AARC Authentication and Authorisation for Research and Collaboration

Coordination policies in a multi proxy set-up

Building Trust across a Landscape of AARC BPA Proxies

David Groep

AARC Policy Area Coordinator

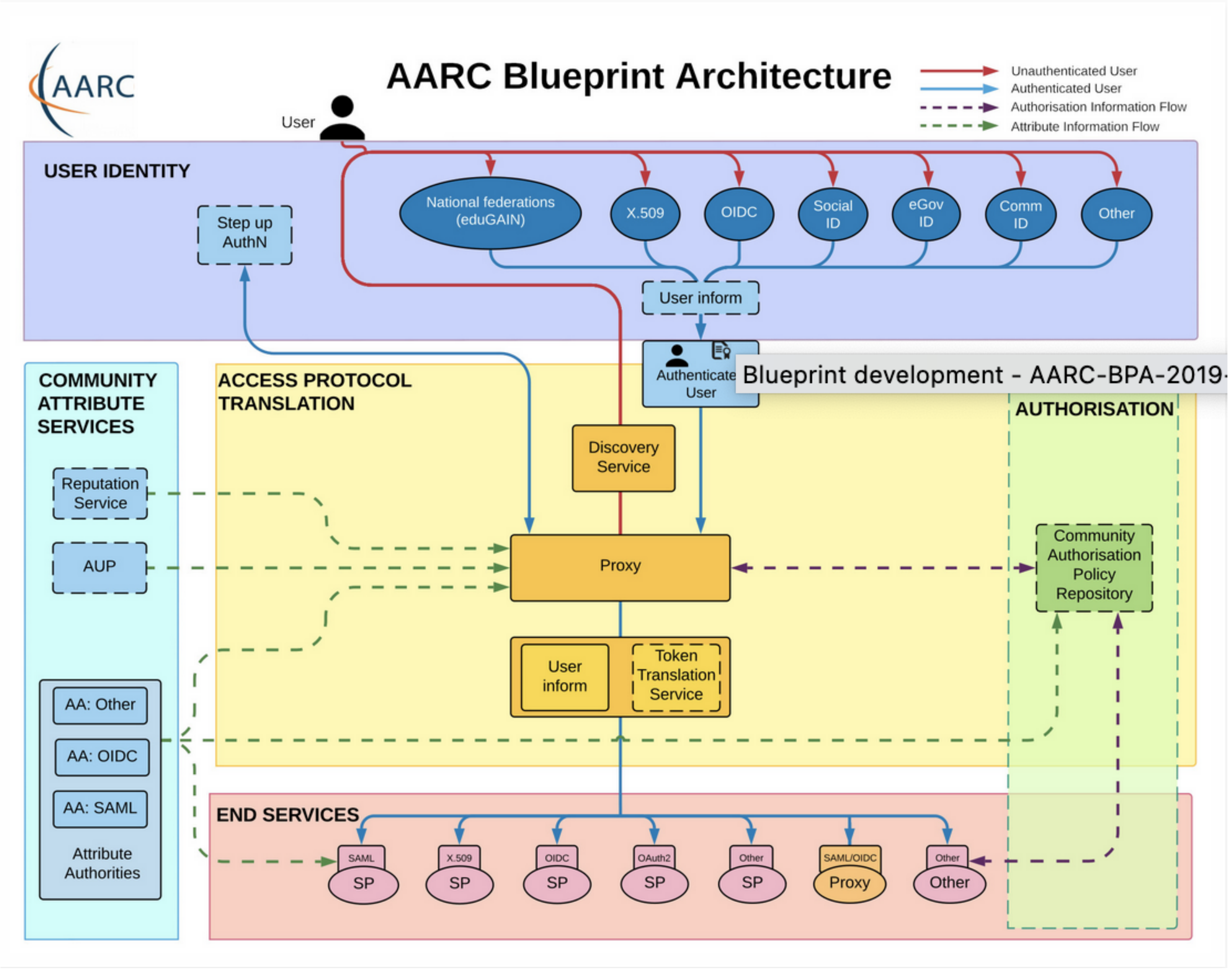
Nikhef Maastricht University

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

FIM4R 18

January 2023

Arguably the best known picture from our AARC community



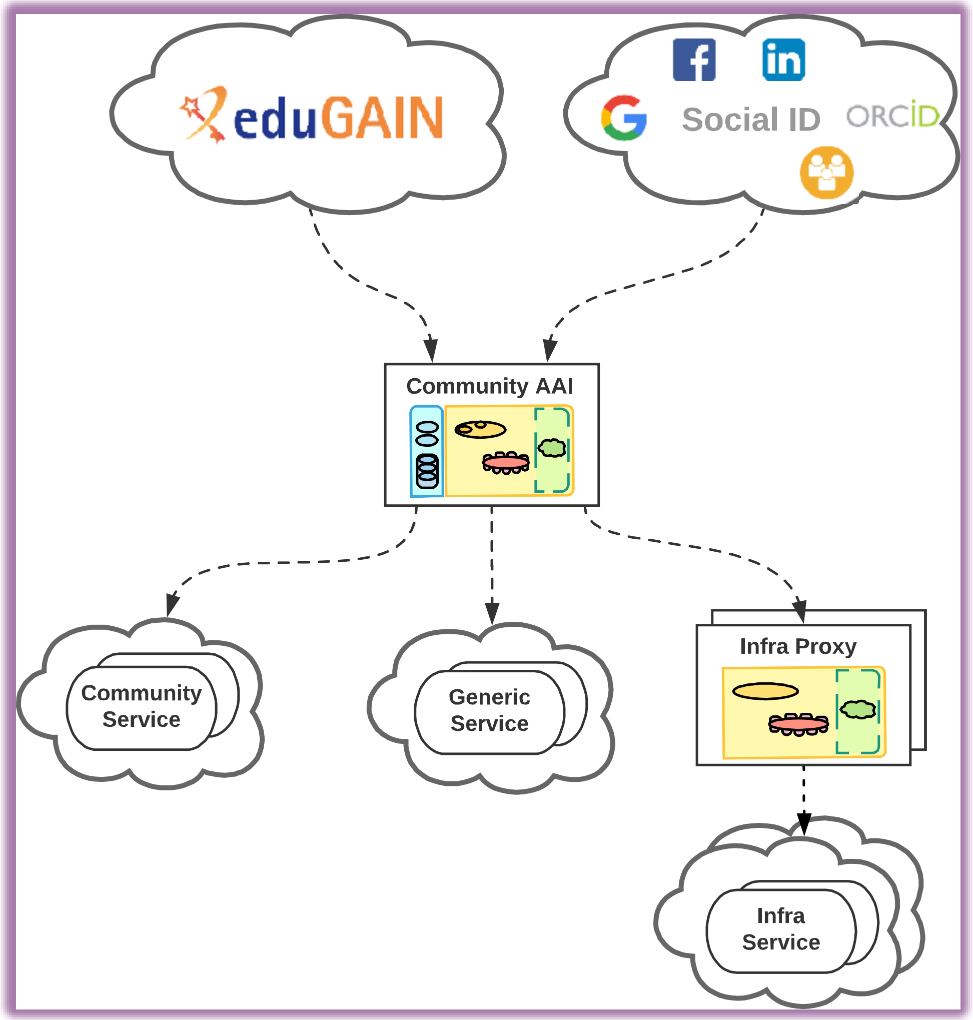
Blueprint development - AARC-BPA-2019-

Beyond a single BPA proxy – complexities in composite infrastructure

EOSC AAI was one of the triggers to extend the BPA but is and will not be the only one!

- 2019 “BPA Reloaded” (AARC-G045) lead us to composite proxy architectures
- and as we see the need grow for multiple instances of community and e-Infra proxies to work together, we end up with …

… a federation of proxies ?! ☺



AARC G045 https://aarc-community.org/guidelines/aarc-g045/
and EOSC AAI Task Force report – ISBN 978-92-76-28113-9, DOI:10.2777/8702

Composite proxies and more proxies!

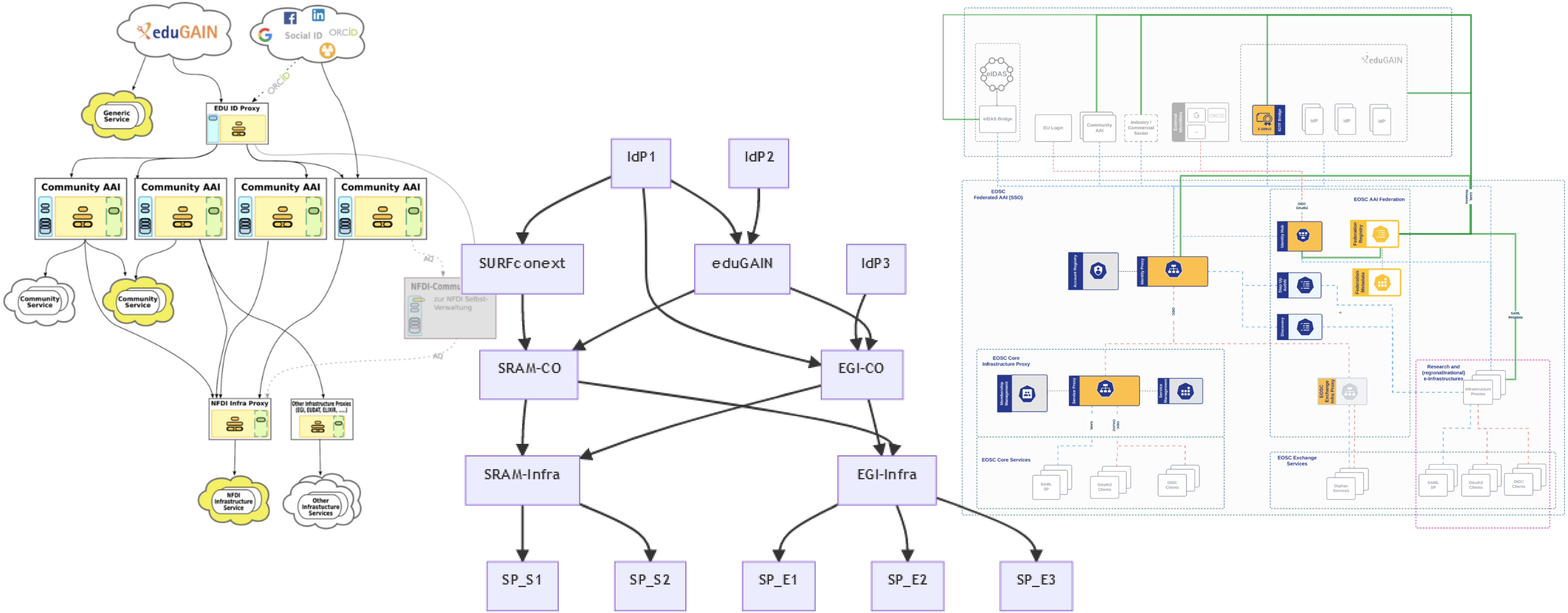
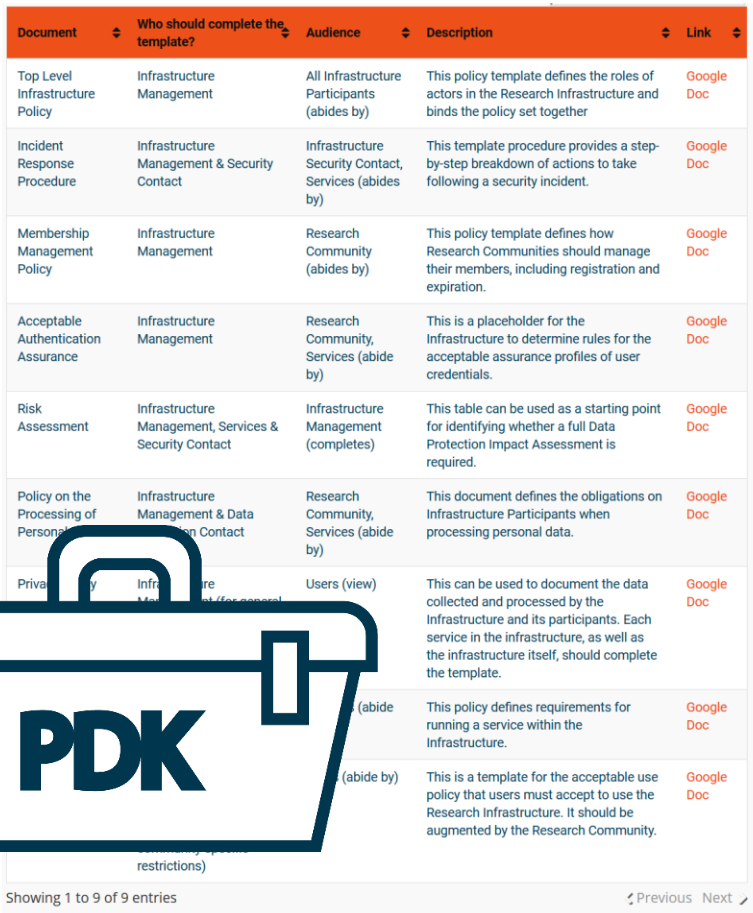


Image (right): EOSC AAI for the EOSC Core and Exchange Federation for the EOSC European Node by Christos Kanellopoulos, Nicolas Liampotis, David Groep (June 2023)
Centre: SURF SRAM, as described by Maarten Kremers (EUGridPMA59 notes) Image (left): Marcus Hardt for the NFDI AAI

And an AARC beyond Sirtfi, RCauth, and the Policy Development Kit?

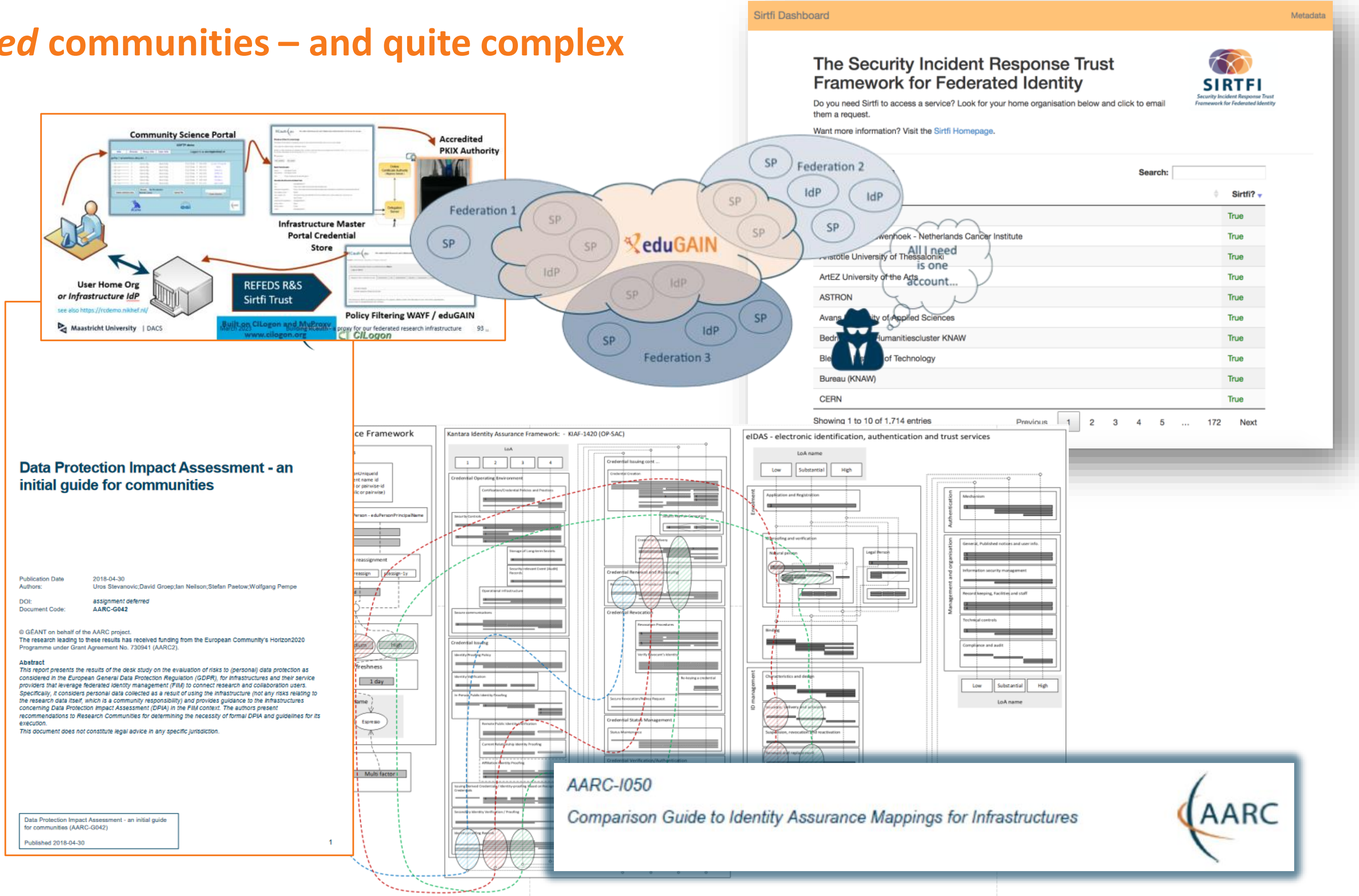
Current PDK is targeted at *large and structured* communities – and quite complex



Document	Who should complete the template?	Audience	Description	Link
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together	Google Doc
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template procedure provides a step-by-step breakdown of actions to take following a security incident.	Google Doc
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.	Google Doc
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.	Google Doc
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.	Google Doc
Policy on the Processing of Personal [illegible]	Infrastructure Management & Data [illegible]n Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.	Google Doc
Priva[illegible]y	Infra[illegible]re Ma[illegible]nt (for general [illegible]	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
[illegible]	[illegible]	[illegible] (abide	This policy defines requirements for running a service within the Infrastructure.	Google Doc
[illegible]	[illegible] restrictions)	[illegible] (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



Community Science Portal
Infrastructure Master Portal Credential Store
Accredited PKIX Authority
User Home Org or Infrastructure IdP
see also https://rcdemo.nikhef.nl/
REFEDS R&S Sirtfi Trust
Policy Filtering WAYF / eduGAIN
Built on CILogon and MyProxy www.cilogon.org
CILogon
Maastricht University | DACS
Federation 1
Federation 2
Federation 3
eduGAIN
SP
IdP
All I need is one account...
ce Framework
Kantara Identity Assurance Framework: KIAF-1420 (OP-SAC)
eIDAS - electronic identification, authentication and trust services
LoA name
Low
Substantial
High
freshness
1 day
Espresso
Multi factor

Sirtfi Dashboard Metadata

The Security Incident Response Trust Framework for Federated Identity

SIRTFI Security Incident Response Trust Framework for Federated Identity

Do you need Sirtfi to access a service? Look for your home organisation below and click to email them a request.

Want more information? Visit the Sirtfi Homepage.

Search:

	Sirtfi?
[illegible]	True
[illegible]wenhoek - Netherlands Cancer Institute	True
[illegible]stotle University of Thessaloniki	True
ArtEZ University of the Arts	True
ASTRON	True
Avans [illegible]ity of Applied Sciences	True
Bedr[illegible]umanitiescluster KNAW	True
Ble[illegible] of Technology	True
Bureau (KNAW)	True
CERN	True

Showing 1 to 10 of 1.714 entries Previous 1 2 3 4 5 … 172 Next

Data Protection Impact Assessment - an initial guide for communities

Publication Date 2018-04-30
Authors: Uros Stevanovic;David Groep;Ian Neilson;Stefan Paetow;Wolfgang Pempe

DOI: *assignment deferred*
Document Code: **AARC-G042**

© 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
This report presents the results of the desk study on the evaluation of risks to (personal) data protection as considered in the European General Data Protection Regulation (GDPR), for infrastructures and their service providers that leverage federated identity management (FIM) to connect research and collaboration users. Specifically, it considers personal data collected as a result of using the infrastructure (not any risks relating to the research data itself, which is a community responsibility) and provides guidance to the infrastructures concerning Data Protection Impact Assessment (DPIA) in the FIM context. The authors present recommendations to Research Communities for determining the necessity of formal DPIA and guidelines for its execution.
This document does not constitute legal advice in any specific jurisdiction.

Data Protection Impact Assessment - an initial guide for communities (AARC-G042)

Published 2018-04-30 1

AARC-I050

Comparison Guide to Identity Assurance Mappings for Infrastructures

AARC

https://aarc-community.org/policy

Effort in AARC TREE to address issues and explore policy needs

- AARC-TREE topics are scoped (and effort assigned to each), with results defined in terms of how guidelines support proxy use cases and communities
- Participatory model, with FIM4R, AEGIS, and community management authorities
- What is needed for operational trust in terms of, *e.g.*, ‘baseline requirements’?

Let’s look at some we identified when writing AARC-TREE …

New good practices … and there are more and different policy needs now

Infrastructure alignment and policy harmonisation: helping out the proxy

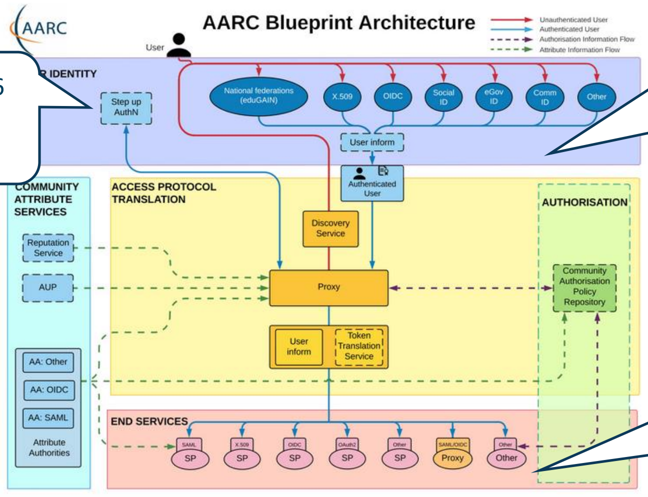
- Operational Trust for Community and Infrastructure BPA Proxies
- Snctfi - increasing acceptance of research infrastructure proxies with R&E identity providers and sources of authentication
- Review infrastructure models for **coordinated AUP, T&C, and privacy notices**, improving cross-infrastructure user experience

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
- FIM4R policy workshop series on validation of the restructured policy framework (together with the new ‘BPA’)

“Operational Trust Framework for Community & Infrastructure Proxies”

In the authentication and service management space there are well-recognised operational security systems available …



RFC6238/4226
FIPS140-2
NISTSP800-53

Authentication/identity sources
Sirtfi and (eduGAIN) baselining
REFEDS Assurance Framework
IGTF AP Profiles
NIST SP800-63
eduGAIN Security Handbook

Service provider operations
ISO27k
Sirtfi
Infrastructure response plans

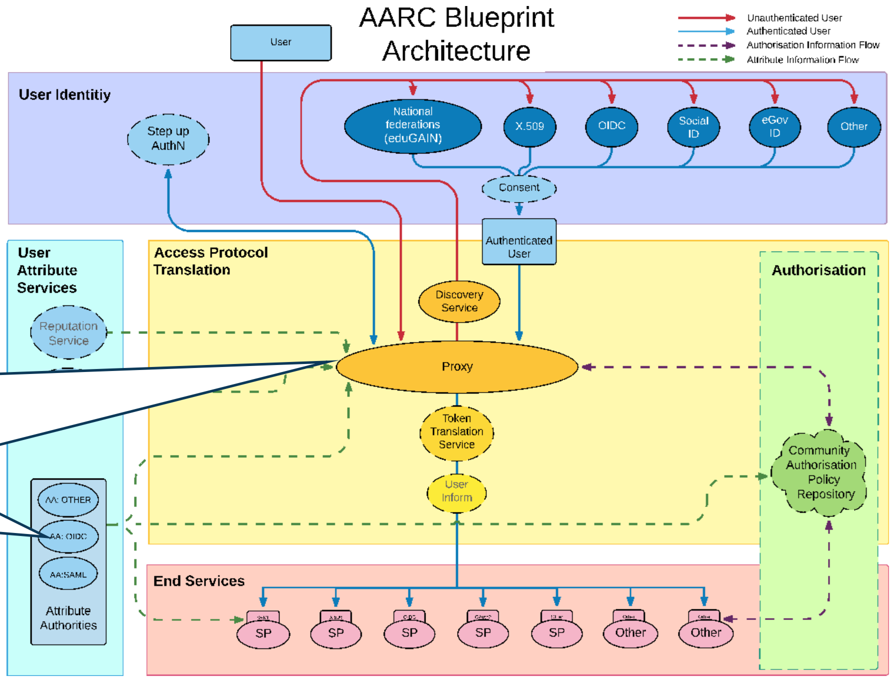
but proxies themselves are (far more!) valuable.
How are these to be protected?
Can we learn from each other as these are proliferating?

AARC G071 is there to help, but do we ‘get the trust across’?

Community membership management directories and attribute authorities

- integrity of membership
- identification, traceability
- site and service security
- network protections
- assertion integrity

> Trust marks and expression



But when proxies are proxying proxies, can we proxy the trust?

Agree to a *common baseline* – that was successful before!

… set of (one or more) guidelines that represent a widely agreed and jointly-developed ***operational trust baseline*** *for infrastructure membership management and proxy components. Supplemented by policy guidance on how to connect sectoral federations with* ***more specific*** *policies. Driven by your (FIM4R, WISE, EOSC, …) feedback, and those of current proxy operators (in AEGIS).*

See https://www.igtf.net/guidelines/aaops/ and https://aarc-community.org/guidelines/aarc-g071/

Can we build on trusted ‘AAOPS’ to increase acceptance of research infrastructure proxies with R&E identity providers

May never get ‘interesting attributes’ apart from affiliation from home IdPs, but …

- still need assurance statements and REFEDS Assurance Framework attribute freshness
- unless ‘well hidden’, proxies are met with scepticism by IdPs to release personalised to R&S

and do Entity Categories ‘traverse’ proxies? and can proxy ops rely on their ‘downstreams’?

Snctfi

review and enhance effectiveness of Snctfi

the set of guidelines that describe a (self-) accessible framework of policies that bind a set of service providers behind an AARC BPA Proxy

and thereby encourage trust in the proxies *and* their connected services

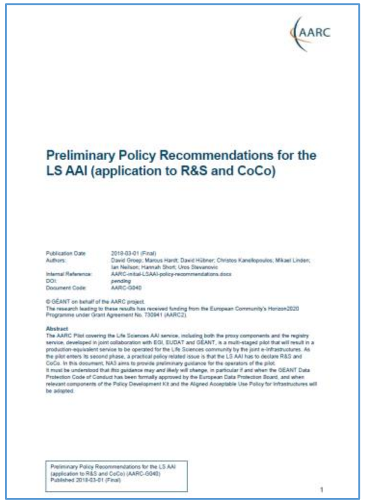
Proxies have their own challenges as well: AUPs, T&Cs, Privacy notices, …

For large ‘multi-tenant’ proxies:

- some subset users in some communities use a set of services – how to 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 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?



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

Publication Date: 2018-03-01 (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 GEANT 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 2018-03-01 (Final)

1

beyond AARC-G040

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

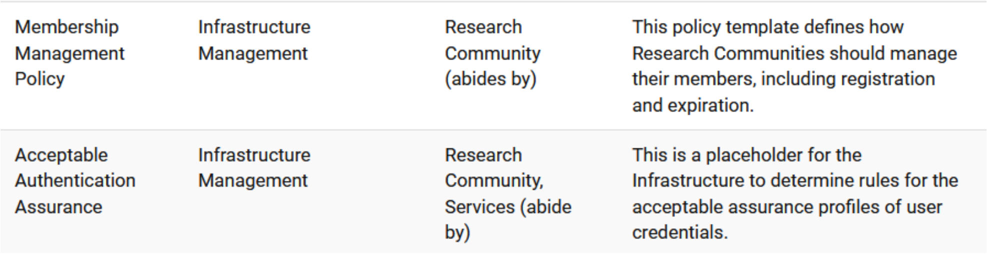
With Fewer Clicks to More Resources!

Helping out the community – a simpler policy toolkit for communities

What we heard through the grapevine (and at TechEx 2022 …) :

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

Leaves both communities and operators of membership management services unclear about trust assurance level of members - current templates in toolkit too complex and prescriptive



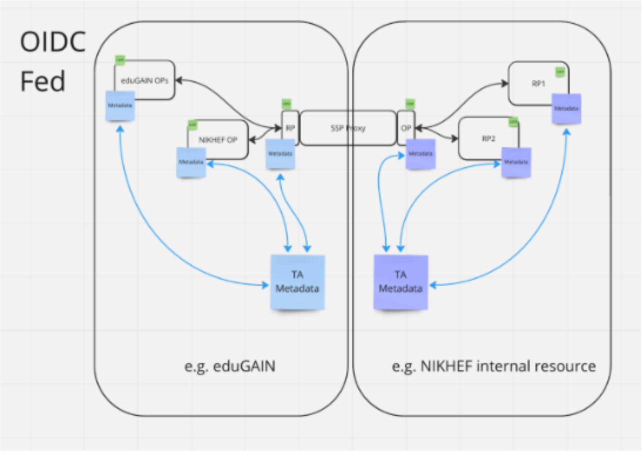
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.

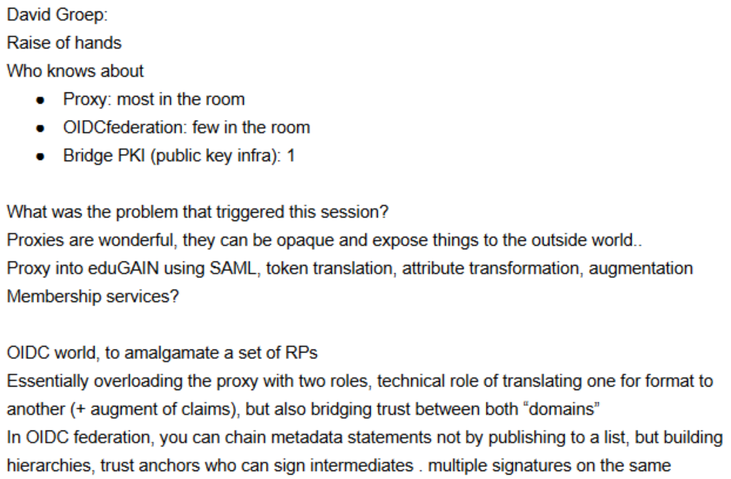
- community consultation on the ‘minimum viable community management’ – we are here!
- template and implementation guidance (FAQ) on community lifecycle management
- how to implement the community management in the (EOSC) AAI services

New trust models – what is the role of the proxy in OIDCFed?

In today’s BPA proxy links both sides by being opaque, **both** for attributes **as well as** for trust

- does it *have* to be that way?
- separate claims/attribute transformation from trust bridging?
- can OIDCfed structure convey trust transparently? Should it?
- can we then be more flexible? or will it just confuse everyone?
- easier to bridge trust *across sectors* this way?
  e.g. linking .edu, .gov, and private sector federations?





David Groep:
Raise of hands
Who knows about

- Proxy: most in the room
- OIDCfederation: few in the room
- Bridge PKI (public key infra): 1

What was the problem that triggered this session?
Proxies are wonderful, they can be opaque and expose things to the outside world..
Proxy into eduGAIN using SAML, token translation, attribute transformation, augmentation
Membership services?

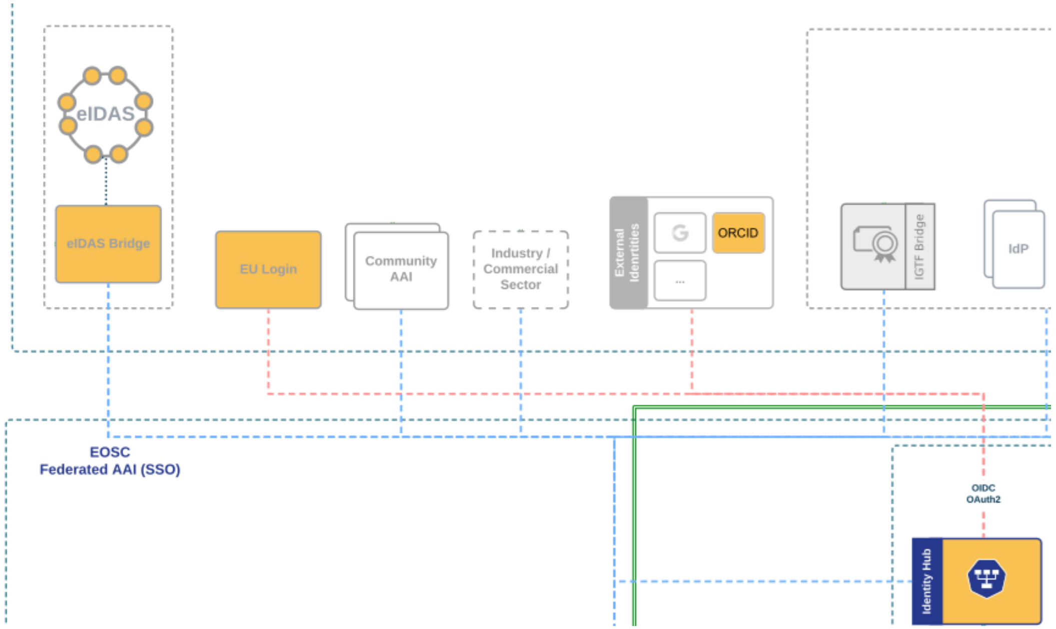
OIDC world, to amalgamate a set of RPs
Essentially overloading the proxy with two roles, technical role of translating one for format to another (+ augment of claims), but also bridging trust between both “domains”
In OIDC federation, you can chain metadata statements not by publishing to a list, but building hierarchies, trust anchors who can sign intermediates . multiple signatures on the same

ACAMP at TechEx23 – and TIIME?

We’ll see more diverse sources of identity & assurance anyway

Most reliable (and most ‘available’) source of assurance may be the European government identity ecosystem.

- Step-up to at least substantial level can now readily be done ‘at home’ by users through their national eID schemes
- Joint work on eIDAS, Erasmus Student Mobility, and more makes this more accessible
- Better attainable than relying on home institutions?



… but:

- what to do with non-European users?
- how to link the identities together

All About You – FIM4R and communities are the driving factor

Also in AARC-TREE we really need a “co-creation process” with you, our FIM4R communities

- we have resources to help run a couple of workshops in the next 2 years
- we need your critical review *and* your ideas and input on both policy and architecture
- start from the high-level requirements and some broad community input

May AARC-TREE be helpful to you … with your input and brain dumps!

Thank you

Any Questions?

davidg@nikhef.nl

AARC

https://aarc-community.org

this work is co-supported by the Trust and Identity work package of the GEANT project (GN5-1)

in collaboration with many, many people in the AARC+ Community!

AARC

Thank you

davidg@nikhef.nl

GÉANT

Networks · Services · People

www.geant.org

This work has been co-supported by projects that have received funding from the European Union's Horizon research and innovation programmes under Grant Agreement No. 101100680 (GN5-1), 856726 (GN4-3), and 730941 (AARC2).