Authentication and Authorisation for Research and Collaboration

Trust framework for proxies and Snctfi research services

AARC-I082, AARC TREE D2.1

David Groep
Policy Area
Nikhef and Maastricht University

PMA+, AARC Policy, EnCo Joint Meeting Prague
May 2025

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/

Specific aims

- Analyse issues with PDK v1
  - mixing policy and procedures
  - cross-border terminology issues
  - audience ‘challenges’
- Leverage the possibility for ‘offloading’ AAI proxy tasks to provides
  - especially for small/midsize communities
- New structure of the PDK – but not the content itself, this is the *framework*
- New BPA2025 components: identity proxy, site-local proxy
- common pitfall for AAI design when governance is not clear

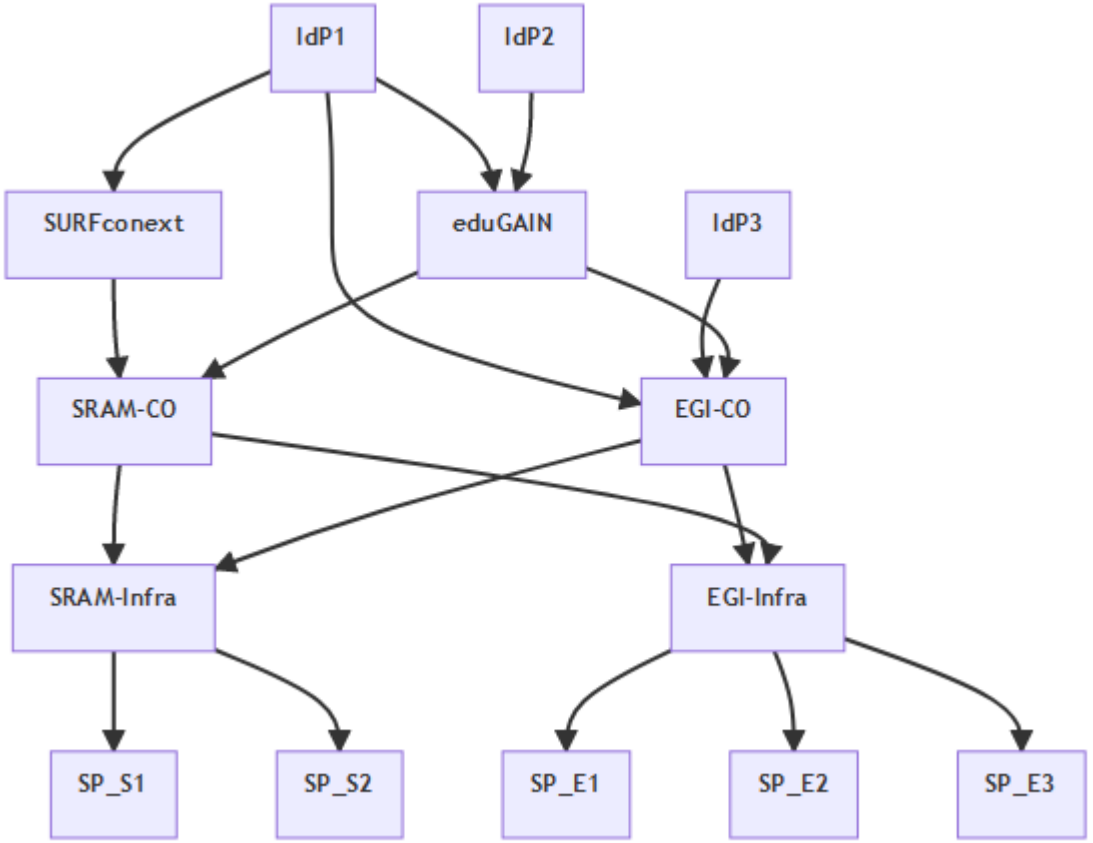
Trust beyond AARC PDK version 1 and the ‘2019’ BPA

“The Trust framework identifies the smallest set of distinct guidelines (policies, good practices, procedures) necessary to cover trust, security, and operational interaction of proxies in composite-proxy scenarios beyond the community-and-infrastructure proxy doublet of AARC-G045.

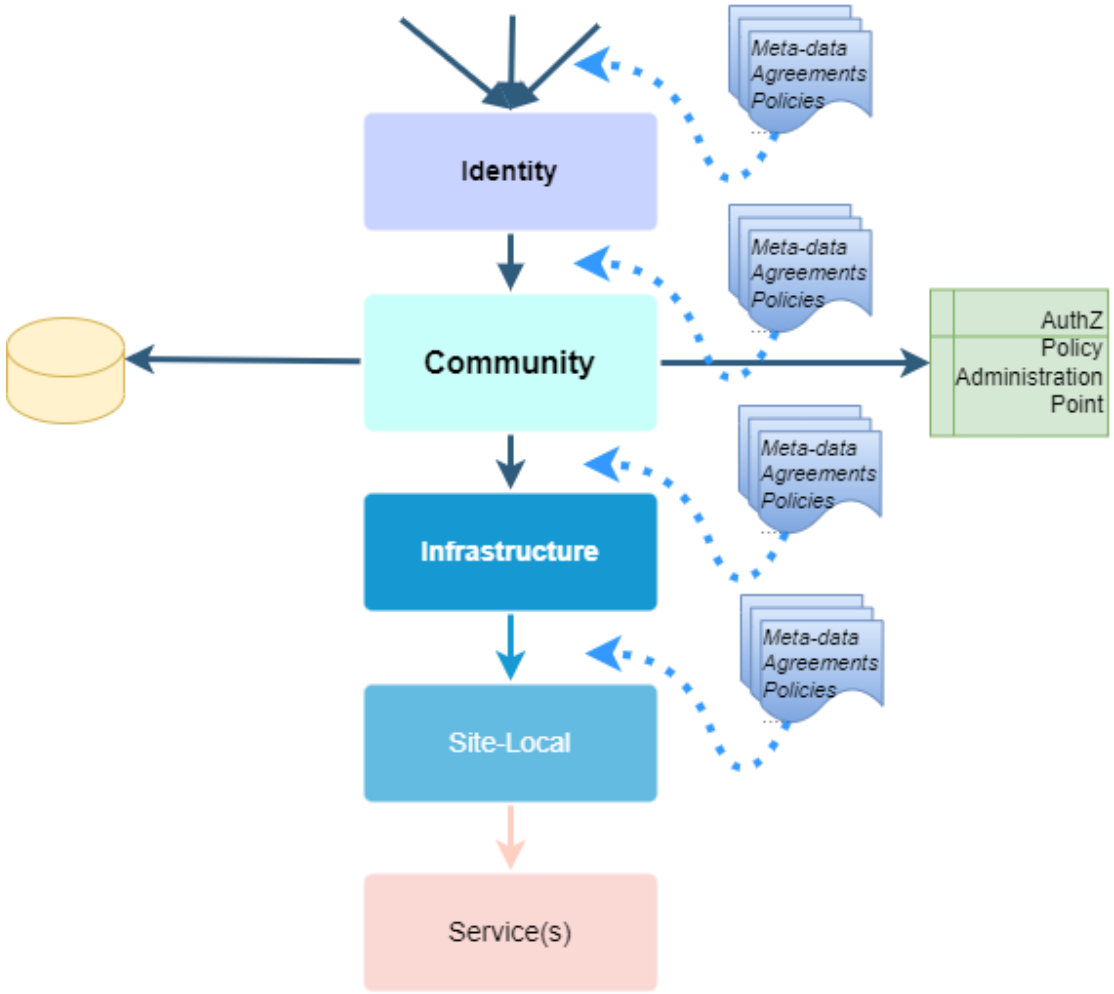
Some elements may already be in place, such as the attribute authority operations security guidance AARC-G071, others have only been identified as needed but have not yet been described in sufficient detail to formulate policy of good practice.

The aim of this paper is to identify the smallest set of distinct guidelines, practices, and procedures needed.”

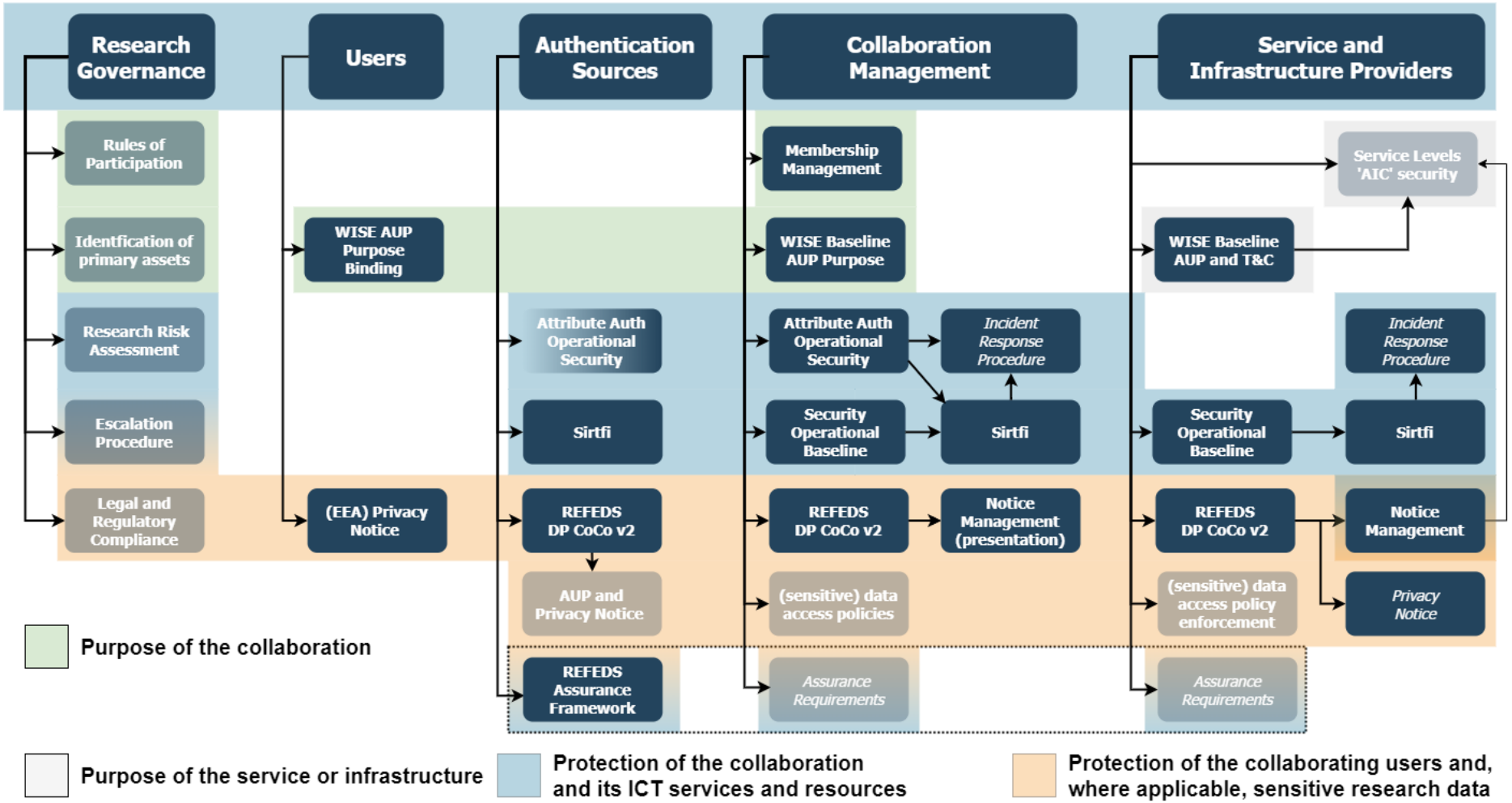
Why Loops Should Be Forbidden (BPA2025)



Proxies and more proxies



Proposed trust framework (and hence PDKv2)



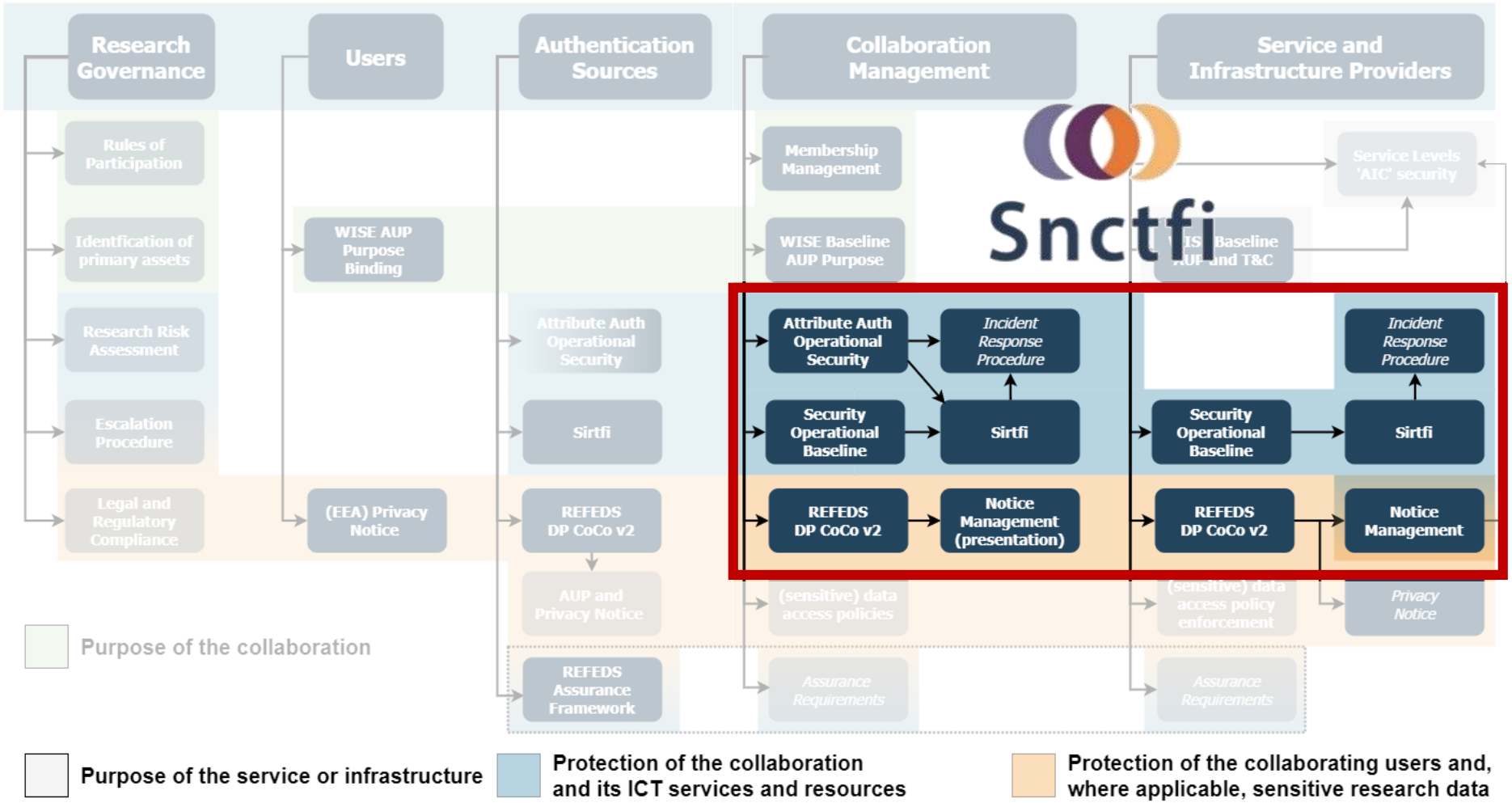
Snctfi

- **20250220 consensus**: Snctfi will be the set of guidelines that define the trust in the proxy itself, that a proxy operator can control and assert. This means: Sirtfi, Security Operational Baseline, GEANT DPCoCov2, AAOPS, and the Notice Management guidelines. This makes Sntfi into a ‘verifiable’ set that can be ‘checked’ when a (community) looks for a provider of proxy/aai services. Most communities will not be running their own.

- Snctfi also affects ‘southbound’ entities (other proxies and SPs) in a similar way that NIS2.0 does it, unless there is a clear way that the proxy itself can absorb the whole issue. This in particular applies to the Security operational baseline, but also DPCOCO. For Sirtfi incident response, the proxy might implement local controls to mitigate the impact form downstream services not doing Sirtfi correctly?

- There are hence parts of the PDK that are not included in Snctfi, such as the Community Membership Management (since the community cannot request that from the proxy they are procuring), not the user-level purpose binding and SLAs.

The Snctfi 'offloadable' platform aspects of the PDKv2



AARC I082 ‘informational’ guidance

Review of AARC I082

Informational pages

- https://wiki.geant.org/display/AARC/AARC-I082+Trust+framework+for+proxies+and+Snctfi+research+services

Direct document link

- https://edu.nl/uu3qt

Thank you

Any Questions?

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).