AARC Authentication and Authorisation for Research and Collaboration

Policy Innovations in Federated Identity

Insights from AARC

Maarten Kremers
AARC Policy WG
SURF, AARC Policy WG, GN5-2 T&I EnCo

SURF

ISGC 2025
Tapei, 21st March 2025

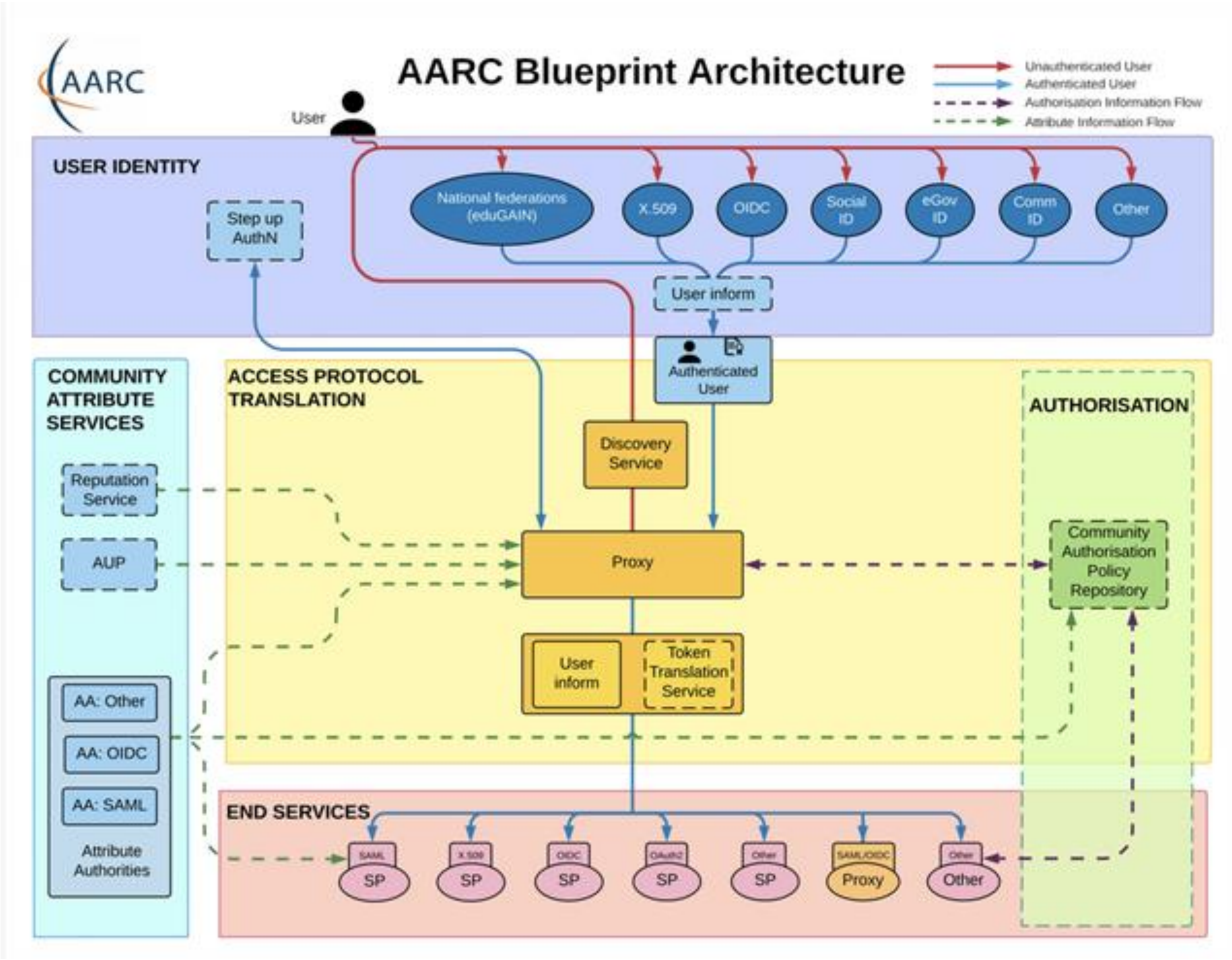
Authentication and Authorisation for Research and Collaboration

With many thanks to the other members
of the policy WG

- David Groep, Nikhef & Maastricht University
- David Kelsey, STFC-RAL
- Catharina Vaendel, Nikhef
- Arnout Terpstra, SURF
- Hannah Short, CERN
- And many others

ISGC 2025
Tapei, 21st March 2025

AARC Blueprint Architecture: many communities and collaboration, and full of fancy colourful pictures and stuff



AARC Blueprint Architecture

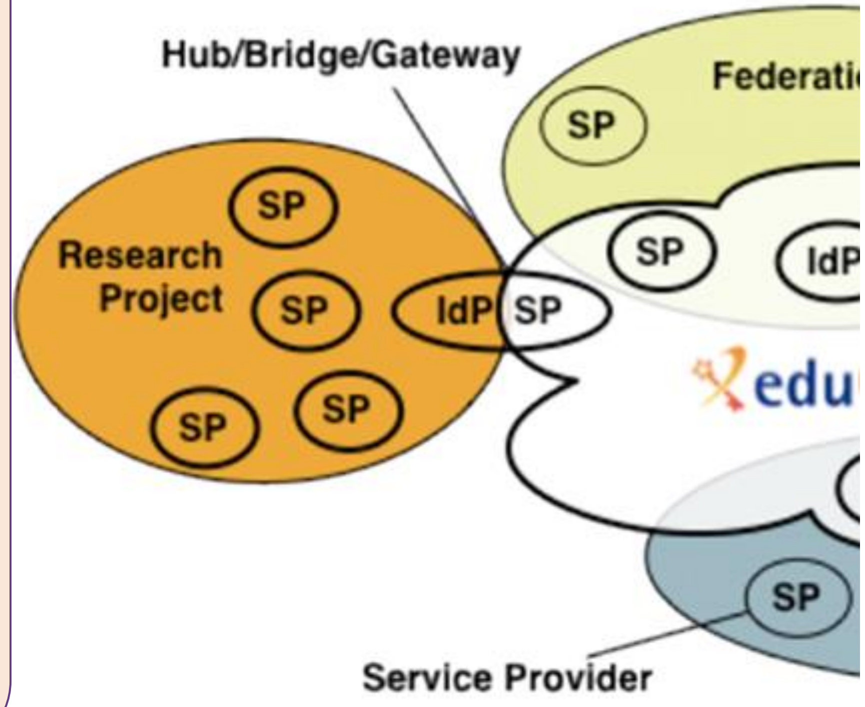
SSHOC
ESCAPE
panosc
photon and neutron open science cloud
eosc
SURF
LSC
LIGO Scientific Collaboration
FENIX
neic
PUHURI
LUMI
DARIAH-EU
Digital Research Infrastructure for the Arts and Humanities
EOSC-Life
eduGAIN
GÉANT

What is the AARC BPA?

The Authentication and Authorization For Research and Collaborations **BluePrint Architecture** provides **a set of building blocks** for software architects and technical decision makers who are designing and implementing access management solutions for international research collaborations. By design the AARC BPA is **technology agnostic** and provides an **architectural design** for those the deploy AAIs.

The AARC BPA: the IdP-SP proxy to enable federated access for research

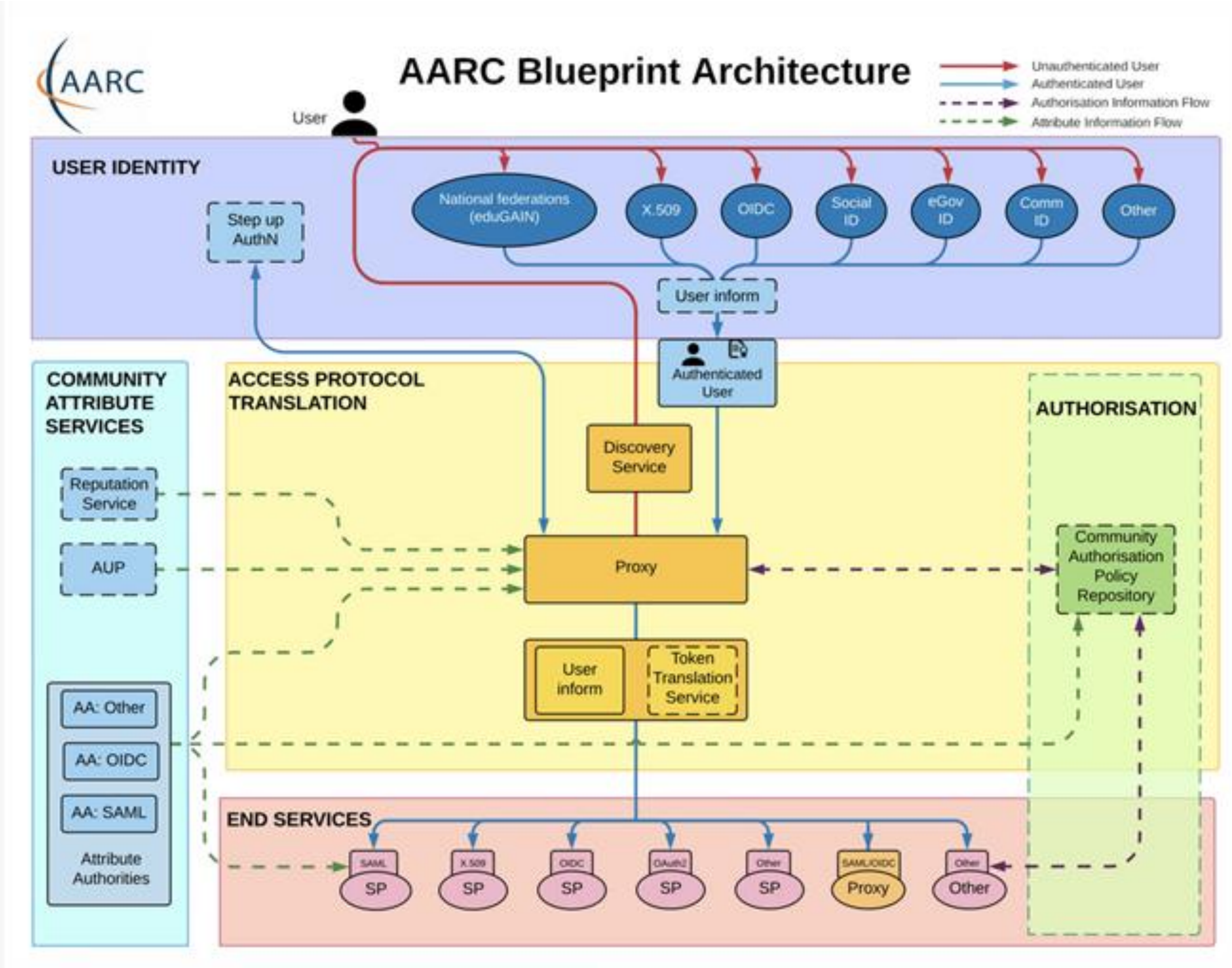
- Access services using **identities from users' Home Organizations**, but **hide complexity** of multiple IdPs, federations, AA technologies
- **One persistent identity** across all the community's services through **account linking**
- **Access** services **based on role(s)** users have **in the collaboration**.
- For both **web** and **non-web** resources
- Integration of **guest identity solutions**
- **Support for stronger authentication assurance** mechanisms

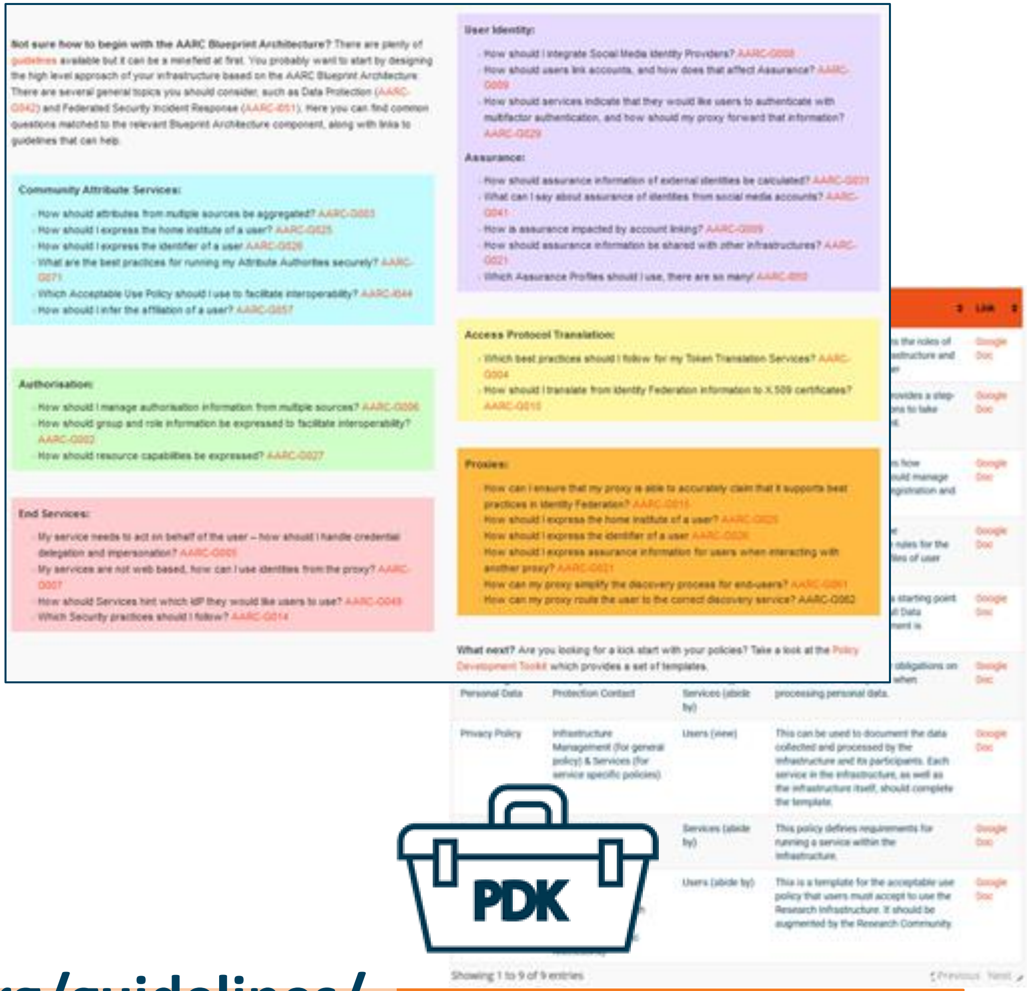


Graphics: Ann Harding and Lukas Hammerle (SWITCH)– from a long time ago now!

Authentication and Authorization for Research Collaboration – https://aarc-community.org/

Interoperability – more than just the nice colours





Not sure how to begin with the AARC Blueprint Architecture? There are plenty of guidelines available but it can be a minefield at first. You probably want to start by designing the high level approach of your infrastructure based on the AARC Blueprint Architecture. There are several general topics you should consider, such as Data Protection (AARC-G042) and Federated Security Incident Response (AARC-I051). Here you can find common questions matched to the relevant Blueprint Architecture component, along with links to guidelines that can help.

Community Attribute Services:

- How should attributes from multiple sources be aggregated? AARC-G053
- How should I express the home institute of a user? AARC-G025
- How should I express the identifier of a user AARC-G026
- What are the best practices for running my Attribute Authorities securely? AARC-G071
- Which Acceptable Use Policy should I use to facilitate interoperability? AARC-I044
- How should I infer the affiliation of a user? AARC-G057

Authorisation:

- How should I manage authorisation information from multiple sources? AARC-G006
- How should group and role information be expressed to facilitate interoperability? AARC-G002
- How should resource capabilities be expressed? AARC-G027

End Services:

- My service needs to act on behalf of the user – how should I handle credential delegation and impersonation? AARC-G001
- My services are not web based, how can I use identities from the proxy? AARC-G007
- How should Services hint which IdP they would like users to use? AARC-G049
- Which Security practices should I follow? AARC-G014

User Identity:

- How should I integrate Social Media Identity Providers? AARC-G008
- How should users link accounts, and how does that affect Assurance? AARC-G009
- How should services indicate that they would like users to authenticate with multifactor authentication, and how should my proxy forward that information? AARC-G029

Assurance:

- How should assurance information of external identities be calculated? AARC-G031
- What can I say about assurance of identities from social media accounts? AARC-G041
- How is assurance impacted by account linking? AARC-G009
- How should assurance information be shared with other infrastructures? AARC-G021
- Which Assurance Profiles should I use, there are so many! AARC-I050

Access Protocol Translation:

- Which best practices should I follow for my Token Translation Services? AARC-G004
- How should I translate from Identity Federation information to X.509 certificates? AARC-G010

Proxies:

- How can I ensure that my proxy is able to accurately claim that it supports best practices in Identity Federation? AARC-G015
- How should I express the home institute of a user? AARC-G025
- How should I express the identifier of a user AARC-G026
- How should I express assurance information for users when interacting with another proxy? AARC-G021
- How can my proxy simplify the discovery process for end-users? AARC-G061
- How can my proxy route the user to the correct discovery service? AARC-G062

What next? Are you looking for a kick start with your policies? Take a look at the Policy Development Toolkit which provides a set of templates.

				Link
			...s the roles of ...astructure and ...er	Google Doc
			...rovides a step- ...ons to take ...d.	Google Doc
			...s how ...ould manage ...egistration and	Google Doc
			...et ...rules for the ...files of user	Google Doc
			...a starting point ...ll Data ...ment is	Google Doc
...Personal Data	...Protection Contact	Services (abide by)	...obligations on ...when processing personal data.	Google Doc
Privacy Policy	Infrastructure Management (for general policy) & Services (for service specific policies)	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
		Services (abide by)	This policy defines requirements for running a service within the infrastructure.	Google Doc
		Users (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

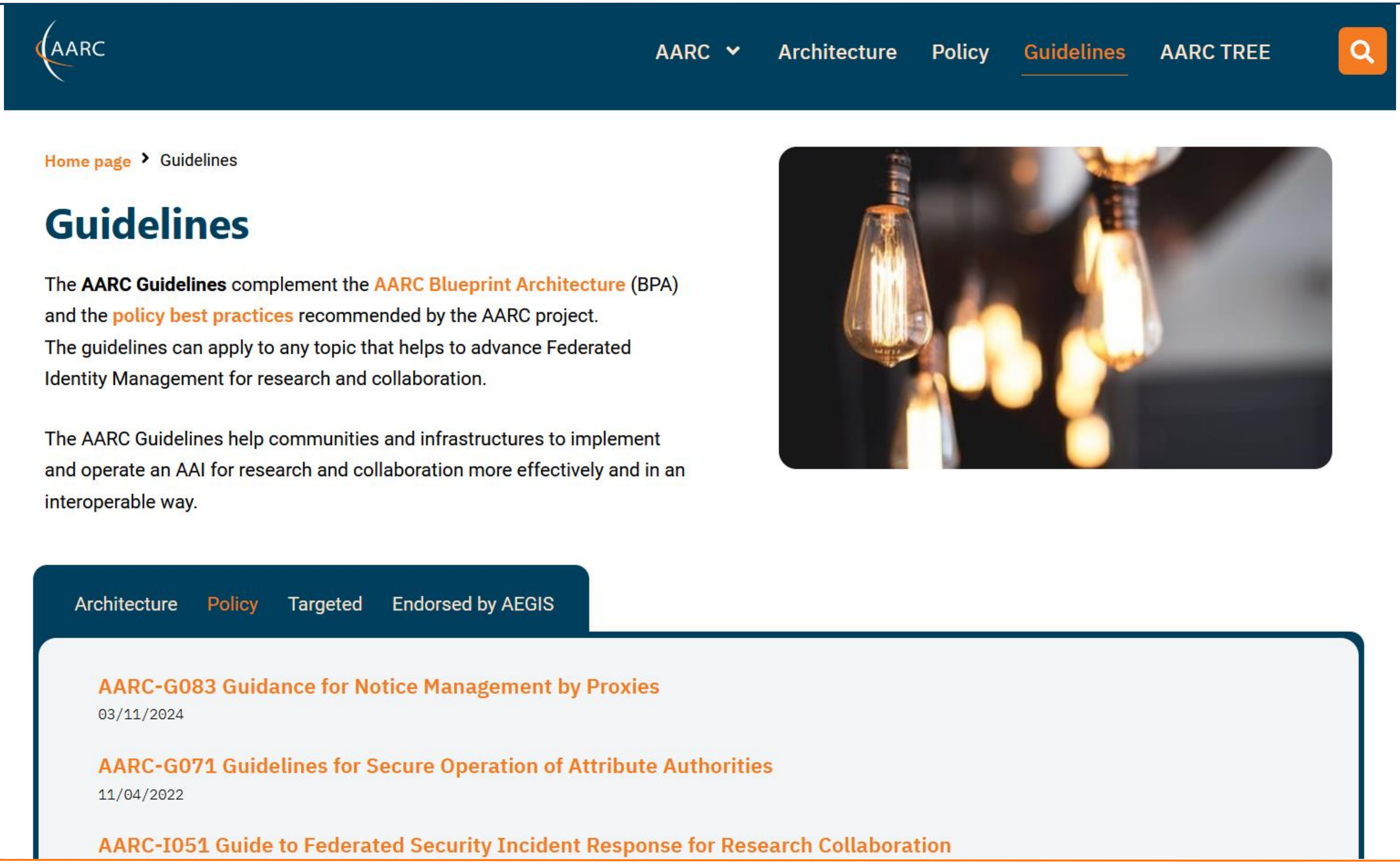
Showing 1 to 9 of 9 entries

Previous Next

PDK

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

A common suite of architecture and policy guidelines



Guidelines

The **AARC Guidelines** complement the AARC Blueprint Architecture (BPA) and the policy best practices recommended by the AARC project. The guidelines can apply to any topic that helps to advance Federated Identity Management for research and collaboration.

The AARC Guidelines help communities and infrastructures to implement and operate an AAI for research and collaboration more effectively and in an interoperable way.

AARC-G083 Guidance for Notice Management by Proxies
03/11/2024

AARC-G071 Guidelines for Secure Operation of Attribute Authorities
11/04/2022

AARC-I051 Guide to Federated Security Incident Response for Research Collaboration

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

AARC BPA Guidelines – evolving interoperability with new guidance

Architecture

- Protocols and profiles
- Attribute specs and transport
- Communications and interfaces

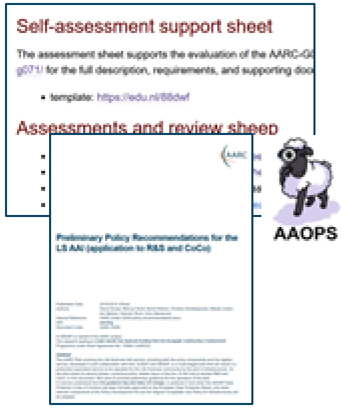
Policy

- ISM interoperability
- Policy development kit
- Trust mechanisms and federation

Policy and good practice underpinning the AARC Blueprint BPA

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)



Self-assessment support sheet

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

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

Assessments and review sheep

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

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

Data Protection Impact Assessment - an initial guide for communities

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

The Challenge

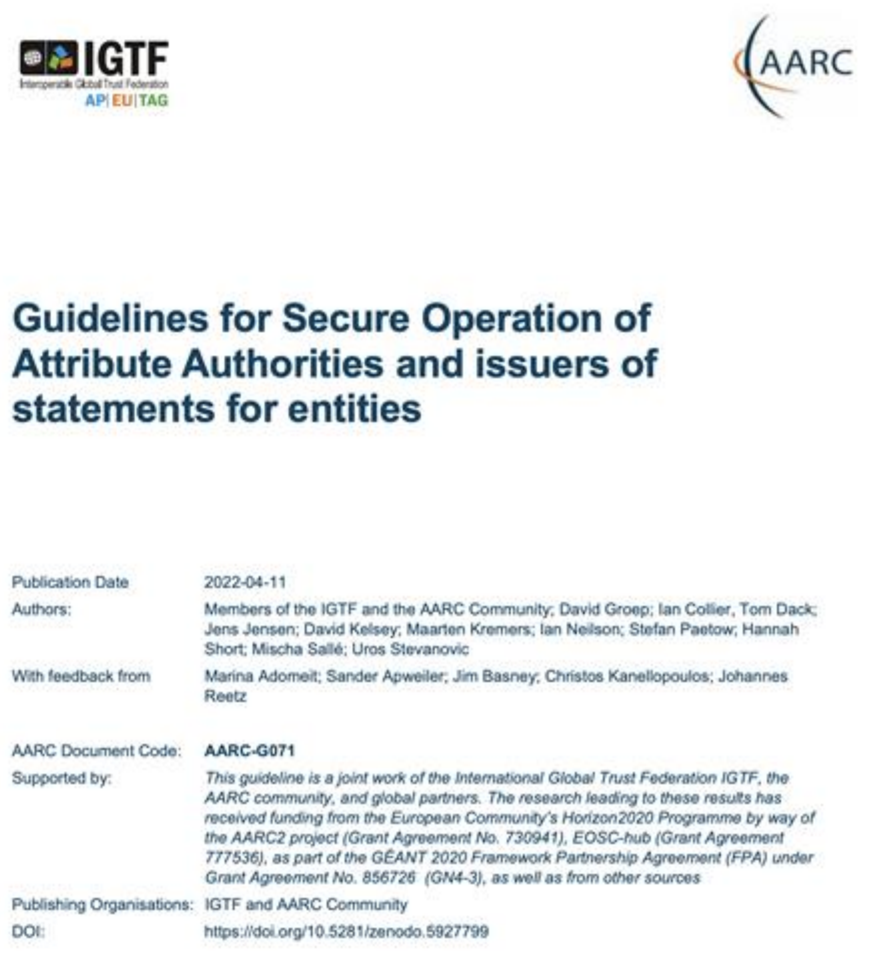
- How to securely operate proxies, attribute authorities and issuers of statements for entities?

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



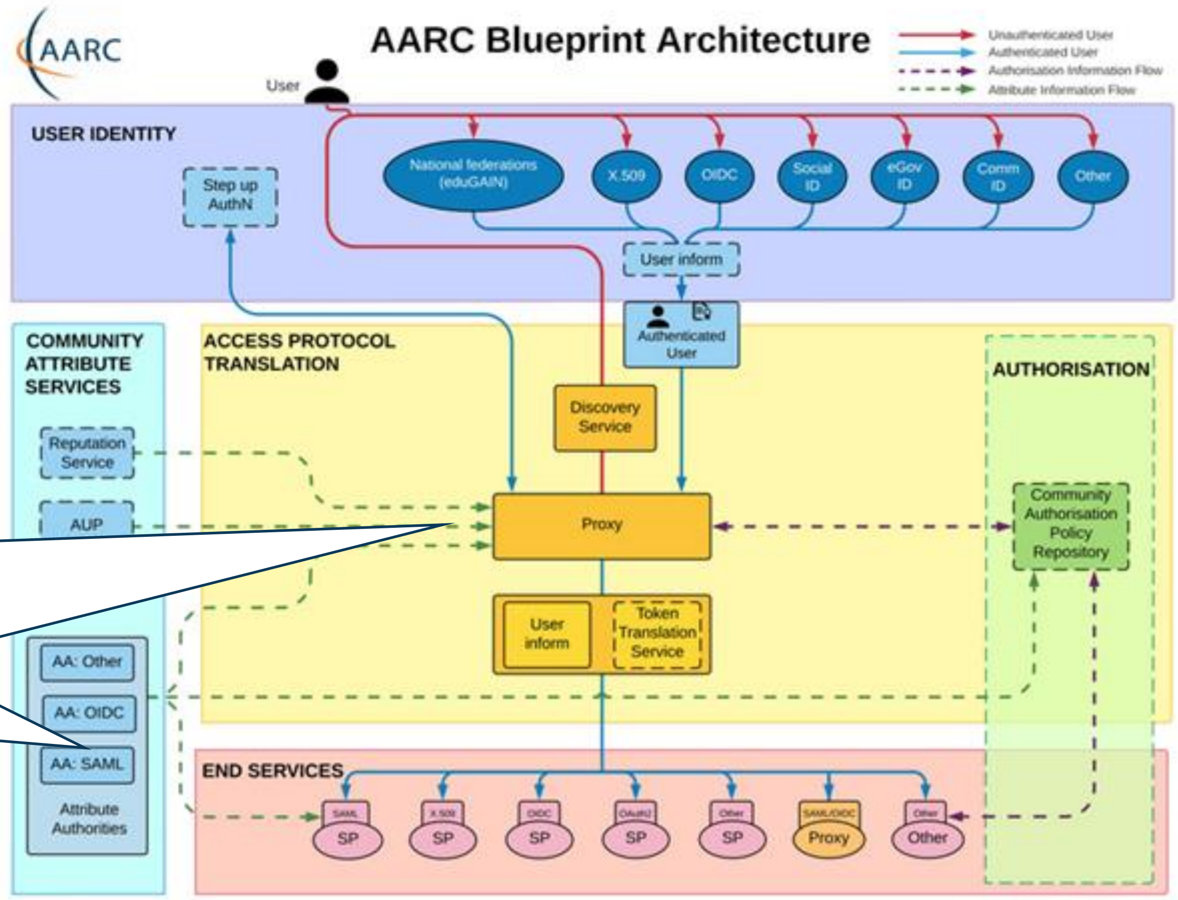
Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities

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

Operational security focus in the BPA: beyond just the IdPs

Community membership management directories and attribute authorities

- integrity of membership
- identification, naming and traceability
- site and service security
- protection on the network
- assertion integrity



Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements
(AARC-I048, in collaboration with IGTF AAOPS)

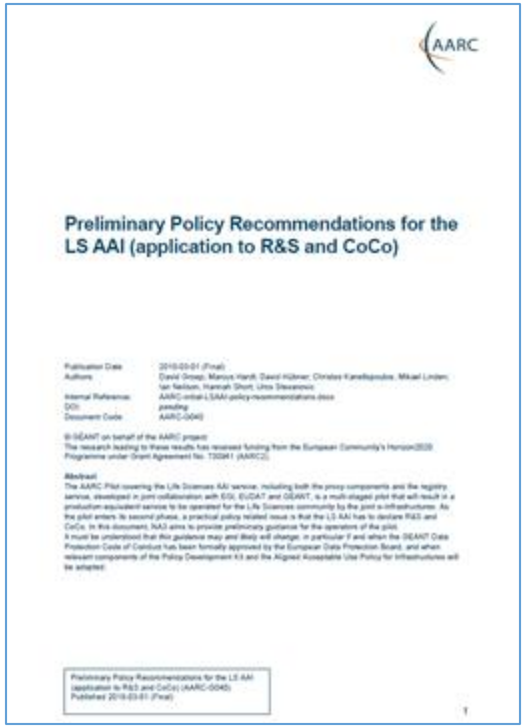
Proxies have more challenges as well: AUPs, T&Cs, Privacy notices, …

For large ‘multi-tenant’ proxies

- some subset users in some communities use a set of services – how to present their Terms and Conditions and their privacy policies, so that 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

For community and dedicated proxies

- when new (sensitive) services join, who needs to see the new T&Cs?
- can we communicate existing acceptance of T&Cs to downstream services?



AARC

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

Publication Date	2019-03-01 (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 GÉANT 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.

Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo) (AARC-G040)
Published 2019-03-01 (Final)

1

beyond AARC-G040

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

‘with fewer clicks to more resources’

WISE Baseline AUP

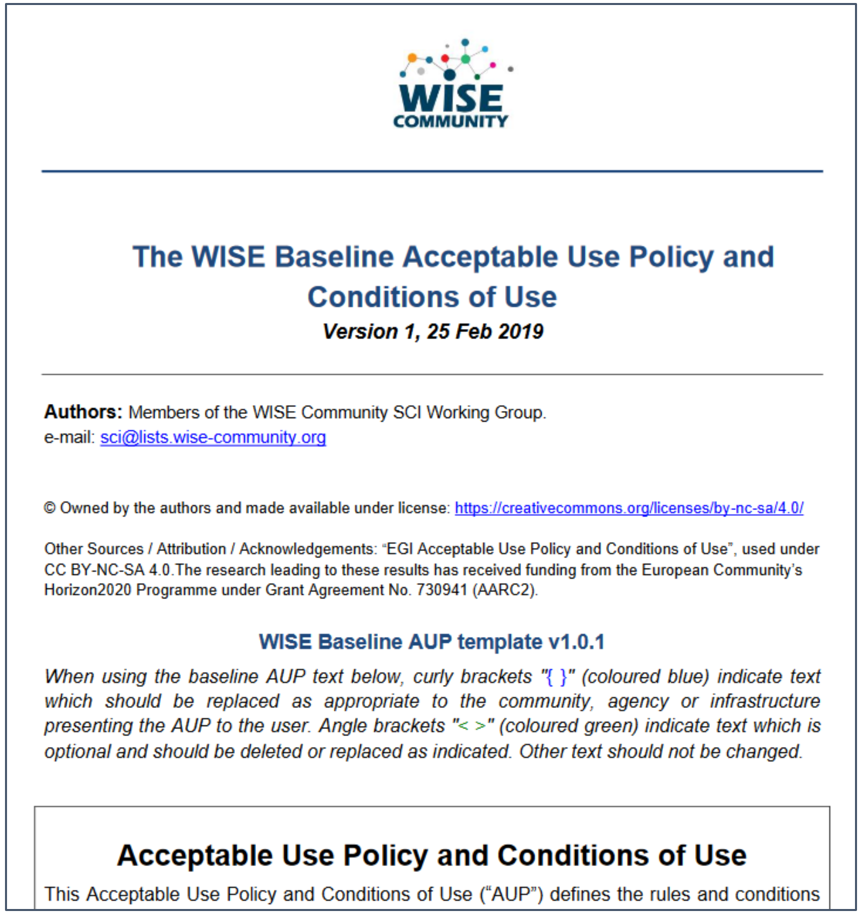
Template for a common and cascading AUP and T&C notice

by intent focusses primarily on *acceptable use*

- do not dwell on unintended use
- guarantee and service levels are T&Cs, not acceptable use interoperability

Placeholder model for

- *scope of the AUP* (purpose binding)
  – mirrored in Service Security operational baseline
- 10 commandments
- placeholder for additional T&Cs
- privacy notice references and authority



The WISE Baseline Acceptable Use Policy and Conditions of Use

Version 1, 25 Feb 2019

Authors: Members of the WISE Community SCI Working Group.
e-mail: sci@lists.wise-community.org

© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/

Other Sources / Attribution / Acknowledgements: "EGI Acceptable Use Policy and Conditions of Use", used under CC BY-NC-SA 4.0.The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

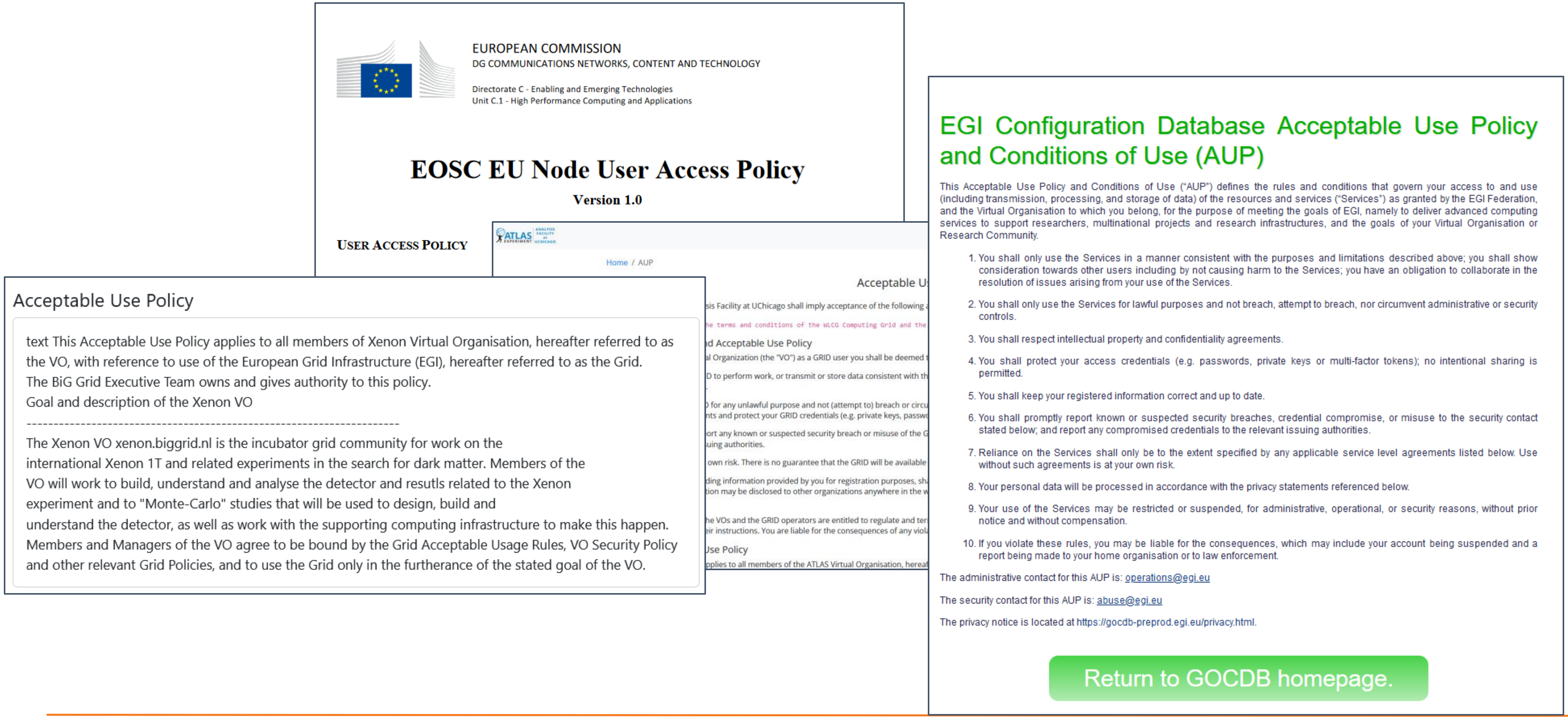
WISE Baseline AUP template v1.0.1

When using the baseline AUP text below, curly brackets "{ }" (coloured blue) indicate text which should be replaced as appropriate to the community, agency or infrastructure presenting the AUP to the user. Angle brackets "< >" (coloured green) indicate text which is optional and should be deleted or replaced as indicated. Other text should not be changed.

Acceptable Use Policy and Conditions of Use

This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules and conditions

How many of these?



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

Home / AUP

Acceptable U

sis Facility at UChicago shall imply acceptance of the following

he terms and conditions of the WLCG Computing Grid and the

d Acceptable Use Policy

al Organization (the "VO") as a GRID user you shall be deemed

D to perform work, or transmit or store data consistent with th

) for any unlawful purpose and not (attempt to) breach or circu
nts and protect your GRID credentials (e.g. private keys, passw

ort any known or suspected security breach or misuse of the G
uing authorities.

own risk. There is no guarantee that the GRID will be available

ding information provided by you for registration purposes, sh
tion may be disclosed to other organizations anywhere in the w

he VOs and the GRID operators are entitled to regulate and ter
eir instructions. You are liable for the consequences of any viol

Use Policy

pplies to all members of the ATLAS Virtual Organisation, hereaf

Acceptable Use Policy

text This Acceptable Use Policy applies to all members of Xenon Virtual Organisation, hereafter referred to as the VO, with reference to use of the European Grid Infrastructure (EGI), hereafter referred to as the Grid.
The BiG Grid Executive Team owns and gives authority to this policy.
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.

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.
6. You shall promptly report known or suspected security breaches, credential compromise, or misuse to the security contact stated below; and report any compromised credentials to the relevant issuing authorities.
7. Reliance on the Services shall only be to the extent specified by any applicable service level agreements listed below. Use without such agreements is at your own risk.
8. Your personal data will be processed in accordance with the privacy statements referenced below.
9. Your use of the Services may be restricted or suspended, for administrative, operational, or security reasons, without prior notice and without compensation.
10. If you violate these rules, you may be liable for the consequences, which may include your account being suspended and a report being made to your home organisation or to law enforcement.

The administrative contact for this AUP is: operations@egi.eu

The security contact for this AUP is: abuse@egi.eu

The privacy notice is located at https://gocdb-preprod.egi.eu/privacy.html.

AARC G082 Notice Management by Proxies

Four presentation models. In order of preference

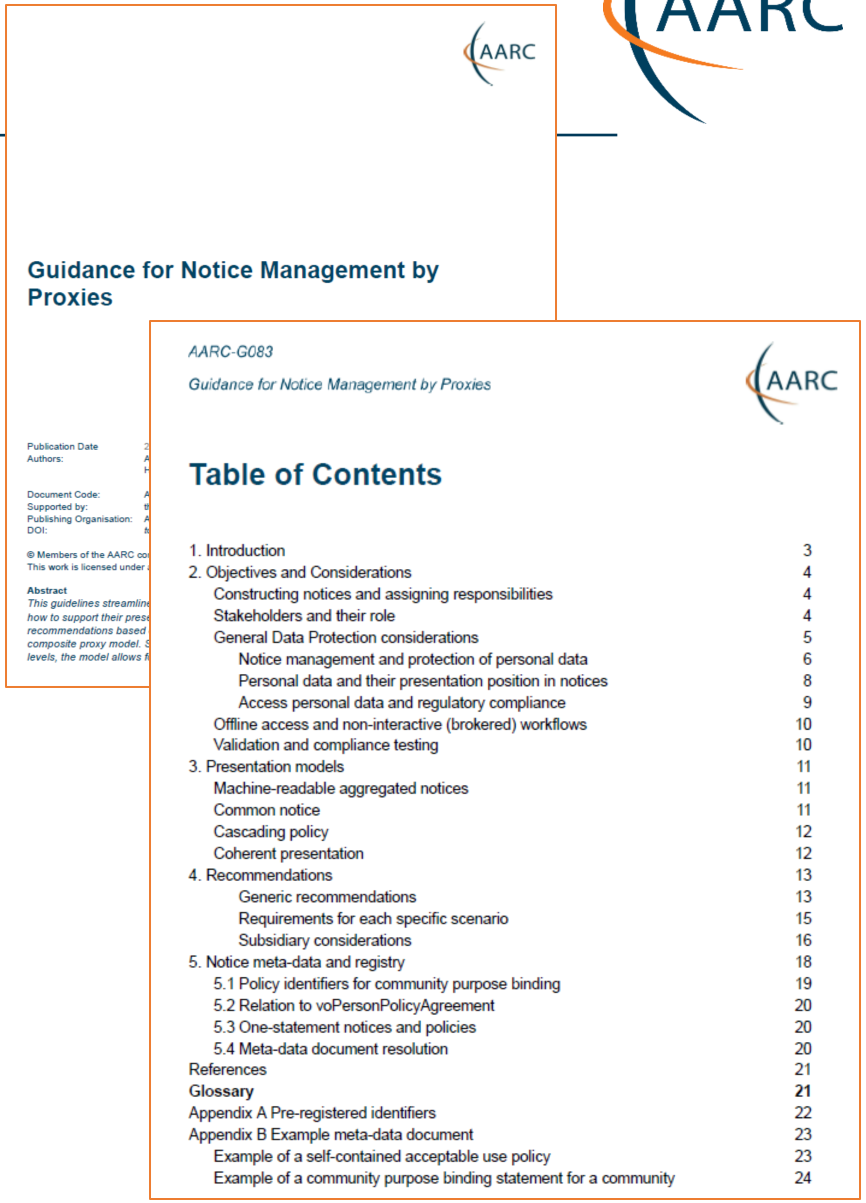
1. machine-readable aggregated notice
2. common notice (single common authority domain)
3. cascading notices (assume responsibility for underlings)
4. coherent presentation (you show what you need, but not more)

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



Guidance for Notice Management by Proxies

Publication Date 2
Authors: A
H

Document Code: A
Supported by: th
Publishing Organisation: A
DOI: to

© Members of the AARC co
This work is licensed under a

Abstract

This guidelines streamline how to support their prese recommendations based composite proxy model. S levels, the model allows f

AARC-G083

Guidance for Notice Management by Proxies

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

https://aarc-community.org/guidelines/aarc-g083/

AARC Ixxx Lightweight Community Management

“small to mid-sized communities do not have the resources to maintain a bespoke community management policy”

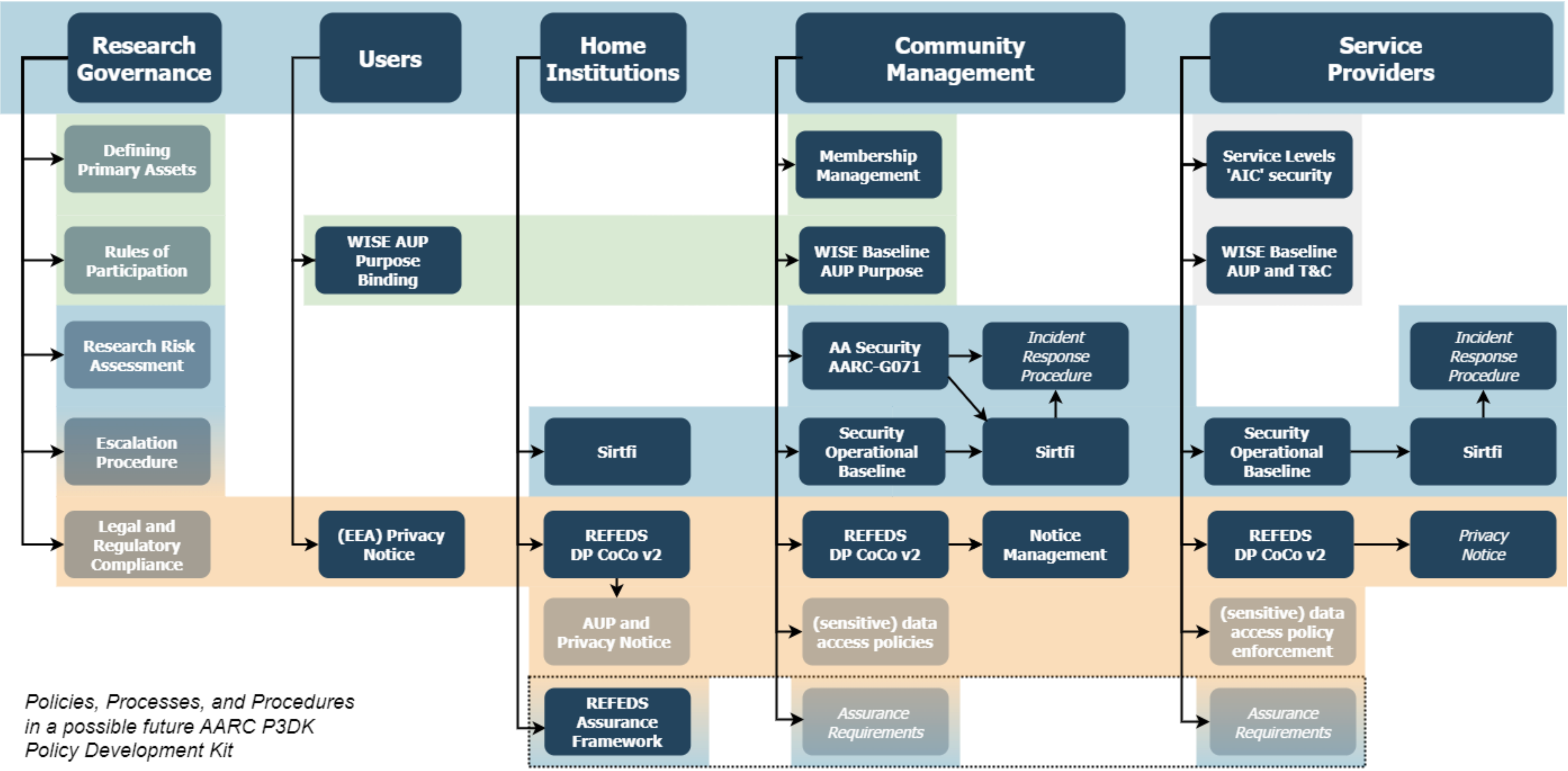
this leaves communities *and SP operators* unclear about trust assurance level of members

This leaves communities *and SP operators* unclear about trust assurance level of members

5 commandments

- **Unique Name**
- **AUP Compliance**
- **Privacy Awareness**
- **Valid Authorizations**
- **Incident Response**

Policy Development Kit: simplify by re-using good practice



Research Governance
- Defining Primary Assets
- Rules of Participation
- Research Risk Assessment
- Escalation Procedure
- Legal and Regulatory Compliance

Users
- WISE AUP Purpose Binding
- (EEA) Privacy Notice

Home Institutions
- Sirtfi
- REFEDS DP CoCo v2 → AUP and Privacy Notice
- REFEDS Assurance Framework

Community Management
- Membership Management
- WISE Baseline AUP Purpose
- AA Security AARC-G071 → Incident Response Procedure; AA Security AARC-G071 → Sirtfi
- Security Operational Baseline → Sirtfi → Incident Response Procedure
- REFEDS DP CoCo v2 → Notice Management
- (sensitive) data access policies
- *Assurance Requirements*

Service Providers
- Service Levels 'AIC' security
- WISE Baseline AUP and T&C
- Security Operational Baseline → Sirtfi → *Incident Response Procedure*
- REFEDS DP CoCo v2 → *Privacy Notice*
- (sensitive) data access policy enforcement
- *Assurance Requirements*

Policies, Processes, and Procedures
in a possible future AARC P3DK
Policy Development Kit

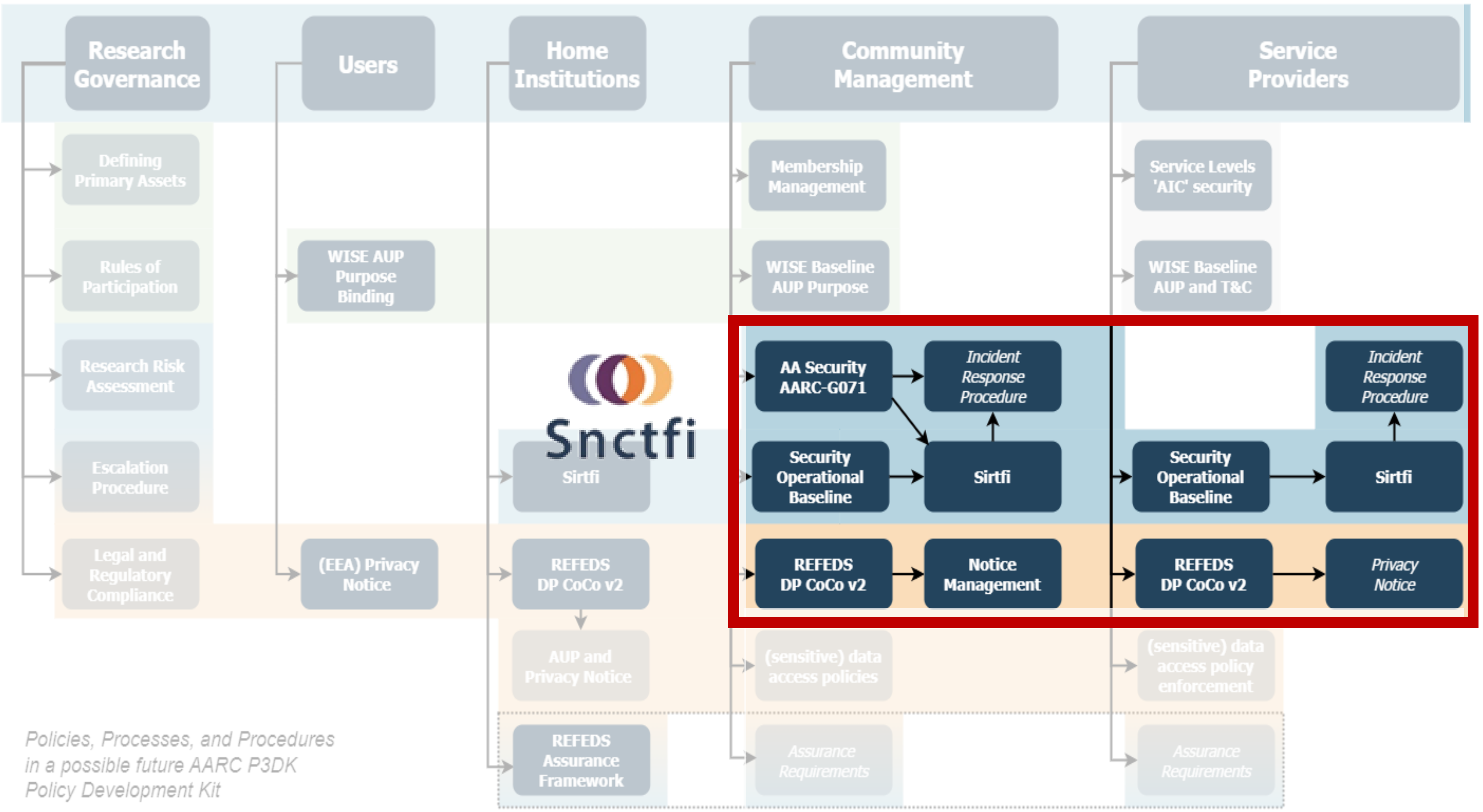
🟩 Purpose of the collaboration

🟦 Protection of the collaboration, its ICT services and resources

🟧 Protection of the collaborating users (and any sensitive research data)

Source: David Groep

Policy Development Kit: simplify by re-using good practice



Research Governance

Users

Home Institutions

Community Management

Service Providers

Defining Primary Assets

Rules of Participation

Research Risk Assessment

Escalation Procedure

Legal and Regulatory Compliance

WISE AUP Purpose Binding

(EEA) Privacy Notice

Snctfi

Sirtfi

REFEDS DP CoCo v2

AUP and Privacy Notice

REFEDS Assurance Framework

Membership Management

WISE Baseline AUP Purpose

AA Security AARC-G071

Incident Response Procedure

Security Operational Baseline

Sirtfi

REFEDS DP CoCo v2

Notice Management

(sensitive) data access policies

Assurance Requirements

Service Levels 'AIC' security

WISE Baseline AUP and T&C

Incident Response Procedure

Security Operational Baseline

Sirtfi

REFEDS DP CoCo v2

Privacy Notice

(sensitive) data access policy enforcement

Assurance Requirements

Policies, Processes, and Procedures in a possible future AARC P3DK Policy Development Kit

🟩 Purpose of the collaboration

🟦 Protection of the collaboration, its ICT services and resources

🟧 Protection of the collaborating users (and any sensitive research data)

communities sourcing ‘well-operated’ community platforms

eduTEAMS

egi

B2ACCESS

SURF
(SRAM)

CILogon

and a few more …

through their scale gets federations to trust our AARC ‘middle boxes’

Source: David Groep

AARC Community - open for all

AARC Engagement Group for Infrastructures

The forum of e/r-Infras that operate an AARC BPA complaint AAI.
It’s a closed group on purpose as we want to get feedback from the hands on group.
They approve the AARC guidelines.

Technical WG

- Led by Nicolas and Christos
- Where technical guidelines are discussed
- Anybody can join the discussion: **https://lists.geant.org/sympa/info/aarc-architecture**

Policy WG

- Led by Dave and David
- Supported by EnCo and IGTF
- Anybody can join the discussion: **policy@aarc-community.org**
  https://lists.geant.org/sympa/info/aarc-na3

With many thanks to David Groep
for Input of the slides

Thank you
Any Questions?

maarten.kremers@surf.nl

AARC

https://aarc-community.org

The work leading to these results has received funding from the European Union 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).