Authentication and Authorisation for Research and Collaboration

AARC Symposium – policy and good practice

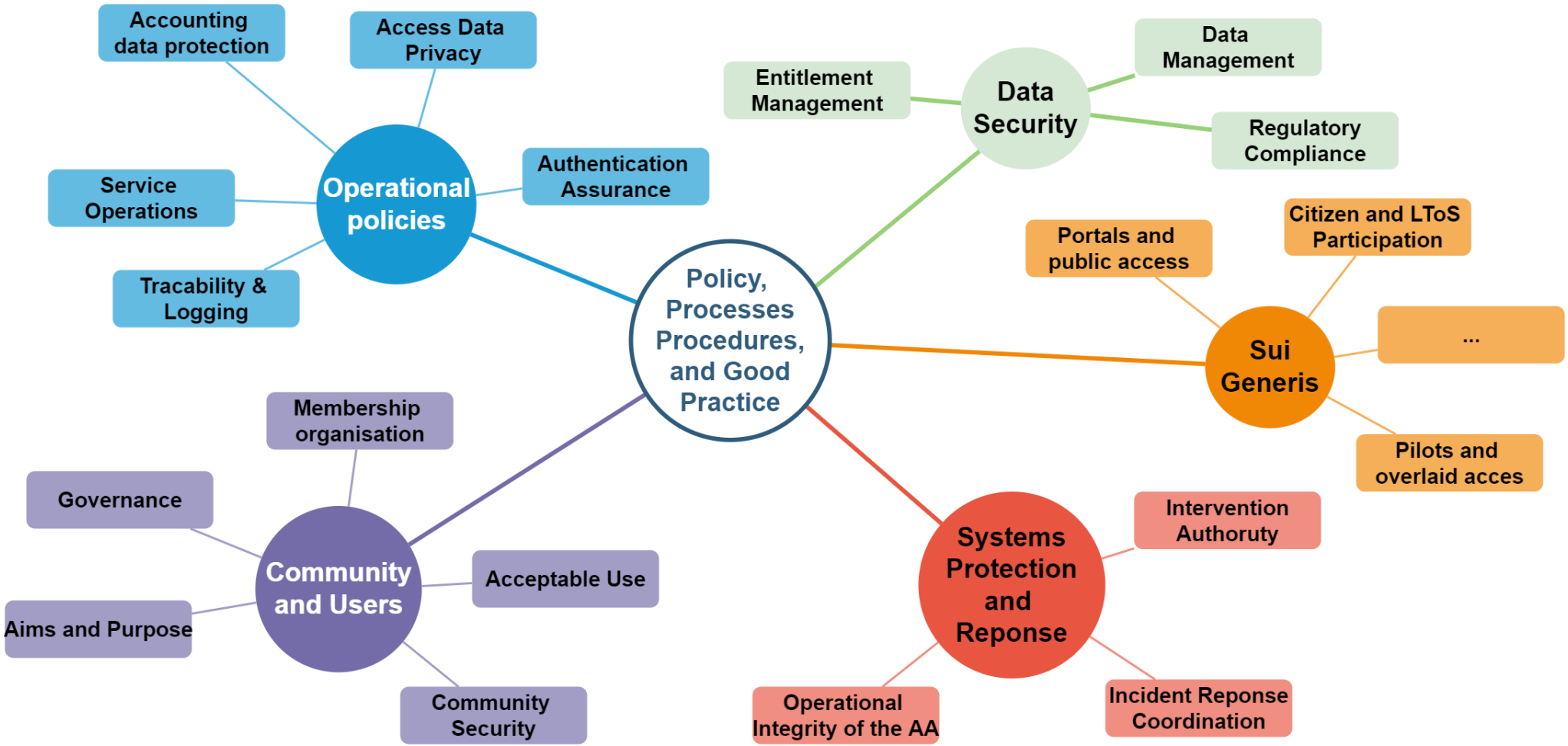
David Groep
AARC Policy Lead

Nikhef Maastricht University

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

AARC Symposium
Amsterdam, February 2026

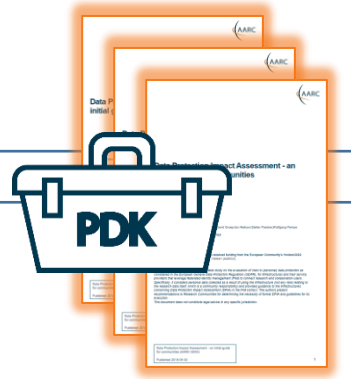
A world of good practice to implement, and policies to share



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)



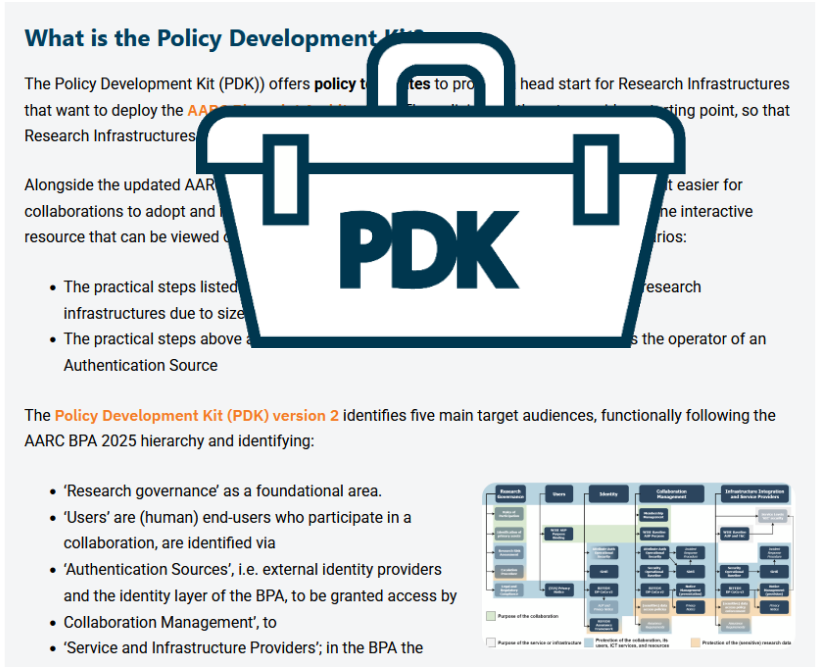
User-centric trust alignment and policy harmonization: ‘helping out the community’

- 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**

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



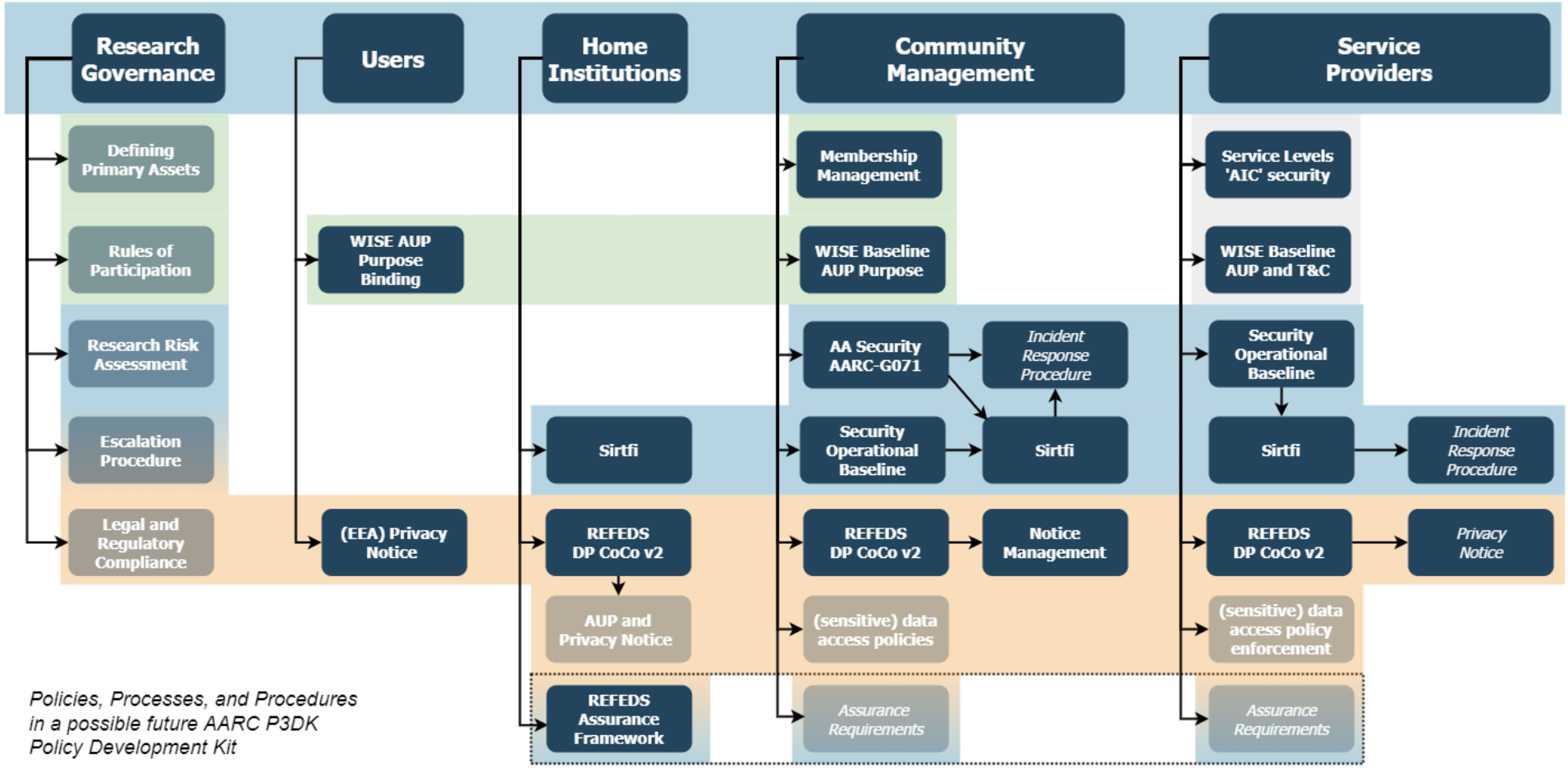
From the AARC2 infrastructure-oriented Policy Development Kit to

a *simpler* and *deployment-oriented*
Policy, Process, and Procedure Development Kit version 2

- comprehensive review of existing policy suite to reduce complexity
- input from national research infrastructures and EOSC nodes, but 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 *full* PDK structure



Today specialised AAI platform providers have established themselves

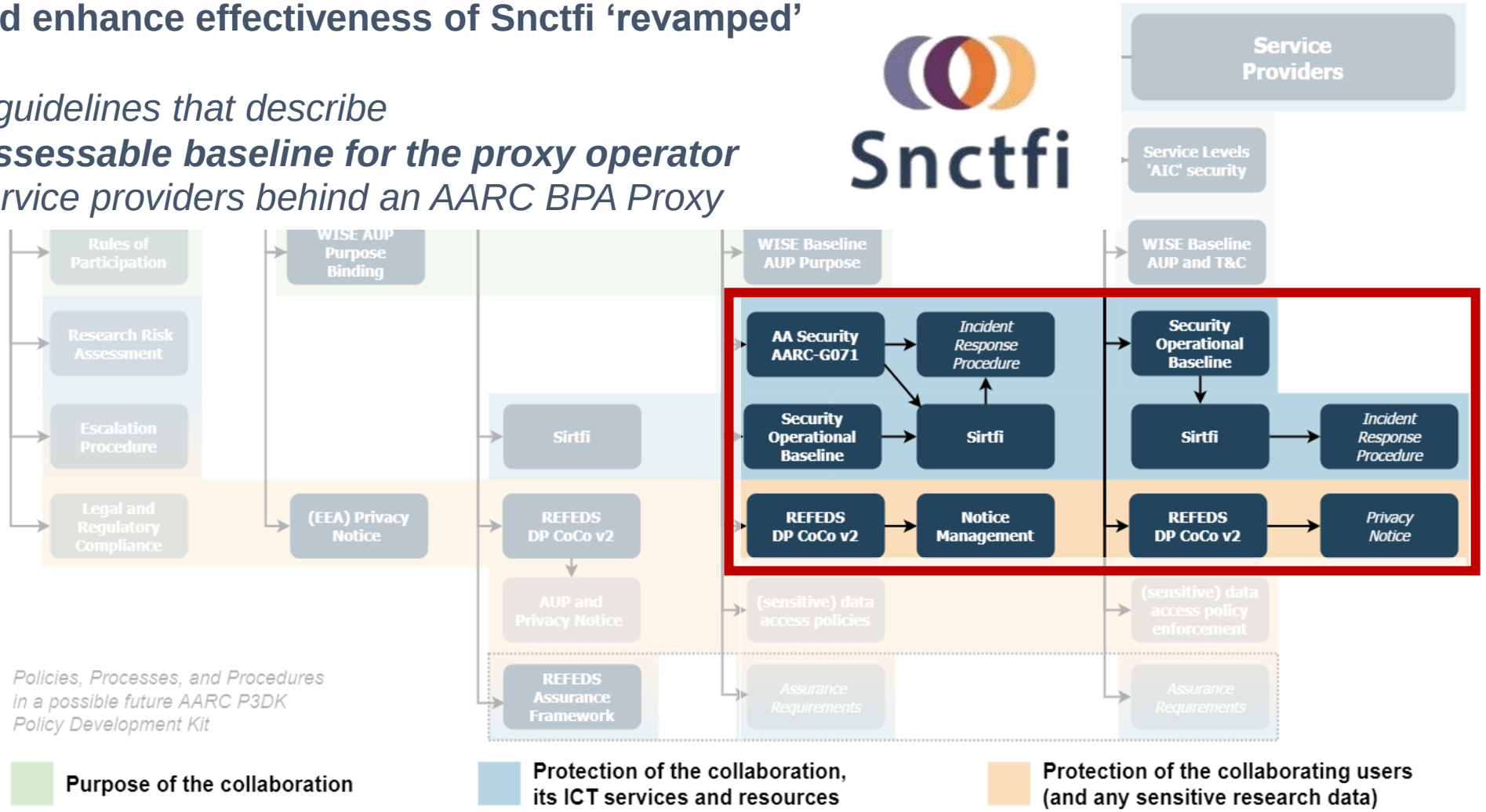
- Previous PDK policies targeted primarily at *infrastructure AAIs* and at *operators* of the few multi-community AAIs
- BPA2025 identifies platform layers, and AAI platform *operators* serving many collaborations and infrastructures with a common layer are a key player today
- A ‘trusted proxy operator’ can now be either self-hosted or used ‘as a service’

This has changed the policy landscape:
the more complex policy implementations can now be ‘sourced’ from trusted providers

AAI infrastructure providers for communities: a new ‘Snctfi’ trust mark

review and enhance effectiveness of Snctfi ‘revamped’

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



More importantly:
AARC Guidelines series as a pathways to policy sustainability and impact

AARC-I082 **Trust framework for proxies and Snctfi research services** landscape analysis and structure

AARC-G083 **Guidance for Notice Management by Proxies** reducing user frustration by streamlining

AARC-G084 **Security Operational Baseline** trusted and secure infrastructure and incident response

AARC-I085 **eID Assurance Model Assessment** investigates capabilities for leveraging national eID

AARC-I086 **Membership Management Policy Development** at light-weight and infrastructure-level

AARC-PDK **Policy Development Kit** an interactive resource for jumpstarting collaboration

Cross-cutting guidelines

AARC-G080 **Blueprint Architecture 2025** as the conceptual foundation

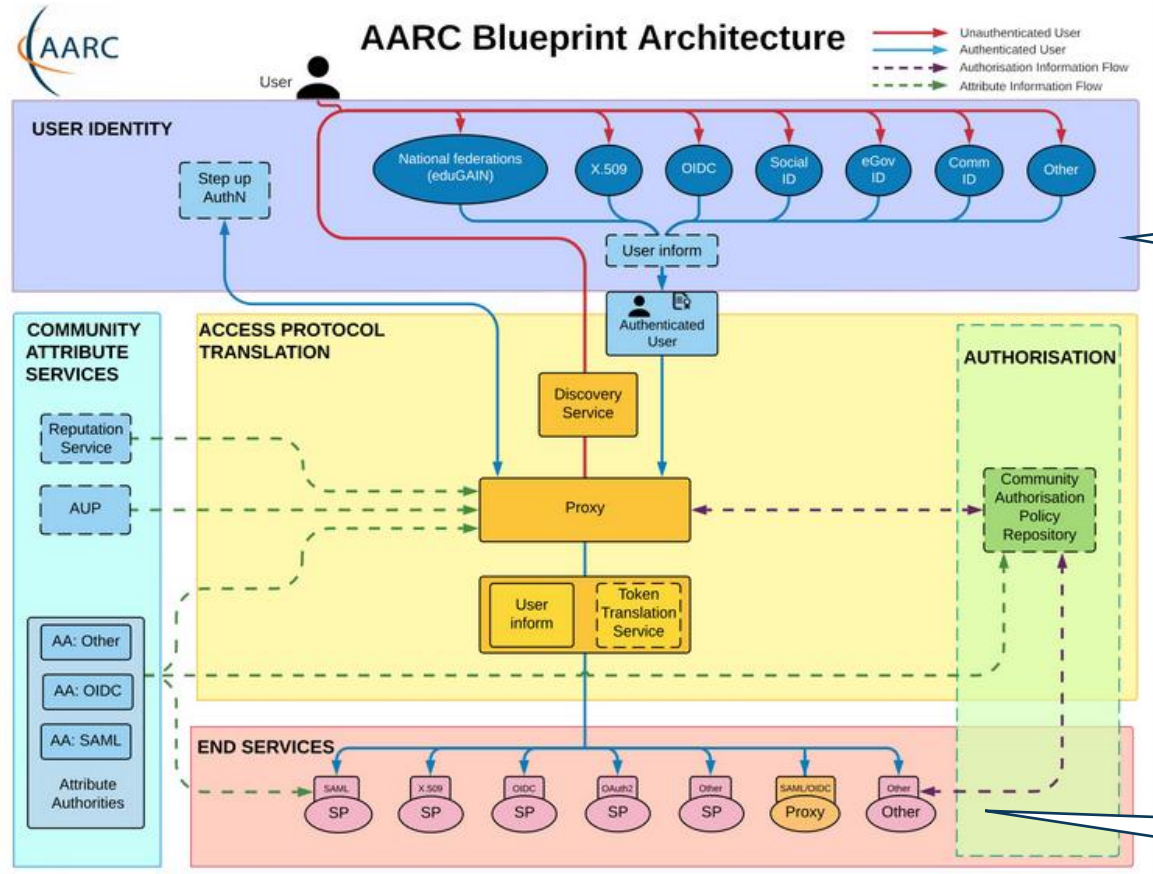
AARC-G081 **Recommendations for Token Lifetimes** balancing usage patterns and security

Adoption stimuli through the Policy Development Kit version 2 for

AARC-G071 'Attribute Authority and Proxy Operations', **AARC-I044** 'Baseline AUP implementation' **AARC-I051** and SIRTFI federated incident response, REFEDS DPCoCo v2, **AARC-G042** 'DPIA' for research collaborations, REFEDS Assurance Framework

https://aarc-community.org/guidelines/; PDK: https://aarc-community.org/policy/policy-development-kit/

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

so … what about standards for the Community Attribute Authority (AA) or for 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 …

AARC-G071

How to establish secure operation for your (AARC BPA) proxy?

The Challenge

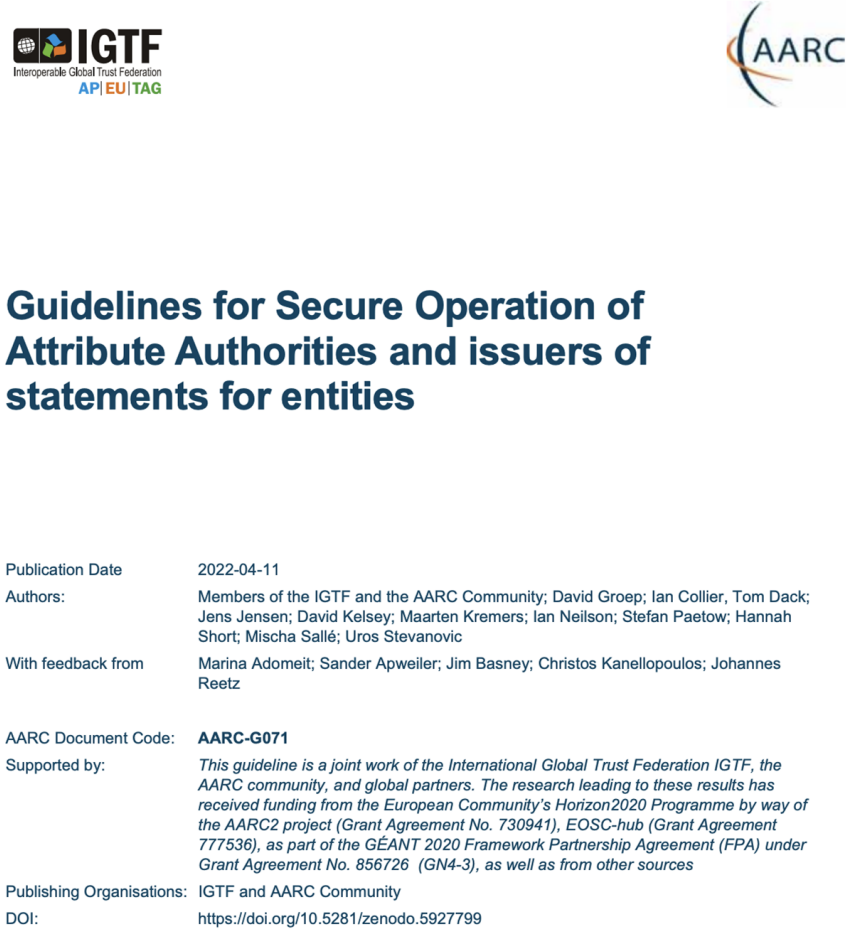
- How to securely operate proxies, attribute authorities and issuers of statements for entities?

Guideline

- AARC-G071 Guidelines for Secure Operation of Attribute Authorities

Summary

- Operational security processes and procedures
- Requirements on traceability, auditability, and logging
- Requirements on the secure operation
- Requirements on securing the interactions



Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities

Publication Date	2022-04-11
Authors:	Members of the IGTF and the AARC Community; David Groep; Ian Collier, Tom Dack; Jens Jensen; David Kelsey; Maarten Kremers; Ian Neilson; Stefan Paetow; Hannah Short; Mischa Sallé; Uros Stevanovic
With feedback from	Marina Adomeit; Sander Apweiler; Jim Basney; Christos Kanellopoulos; Johannes Reetz
AARC Document Code:	**AARC-G071**
Supported by:	*This guideline is a joint work of the International Global Trust Federation IGTF, the AARC community, and global partners. The research leading to these results has received funding from the European Community's Horizon2020 Programme by way of the AARC2 project (Grant Agreement No. 730941), EOSC-hub (Grant Agreement 777536), as part of the GÉANT 2020 Framework Partnership Agreement (FPA) under Grant Agreement No. 856726 (GN4-3), as well as from other sources*
Publishing Organisations:	IGTF and AARC Community
DOI:	https://doi.org/10.5281/zenodo.5927799

Deployment guidance, self-assessment, and peer feed-back

4.2. Attribute Management and Attribute Release

AMR-1

The Community must define and document the semantics, lifecycle, data protection, and release policy of attributes stored or asserted by the AA.

The community should follow the guidance from relevant policy documents. In particular, the Policy Development Kit has recommendations on Community Membership Management. It is recommended to use standardised attributes where possible, e.g. from eduPerson [EPSC] or SCHAC [SCHAC], and their semantics must be respected.

If Communities make modifications to the attribute set, their semantics, or release policies, it is recommended that they inform both their relying parties as well as the AA Operator thereof, since the AA operator may have implemented checks for schema consistency. The Community is ultimately responsible for the values and semantics of the attributes.

AMR-2

The AA Operator must implement the community definitions as defined and documented, for all the AAs it operates.

By implementing these requirements, the AA operator will support the chain of trust between Community and the RPs. An AA Operator must only host those communities for which it can implement the requirements.

AMR-3

It is recommended that the AA Operator provide a capability for the community to

Assessments and review shee

- WLCG - https://docs.google.com/spreadsheet
- UK-IRIS - https://docs.google.com/spreadshee
- eduTEAMS (Core AAI platform) - *in progress*
- SURF SRAM - https://docs.google.com/sprea
- NFDI - Academic ID - https://docs.google.com
- NFDI - didmos - https://docs.google.
- NFDI - Reg App - https://docs.googl
- NFDI - Unity - https://docs.google.co

http://wiki.eugridpma.org/Main/AAOperationsGuidelines

AARC-G084

Proxy Operations: Information Security and Security Operational Baseline

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

Service Security Policy from AARC PDK v1
was successful but diverged in several directions:

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

The new PDK in AARC TREE converges on a common **Baseline** - with guidance and FAQ

- Included in the EOSC AAI WG Federation 2025

AARC-G084

Security Operational Baseline for Proxies and Services

Security Operational Baseline fo and Services

Publication Date 2025-03-28
Authors: David L. Groep (ed.);Alf Moens;Daniel Kouřil;Baptise (Kelsey;Ian Neilson;Linda Cornwall;Matt Viljoen;Pinja K Niederberger;Romain Wartel;Sven Gabriel;and Urpo K

Document Code: AARC-G084
DOI: (to be assigned)

Framework: Policy Development Kit v2

Abstract

The Security Baseline provides a reference set of minimum expectations and req those offering services to users, communities, and other participants in a distribu those providing access to services or assembling service components. It aims to trust between all Participants in the Infrastructure to enable reliable and secure Ir

Security Operational Baseline for Proxies and Services (AARC-G084)

Published 2025-03-28

3. Security Baseline

To adhere to the Security Operational Baseline, you must:

1. comply with the SIRTFI[1] security incident response framework for structured and coordinated incident response
2. ensure that your 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 your Service’s participation in the Infrastructure.
5. respect the legal and contractual rights of Users and others with regard to the personal data processed, and only use access personal 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. operate 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, specifically those with which there is a direct trust relationship, in the reporting and resolution of security events or incidents related to their participation in the infrastructure and those affecting the infrastructure as a whole.
10. honour the obligations on 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 the 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.

[1] https://refeds.org/sirtfi/

AARC-G084 https://doi.org/10.5281/zenodo.7396724

The 12 points of AARC-G084

AARC-G084

1. comply with the SIRTFI security incident response framework for structured and coordinated incident response [ref to SIRTFI]
2. ensure that your 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 your Service's participation in the Infrastructure.
5. respect the legal and contractual rights of Users and others with regard to the personal data processed, and only use access personal 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. operate 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, specifically those with which there is a direct trust relationship, in the reporting and resolution of security events or incidents related to their participation in the infrastructure and those affecting the infrastructure as a whole.
10. honour the obligations on 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 the 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

FAQ and implementation guidance

AARC-G084

https://wiki.geant.org/spaces/AARC/pages/1049624759/view

Pages / ... / AARC-G084 Security Operational Baseline

Security Operational Baseline FAQ and Recommendations

Created by David Groep on May 24, 2025 • 11 minute read

The Security Operational Baseline (AARC-G084) sets minimum expectations and puts requirements on the behaviour of those offering services to
and on communities connected to a federated infrastructure, when interacting with the infrastructure peers and services. Worded in an intention
concise manner, the 12 key requirements may give rise to additional questions, or in general can benefit from concrete examples and guidance.
"FAQ" document, each of the key baseline items is put in context with additional examples, best practices, and generally helpful ideas.

- Can you elaborate on what is meant by item 9 and its incident response requirements?
- What are 'IT security best practices' in item 7?
- What does "honour the confidentiality requirements of information" in item 4 mean?
- What are “the legal and contractual rights of Users and others with regard to their personal data processed as part of service delivery” in item 5?
- "Retain system generated information (logs)" in item 6 sounds rather open-ended. What do I need to do? And why?
- “Aggregated centrally wherever possible, and protected from unauthorised access or modification” in item 6, how and why?
- Log aggregation in the layered and composite infrastructure
- What about the 'reconstruction of a coherent and complete view of activity' when you have a a ‘layered technology stack’ mentioned in item 6?
- What are “Named persons”?

Can you elaborate on what is meant by item 9 and its incident response requirements?

Item 3 talks about security incident response. In an interwoven environment it is vital that data about incidents is shared and communicated to detect, analyse, contain and eradicate malicious actors while preserving the necessary evidence for analysis and post-processing. For most infrastructures, there is a dedicated team of incident response specialists to aid with this task. This team can also communicate between different service providers affected by

Home page › Guidelines › AARC-G084

March 28, 2025

AARC-G084 Security Operational Baseline

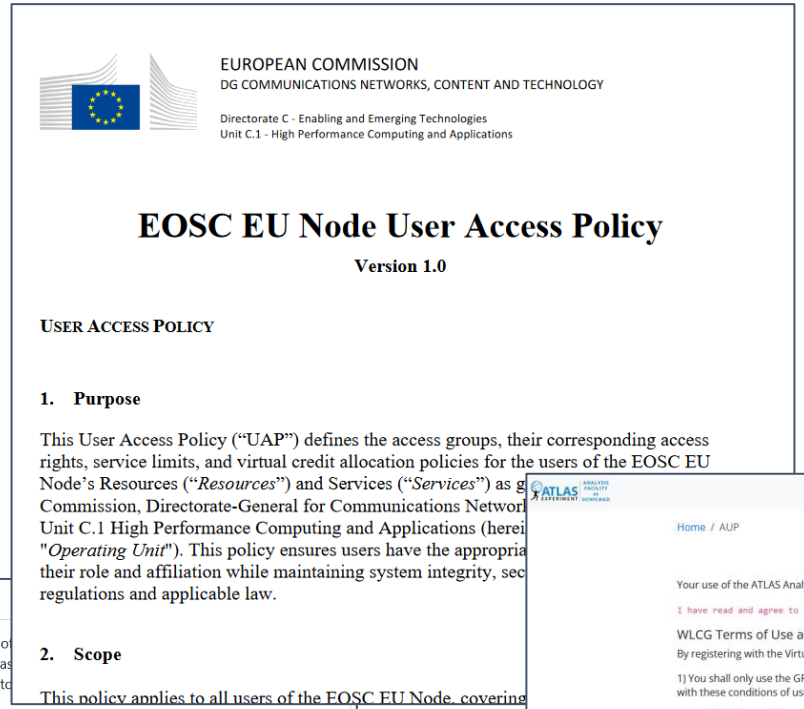
The Security Baseline provides a reference set of minimum expectations and requirements of the behaviour of those offering services to users, communities, and other paricipants in a distributed proxy ecosystem, and of those providing access to services or assembling service components. It aims to establish a sufficient level of trust between all Participants in the Infrastructure to enable reliable and secure Infrastructure operation.

Document URL: https://wiki.geant.org/download/attachments/999948380/AARC-G084-Security-Operational-Baseline-PDKv2.pdf
Development information: https://wiki.geant.org/spaces/AARC/pages/999948380/AARC-G084+Security+Operational+Baseline
Status: pending approval by AEGIS
DOI: 10.5281/zenodo.17349890
Errata: none
Supersedes:

Supporting documentation, implementation suggestions and background information is available in the Security Operational Baseline FAQ and Recommendations.

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

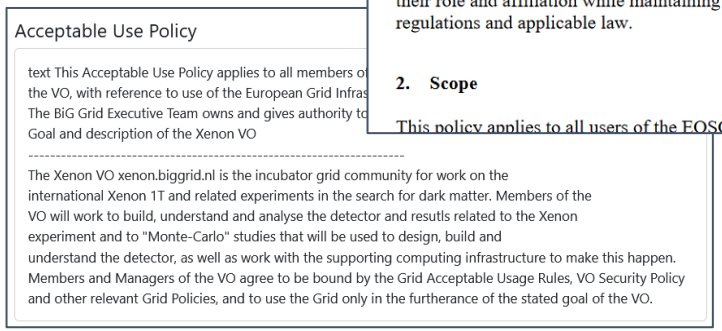
USER ACCESS POLICY

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

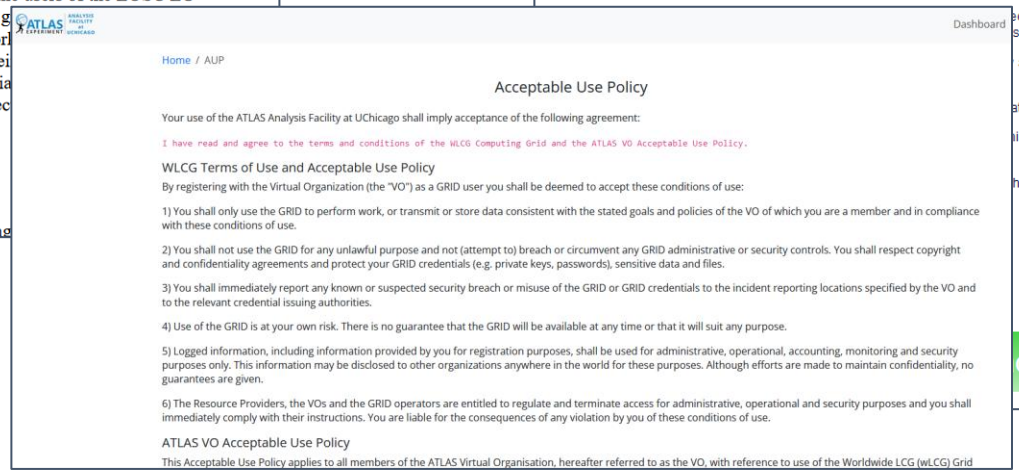
This policy applies to all users of the EOSC EU Node, coverin



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

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.

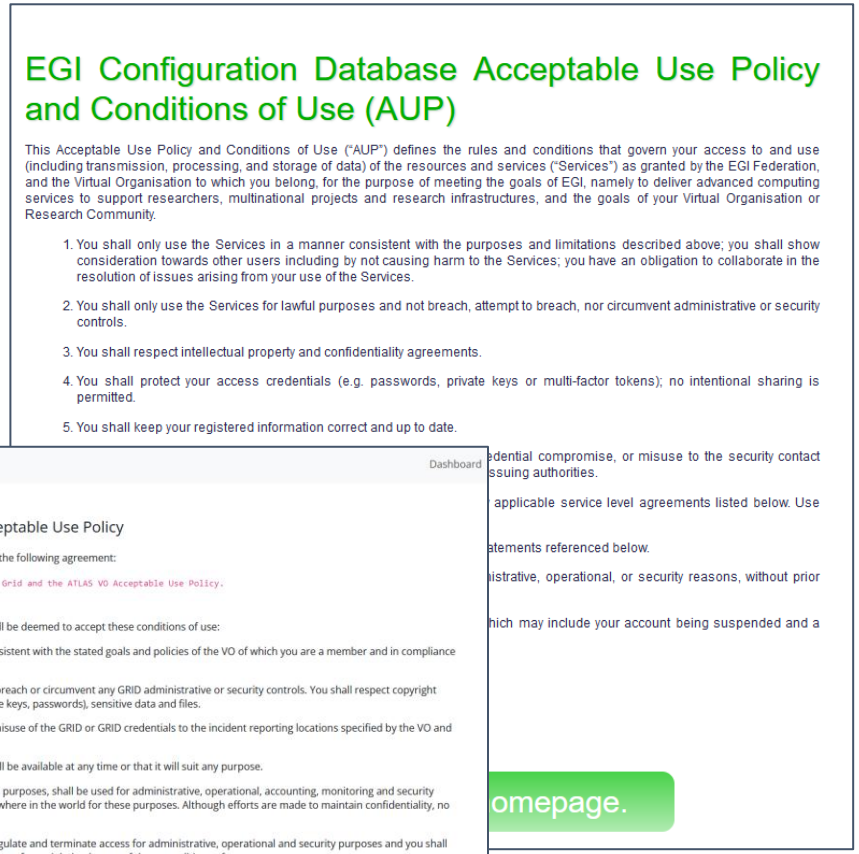
4) Use of the GRID is at your own risk. There is no guarantee that the GRID will be available at any time or that it will suit any purpose.

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



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.

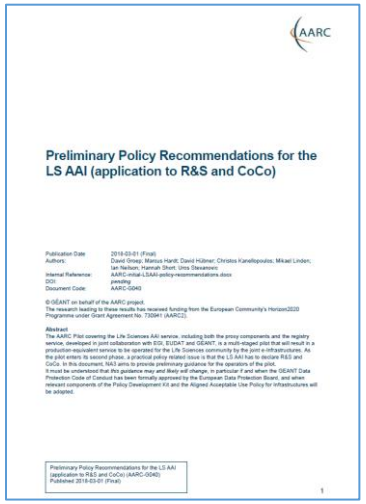
Proxies have their ‘experience challenges’: AUPs, T&Cs, Privacy notices, …

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 actually 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 bespoke guidance

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!

New AARC guidance on Notice Management by Proxies

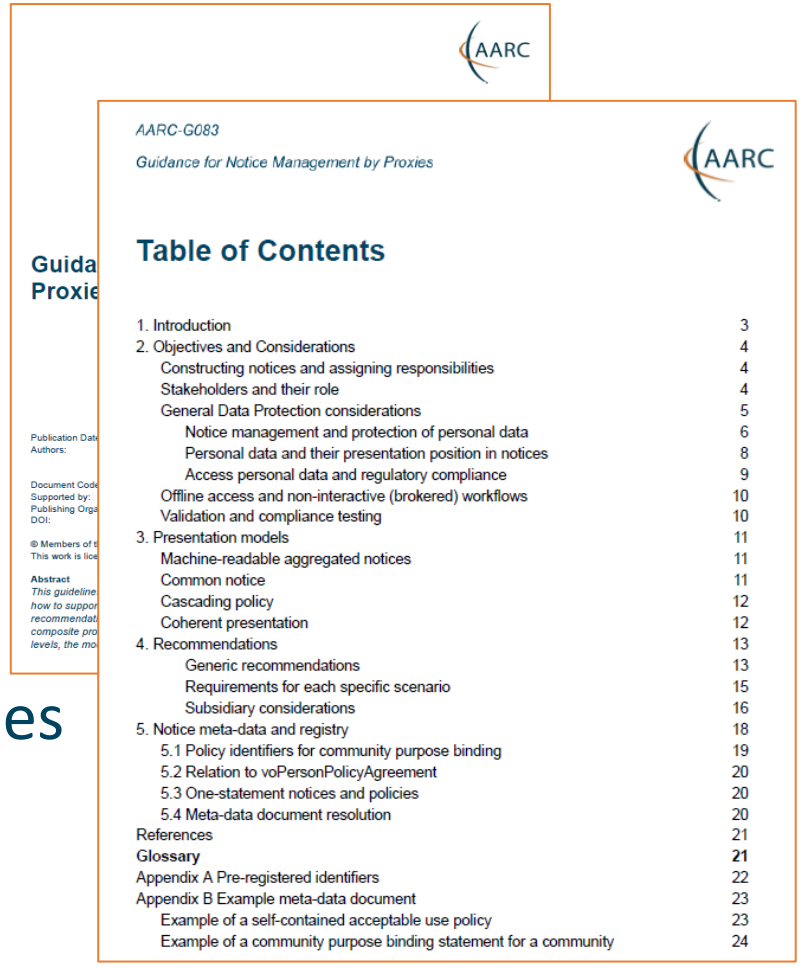
AARC-G083

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

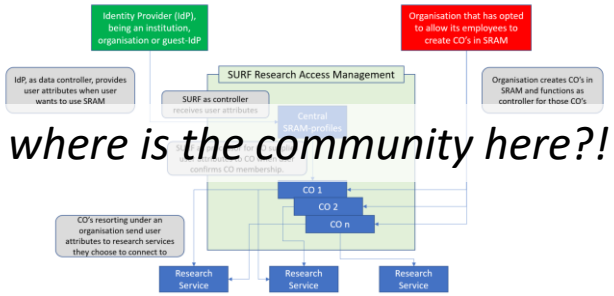
Notice presentation (PoC example implementation from the Validator)

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?!

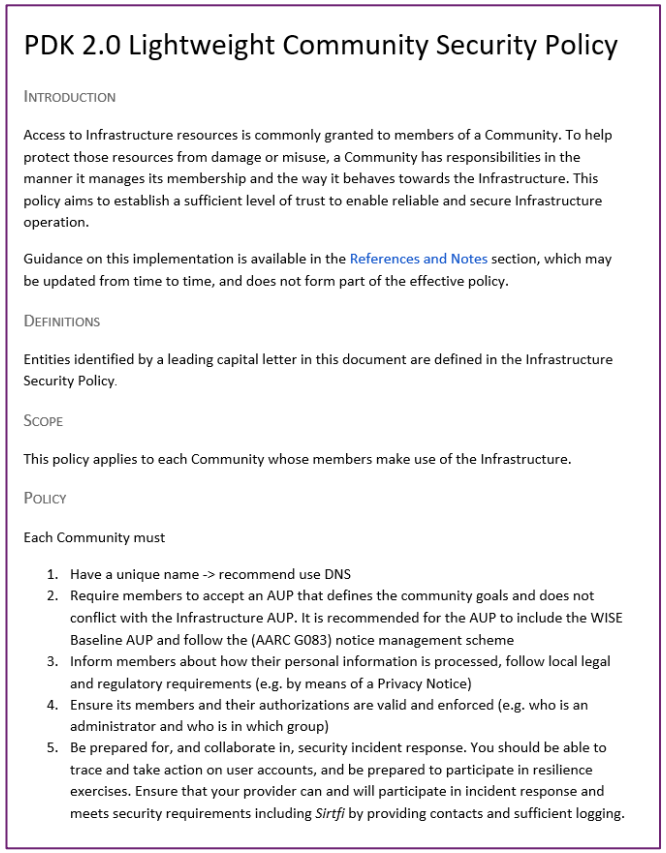
But both communities and operators of membership management services are today unclear about trust assurance level of members: current templates in toolkit too complex and prescriptive

- 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

I086: 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.

https://aarc-community.org/guidelines/aarc-i086/

Build trusted baseline expectations to increase reach of RI proxies

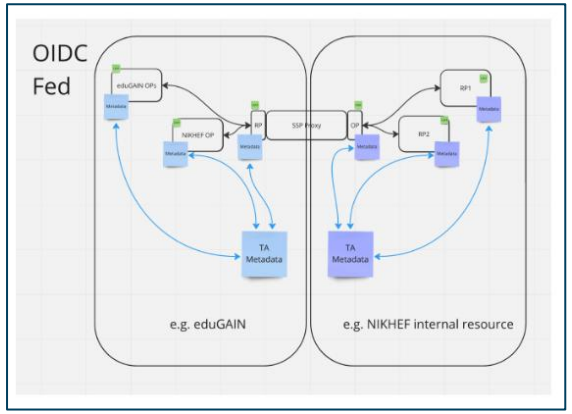
… with R&E identity providers … and with new sources of information

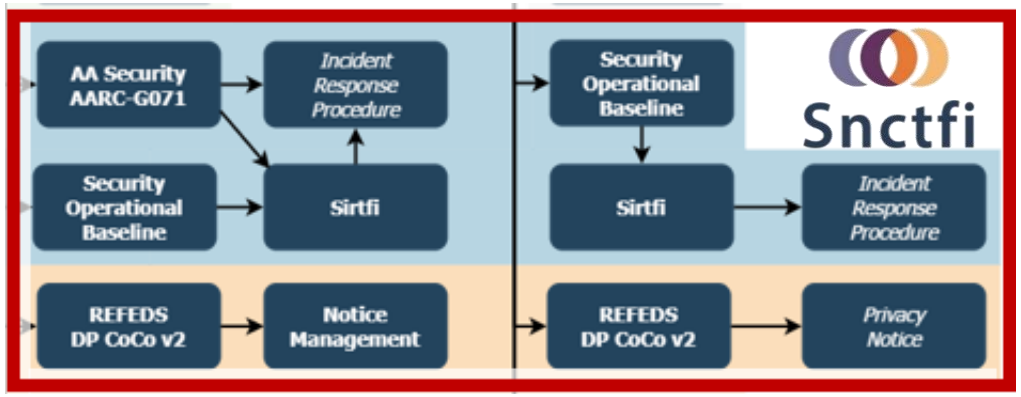
'guidelines on cross-sectoral trust in novel federated access models'

Service and data providers need *unique identifier and affiliation,* with name and email, and 'fresh' assurance from home IdPs, but:

- proxies have met with scepticism by IdPs:
  lack of even basic personalised and R&S attribute release
- how do these trust qualities 'traverse' proxies?
- how do operators rely on adherence to guidelines by their 'downstream' providers?

Position of the proxy makes trust bidirectional, and ***platform operators*** *are facilitating this trust today*

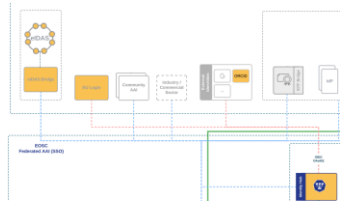




More diverse sources of researcher identity & assurance with eID wallets

Most reliable (and most 'available') source of assurance could be government identity!

- Step-up can now readily be done 'at home' by users through their national eID schemes
- eID wallets could solve the blockage by home IdPs to release assurance



… but their applicability to research and education use cases remains limited:

- eIDAS 1.0 suffers from inconsistent national uptake, asymmetrical cross-border connectivity, and protocol incompatibilities
- eIDAS 2 *at this point in time*, has incomplete roll-out, national implementations vary widely, and support for non-governmental use cases remains immature
- non-European users in Europe and international linking are not addressed at all today

Verifiable Credentials and digital wallets offer a complementary path forward, but lack of ecosystem maturity, lack of common standards, and adoption are (too) far in the future …

AARC TREE D2.2 | AARC PDK

Bringing it together: the Policy Development Kit

PDK v2 has guidelines *and* explanations, hints, and accessible recommendations

Practical steps to getting started with Policies for a Research Collaboration

Policy may appear a daunting or overly complex task if you start on your resear
you can quickly navigate the policy space and avoid the most common pitfalls.
starting with your trusted collaboration quickly and smoothly:

- Define a unique name for your collaboration, preferably from the domain na
- Identify a governance body to make policy decisions
- Define the purpose of your collaboration - this will be used for your AUP
- Think about your crown jewels, risks, any regulations and legal things, privac
- Define or adopt as-is the basic set of six policy documents for collaboration
- Review the AEGIS endorsed guidelines required for AARC compliance and en
- Ensure that the policies are presented to and accepted by the relevant audie
- Publish your documents and responsible parties at a suitable location

Define the purpose of your collaboration - this will be used for your AUP

Why? As you connect services and infrastructures to your collaboration via the AAI, these will have their 'acceptable' (and unacceptable) use defined. They provide services based on what what you, as a collaboration, are planning to do, pay for, or because of shared goals and ambitions. Your users should be acting as part of your community, so also they need clarify as to what the collaboration is for. To prevent each and every infrastructure and service provider asking the users to comply with their acceptable use - and having to remember on your behalf what the collaboration's goal in life in - the common WISE Baseline AUP can do that in one go. But for that the purpose of use needs to be clear. Only you (as in: the collaboration) can provide that clarity

Recommendation: be clear and concise in how to word your purpose. A one-line sentence is needed to be inserted verbatim into the WISE Baseline AUP that you should show to users enrolling in your collaboration (or that your AAI service provider will show on your behalf when new users join). This is not the place to write a grant proposal ...

Applicable guidance: WISE AUP, AARC-I044 (AUP implementation guide), AARC-G083 (notice management), Governance - primary assets, Governance - risk assessment

Think about your crown jewels, risks, any regulations and legal things, privacy - and what to do if things go wrong ...

Define or adopt as-is the basic set of six policy documents for collaboration - and seek endorsement by your governance body

Why? This basic set of 6 documents helps get a sufficient set of collaboration guidelines quickly - you can always adapt them later

Recommendation: these are the documents you surely need - or you need to ask from your AAI provider:

- Membership Management
- Acceptable Use and Terms and Conditions
- Privacy Notice

- Research Risk Assessm
- Rules of Participation
- The REFEDS Data Prote
- WISE AUP

This policy establishes practices that are adopted by <collaboration X> in the management of its members. Accurate management of a collaboration's members and their authorisation attributes is fundamental to ensuring secure access control. Trust between <collaboration X>, underlying infrastructure and partner collaborations may be established by rigorous application of this policy.

COLLABORATION MANAGER

MEMBERSHIP LIFE CYCLE REQUIREMENTS

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

In the end, it's all about enabling research: FIM4R & collaboration are our driving factors

The AARC Community uses a "co-creation process" through FIM4R

- Research community requirements and reflection
- Global forum with strong European focus
- Enhanced by strategic co-location with trust and identity events

Impact on accessibility of the AAI infrastructure for *user communities*

- by identifying inconsistencies in access management and policy, and
- co-creating the architecture & getting researcher reflection early for proposed solutions

'Copenhagen, Boston, Reading, Denver, Amsterdam, …'

The AARC Policy Tree …

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

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).