

AARC Policy Harmonisation

Despite all potential differences between user communities, research infrastructures, federations, identity providers, and e-Infrastructures, they all work towards a common goal. And they are sufficiently alike that they might share some common policy frameworks. While it is always tempting to make ad-hoc policies, an open research commons benefits hugely from mutual understanding based on set of a harmonized policy frameworks and ways to compare the various best practice aspects.

The Policy and Best Practice Harmonisation activity works on operational and security aspects and policies to complement the technical research work carried out in the architecture and the infrastructures, and delivers a set of recommendations and good practices to implement a scaleable and cost-effective policy and operational framework driven by the use cases from the AARC Community. Policy harmonisation produces both [generic guidelines](#) (such as on operational security and traceability for proxies, acceptable use policy matching, and trust and assurance models) as well as [specific guidelines for communities](#) that are implementing the Blueprint Architecture.



In-person meeting: PMA+ February 2025 meeting

In-person AARC Policy Coordination meeting (remote participation possible of course): <https://indico.cern.ch/event/1461429/> at the 63rd EUGridPMA+ meeting.

Note: This meeting will replace the weekly I082 call on Wed Feb 5, 2025



Policy Coordination calls

There are monthly Policy Coordination Calls the 3rd Monday of the month

- call details at <https://indico.nikhef.nl/category/101/>.
- review notes at <https://sharemd.nikhef.nl/s/gfrboBQm->

Trust Framework documents review (AARC-I082/AARC-TREE D2.1): weekly calls Wednesday 09.00 AM Europe/Amsterdam time

- <https://nikhef-nl.zoom.us/j/85962833769>

Current work items (supported by AARC TREE)

- [AARC-I082 - Trust framework for proxies and Snctfi research services](#)
- EU Identity Wallets (VCs) and assurance step-up

Under review

- [AARC-G084 - Security Operational Baseline](#) (public page: <https://aarc-community.org/guidelines/aarc-g084/>)

Recently completed documents and guidelines

- [AARC-G083 - Guidance for Notice Management by Proxies](#)

Policy activities are continuously evolving

- [Security Incident Response in federated environments](#)
 - [including guidelines on how to properly protect your community attribute system](#)
 - [and how to prepare and what to do in case of incidents](#)
 - traceability of events through a (network of) AARC BPA Proxies
- Service- and Infrastructure-centric policy support, including
 - [Protection of \(mainly personal\) data that is generated as a result of infrastructure use \(e.g. in accounting\) and the impact of GDPR](#)
 - [Attribute release from the proxy](#)
 - [Security For Collaboration among Infrastructures assessment](#) (AAOPS-G071 Review)
- e-Researcher centric policies,
 - simplified policy development kit also for smaller and mid-sized communities
 - alignment of [Acceptable Use Policies](#)
 - [Assurance Level baseline and differentiated assurance profiles](#) (alongside [a self-assessment tool](#)) including the use of government e-ID for step-up of assurance
 - [untangling identity assurance framework complexity](#)
 - novel federation models and trust paths (e.g. in OpenID Connect Federation)
- [Engagement and coordination](#) with FIM4R and the global community
- Support for Infrastructures and Communities with the [Policy Development Kit \(PDK\)](#)

Lastly, it is imperative that any policies are agreed to in a scalable way: bi-lateral agreements do not work in a multi-stakeholder environment. The [work on scalable policy negotiation](#) addresses this issue by exploring ways of expressing and agreeing policy in a federated world: [Snctfi](#).

Take [the slide tour](#), or read our [whitepapers](#) and [guidelines](#)

