



Authentication and Authorisation for Research and Collaboration

## **AARC – the blueprint for interoperable AAI in our federated world**

*an overview for the ESCAPE WP2/WP5 community*

**David Groep**

AARC AEGIS policy area coordinator

Nikhef



ESCAPE WP2-WP5 workshop

Amsterdam, July 2019

# AARC – leverage federated identity to facilitate research collaboration



# Where did we come from & where should we go ...



  
European  
Commission

## Advancing Technologies and Federating Communities

A Study  
on Authentication  
and Authorisation Platforms  
For Scientific Resources  
in Europe

FINAL REPORT  
A study prepared for the European Commission  
DG Communications Networks, Content & Technology



### Federated Identity Management for Research Collaborations

Paper Type: Research paper  
Date of this version: 28 August 2013

#### Abstract

Federated identity management (FIM) is an arrangement that can be made among multiple organisations that lets subscribers use the same identification data to obtain access to the secured resources of all organisations in the group. Identity federation offers economic advantages, as well as convenience, to organisations and their users. For example, multiple institutions can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust.

A number of laboratories including national and regional research organisations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries.

Driven by these needs, representatives from a variety of research communities, including photon/neutron facilities, social science & humanities, high-energy physics, atmospheric science, bioinformatics and fusion energy, have come together to discuss how to address these issues with the objective to define a common policy and trust framework for Identity Management based on existing structures, federations and technologies.

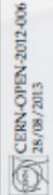
This paper will describe the needs of the research communities, the status of the activities in the FIM domain and highlight specific use cases. The common vision for FIM across these communities will be presented as well the key stages of the roadmap and a set of recommendations intended to ensure its implementation.

**Keywords**  
federated identity management, security, authentication, authorization, collaboration, community

#### Introduction

Federated identity management (FIM) is an arrangement that can be made among multiple organisations that lets subscribers use the same identification data to obtain access to the secured resources of all organisations in the group. Identity federation offers economic advantages, as well as convenience, to organisations and their users. For example, multiple institutions can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust.

A number of laboratories including national and regional research organisations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries. Many of the users have accounts at several research organisations and will need to use services provided by yet more organisations involved in research collaborations. All these identities and services need to be able work together without the users being obliged to remember a growing number of accounts and passwords. As the user communities served by these organisations are growing they are also becoming younger and this younger generation has little tolerance for artificial barriers, many being the relics of technology and policies that could, if reasoned, also evolve. This "Facebook" generation [1] has triggered a change in the attitude towards IT tools. One expects to be able to share data, software, results, thoughts and emotions with whomever they choose, when they choose. The boundaries between work and social life are less sharp, and it is expected that tools blend into this environment seamlessly. The interaction with commercial services such as the social networks must not imply that the users and research communities relinquish control over access to resources and security policies. The frequency of use will vary between the different users. Some will use these new tools continuously each day while others will log in a few times per year. This implies that operation has to be very intuitive, preferentially in a style known from common commercial devices and applications (PCs, smart phones, tablets etc).

  
CERN-OPEN-2012-006  
28/08/2013



Access services based on role(s)

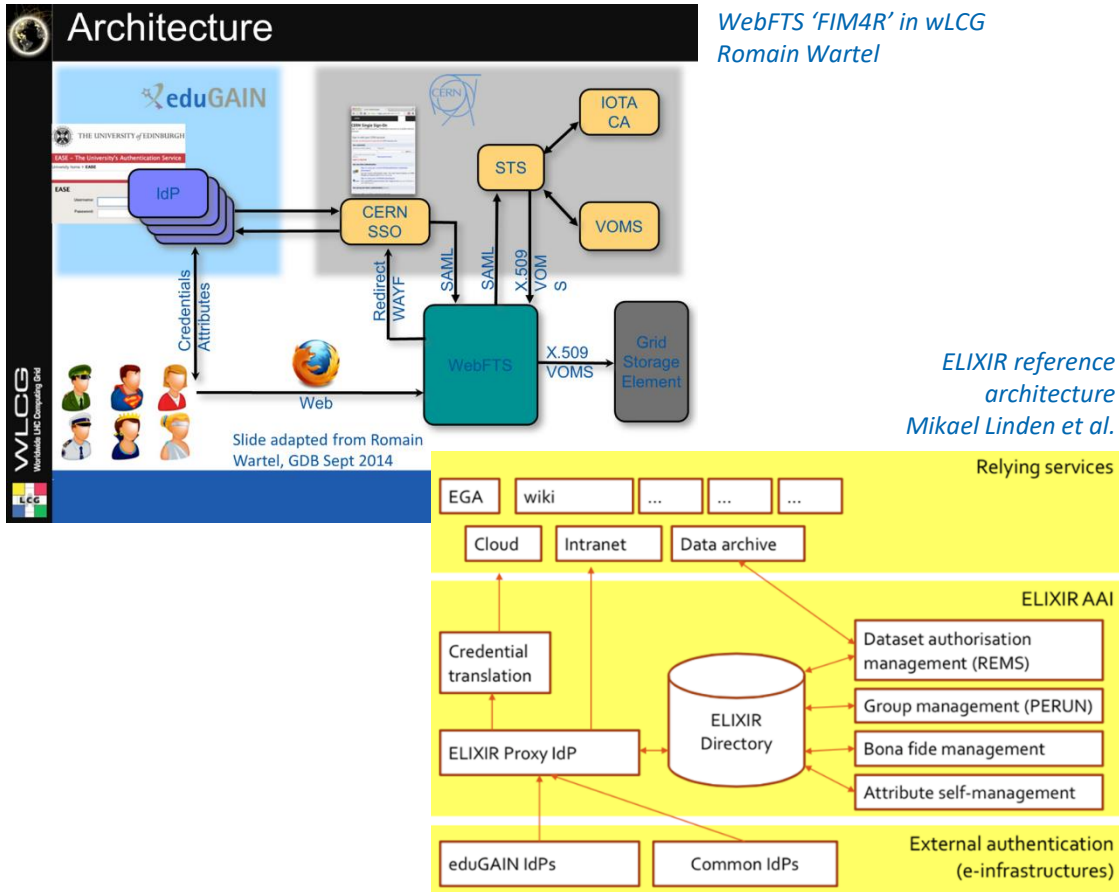
One **persistent** identifier across  
community's services

Easy way to **connect to eduGAIN**

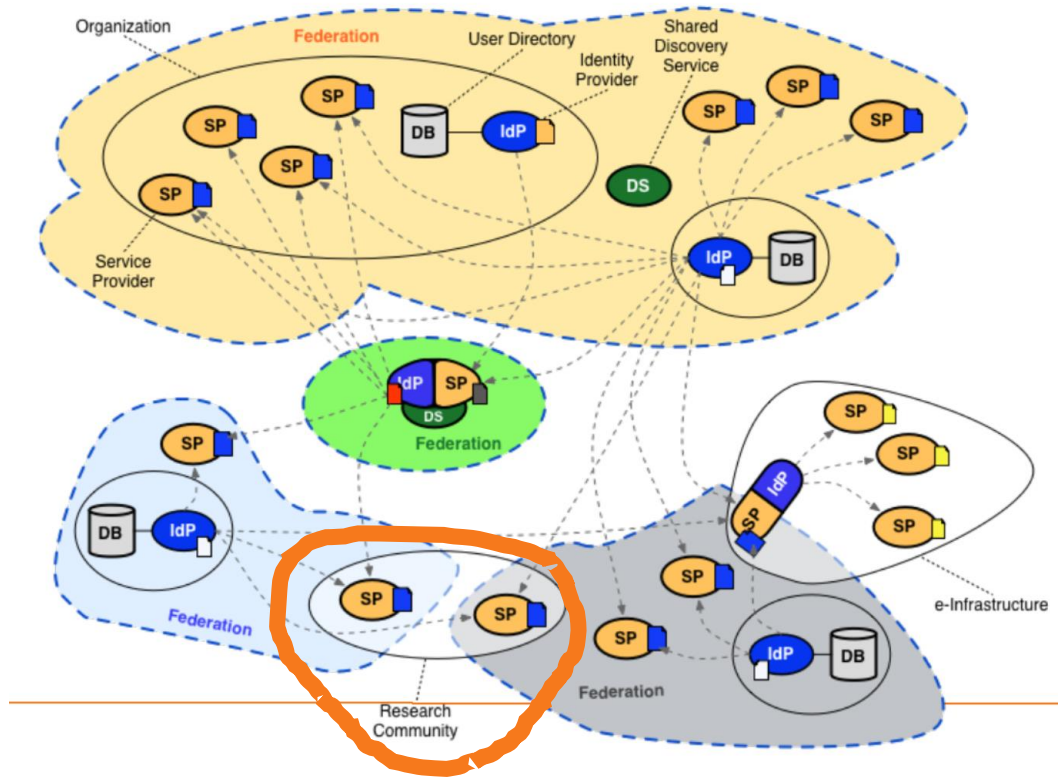
The eduGAIN logo features a stylized orange and red icon of a star or comet on the left, followed by the text "eduGAIN" in a blue and orange sans-serif font.

eduGAIN

# Whence we came – collaborative research AAs predating AARC



communities had either invented their own 'proxy' model to abstract complexity



or they were composed of many services each of which had to manage federation complexity

# Identified common challenges

## Communities / e-infrastructures surveyed in AARC



Homeless users

User friendliness

PII Data Protection

Community based AuthZ

SP friendliness

Credential translation

Bridging Communities

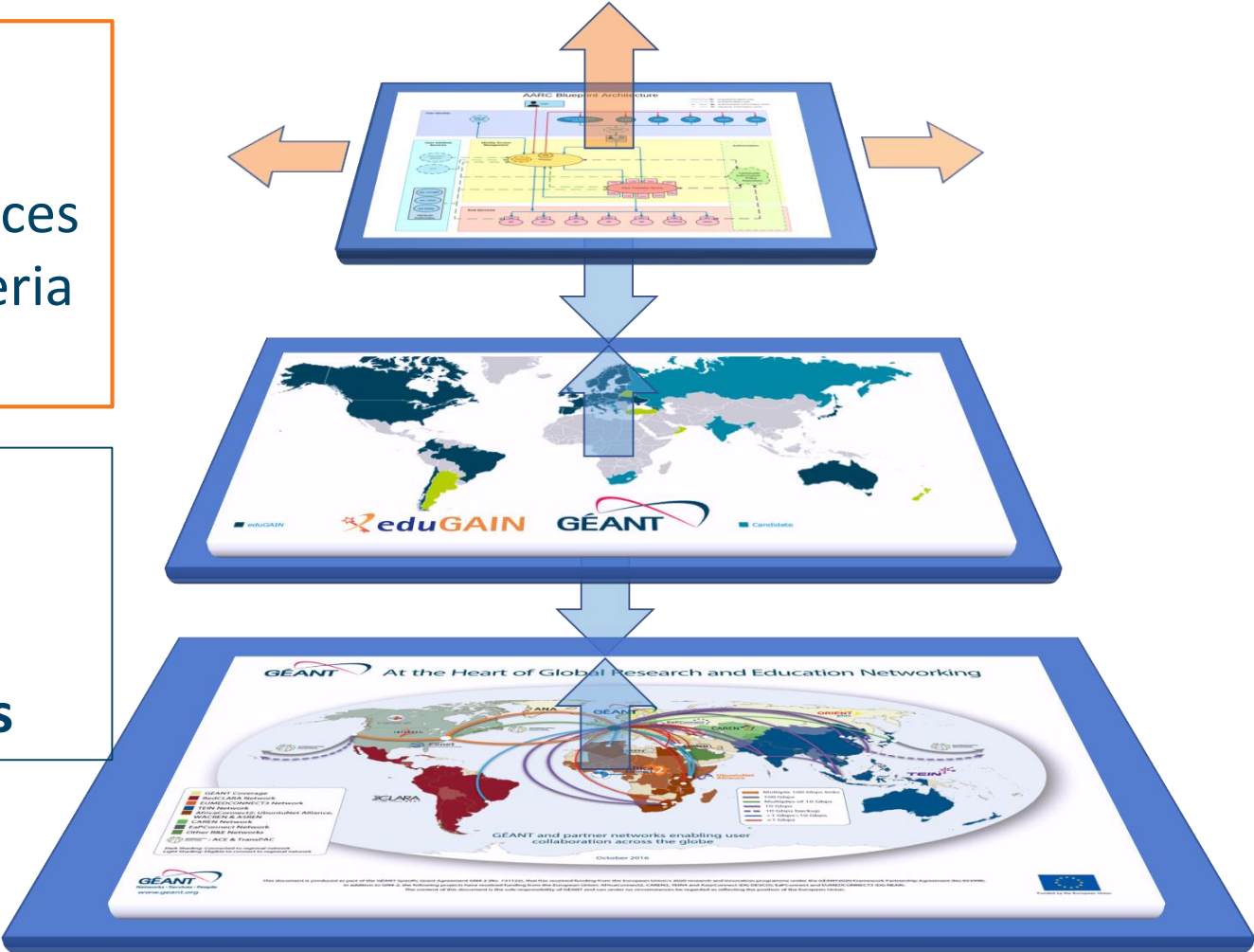
Engaging SPs



# The AARC Blueprint Architecture to bring everyone together

Defines a **model** and **building blocks** to address researcher needs  
**Cross-domain interoperation** and services based on community and provider criteria expressed using **common guidelines**

Allows researchers to use **ONE** digital identity to access **MANY** services and resources available through **eduGAIN** and in **collaborative r/e-Infrastructures**

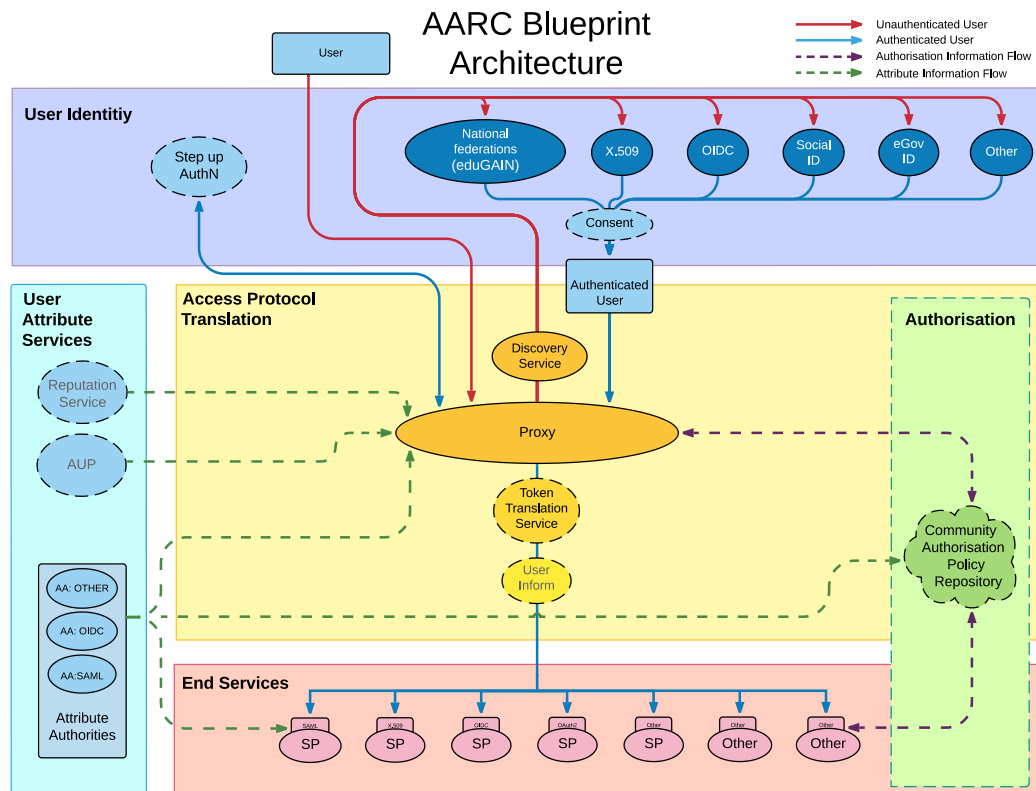


Key int





<https://aarc-project.eu/architecture/>



## Guidelines and supporting documents

- *reference architecture*
- *conventions and community standards*
- *best policy practices*
- *implementation hints*
- *training for 'FIM' communities*

# Making the proxy behave: infrastructure and community policy support

## Guidelines

The **AARC Guidelines** complement the **AARC Blueprint Architecture (BPA)** and the **policy best practices** recommended by the AARC project. The guidelines can apply to any topic that helps to advance Federated Identity Management for research and collaboration.

The AARC Guidelines help communities and infrastructures to implement and operate an AAI for research and collaboration more effectively and in an interoperable way.



- Architecture Guidelines
- Policy Guidelines
- Targeted Guidelines
- Upcoming Guidance

### AARC-G014 Security Incident Response Trust Framework for Federated Identity

Sirtfi provides a mechanism to identify trusted, operationally secure eduGAIN participants and facilitate effective incident response collaboration. [more information](#)

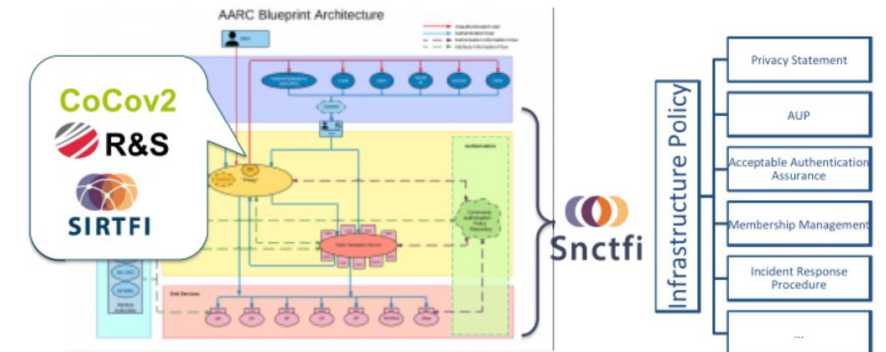
### AARC-G015 Scalable Negotiator for a Community Trust Framework in Federated Infrastructures

The Snctfi framework identifies operational and policy requirements to help establish trust between federations or in another infrastructure, in each case joined via a Service Provider to Identity Provider. [more information](#)

### AARC-G021 Exchange of specific assurance information between

infrastructures and generic e-infrastructures comprise an 'effective' assurance profile derived by resulting assurance assertion obtained between infrastructures so that it need not be re-computed by the provider. This document describes the assurance profiles recommended to be used by the infrastructures. [more information](#)

[aarc-community.org/guidelines](https://aarc-community.org/guidelines)



- Architecture Guidelines
- Policy Guidelines
- Targeted Guidelines
- Upcoming Guidance

### AARC-G040 Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)

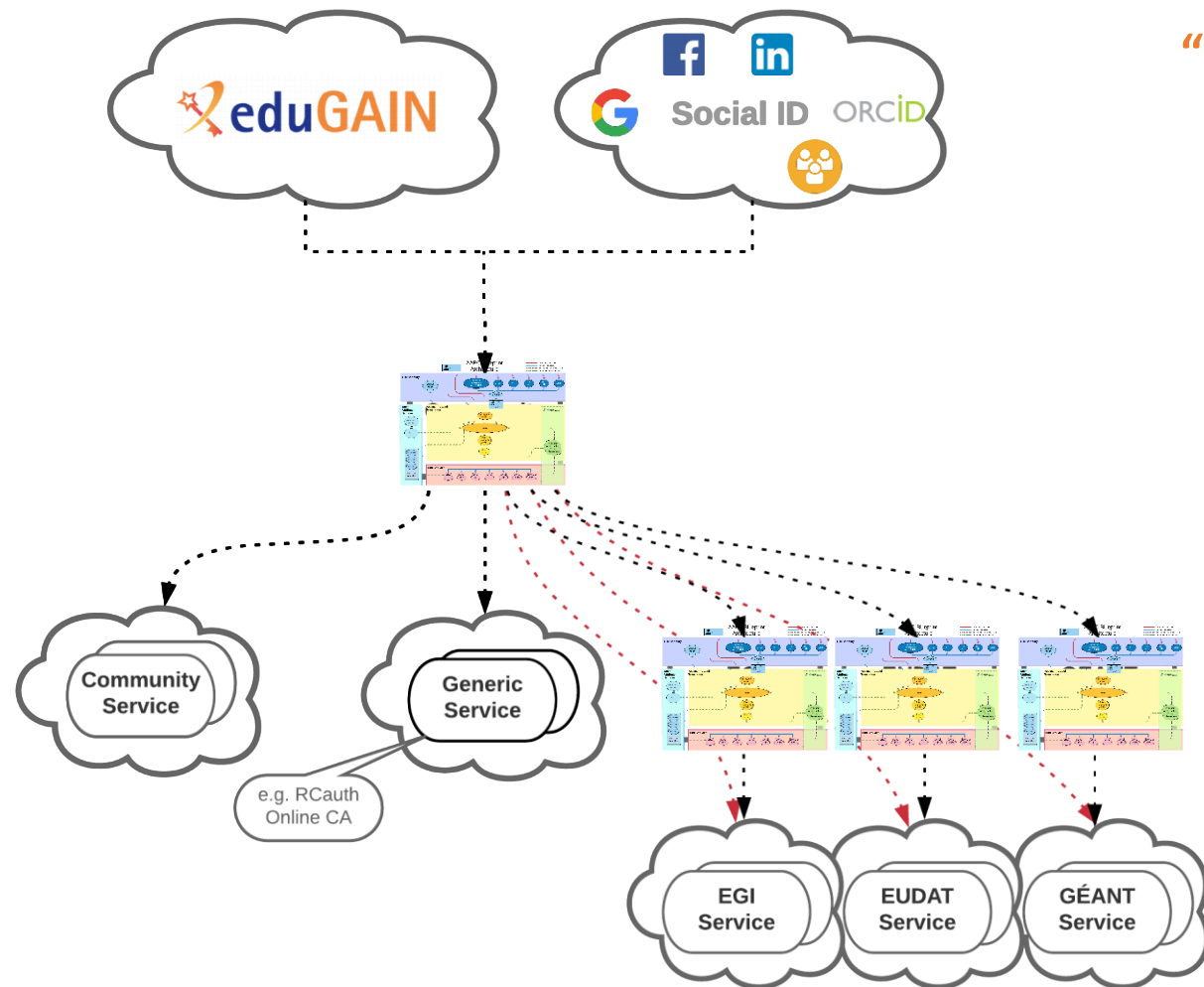
The Life Sciences AAI Service (LS AAI), developed in joint collaboration with EDI, EUDAT and GÉANT, will result in a production-equivalent service to be operated for the Life Sciences community by the joint e-infrastructures. As the pilot enters its second phase the LS AAI has to declare compliance to R&S and CoCo towards the R&E federations. This document provides preliminary guidance for the operators of the pilot LS AAI. [more information](#)

# Evolution of the Blueprint Architecture

## “Community-first” BPA approach

- Researchers sign in using their institutional (eduGAIN), social or community-managed IdP via their Research Community AAI
- Community-specific services are connected to a single Community AAI
- Generic services (e.g. RCauth.eu Online CA) can be connected to more than one Community AAI proxies
- e-Infra services are connected to a single e-infra SP proxy service gateway, e.g. B2ACCESS, Check-in, Identity Hub, etc

[https://aarc-project.eu/wp-content/uploads/2019/05/AARC2-DJRA1.4\\_v2-FINAL.pdf](https://aarc-project.eu/wp-content/uploads/2019/05/AARC2-DJRA1.4_v2-FINAL.pdf)





# The evolved role for policy and best practices for the AARC Community

## Policy Guidelines for the Proxy and Infrastructure Consultancy role for *communities & infrastructures*

- work items address policy aspects of the architecture & implementation, *e.g.*,
  - AARC-G041** *Assurance derived from social media*
  - AARC-G048** *Secure Operation of Attribute Authorities ...*
- address ‘pilots’ from the AARC communities, or Infrastructures, *e.g.*
  - AARC-G040** *Policy Recommendations for the LS AAI (application to R&S and CoCo)*
  - AARC-I044** *Implementers Guide to the WISE Baseline Acceptable Use Policy*

You see the policy work ‘homed’ in your favourite forums: WISE, IGTF, REFEDS, FIM4R

joint work  
with peers in



## introduction video – training – 9 reference templates – continued improvement

### Get Started with Policies

A [Moodle course](#) is available to learn more about Policies for the AARC Blueprint Architecture and videos from this course are also available on the [AARC playlist](#) on YouTube GÉANTtv.

A [PDK promo video](#) is also available to share.

Supporting documents are available below for download.

### Download Material

Show 100  entries

Search:

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	<a href="#">Google Doc</a>
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.	<a href="#">Google Doc</a>
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.	<a href="#">Google Doc</a>
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.	<a href="#">Google Doc</a>
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.	<a href="#">Google Doc</a>
Policy on the	Infrastructure Management & Data	Research Community	This document defines the obligations on Infrastructure Participants when	<a href="#">Google</a>

joint work  
with peers in



## Example – the WISE Baseline AUP *developed in WISE-SCI*



The WISE Baseline Acceptable Use Policy and  
Conditions of Use  
Version 1.0.1 (draft), 25 Feb 2019

Authors: Members of the WISE Community SCI Working Group.  
e-mail: [sci@lists.wise-community.org](mailto:sci@lists.wise-community.org)

© Owned by the authors and made available under license: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: "EGI Acceptable Use Policy and Conditions of Use", used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

DRAFT WISE Baseline AUP template v1.0.1

When using the baseline AUP text below, curly brackets "{ }" (coloured blue) indicate text

- **shown only once** to user during registration
- information on ***expected behaviour*** and restrictions
- **can optionally be augmented** with additional community or infrastructure specific clauses ***but numbered clauses should not be changed***
- registration point may be operated directly by research community or by third party on community's behalf

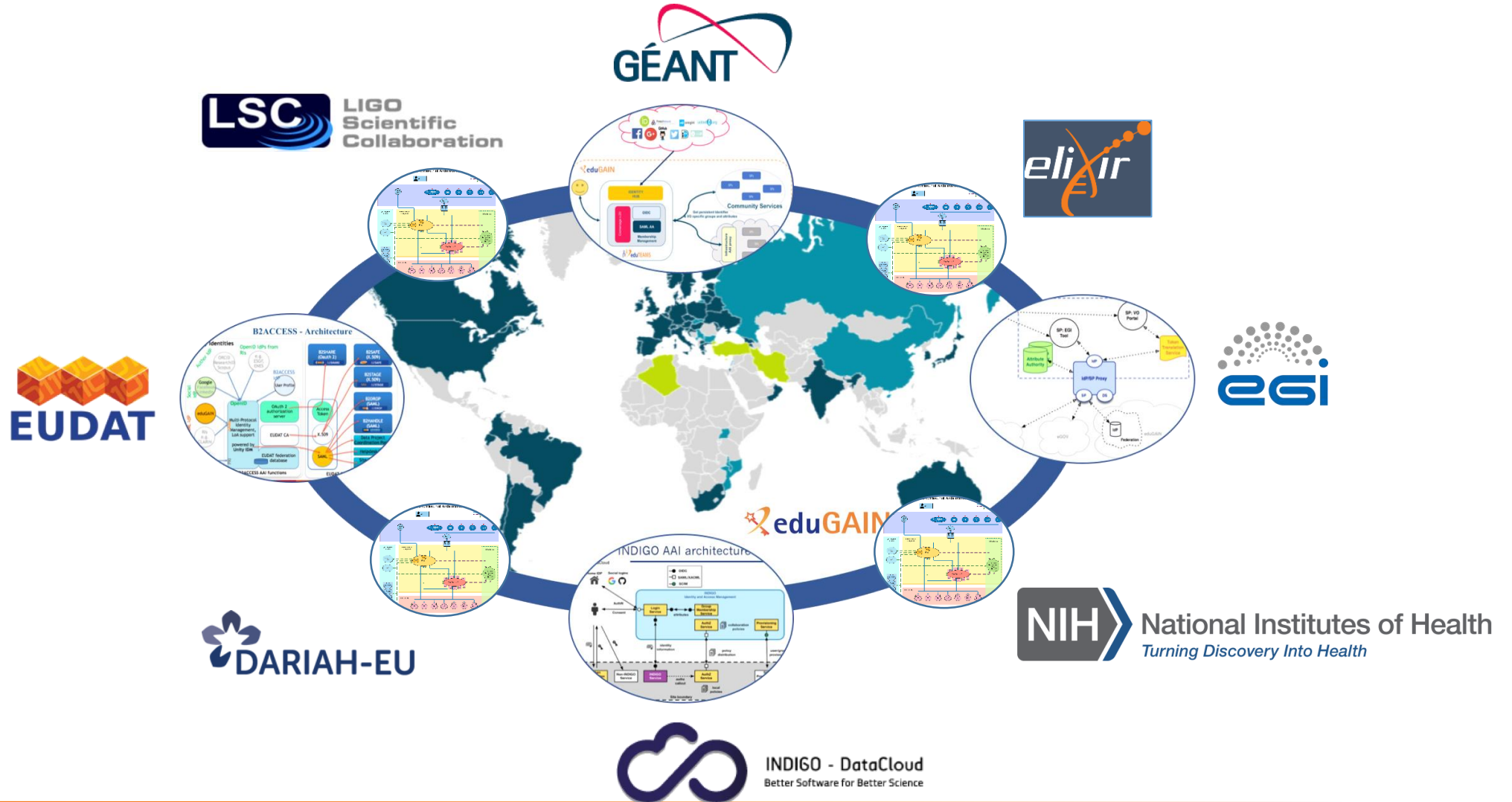
### Other information shown to user during registration

- ***Privacy Notice*** – information about processing & user rights
- ***Service Level Agreements*** – information about what user can expect from the service in terms of 'quality'
- ***Terms of Service*** – optional, with the 'benefits' to the user



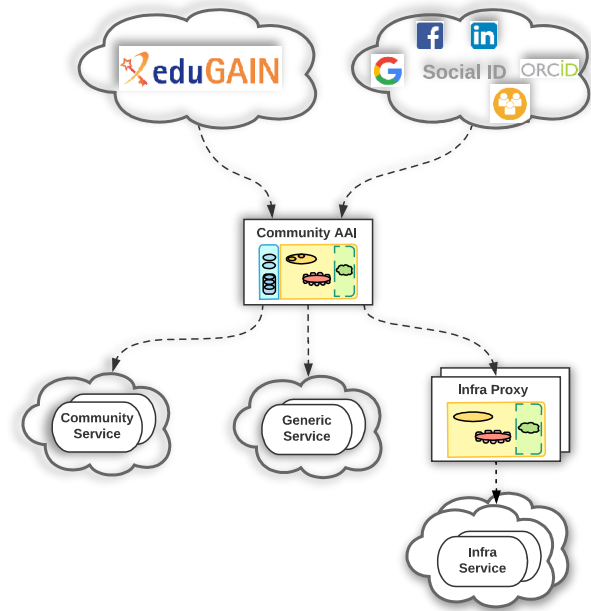


# AARC Blueprint Architecture Implementations



# Deploying a federated AAI? You don't have to be on your own!

- Communities with **existing Community AAI** connect to e-Infra Proxies and access generic e-Infra services via 'community first' proxy-cascade
- They **increasingly outsource technical AAI – retaining content control**
  - using either dedicated or multi-tenant deployments of AAI services operated in EOSC
- Multi-tenant deployments
  - aimed at medium-to-small research communities/groups or individual researchers
  - community members, groups and authorisation attributes are still managed by community managers
- Dedicated deployments
  - customisation of user-facing elements: IdP discovery, enrolment, membership UI
  - customisation of AAI behaviour (attribute aggregation rules, service entitlements)
  - providers offer option of *bespoke* AAI Solutions, which might include individual components from the GÉANT eduTEAMS, EGI Check-in, INDIGO IAM, EUDAT B2ACCESS, and PERUN



# Implementation in the generic e-Infrastructures and AAI offerings

	EUDAT B2ACCESS	EGI Check-in	GEANT eduTEAMS	INDIGO IAM
Alignment of user attribute/claim names	✓	✓	✓	Sept 2019
Alignment of VO/group membership and role information	✓	✓	✓	Sept 2019
Alignment of resource capabilities information	July 2019	Jun 2019	✓	Sept 2019
Alignment of affiliation information	TBC	Sep 2019	Sep 2019	Sept 2019
Alignment of assurance information	TBD	TBD	TBD	TBD
Alignment of privacy statements	✓	✓	✓	✓
Alignment of operational security and incident response policies	✓	✓	✓	✓
Alignment of Acceptable Use Policies (AUPs)	July 2019	✓	✓	Sept 2019







## LIGO Scientific Collaboration

*How the LSC community used AARC Blueprint Architecture to support federated identities in their AAI*



## Digital Research Infrastructure for the Arts and Humanities

*How DARIAH is deploying the AARC Blueprint Architecture to improve interoperability.*



## EISCAT\_3D

*How EISCAT\_3D use the AARC Blueprint Architecture to replace an outdated AAI.*



## LifeWatch ERIC

*How LifeWatch used the AARC Blueprint Architecture to find their solution*



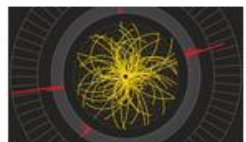
## European Plate Observing System

*How EPOS implemented a robust AAI following AARC's recommendations*



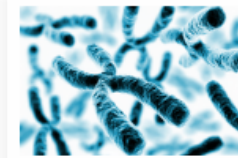
## Cherenkov Telescope Array

*How CTA is deploying elements of the AARC Blueprint Architecture to build an AAI for thousands of astronomers.*



## Worldwide LHC Computing Grid

*How WLCG is using the AARC Blueprint Architecture as a backdrop for the discussions as a reference frame for best practices.*



## CORBEL

*How a consortium of e-infrastructures is using the AARC Blueprint Architecture to respond to the AAI requirements of biomedical Research Infrastructures*

# Thank you

## Any Questions?

davidg@nikhef.nl



<https://aarc-community.org>



© GÉANT on behalf of the AARC project.

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).

