AARC Authentication and Authorisation for Research and Collaboration

AARC TREE: Enhancing our Research Collaborations

even better research with secure collaborative authentication & authorization

David Groep

AARC Community policy lead, for the AARC Collaboration

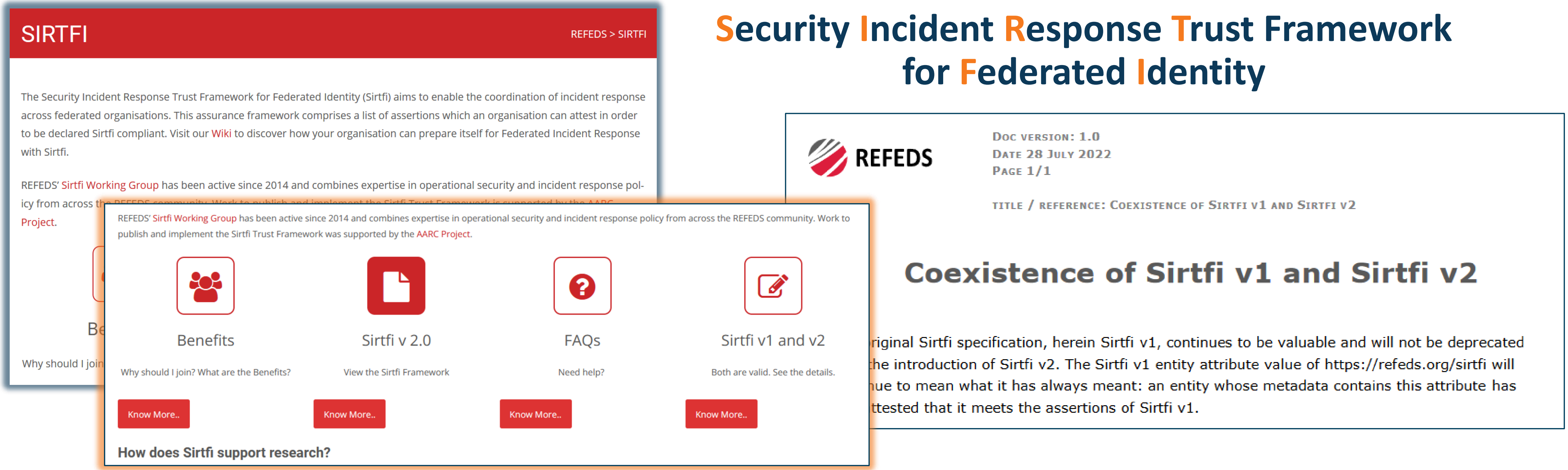
Nikhef Maastricht University

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

GÉANT Security Days 2024
Prague, April 2024

Probably most well-known AARC result to this audience …

Security Incident Response Trust Framework for Federated Identity



SIRTFI

REFEDS > SIRTFI

The Security Incident Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response across federated organisations. This assurance framework comprises a list of assertions which an organisation can attest in order to be declared Sirtfi compliant. Visit our Wiki to discover how your organisation can prepare itself for Federated Incident Response with Sirtfi.

REFEDS' Sirtfi Working Group has been active since 2014 and combines expertise in operational security and incident response policy from across th

Project.

Be

Why should I join

REFEDS' Sirtfi Working Group has been active since 2014 and combines expertise in operational security and incident response policy from across the REFEDS community. Work to publish and implement the Sirtfi Trust Framework was supported by the AARC Project.

Benefits	Sirtfi v 2.0	FAQs	Sirtfi v1 and v2
Why should I join? What are the Benefits?	View the Sirtfi Framework	Need help?	Both are valid. See the details.
Know More..	Know More..	Know More..	Know More..

How does Sirtfi support research?

REFEDS

DOC VERSION: 1.0
DATE 28 JULY 2022
PAGE 1/1

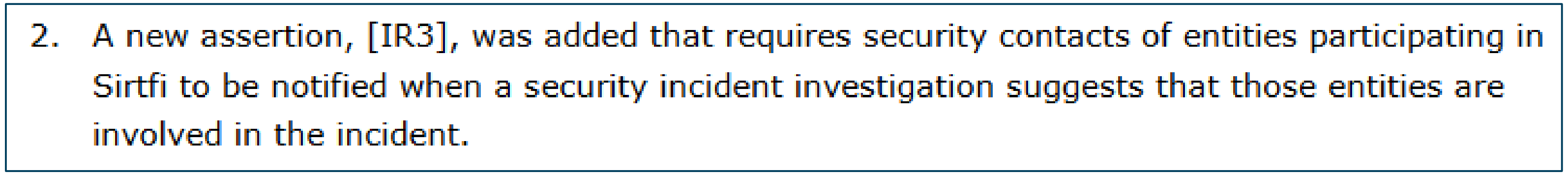
TITLE / REFERENCE: COEXISTENCE OF SIRTFI V1 AND SIRTFI V2

Coexistence of Sirtfi v1 and Sirtfi v2

riginal Sirtfi specification, herein Sirtfi v1, continues to be valuable and will not be deprecated
the introduction of Sirtfi v2. The Sirtfi v1 entity attribute value of https://refeds.org/sirtfi will
ue to mean what it has always meant: an entity whose metadata contains this attribute has
ttested that it meets the assertions of Sirtfi v1.

https://refeds.org/SIRTFI

SIRTFI
Security Incident Response Trust Framework for Federated Identity



2. A new assertion, [IR3], was added that requires security contacts of entities participating in Sirtfi to be notified when a security incident investigation suggests that those entities are involved in the incident.

But that is only part of a much larger, federated, story …

AUSTRALIAN ACCESS FEDERATION
The UK Access Management Federation FOR EDUCATION AND RESEARCH
aconet
caf
SWITCHaai
grnet
DFN-AAI
SIFULAN
confia
SIR
IGTF
Interoperable Global Trust Federation
AP | EU | TAG
Edugate
Gaining Access to Education
SURF
CONEXT
RCTSaai
REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE
MiNGA
idem garr aai
RENATER
CONNECTEUR DE SAVOIRS
FEIDE
GakuNin
Colfire
Colombian Federation of Identity for Research and Education renata
TAAT
Comunidad Federada REUNA
SWAMID
CILogon
uakiri
AAI @EduHr
arnes
eduID

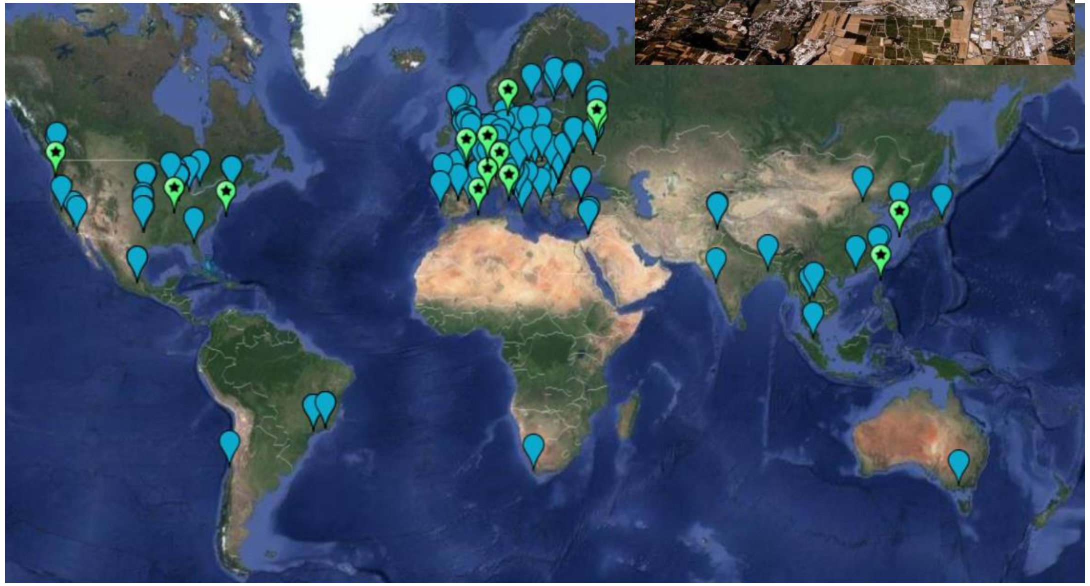
slide inspiration: Licia Florio, NORDUNET

Research Collaboration: an inherently-cross-domain issue .. and solution

Example from the LHC Computing infrastructure WLCG

170 sites
~50 countries & regions
~20000 users

just *how* many interactions ??



AuthN & AuthZ, as well as security & compliance should align with collaboration structures, and be **outward facing:** open, scalable, and multi-domain

people photo: a small part of the CMS collaboration in 2017, Credit: CMS-PHO-PUBLIC-2017-004-3; site map: WLCG sites from Maarten Litmaath (CERN) 2021

Federated Identity Management and global collaboration

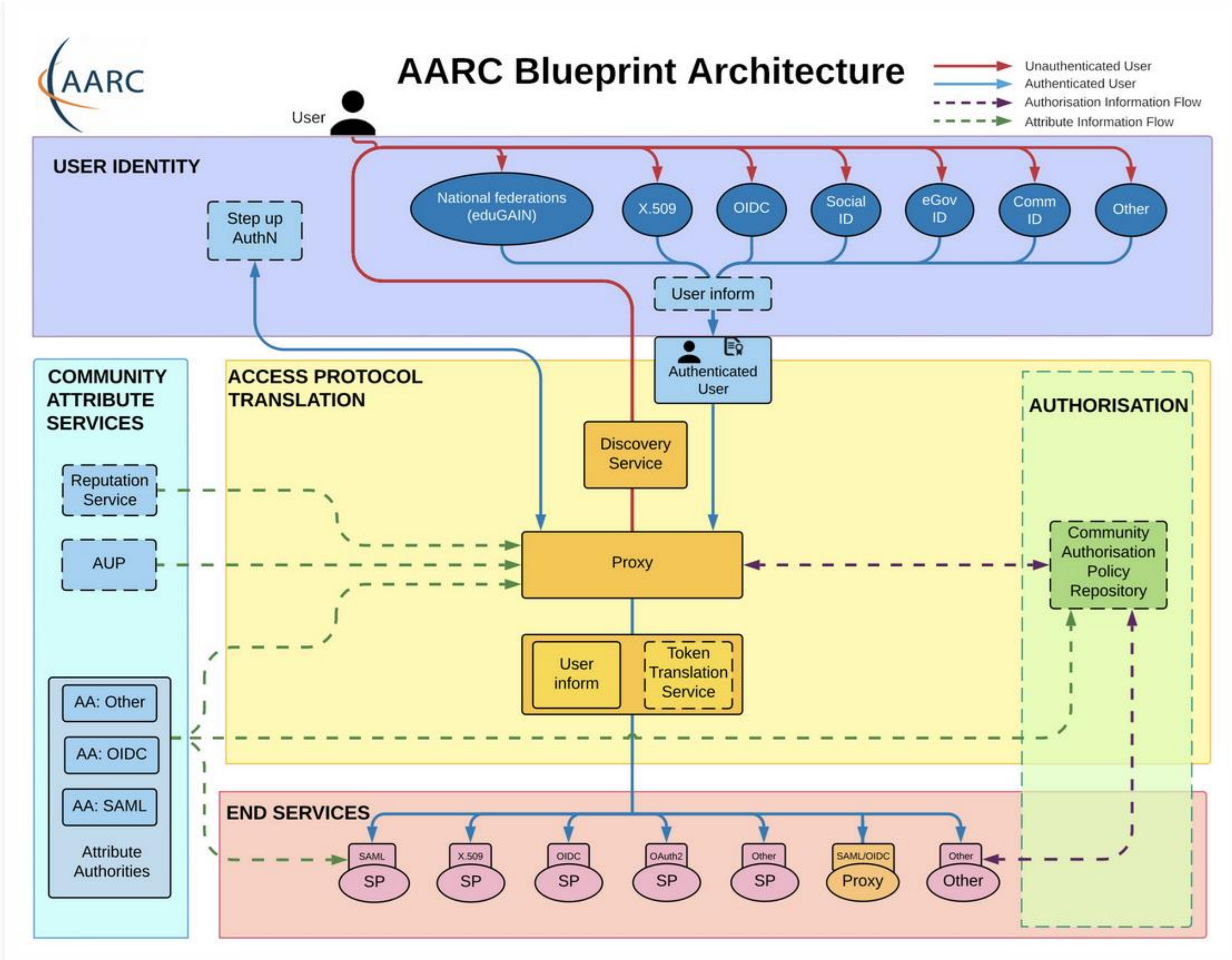
- Access services using **identities from their Home Organizations**,
- but **hide complexity** of multiple IdPs, federations, AA technologies
- with **one persistent identity**

  across all the community’s services through **account linking**
- **Access** services **based on role(s)** users have **in the collaboration**.

  linking *not known* to your “SP” services, the IdPs – or to eduGAIN
- for both **web** and **non-web** resources
- Integration of **guest identity solutions**
- **support for stronger authentication assurance** mechanisms

Authentication and Authorization for Research Collaboration – AARC (Licia Florio *et al.*) – https://aarc-community.org/

AARC – ‘just eduGAIN is not enough’



FENIX RESEARCH INFRASTRUCTURE

SSHOC

LSC LIGO Scientific Collaboration

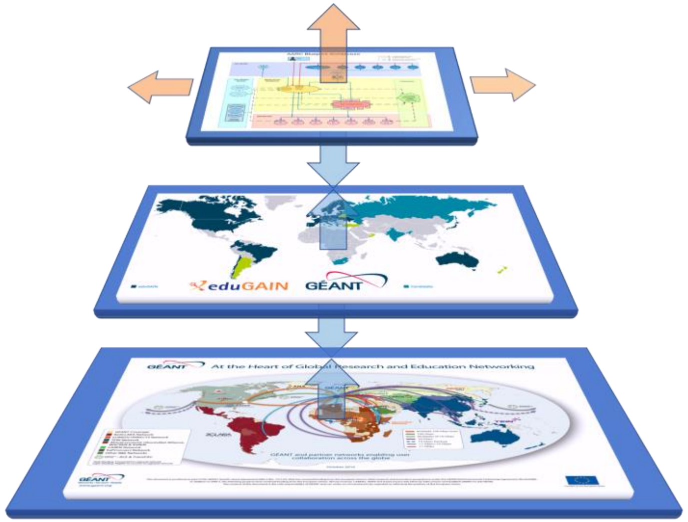
panosc photon and neutron open science cloud

EOSC-Life

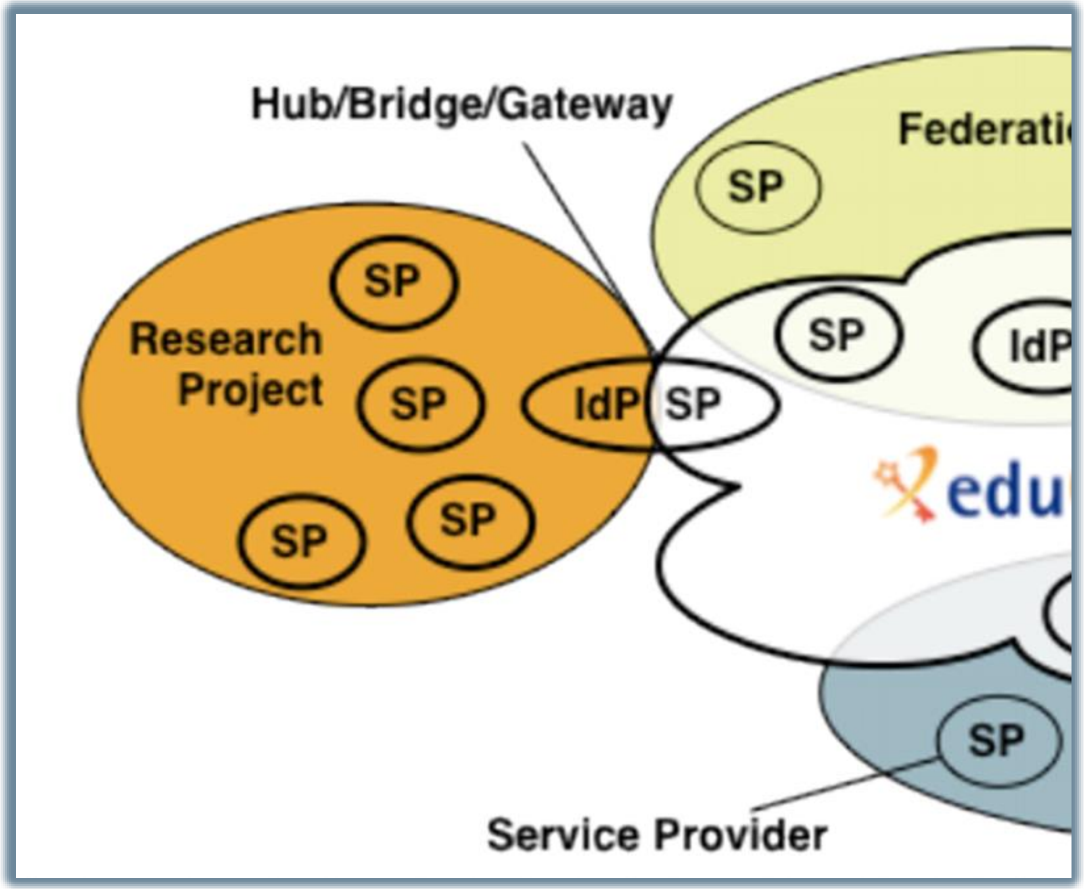
ESCAPE

neic PUHURI LUMI

DARIAH-EU Digital Research Infrastructure for the Arts and Humanities

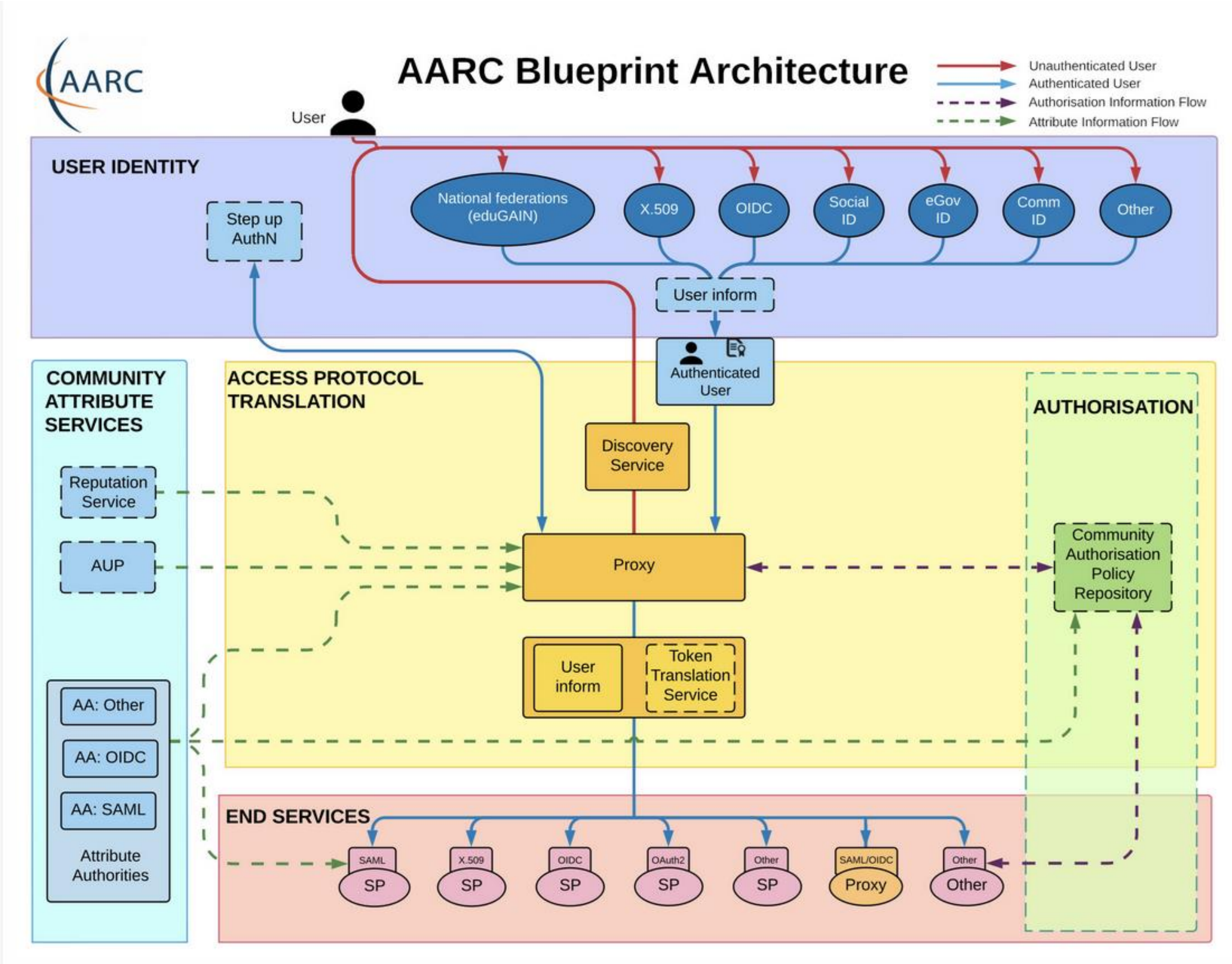


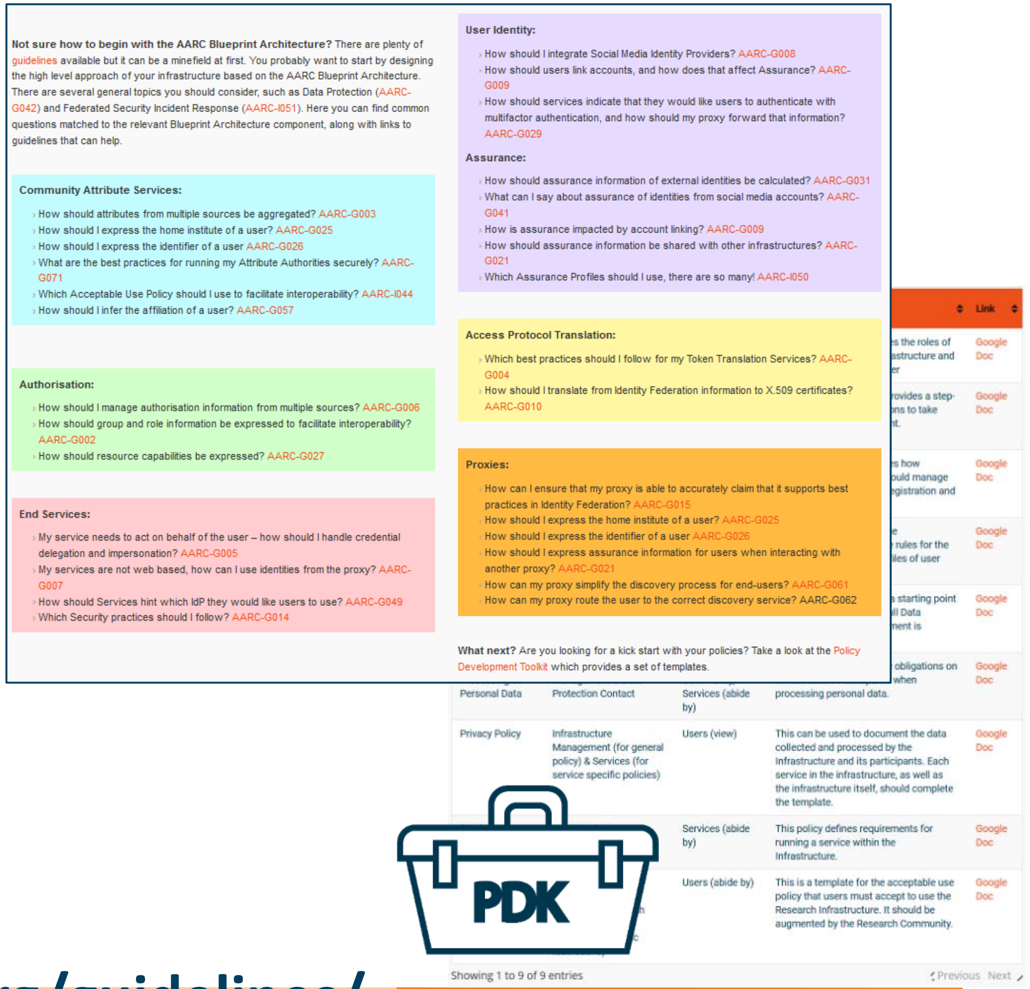
The IdP-SP proxy: a First-class Citizen



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

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-G003
- 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-G005
- 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

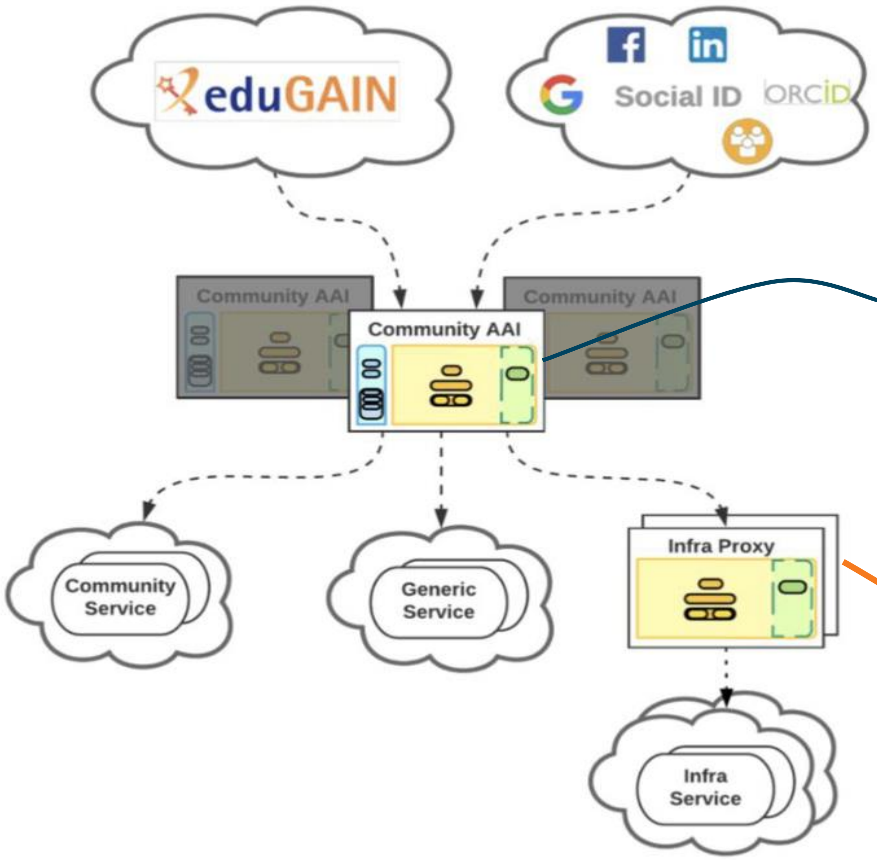
What next? Are you looking for a kick start with your policies? Take a look at the Policy Development Toolkit which provides a set of templates.

				Link
			s the roles of astructure and er	Google Doc
			rovides a step- ons to take nt.	Google Doc
			s how ould manage egistration and	Google Doc
			e rules for the iles 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

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

The Community AAI and the Infrastructure Proxy – structuring elements



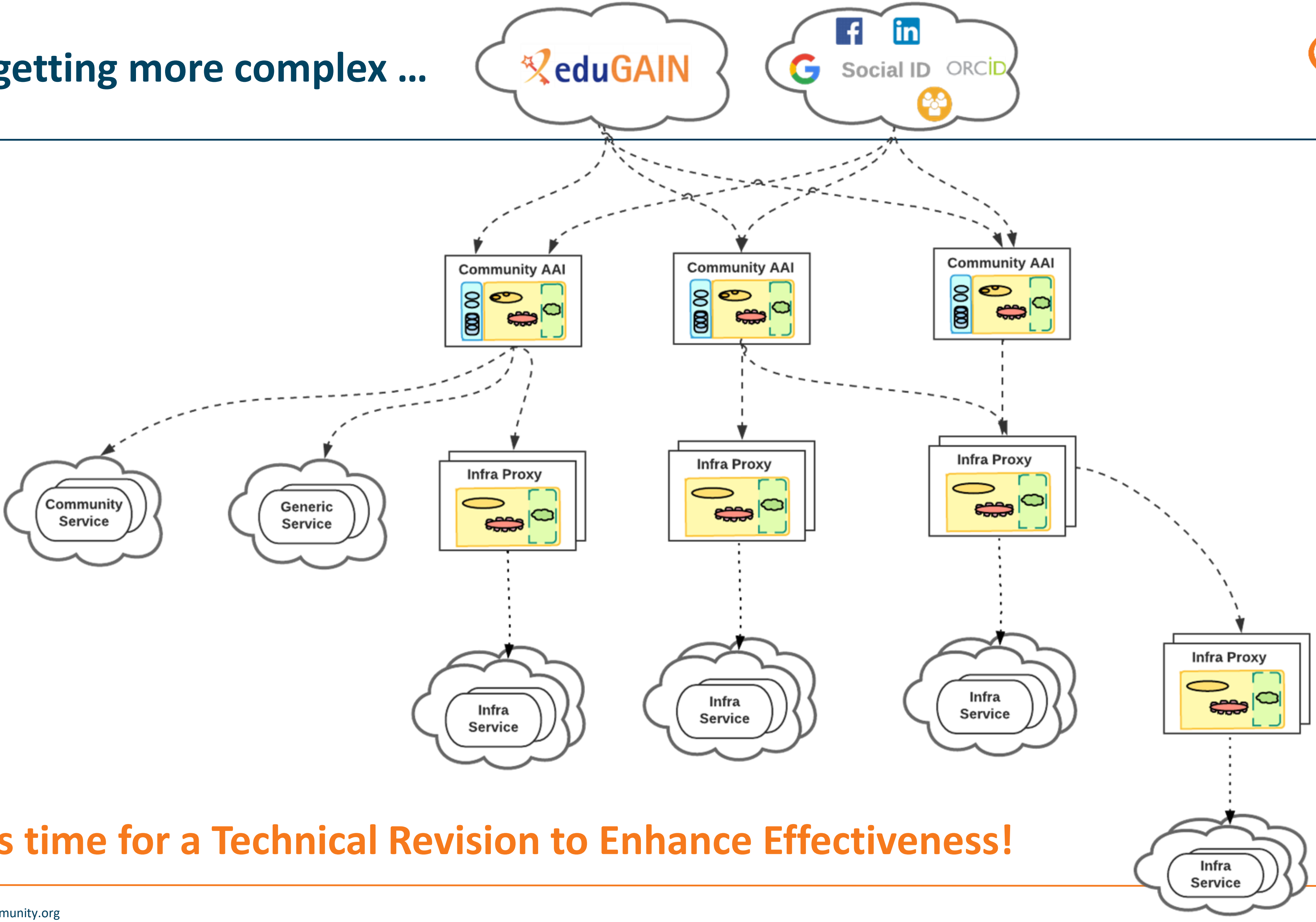
Community AAI

The purpose of the Community AAI is to streamline researchers' access to services, both those provided by their own infrastructure as well as the services provided by infrastructures that are shared with other communities.

Infrastructure Proxy

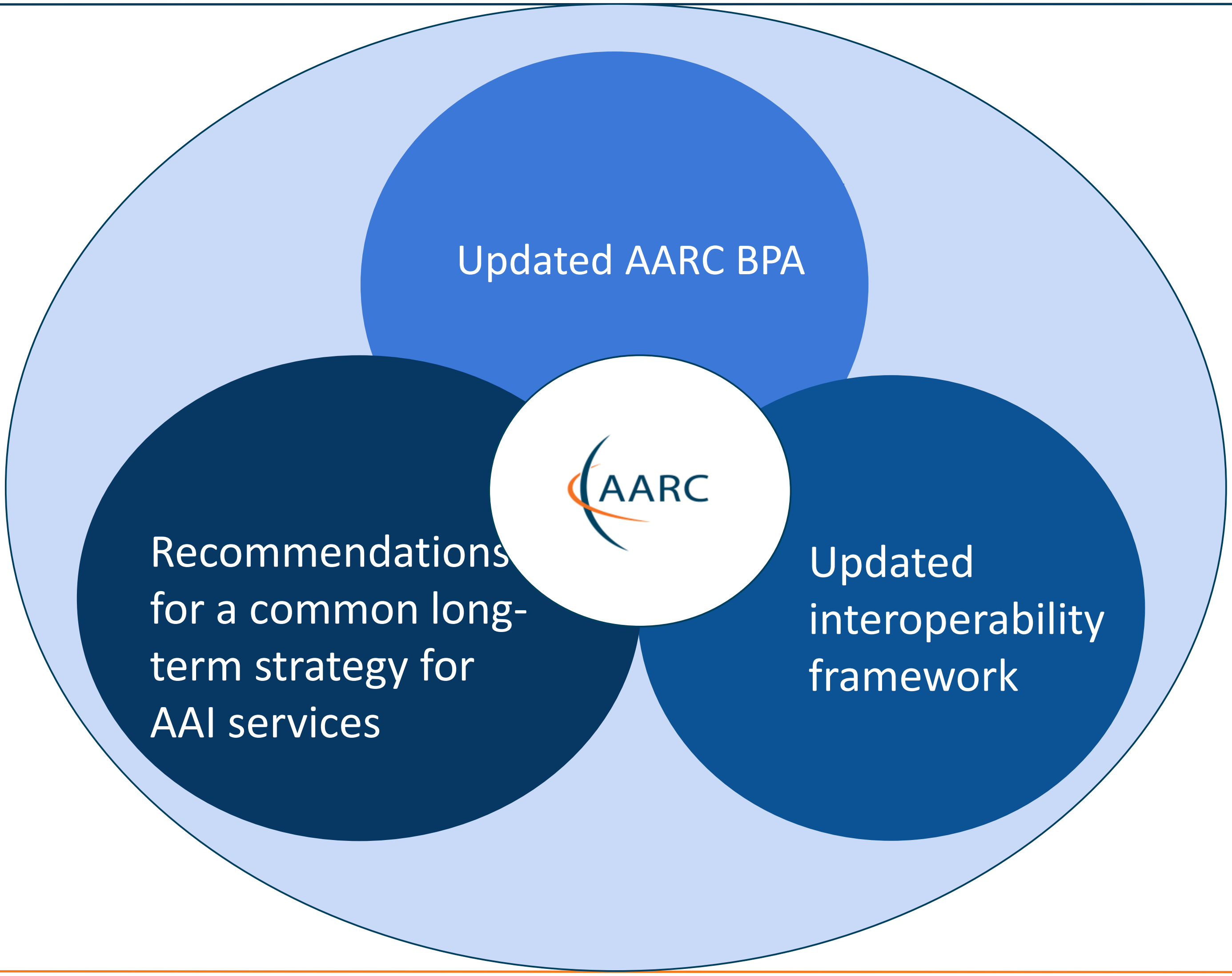
The Infrastructure Proxy, enables Infrastructures with a large number of resources, to provide them through a single integration point, where the Infrastructure can maintain centrally all the relevant Policies and business logic for making available these resources to multiple communities

But it’s getting more complex …



… it’s time for a Technical Revision to Enhance Effectiveness!

AARC TREE Main Facts: Expected results



Updated AARC BPA

Recommendations for a common long-term strategy for AAI services

Updated interoperability framework

The AARC TREE in the Trust and Identity Landscape

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

Evolve the BPA to address the more complex (and the simpler) worlds

Guidelines for **expression of community user attributes**

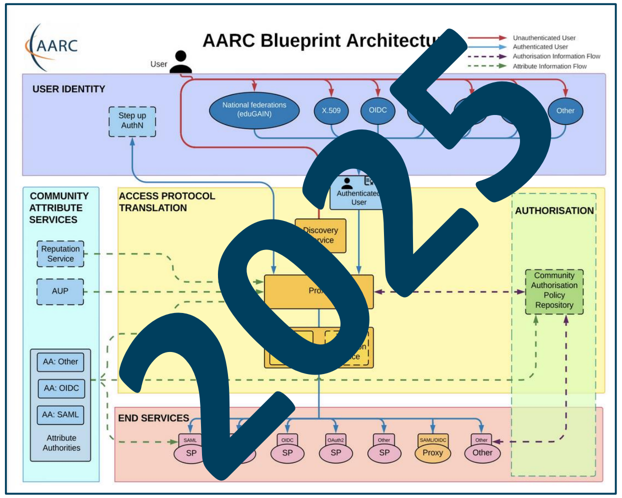
- **reduce inconsistencies** between implementations
- improve **interoperability** & **end-user usability** across research community communities and infrastructures

Extend AARC BPA

- improve **scalability**
- leverage emerging standards like **OpenID Federation**

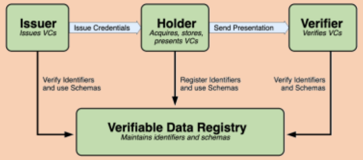
Authorisation guidelines

- best practises to enable efficient & effective **sharing of federated resources**



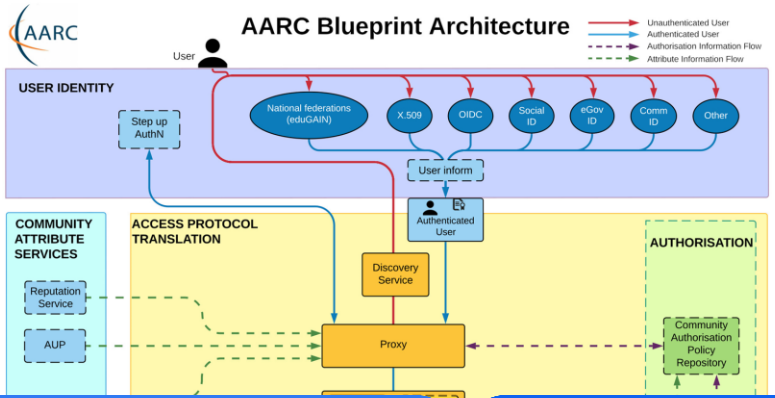
Decentralised identities

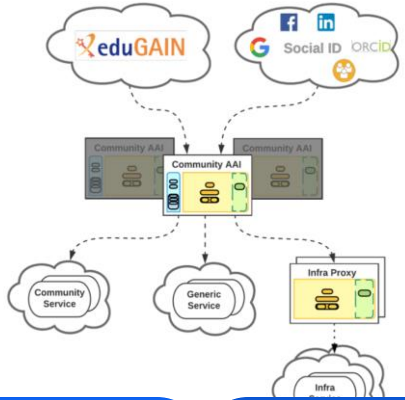
- guidance for **digital wallets** linked to BPA


Issuer
Issues VCs
Issue Credentials
Holder
Acquires, stores, presents VCs
Send Presentation
Verifier
Verifies VCs
Verify Identifiers and use Schemas
Register Identifiers and use Schemas
Verify Identifiers and Schemas
Verifiable Data Registry
Maintains identifiers and schemas

AARC Blueprint Architecture ‘BPA2025’

AARC BPA 2019


AARC
AARC Blueprint Architecture
Unauthenticated User
Authenticated User
Authorisation Information Flow
Attribute Information Flow
User
USER IDENTITY
Step up AuthN
National federations (eduGAIN)
X.509
OIDC
Social ID
eGov ID
Comm ID
Other
User inform
Authenticated User
COMMUNITY ATTRIBUTE SERVICES
Reputation Service
AUP
ACCESS PROTOCOL TRANSLATION
Discovery Service
Proxy
AUTHORISATION
Community Authorisation Policy Repository



OpenID Federations

+

AuthZ for Federated Resources

+

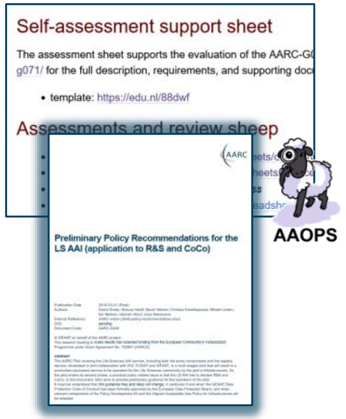
Decentralised Identities & Wallets

AARC BPA 2025

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-G0

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

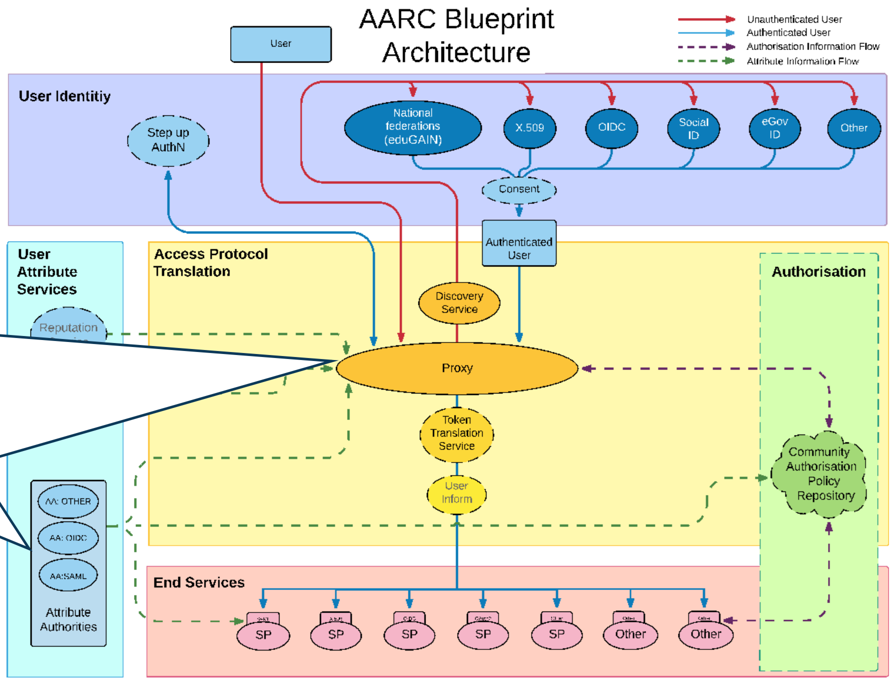
Anchored in the researcher user communities by **co-creation with FIM4R**

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

Membership management service, attribute authorities, and proxy/token translator

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

> Trust marks and expression

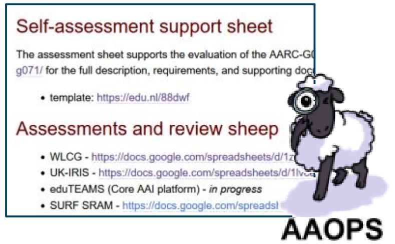


But when proxies are proxying proxies, can we proxy the trust?

Agree to a

common baseline

… an approach that was successful previously!



Self-assessment support sheet

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

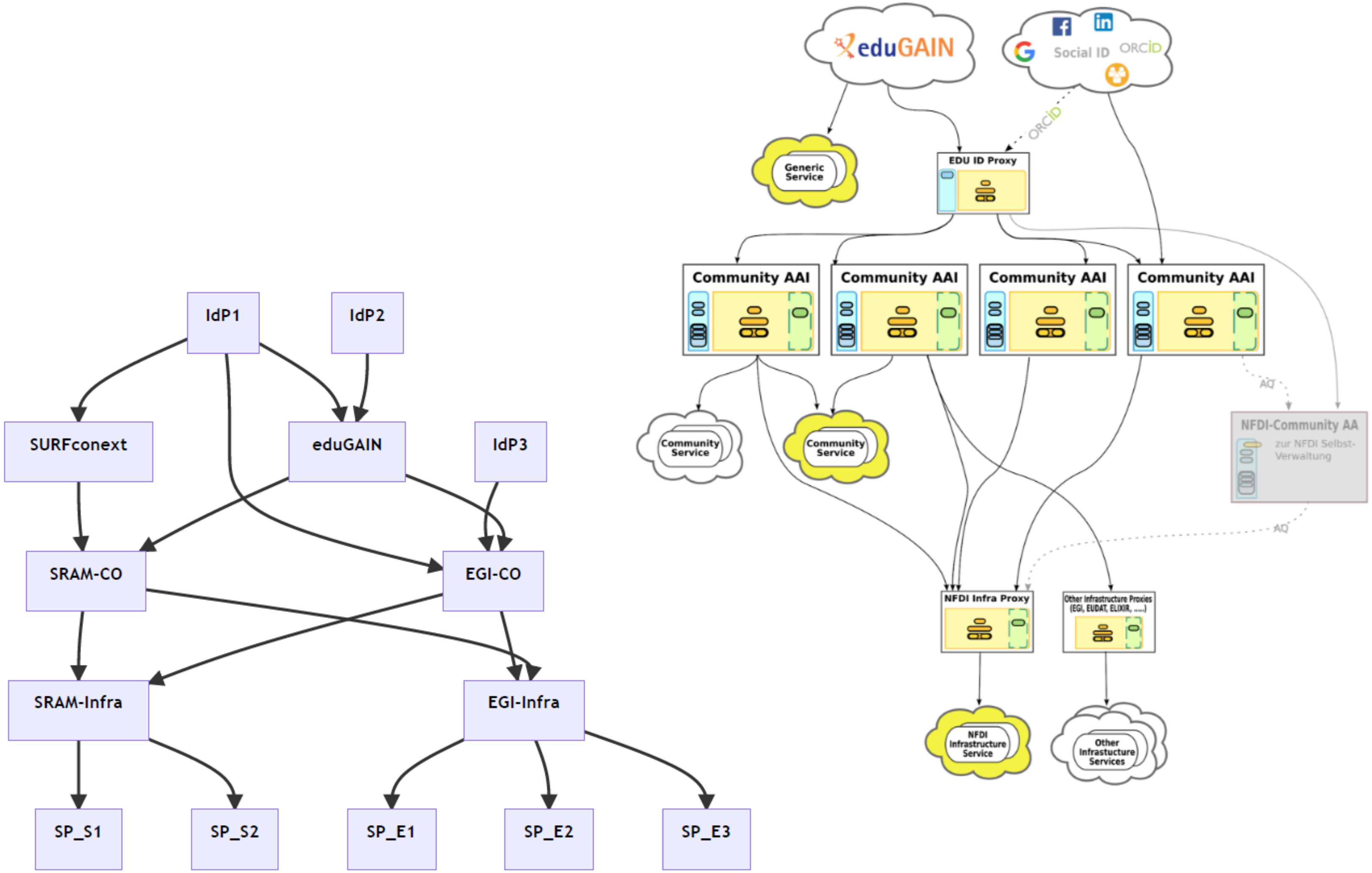
- template: https://edu.nl/88dwf

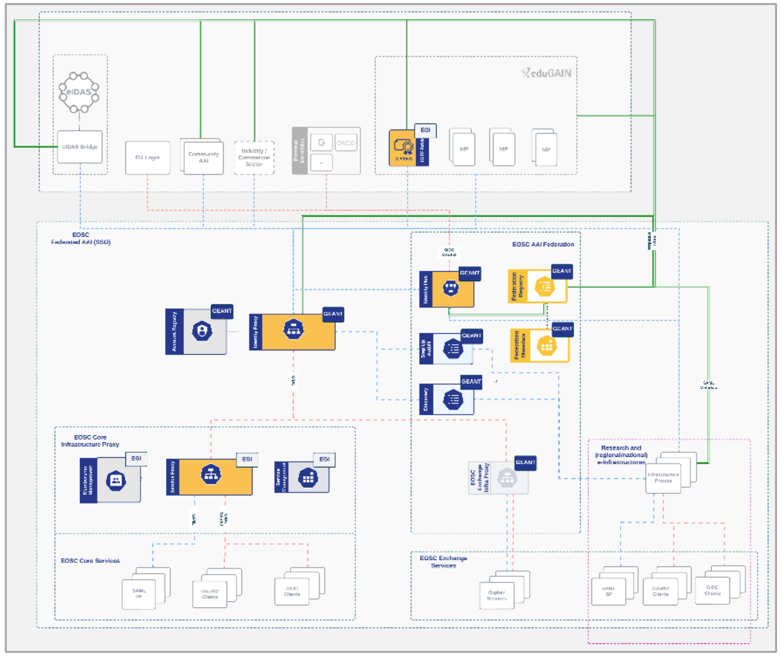
Assessments and review sheep

- WLCG - https://docs.google.com/spreadsheets/d/1z
- UK-IRIS - https://docs.google.com/spreadsheets/d/1lvc
- eduTEAMS (Core AAI platform) - *in progress*
- SURF SRAM - https://docs.google.com/spreads

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

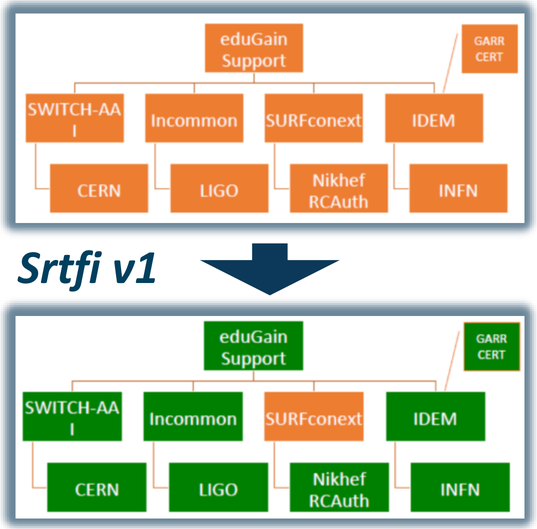
Our federated world is growing more complex

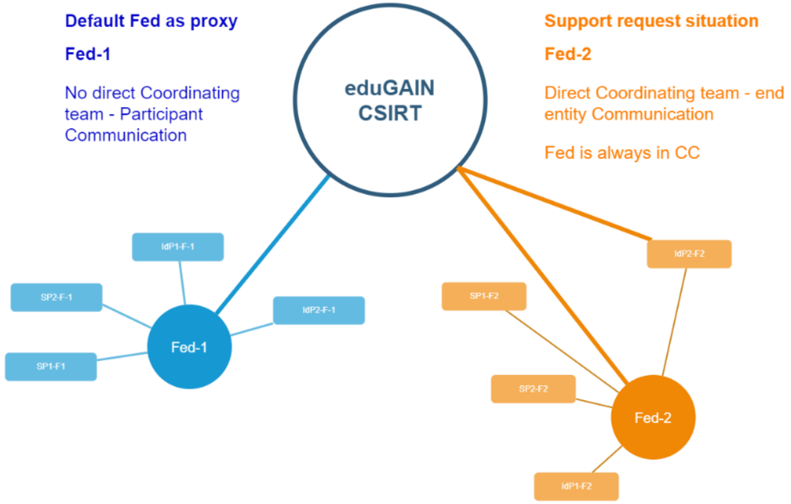




Images: SURF SSRAM and EGI by Maarten Kremers, NDFI AAI (Marcus Hardt), EOSC AAI for the EOSC Core and Exchange Federation for the EOSC European Node by Christos Kanellopoulos, Nicolas Liampotis, David Groep (June 2023 version)

Response and traceability across IdP-SP Proxies and the limits of Sirtfi





Default Fed as proxy

Fed-1

No direct Coordinating team - Participant Communication

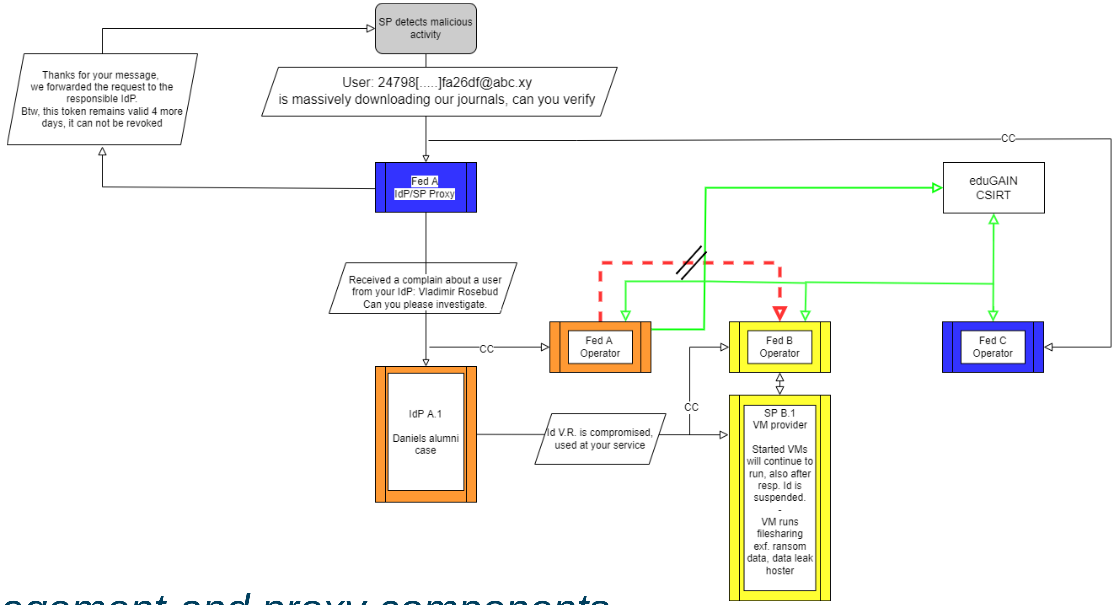
eduGAIN CSIRT

Support request situation

Fed-2

Direct Coordinating team - end entity Communication

Fed is always in CC



SP detects malicious activity

User: 24798[.....]fa26df@abc.xy
is massively downloading our journals, can you verify

Thanks for your message,
we forwarded the request to the responsible IdP.
Btw, this token remains valid 4 more days, it can not be revoked

Fed A
IdP/SP Proxy

Received a complain about a user from your IdP: Vladimir Rosebud
Can you please investigate.

IdP A.1

Daniels alumni case

Id V.R. is compromised, used at your service

SP B.1
VM provider

Started VMs will continue to run, also after resp. Id is suspended.
-
VM runs filesharing exf. ransom data, data leak hoster

*Guidelines for a joint **operational trust baseline** for membership management and proxy components, supplemented by policy guidance for sectoral federations with more specific policies where needed*

- *‘How can we **convey the trust in what is in and behind the proxy**?’*
- *‘How to provide **timely traceability** between services and identities through the proxy?’*

Based on requirements from FIM4R, WISE, and the proxy operators in AEGIS.

GÉANT | eduGAIN | CSIRT

joint work with GN5-1 EnCo and eduGAIN CSIRT

images: AARC Sirtfi v1 exercise (Hannah Short), eduGAIN security TTX (Sven Gabriel, eduGAIN CSIRT)

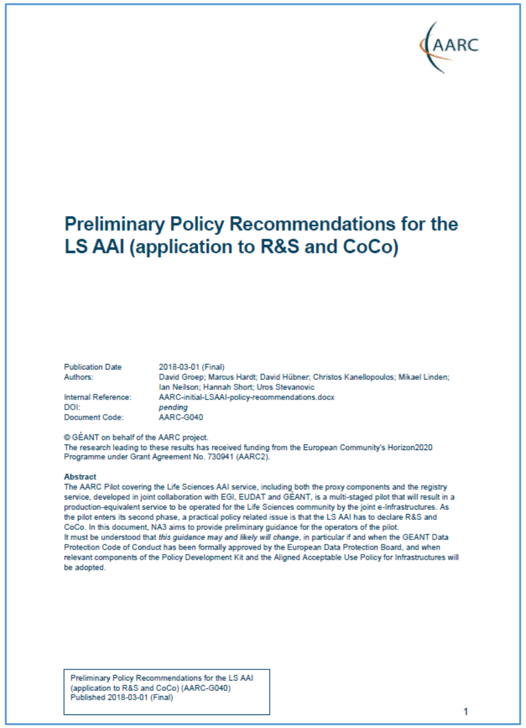
Proxies have their own challenges as well: AUPs, T&Cs, Privacy notices, …

For large ‘multi-tenant’ proxies

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

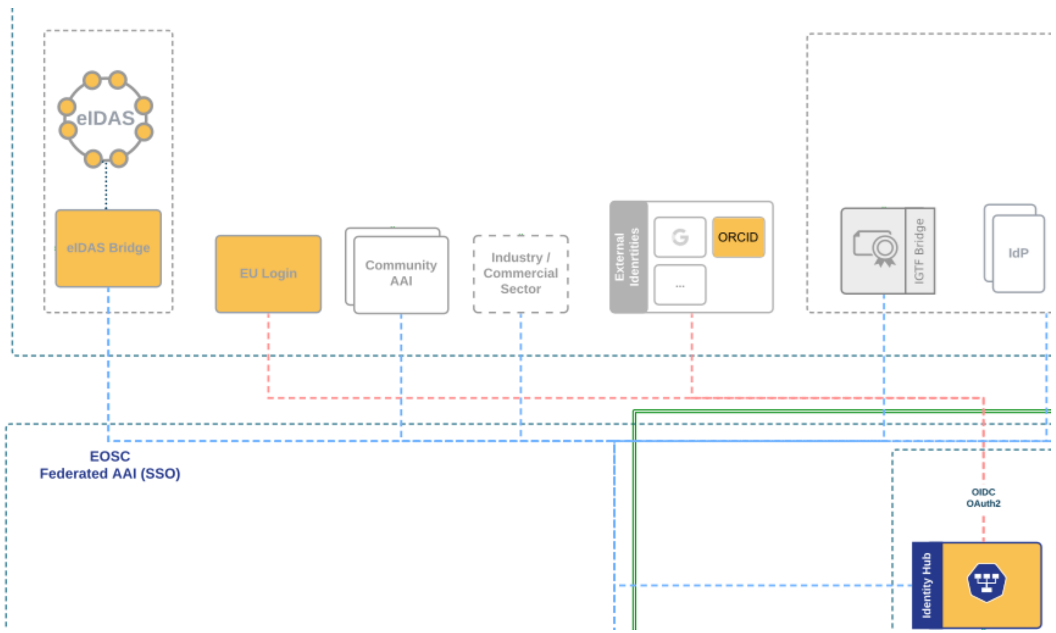
What is an acceptable user experience in clicking through agreements?
What is effective in exploiting the WISE Baseline AUP? What do researchers need?

‘with fewer clicks to more resources’

And .. we’ll be seeing more, and diverse, sources of identity assurance

An ‘available’ persistent source of assurance may be the (European) government-ID ecosystem

- step-up to at least *substantial* level can now readily be done ‘at home’ by many users through their national eID schemes
- Joint work on eIDAS, Erasmus Student Mobility, and more makes this more accessible
- step-up-as-a-service as a fall-back (like in .se)
- better attainable than relying on home institutions?



… but:

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

All about enabling research: FIM4R & communities are a key factor

Also in AARC-TREE we target a “co-creation process”

- support FIM4R to increase the reach of workshops in the next 2 years
- community review, ideas, and input on both policy and architecture
- start from the high-level requirements and broad community input

whatever we build must be *usable and available* by researcher communities first of all, and align to interoperability standard and open, collaborative research goals

Really a global activity: we want to engage everyone, in AARC TREE and beyond

Compendium and Recommendations

Key result in the ‘2nd year’ (April 2025 - February 2026) is the **Compendium**

'**compendium of AARC best practices’** with **recommendations** for a common long-term strategy for AAI services in pan-European Research Infrastructures in Europe

- based on the use case input and researcher requirements
- promotes coherent and interoperable architecture and policy
- **iterate and validate** with the infrastructures at large

describe the road that collaborative research infrastructure AAI will take!

Image generated by Adobe Firefly 2 with the text prompt “image of a broad-leaved lemon tree with a person sitting below it leaning against the trunk in the sunshade”

Let’s climb the AARC TREE together:
work with us on our joint security challenges!

Thanks to the AARC Community, including folk from whom I re-used graphics and material in this overview. In random order: Licia Florio, Nicolas Liampotis, Christos Kanellopoulos, Marina Adomeit, Janos Mohacsi, Ilaria Fava, Slavek Licehammer, Dave Kelsey, Ian Neilson, Marcus Hardt, Mischa Salle, Hannah Short, and Maarten Kremers.

Thank you

Any Questions?

davidg@nikhef.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).