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.

Policy Coordination calls

There are monthly Policy Coordination Calls, currently supported by AARC TREE and the global community. You can of course review the notes at https://sharemd.nikhef.nl/s/gfrboBQm-, but are also warmly invoted to join the calls on the 3rd Monday of the month. You can find the call details at https://indico.nikhef.nl/category/101/

In AARC, we place primary focus on a selected set of elements that are currently the most pressing for either communties or generic Infrastructure AAIs:

- Security Incident Response in federated environments
  - including guidelines on how to property 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 kti 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.

Read the AARC2 First Year Report and the AARC TREE white papers to get to grips with our policy coordination activities, take the slide tour, or read our whitepapers and guidelines