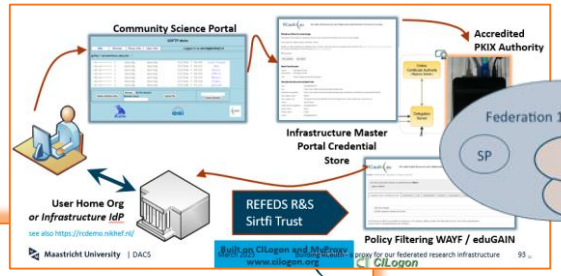
Showing 1 to 9 of 9 entries Previous Next

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 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.



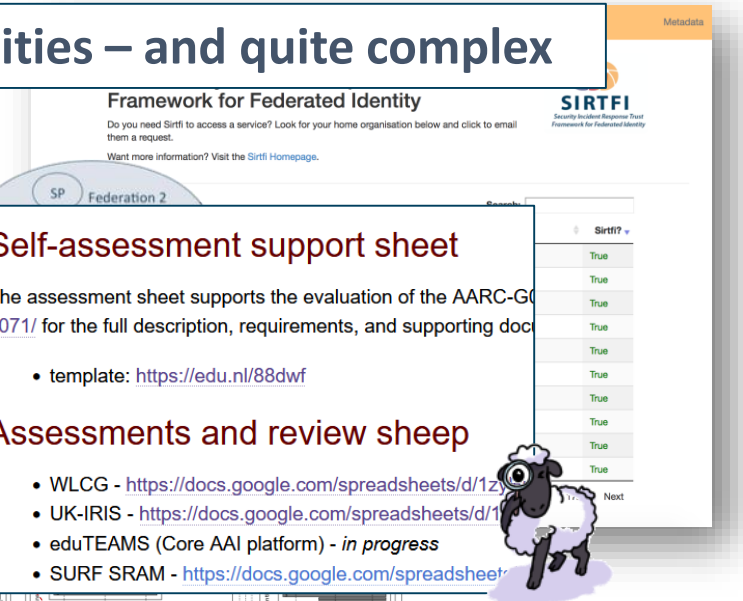
Data Protection Impact Assessment - an initial guide for communities

Publication Date 2018-04-30
Authors: Uros Stevanovic;David Groep;Ian Neilson;Stefan Paetow;Wolfgang Pempe
DOI: *assignment deferred*
Document Code: AARC-G042

© 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
This report presents the results of the desk 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 risks 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 FIM 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

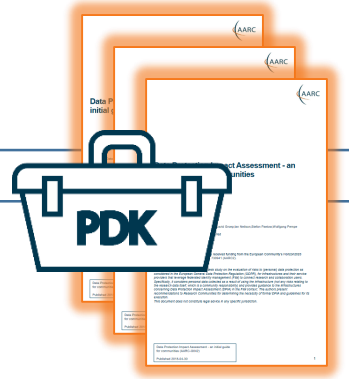


AARC-I050
Comparison Guide to Identity Assurance Mappings for Infrastructures

Two-pronged approach for policy and good practice for AARC BPA 2025

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’

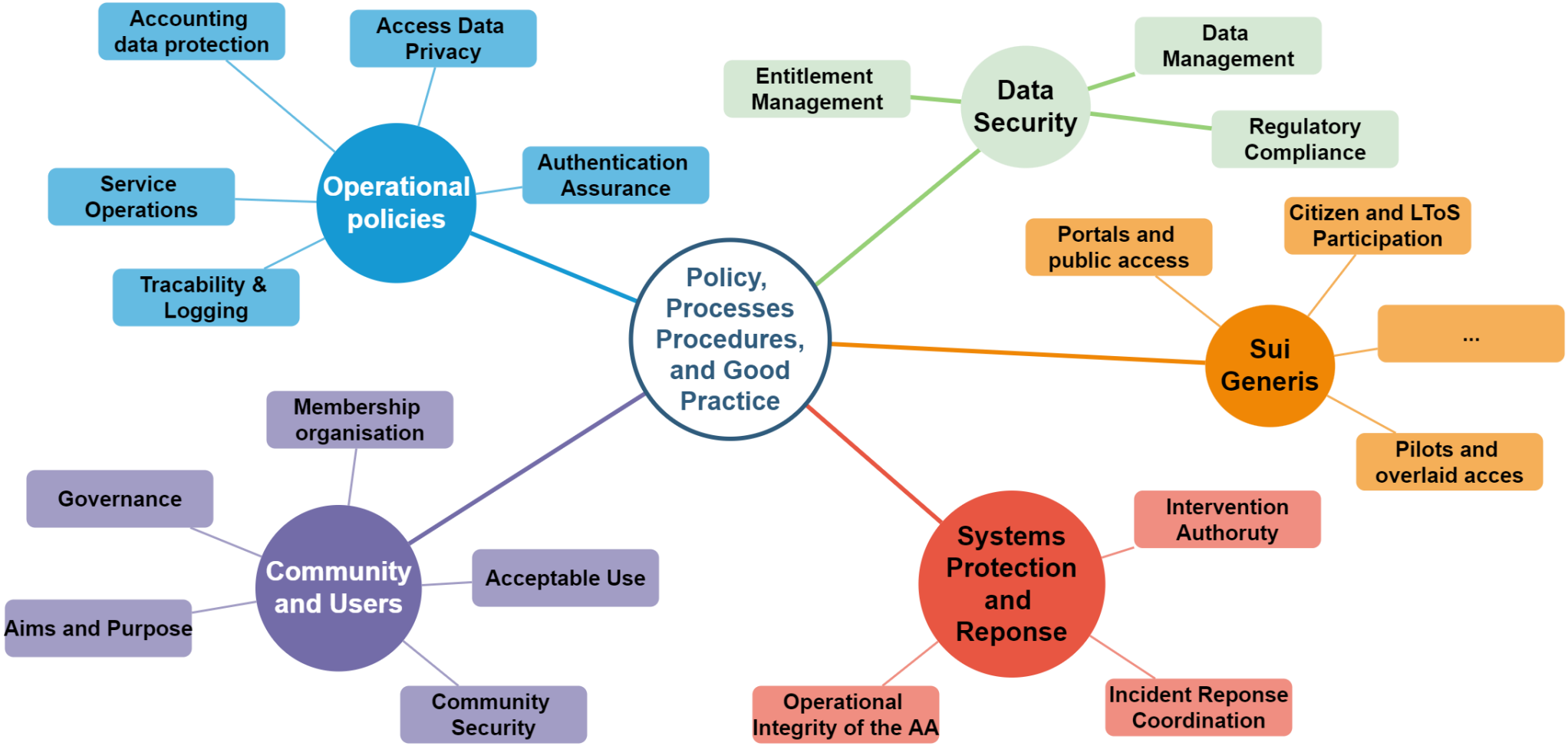
- Lightweight community management policy template
- Guideline on cross-sectoral trust in novel federated access models
- Assurance in research services through (eIDAS) public identity assertion

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

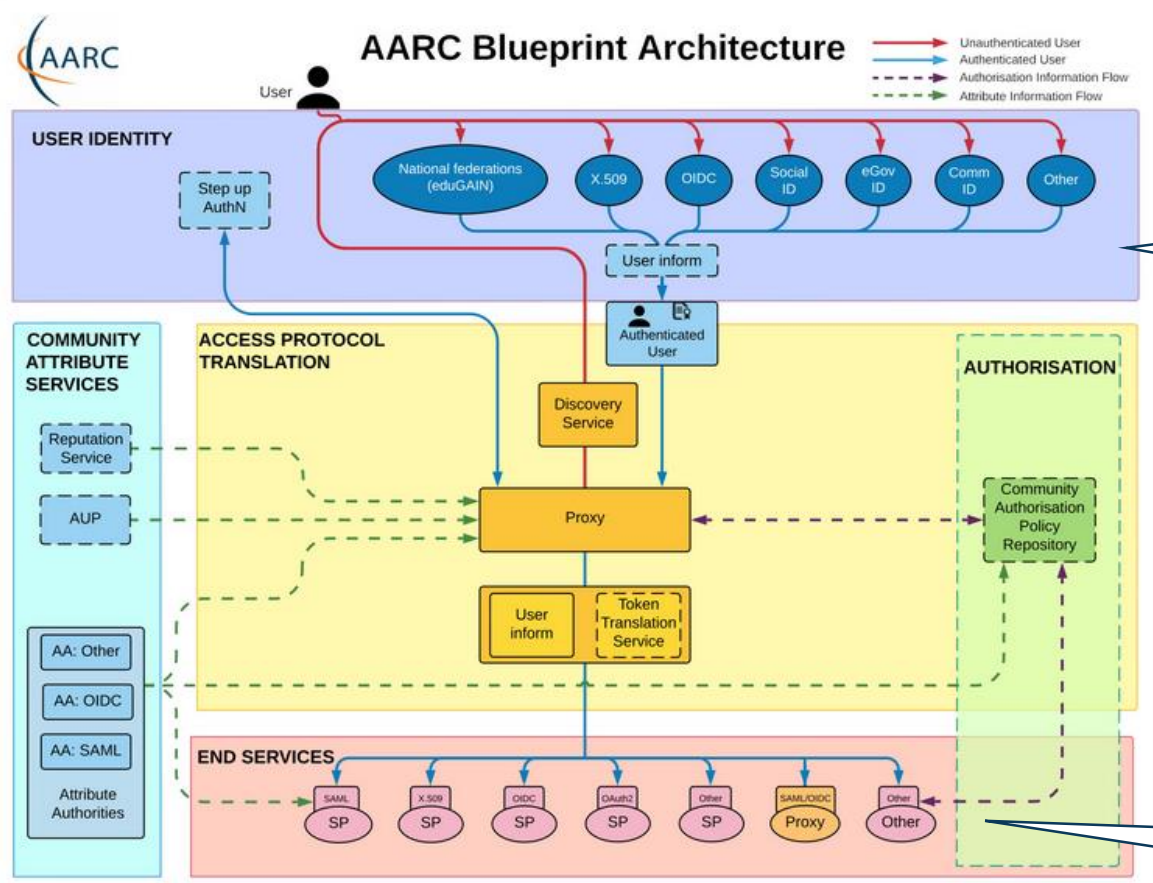
WP2 Policy Deliverables

	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

Many policy aspects and trusted security practices to consider!



Practices we already have, practices we need to harmonise



Authentication/identity sources
NIST SP800-63
FIPS140
ISO 27001
IGTF AP Profiles
REFEDS MFA
REFEDS Assurance Framework

AARC-G071
for the Community Attribute Authority (AA) and operation of the Proxy

Service provider operations
ISO27k
NIS2
ITSRM2

 while for identity sources and for services there is extensive normalisation, our AARC BPA 'proxy' did not …

Proxy Operations: Information Security and Security Operational Baseline

‘address information security for disciplines and infrastructures - some of which process sensitive data’

Baseline Service Security policy

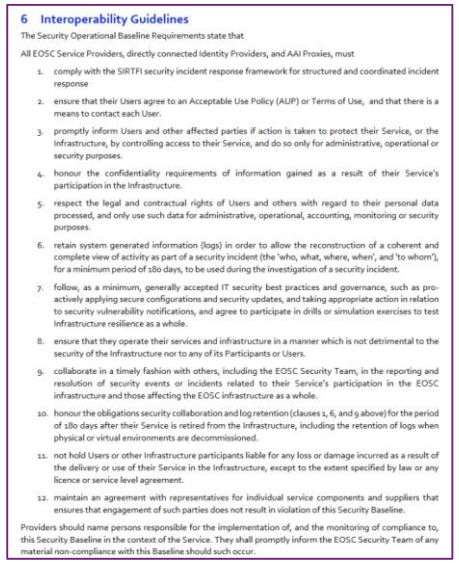
the AARC PDK v1 was very successful, but diverged in several directions:

- national implementations and specialisations
- was included in the EOSC Interoperability Framework as the ‘Security Operational Baseline’

but has not been brought home to the broader research community – yet …

AARC TREE now re-aligning these in the new PDK - **with guidance and FAQs**

Just ported it back as AARC-G084



6 Interoperability Guidelines

The Security Operational Baseline Requirements state that

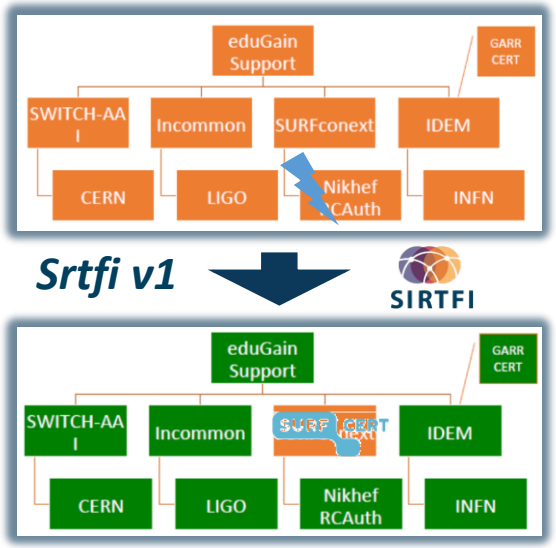
All EOSC Service Providers, directly connected Identity Providers, and AAI Proxies, must

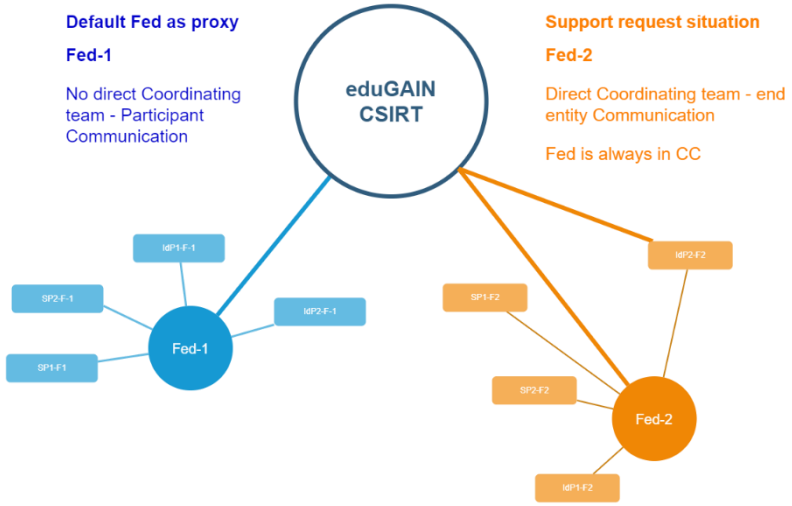
1. comply with the SIRTFI security incident response framework for structured and coordinated incident response
2. ensure that their Users agree to an Acceptable Use Policy (AUP) or Terms of Use, and that there is a means to contact each User.
3. promptly inform Users and other affected parties if action is taken to protect their Service, or the Infrastructure, by controlling access to their Service, and do so only for administrative, operational or security purposes.
4. honour the confidentiality requirements of information gained as a result of their Service's participation in the Infrastructure.
5. respect the legal and contractual rights of Users and others with regard to their personal data processed, and only use such data for administrative, operational, accounting, monitoring or security purposes.
6. retain system generated information (logs) in order to allow the reconstruction of a coherent and complete view of activity as part of a security incident (the 'who, what, where, when', and 'to whom'), for a minimum period of 180 days, to be used during the investigation of a security incident.
7. follow, as a minimum, generally accepted IT security best practices and governance, such as pro-actively applying secure configurations and security updates, and taking appropriate action in relation to security vulnerability notifications, and agree to participate in drills or simulation exercises to test Infrastructure resilience as a whole.
8. ensure that they operate their services and infrastructure in a manner which is not detrimental to the security of the Infrastructure nor to any of its Participants or Users.
9. collaborate in a timely fashion with others, including the EOSC Security Team, in the reporting and resolution of security events or incidents related to their Service's participation in the EOSC infrastructure and those affecting the EOSC infrastructure as a whole.
10. honour the obligations security collaboration and log retention (clauses 1, 6, and 9 above) for the period of 180 days after their Service is retired from the Infrastructure, including the retention of logs when physical or virtual environments are decommissioned.
11. not hold Users or other Infrastructure participants liable for any loss or damage incurred as a result of the delivery or use of their Service in the Infrastructure, except to the extent specified by law or any licence or service level agreement.
12. maintain an agreement with representatives for individual service components and suppliers that ensures that engagement of such parties does not result in violation of this Security Baseline.

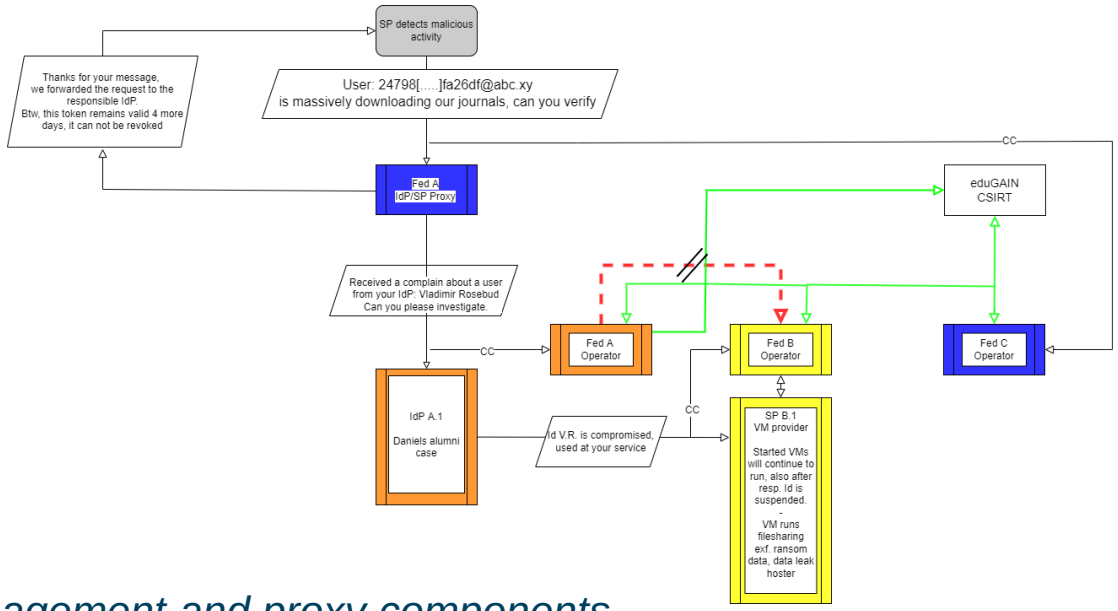
Providers should name persons responsible for the implementation of, and the monitoring of compliance to, this Security Baseline in the context of the Service. They shall promptly inform the EOSC Security Team of any material non-compliance with this Baseline should such occur.

https://doi.org/10.5281/zenodo.7396724

Response and traceability across IdP-SP Proxies: beyond 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 'Enabling Communities' and eduGAIN CSIRT

images: AARC Sirtfi v1 exercise (Hannah Short), eduGAIN security TTX (Sven Gabriel, eduGAIN CSIRT)

With fewer clicks to more resources – while keeping the user informed

reference models for acceptable use policy and privacy notice collection to improve cross-infrastructure user experience

EUROPEAN COMMISSION
DG COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY

Directorate C - Enabling and Emerging Technologies
Unit C.1 - High Performance Computing and Applications

EOSC EU Node User Access Policy

Version 1.0

USER ACCESS POLICY

1. Purpose

This User Access Policy ("UAP") defines the access groups, their corresponding access rights, service limits, and virtual credit allocation policies for the users of the EOSC EU Node's Resources ("*Resources*") and Services ("*Services*") as g
Commission, Directorate-General for Communications Networ
Unit C.1 High Performance Computing and Applications (herei
"*Operating Unit*"). This policy ensures users have the appropria
their role and affiliation while maintaining system integrity, sec
regulations and applicable law.

2. Scope

This policy applies to all users of the EOSC EU Node, covering

EGI Configuration Database Acceptable Use Policy and Conditions of Use (AUP)

This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services ("Services") as granted by the EGI Federation, and the Virtual Organisation to which you belong, for the purpose of meeting the goals of EGI, namely to deliver advanced computing services to support researchers, multinational projects and research infrastructures, and the goals of your Virtual Organisation or Research Community.

1. You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show consideration towards other users including by not causing harm to the Services; you have an obligation to collaborate in the resolution of issues arising from your use of the Services.
2. You shall only use the Services for lawful purposes and not breach, attempt to breach, nor circumvent administrative or security controls.
3. You shall respect intellectual property and confidentiality agreements.
4. You shall protect your access credentials (e.g. passwords, private keys or multi-factor tokens); no intentional sharing is permitted.
5. You shall keep your registered information correct and up to date.

edential compromise, or misuse to the security contact
ssuing authorities.

applicable service level agreements listed below. Use

atements referenced below.

istrative, operational, or security reasons, without prior

hich may include your account being suspended and a

omepage.

Acceptable Use Policy

text This Acceptable Use Policy applies to all members o
the VO, with reference to use of the European Grid Infras
The BiG Grid Executive Team owns and gives authority to
Goal and description of the Xenon VO

The Xenon VO xenon.biggrid.nl is the incubator grid community for work on the international Xenon 1T and related experiments in the search for dark matter. Members of the VO will work to build, understand and analyse the detector and resutls related to the Xenon experiment and to "Monte-Carlo" studies that will be used to design, build and understand the detector, as well as work with the supporting computing infrastructure to make this happen. Members and Managers of the VO agree to be bound by the Grid Acceptable Usage Rules, VO Security Policy and other relevant Grid Policies, and to use the Grid only in the furtherance of the stated goal of the VO.

ATLAS Analysis Facility at UChicago

Dashboard

Home / AUP

Acceptable Use Policy

Your use of the ATLAS Analysis Facility at UChicago shall imply acceptance of the following agreement:

I have read and agree to the terms and conditions of the WLCG Computing Grid and the ATLAS VO Acceptable Use Policy.

WLCG Terms of Use and Acceptable Use Policy

By registering with the Virtual Organization (the "VO") as a GRID user you shall be deemed to accept these conditions of use:

1) You shall only use the GRID to perform work, or transmit or store data consistent with the stated goals and policies of the VO of which you are a member and in compliance with these conditions of use.

2) You shall not use the GRID for any unlawful purpose and not (attempt to) breach or circumvent any GRID administrative or security controls. You shall respect copyright and confidentiality agreements and protect your GRID credentials (e.g. private keys, passwords), sensitive data and files.

3) You shall immediately report any known or suspected security breach or misuse of the GRID or GRID credentials to the incident reporting locations specified by the VO and to the relevant credential issuing authorities.

4) Use of the GRID is at your own risk. There is no guarantee that the GRID will be available at any time or that it will suit any purpose.

5) Logged information, including information provided by you for registration purposes, shall be used for administrative, operational, accounting, monitoring and security purposes only. This information may be disclosed to other organizations anywhere in the world for these purposes. Although efforts are made to maintain confidentiality, no guarantees are given.

6) The Resource Providers, the VOs and the GRID operators are entitled to regulate and terminate access for administrative, operational and security purposes and you shall immediately comply with their instructions. You are liable for the consequences of any violation by you of these conditions of use.

ATLAS VO Acceptable Use Policy

This Acceptable Use Policy applies to all members of the ATLAS Virtual Organisation, hereafter referred to as the VO, with reference to use of the Worldwide LCG (wLCG) Grid

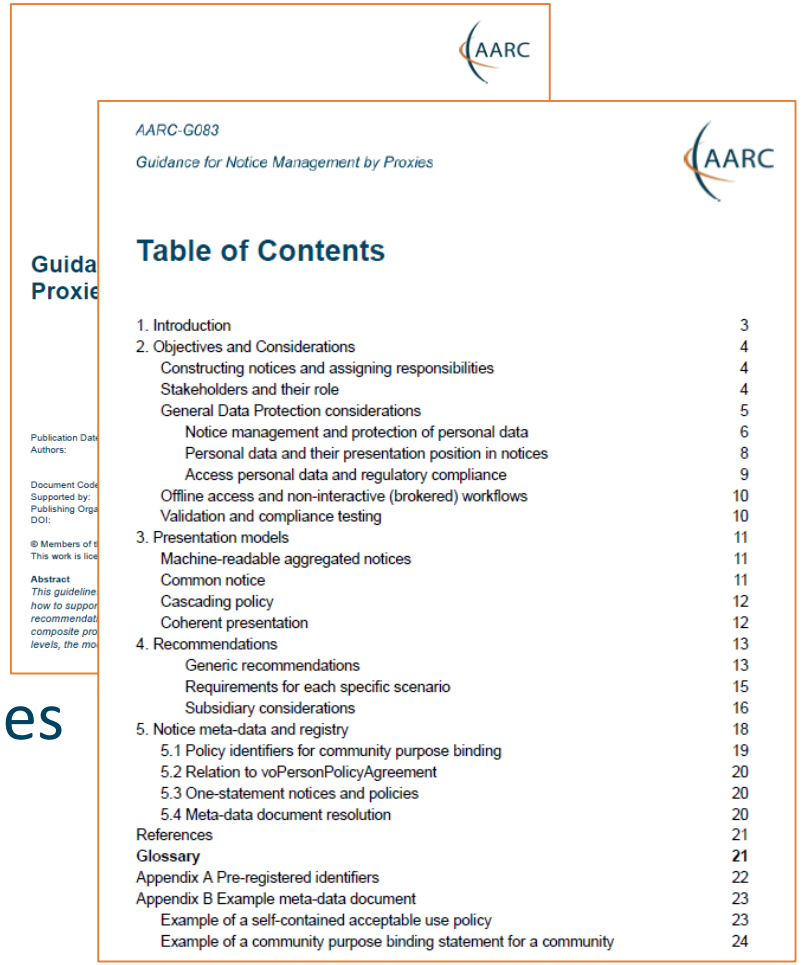
New AARC guidance on Notice Management by Proxies (AARC-G083)

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)

Recommend WISE Baseline AUP plus model to **construct notices and communicate acceptance** based on the AARC ID-community-infra 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



AARC-G083

Guidance for Notice Management by Proxies

Table of Contents

Developing the Trust framework, guidelines and best practice for BPA proxies and interaction with research services

minimise the number of divergent policies
empower identity providers, service providers, user communities to rely on interoperable policies

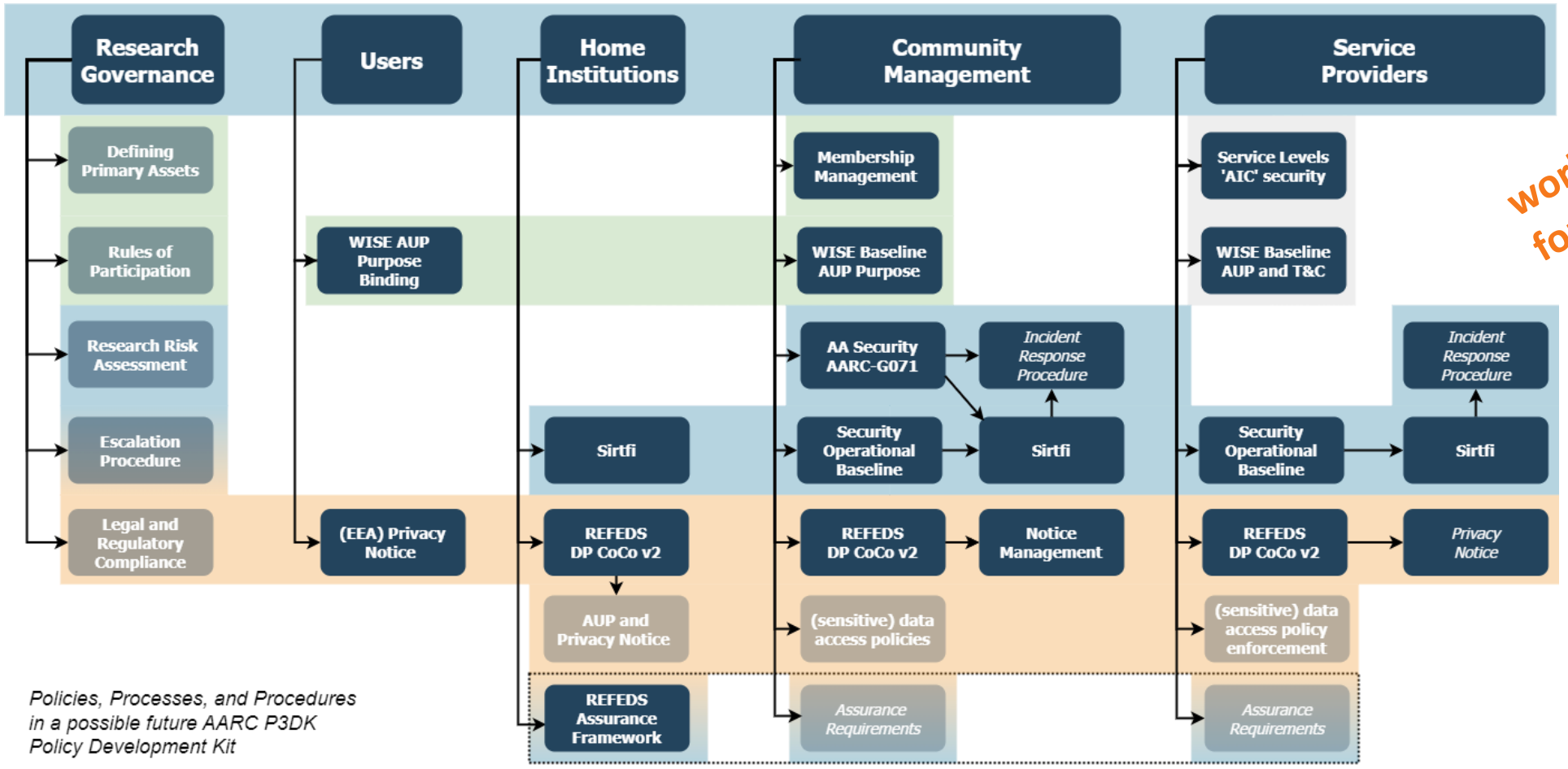
From the old PDK to a new
Policy, Process, and Procedure Development Kit ('P3DK')

Simplify!

- comprehensive review of the existing policy suite
- input from national research infrastructures and nodes
- not *only* in Europe but e.g. also Australia
- leverage the works we co-created with REFEDS and EOSC

https://aarc-community.org/policies/policy-development-kit/

Building the trust framework: development of the new P3DK structure

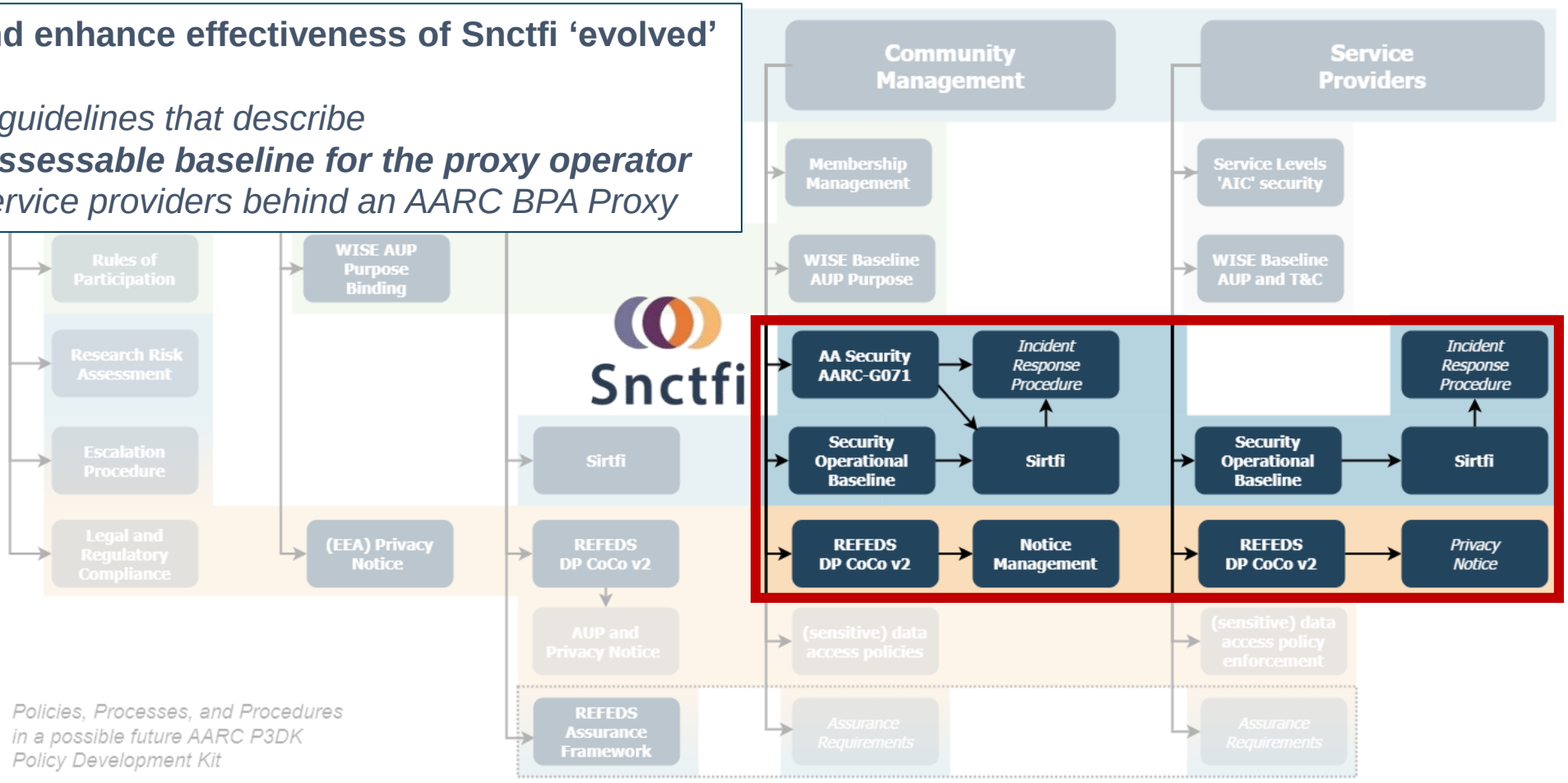


work in progress for D2.1 (May '25)

AAI infrastructure providers for communities: a new 'Snctfi' trust mark

review and enhance effectiveness of Snctfi 'evolved'

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

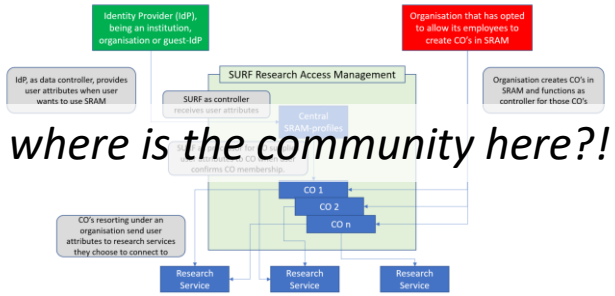


Helping out the community – a simpler policy toolkit for communities

provide a revised policy development kit for mid-sized communities using the research infrastructures

Requirement from the AAI operators in FIM4R and BPA operators:

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



where is the community here?!

But both communities and operators of membership management services are today unclear about trust assurance level of members: current templates in toolkit too complex and prescriptive

work in progress for user trust alignment

- develop 'minimum viable community management' for most small and mid-sized use cases
- give template and implementation guidance (FAQ) on community lifecycle management
- leverage complement of PDK practices that communities can 'source' from trusted providers

Simplified Community Management policy – down to five items!

Each Community must

- Have a **unique name** (we recommend use DNS domain names)
- Require **members to accept an AUP** that defines the community goals and does not conflict with the Infrastructure AUP. It is recommended for the AUP to include the WISE Baseline AUP and follow the (AARC G083) notice management scheme
- Inform members about how their **personal information is processed**, follow local legal and regulatory requirements (e.g. by means of a Privacy Notice)
- Ensure its **members and their authorizations are valid** and enforced (e.g. who is an administrator and who is in which group)
- Be prepared for, and collaborate in, **security incident response**. You should be able to trace and take action on user accounts, and be prepared to participate in resilience exercises. Ensure that your provider can and will participate in incident response and meets security requirements including *Sirtfi* by providing contacts and sufficient logging.

PDK 2.0 Lightweight Community Security Policy

INTRODUCTION

Access to Infrastructure resources is commonly granted to members of a Community. To help protect those resources from damage or misuse, a Community has responsibilities in the manner it manages its membership and the way it behaves towards the Infrastructure. This policy aims to establish a sufficient level of trust to enable reliable and secure Infrastructure operation.

Guidance on this implementation is available in the References and Notes section, which may be updated from time to time, and does not form part of the effective policy.

DEFINITIONS

Entities identified by a leading capital letter in this document are defined in the Infrastructure Security Policy.

SCOPE

This policy applies to each Community whose members make use of the Infrastructure.

POLICY

Each Community must

1. Have a unique name -> recommend use DNS
2. Require members to accept an AUP that defines the community goals and does not conflict with the Infrastructure AUP. It is recommended for the AUP to include the WISE Baseline AUP and follow the (AARC G083) notice management scheme
3. Inform members about how their personal information is processed, follow local legal and regulatory requirements (e.g. by means of a Privacy Notice)
4. Ensure its members and their authorizations are valid and enforced (e.g. who is an administrator and who is in which group)
5. Be prepared for, and collaborate in, security incident response. You should be able to trace and take action on user accounts, and be prepared to participate in resilience exercises. Ensure that your provider can and will participate in incident response and meets security requirements including *Sirtfi* by providing contacts and sufficient logging.

work in progress for user trust alignment

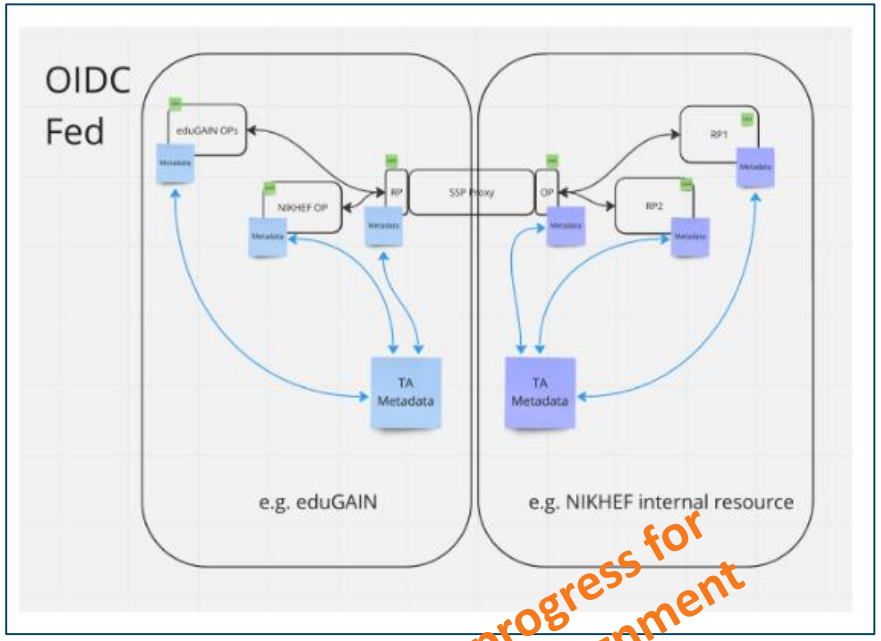
Can we build on a trusted baseline and expectations to increase acceptance of research infrastructure proxies with R&E identity providers

guidelines on cross-sectoral trust in novel federated access models

Even though *unique identifier, name, email, and affiliation* are most relevant 'home' attributes, we

- still need assurance statements and know attribute freshness
- we have proxies met with scepticism by IdPs:
  lack of personalised and R&S attributes
- do trust qualities 'traverse' proxies?
- can operators rely on their 'downstream' providers?

Does more trust in proxies and services help our users?



work in progress for user trust alignment

Joined up with the Wallet work both for models and assurance

More diverse sources of identity & assurance

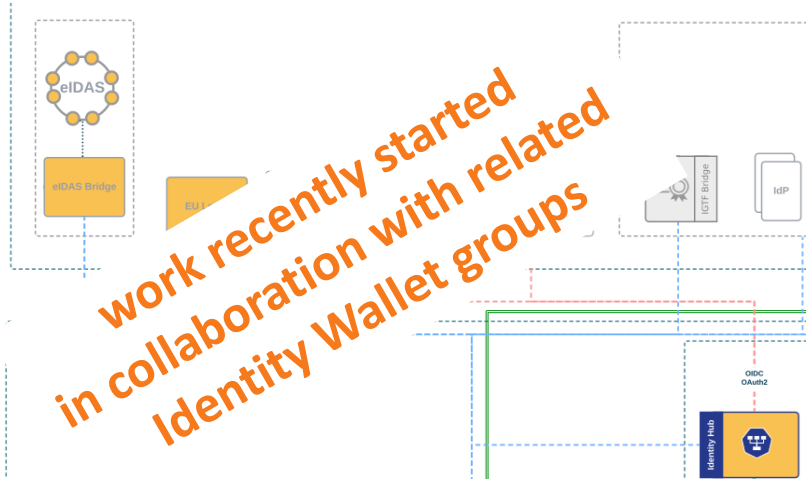
investigate researcher assurance through eID wallets and public (eIDAS) identity assurances.

Most reliable (and most ‘available’) source of assurance may be the government identity ecosystem

- Step-up can now readily be done ‘at home’ by users through their national eID schemes
- Better attainable than relying on home institutions?
- eIDAS 2 and EU ID Wallets, in combination with OpenID Federation pilots look promising!

… but:

- what to do with non-European users? And how to link identities?



One AARC (Policy) Tree …

Everyone will sit under their AARC TREE,
and no one will make them afraid

… but there should be talk under the tree!

Thank you

Any Questions?

davidg@nikhef.nl

https://aarc-community.org

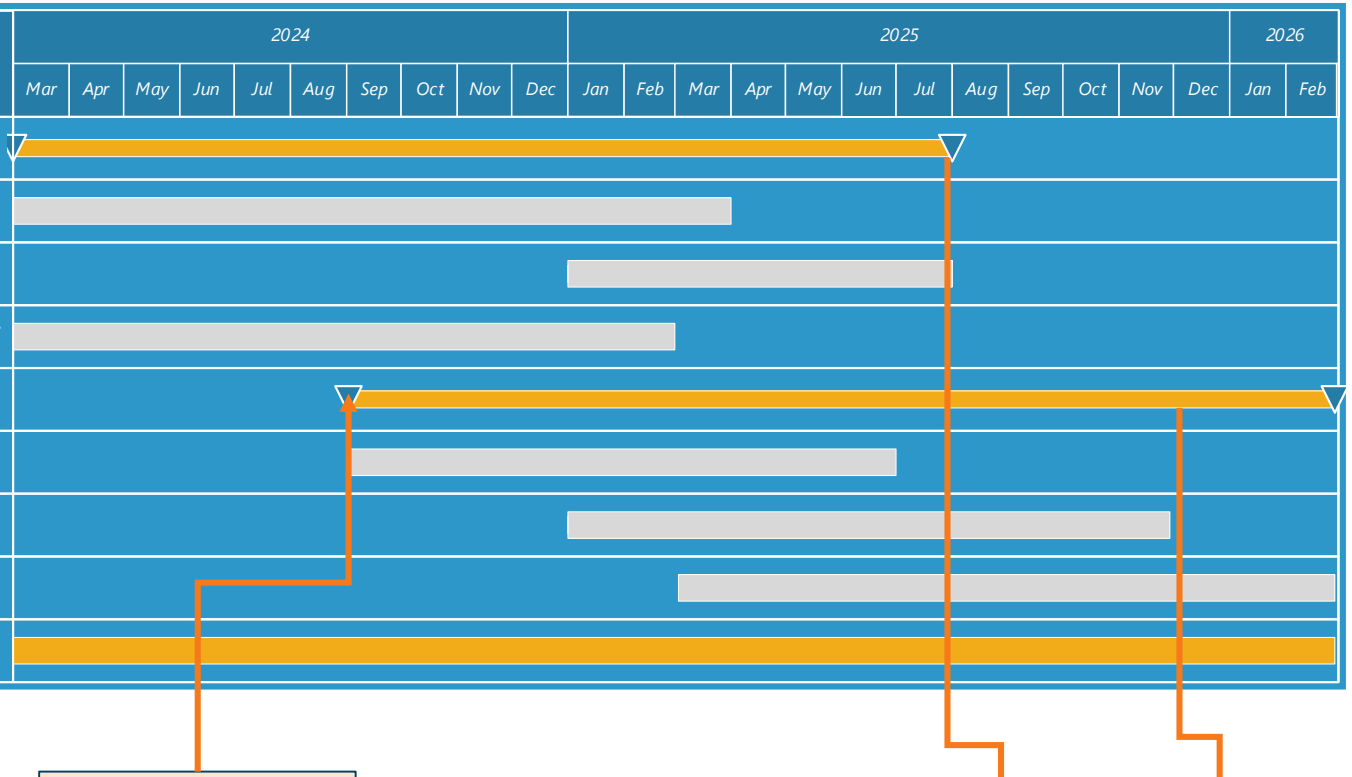
The work leading to these results has received funding from
the European Union's Horizon research and innovation programme and other sources.

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).

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



WP3 Use Case Analysis

WP5 Compendium

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