Authentication and Authorisation for Research and Collaboration

AARC multi-community BPA and assurance mapping

Harmonisation of policy, practice and architecture

David Groep
Policy and Best Practice Coordination
Nikhef

Nikhef

IGTF All Hands meeting Taipei
April 1, 2019

In collaboration with and co-supported by EOSC-HUB

Supported by the Dutch National e-Infrastructure coordinated by SURF

SURF

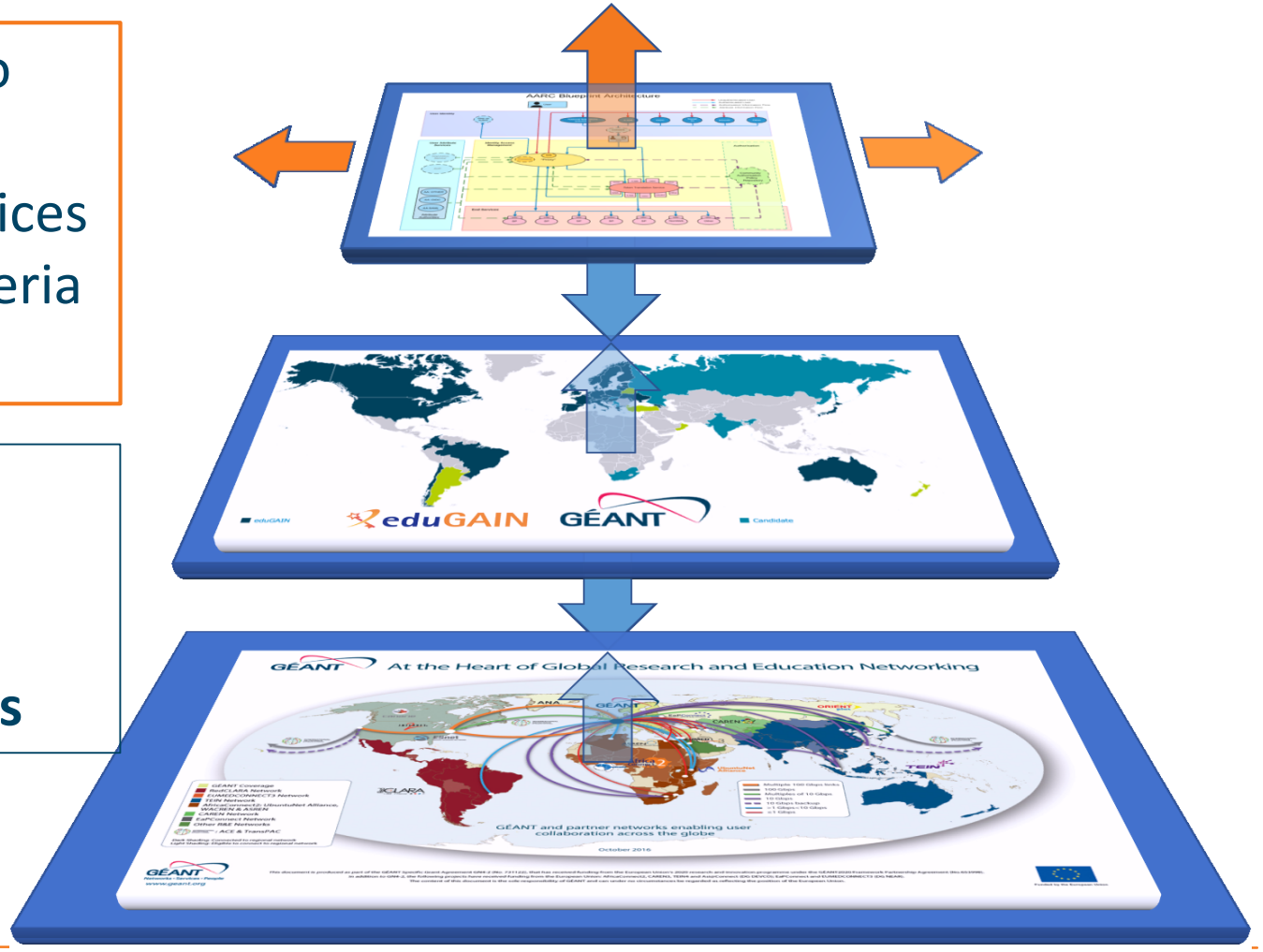
Welcome to the Research and e-Infrastructure Collaboration Landscape

Communities / e-infrastructures surveyed in AARC

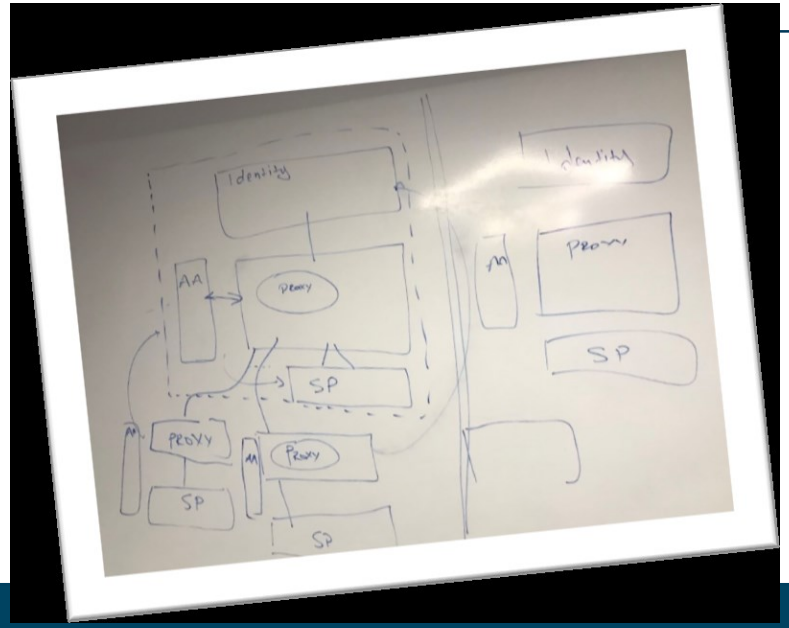
The AARC Blueprint Architecture to bring everyone together

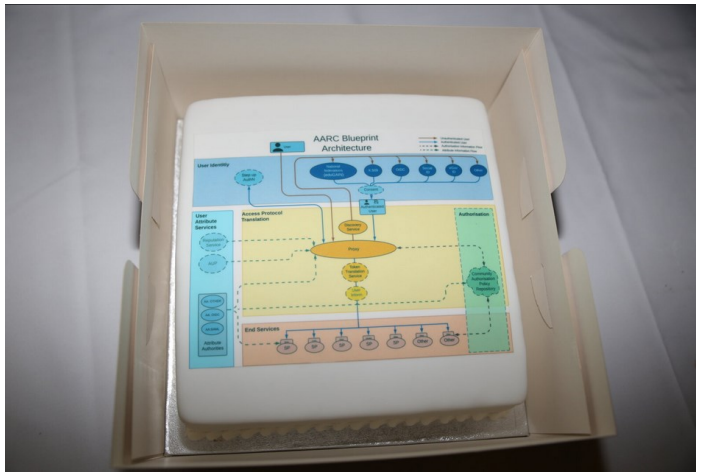
Defines a **model** and **building blocks** to address researcher needs
Cross-domain interoperation and services based on community and provider criteria expressed using **common guidelines**

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



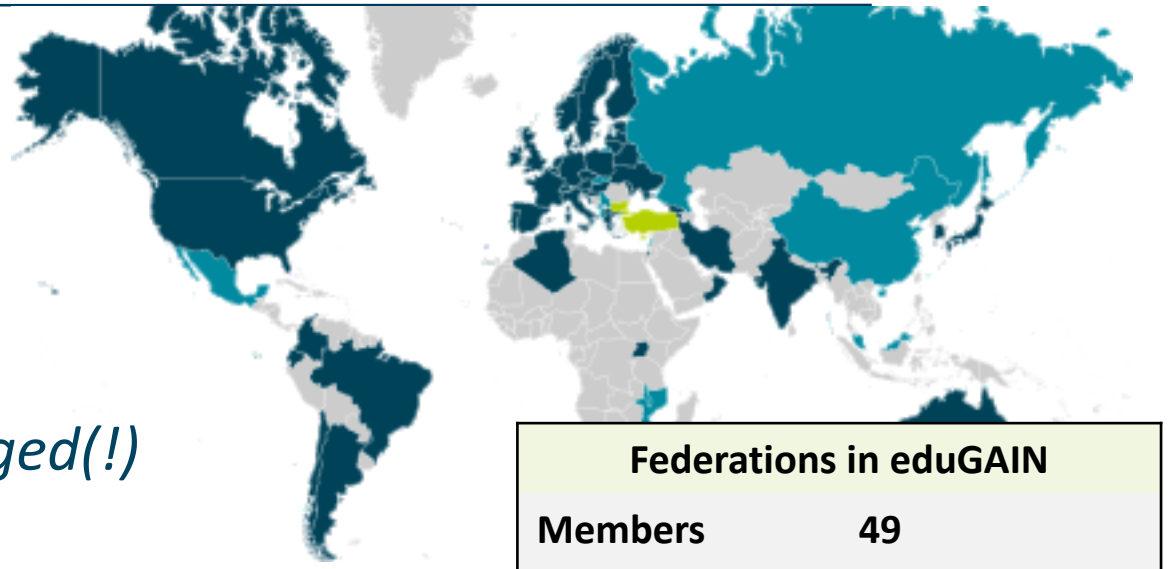
Blueprint for an AAI serving research and collaboration





The AARC Proxy Architecture model

Identity providers – eduGAIN, social, eGov, …



over 50 members & many different models

- *architecture (hub-and-spoke vs mesh)*
- *baseline policies present or absent*
- *non-reassigned id and attributes:*
  'by default', optional, or sometimes discouraged(!)
- *tagging of entities and IdPs ('categories'):*
  open, limited, or needs implementation repeatedly
- *constituency: including or excluding e.g. private R&D*
- *paid option or part of NREN base services package*
- *support available for organisational IdP software (e.g. ADFS)*

and then there is social ID for (citizen) science, eGov IDs *&c*

Federations in eduGAIN	
Members	49
Voting-only	6
Candidates	13
Entities in eduGAIN	
All	4538
IdPs	2654
SPs	1888
Standalone AAs	5

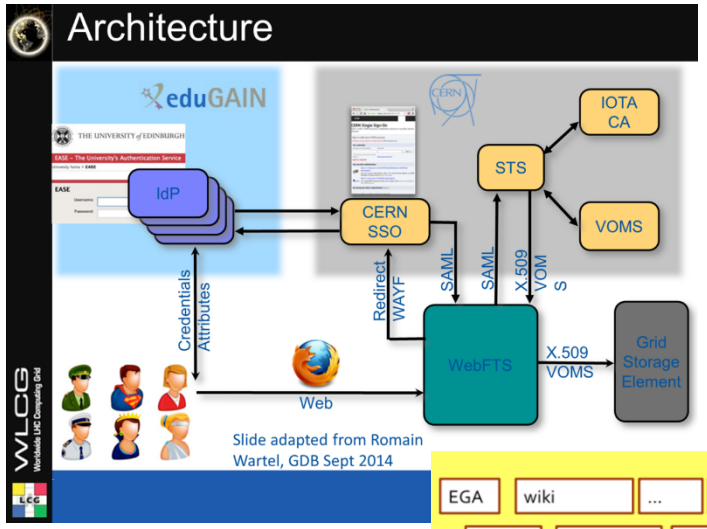
data: technical.edugain.org as of 11 March 2018

Identified common challenges

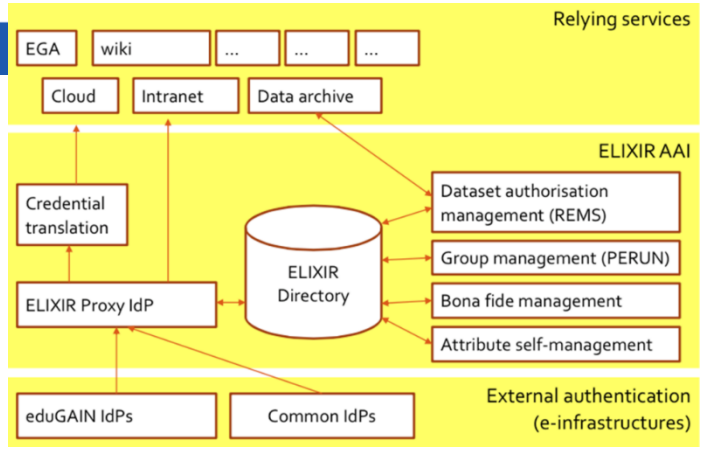
Communities / e-infrastructures surveyed in AARC

- Homeless users
- User friendliness
- PII Data Protection
- Community based AuthZ
- SP friendliness
- Credential translation
- Bridging Communities
- Engaging SPs

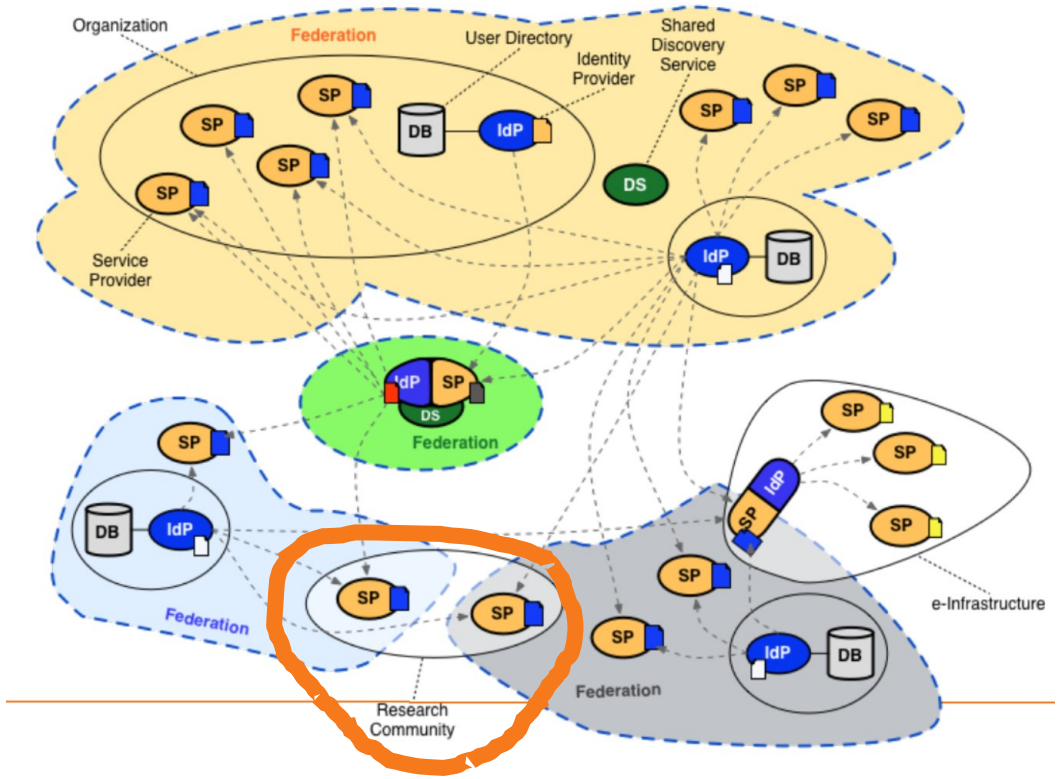
Whence we came – collaborative research AAIs predating AARC



WebFTS 'FIM4R' in wLCG
Romain Wartel



ELIXIR reference architecture
Mikael Linden et al.

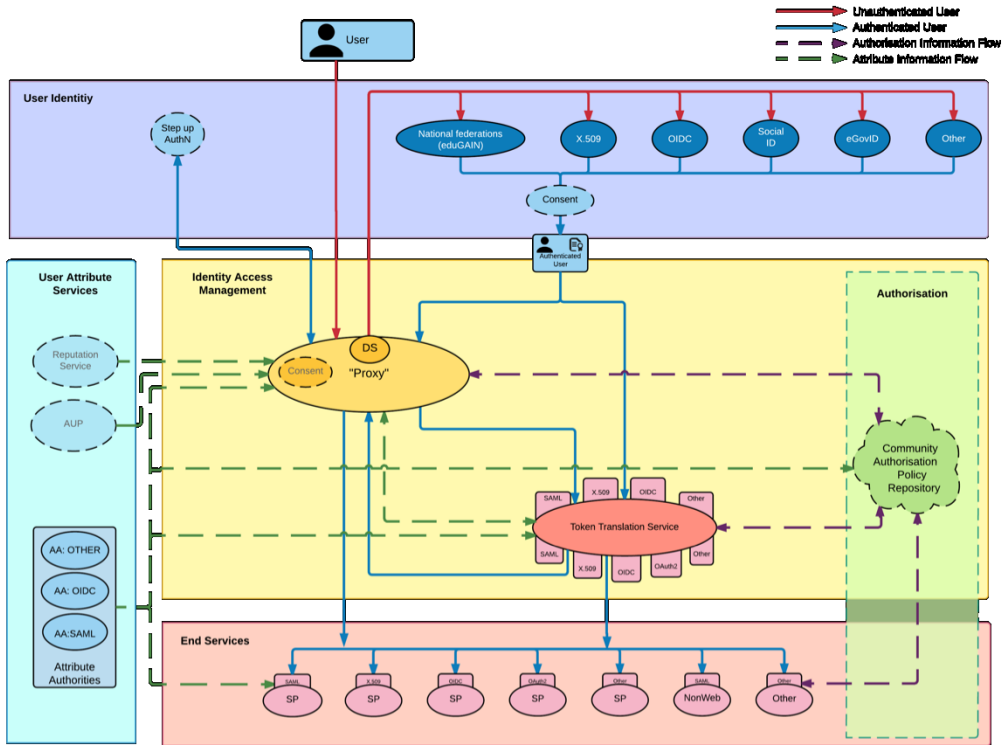


communities had either invented
their own 'proxy' model to abstract complexity

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

AARC Blueprint Process

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



Guidelines and supporting documents

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

https://aarc-project.eu/guidelines/

Harmonisation at the proxy – the technical bits
user identity layer and attribute services

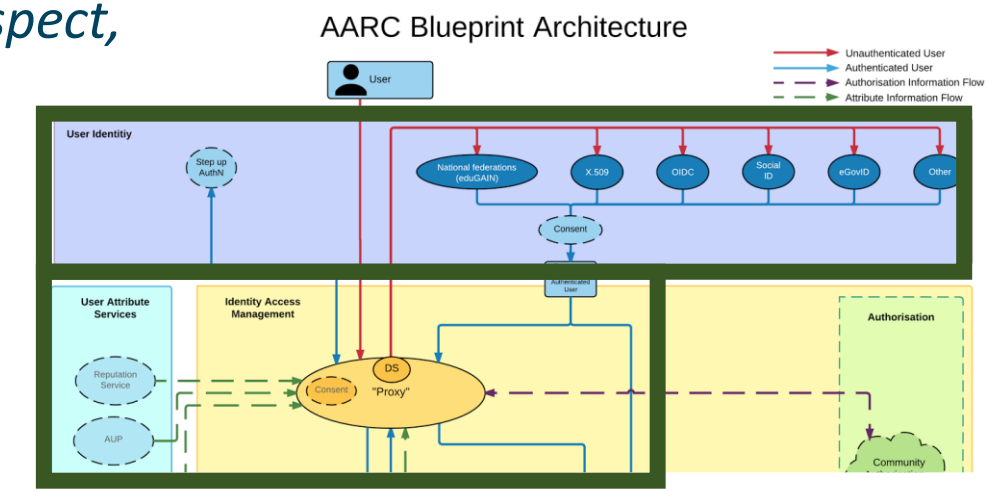
To harmonise incoming attributes, the proxy will need *state*

Long term state

- assignment of infrastructure-specific unique identifier
  current recommendation: eduPersonUniqueID or *sub* (type: public)
- heuristics to determine 'unexpected' changes in source IdPs
  even SAML NameID and eduPersonTargetedId may be suspect, and ePPN is not guaranteed
  (see Christos' post on REFEDS list 2019-03-22 at 22:05)
- account linking

Ephemeral state

- SSO caching
- optional step-up authentication done for this session
- assurance profile based on linked authentications



https://aarc-project.eu/guidelines/#architecture

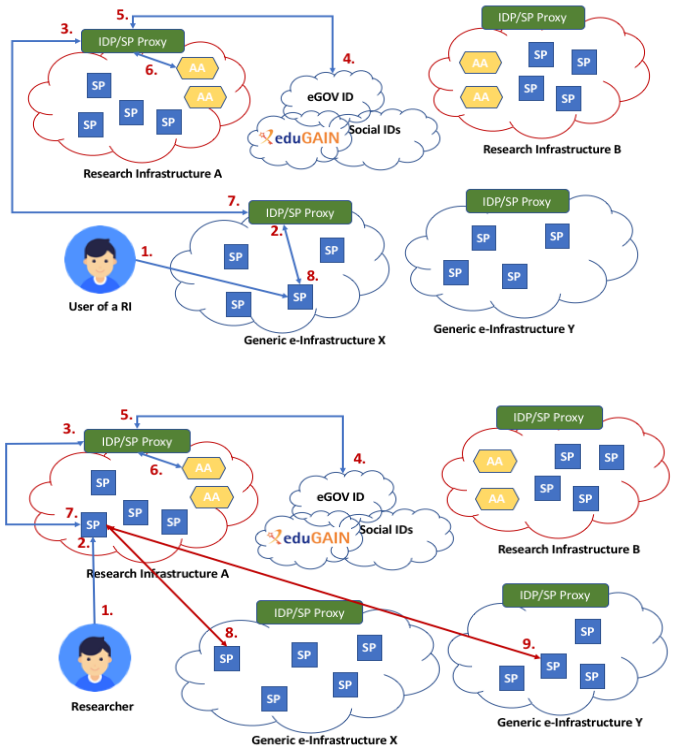
AARC2: Collect community feedback and requirements about cross-infrastructure interoperability

Use-Cases for Interoperable Cross-Infrastructure AAI

Analysis of **research community specific use cases** of cross-infrastructure access to services/resources:

- DARIAH
- Life Science
- EPOS
- …

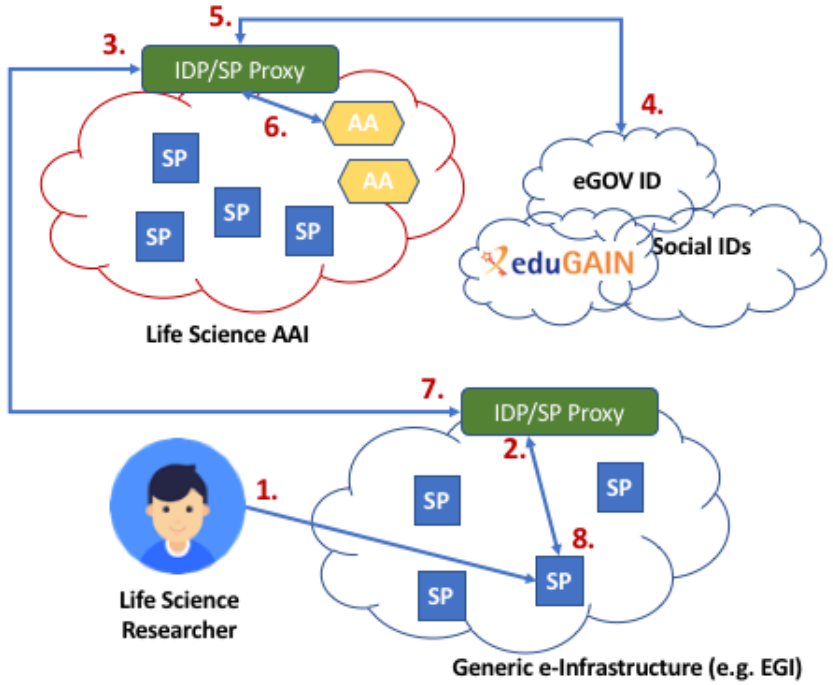
Generic use cases



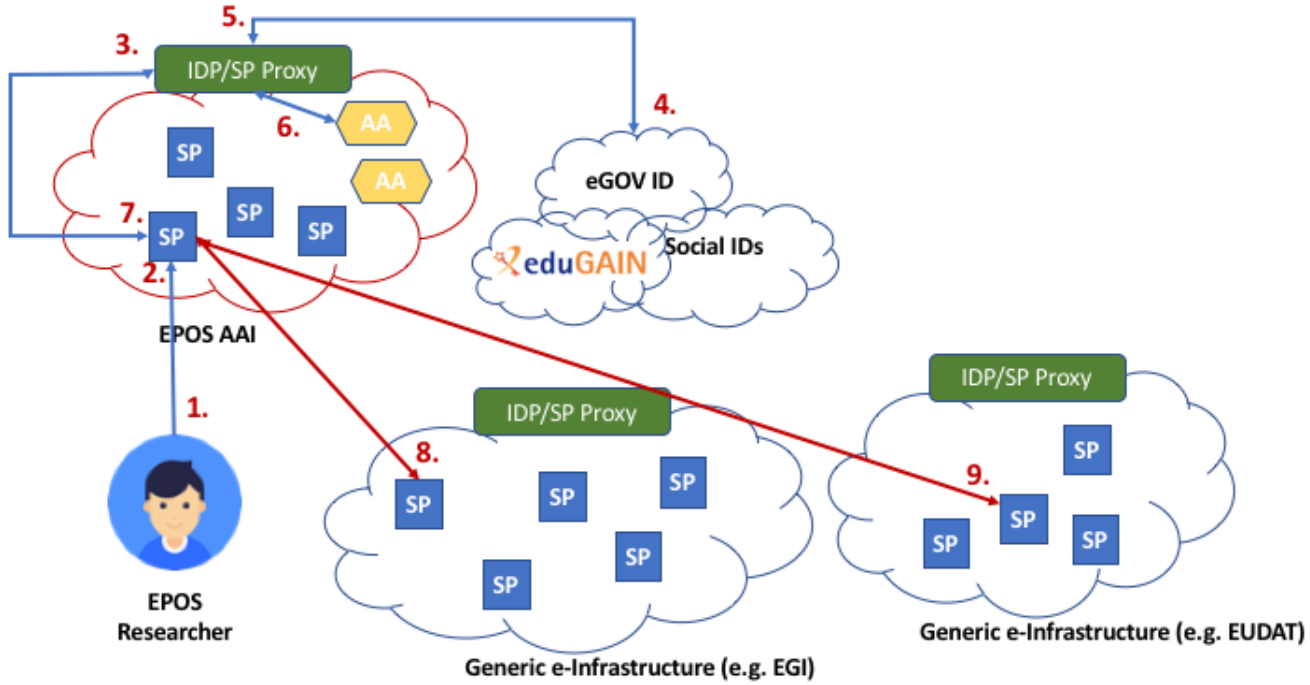
AARC2: Collect community feedback and requirements about cross-infrastructure interoperability

Use-Cases for Interoperable Cross-Infrastructure AAI

Generic Use Case 1 - Research Infrastructure users accessing e-Infrastructure services

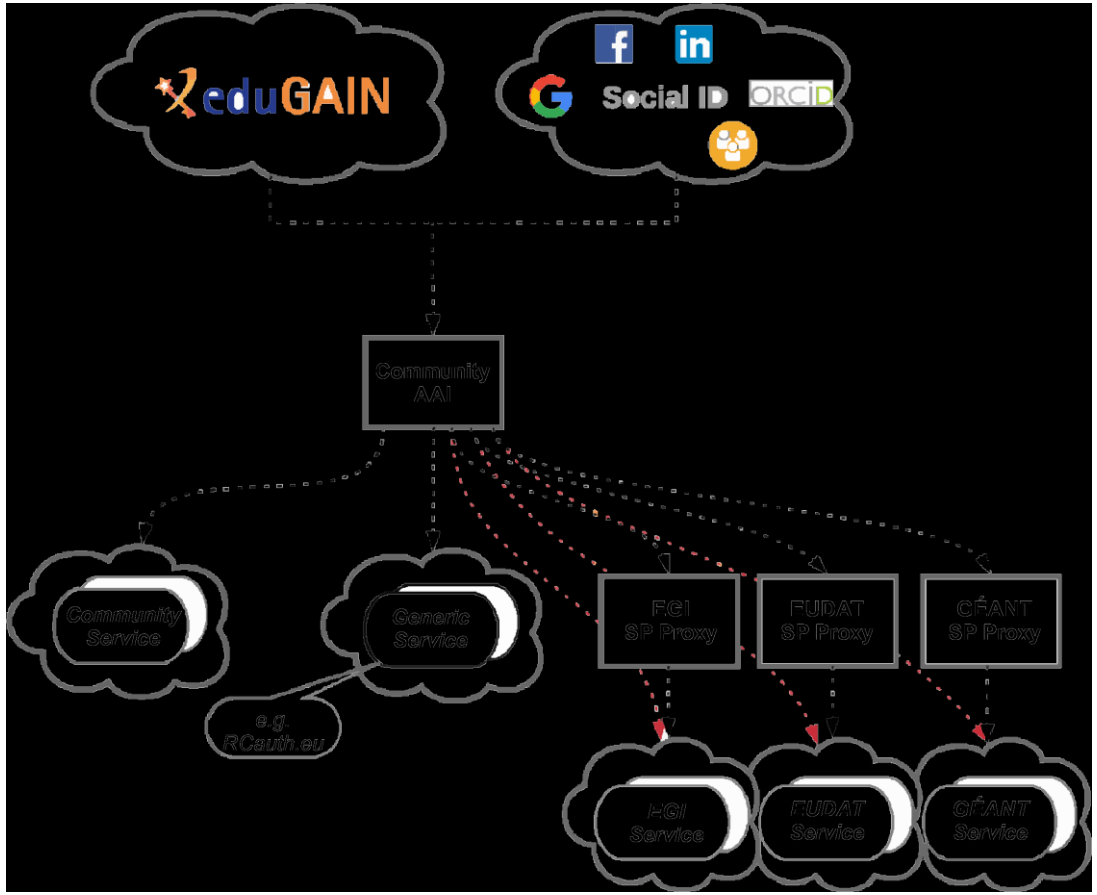


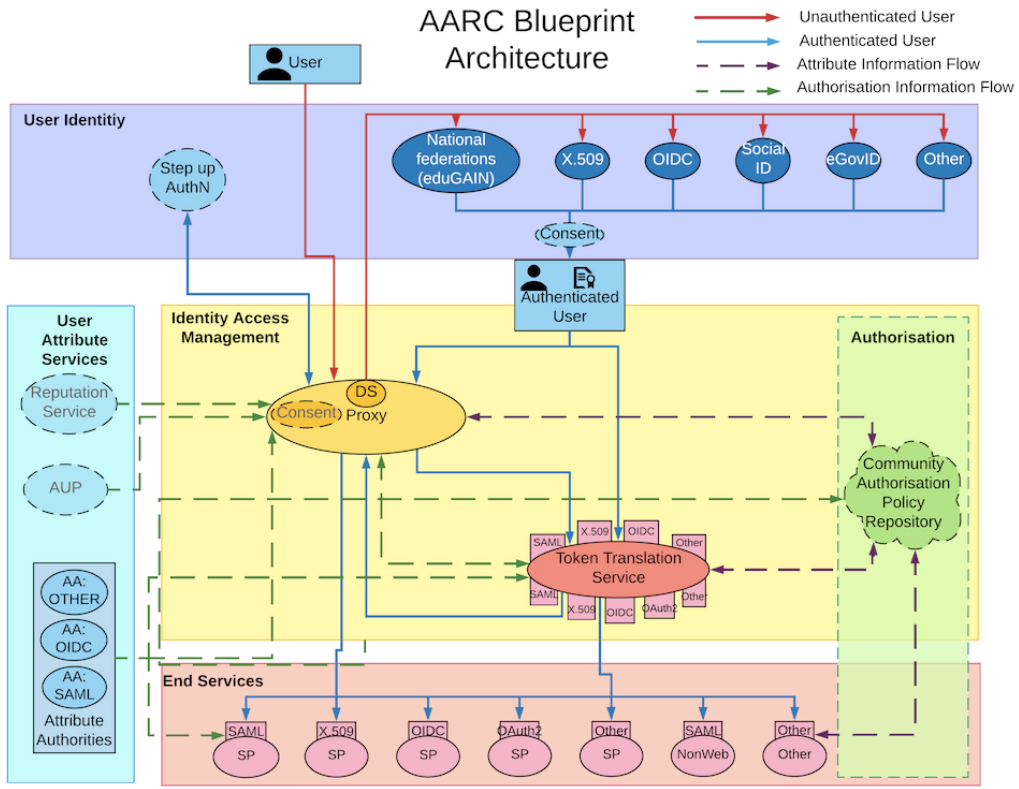
Generic Use Case 2 - Research Infrastructure services accessing e- Infrastructure resources on behalf of the user



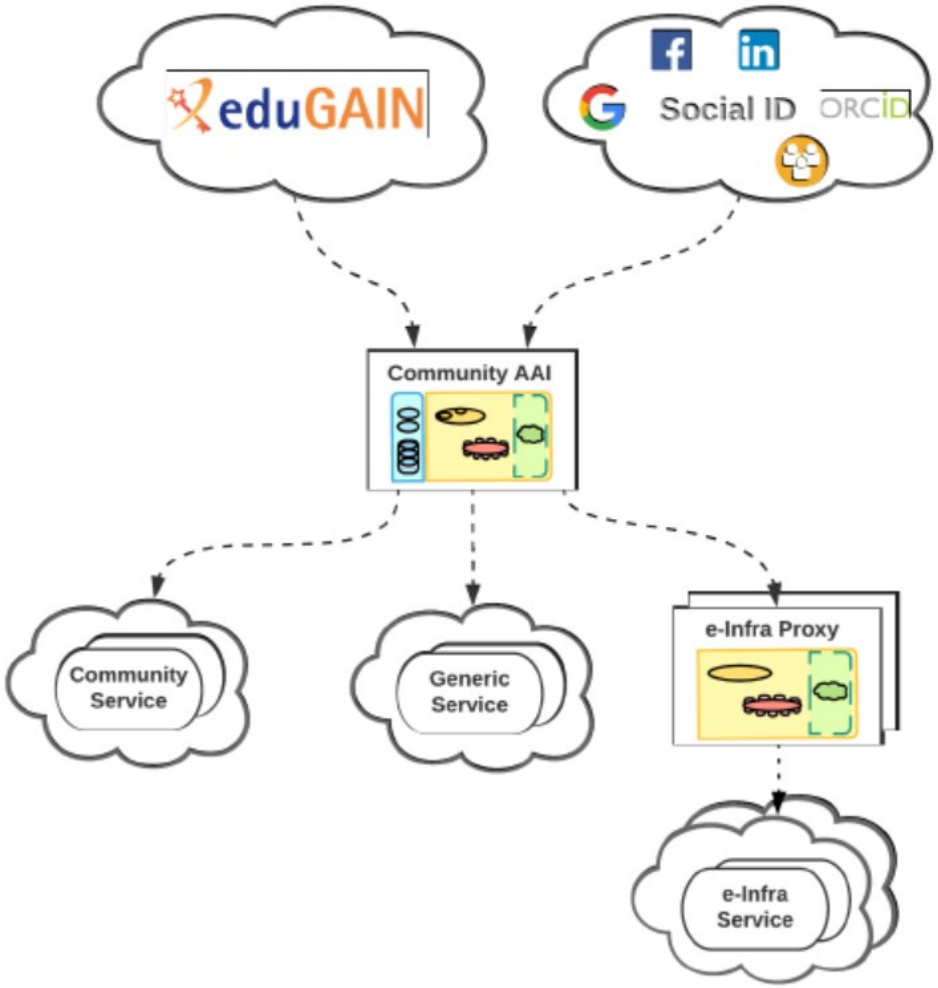
Evolving the AARC BPA to address multi-proxy scenarios

Mesh of services tends to group together in ‘conglomerates’: community-specific services, generic services offered to multiple communities, e-Infrastructures offering combined services





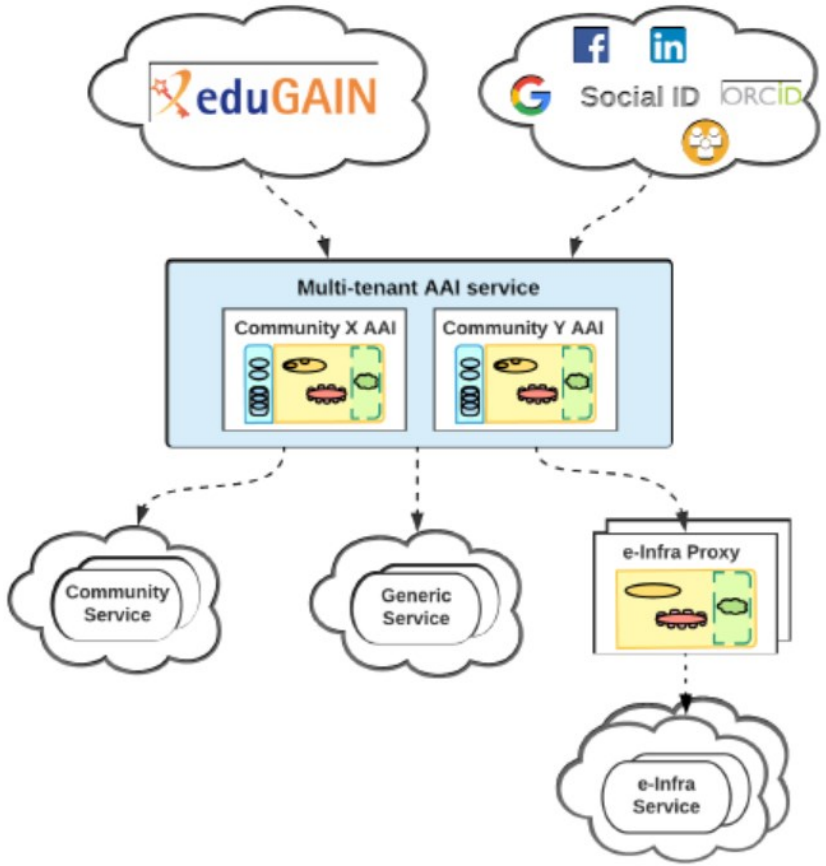
Community-First AAI approach



Community-first AARC 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 proxy
- e-Infra services are connected to a single e-infra SP proxy service gateway,
  e.g. B2ACCESS, Check-in, Identity Hub, *etc*

But architecture is not necessarily implementation: hosted AAIs!



Multiple offerings emerging (but the choice is non-trivial…)

- Seen initially for LSAAI as single-tenant ‘hosted’
- EOSC-hub e-Infra proxies: gain access to generic e-Infra services either dedicated or multi-tenant deployments of AAI services operated by EOSC-hub

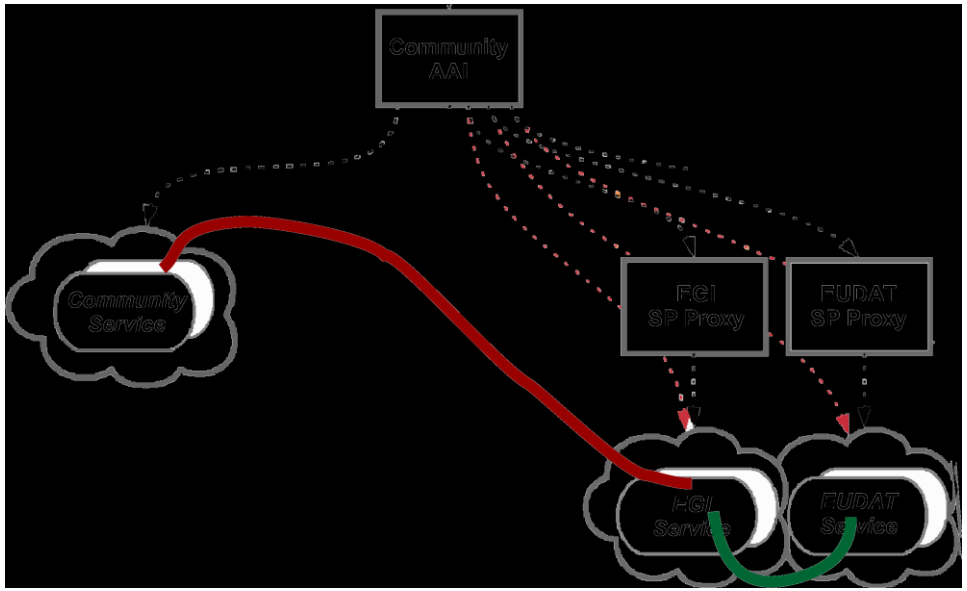
Multi-tenant deployments:

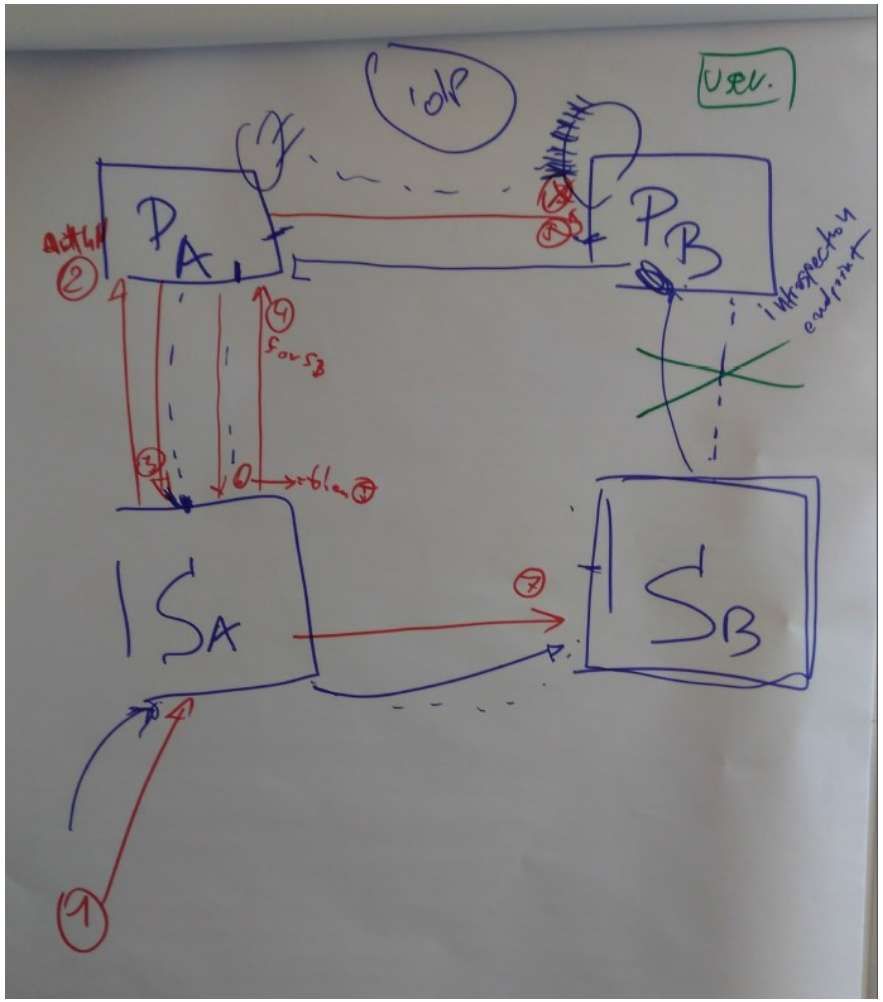
- aimed at medium-to-small research communities/groups or individual researchers.
- community members, groups and authorisation attributes are still managed by community managers

Dedicated deployments:

- allow customisation of user-facing interfaces: IdP discovery page, enrolment, group membership UI
- customisation of AAI proxy behaviour(e.g. attribute aggregation rules, service entitlements)
- possibility of *bespoke* AAI solutions, which might include individual Components from the GÉANT eduTEAMS, EGI Check-in, INDIGO IAM, EUDAT B2ACCESS, and PERUN (like in LSAAI)

Multi-BPA in practice: the cross-infra OAuth2 delegation scenario example





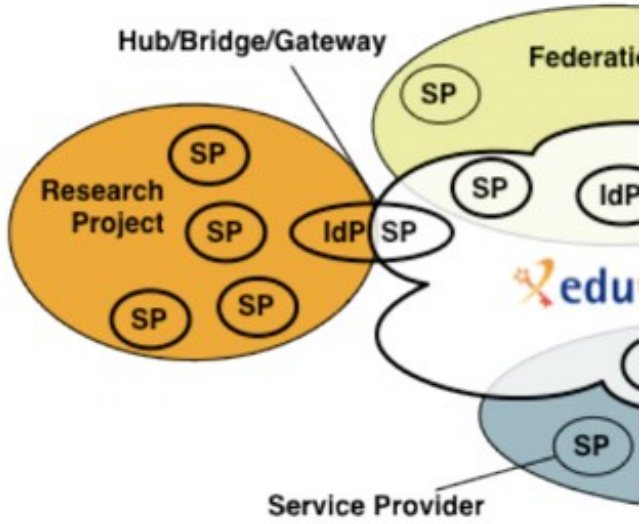
'How can Service Sb recognize and process an access token coming from a job at Sa in another infrastructure, without either Sa or Sb having to be modified, Sb being able to trust Pb, and access tokens being both scoped and encrypted to the proper protected resource Sb?
In the multi-BPA model, this can work using an (updated draft) OAuth Token Exchange flow that does exactly what you want – if the process at Sa asks Pa to exchange its Sa token at Pb – which means Pb should trusts Pa, which it has to do anyway. And so Pb is fed a token it can verify at its own Pb infra proxy'

Proxies: more than technology

A policy framework for service providers groups and proxies in the BPA

Snctfi

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures



Snctfi v1.0 AARC

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi)

Licia Florio (GÉANT), David Groep (Nikhef), Christos Kanellopoulos (GÉANT), David Kelsey (STFC), Mikael Linden (CSC), Ian Neilson (STFC), Stefan Paetow (Jisc), Wolfgang Pempe (DFN), Vincent Ribaillier (IDRIS-CNRS), Mischa Salle (Nikhef), Hannah Short (CERN), Uros Stevanovic (KIT) and Gerben Venekamp (SURFsara)

AARC - Version 1.0 - 26 Apr 2017

e-mail: david.kelsey@stfc.ac.uk

Abstract: This paper identifies operational and policy requirements to help establish trust between an Infrastructure and identity providers either in an R&E Federation or in another Infrastructure, in each case joined via a Service Provider to Identity Provider proxy.

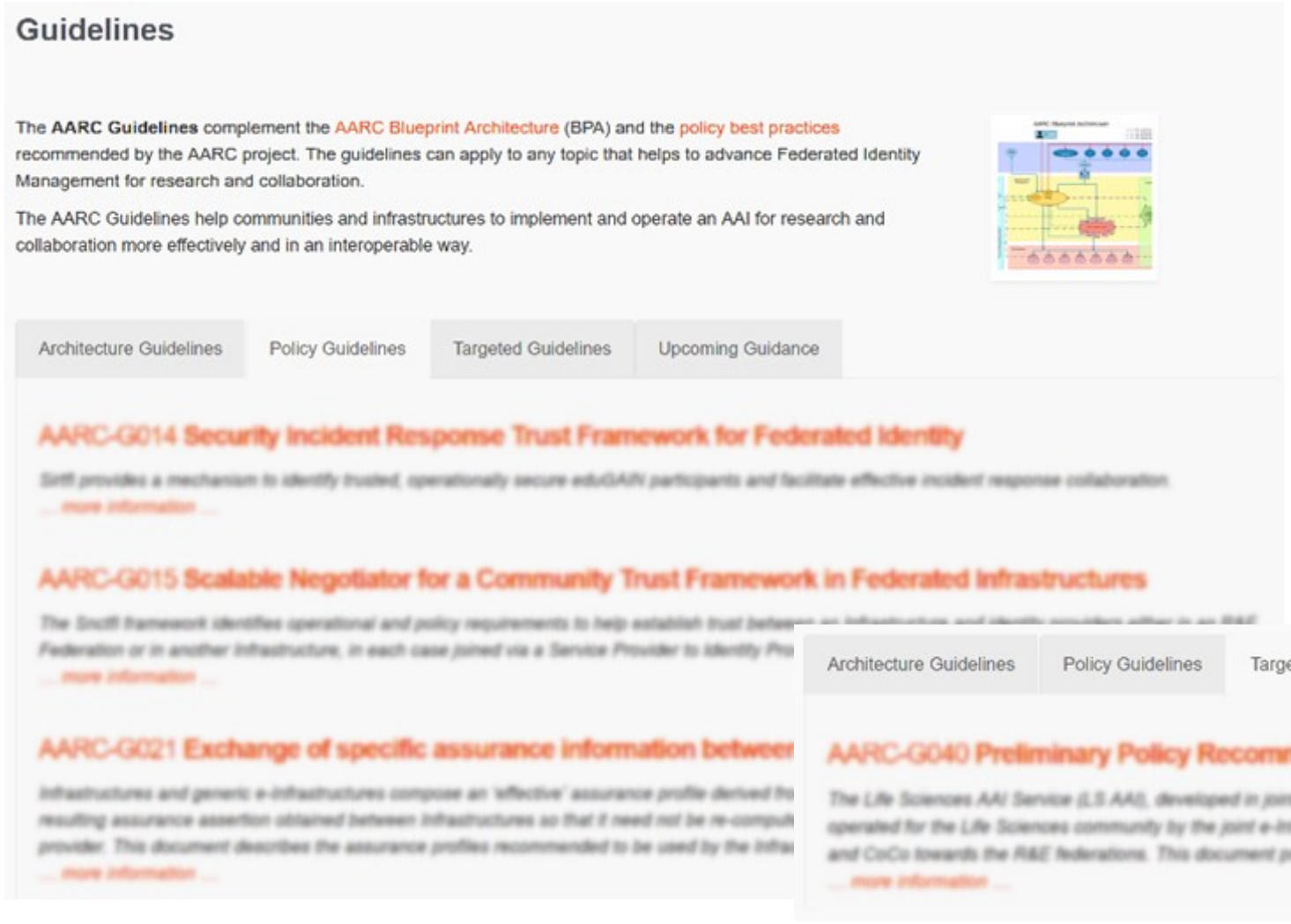
Audience: This document is intended for use by the personnel responsible for the management, operation and security of an Infrastructure and those wishing to assess its trustworthiness.

Derived from **SCI**, the framework on *Security for Collaboration in Infrastructures*

WISE **I**nformation **S**ecurity for **E**-infrastructures got global endorsement SCI in June 2017

graphic IdP-SP bridge: Lukas Hammerle and Ann Harding, SWITCH

Filling the framework: generic and community-targeted guidance



aarc-project.eu/guidelines

aarc-project.eu/policies/policy-development-kit/

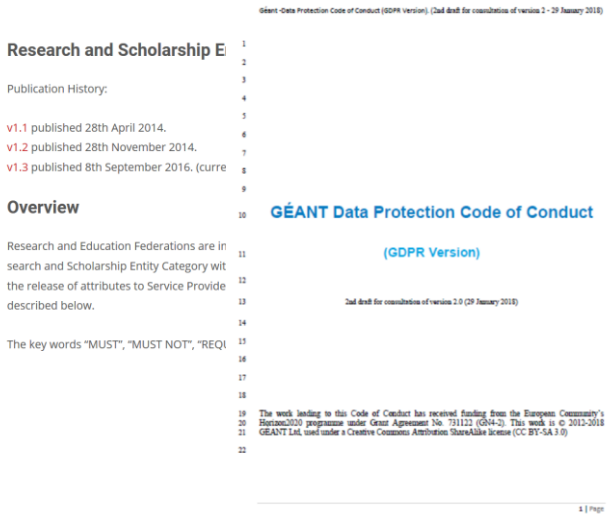
Snctfi *covers both* service-centric and some researcher-centric *policies*

Implementing *Snctfi*: interpreting generic policies for BPA Proxy use cases

REFEDS

research-and-scholarship

REFEDS R&S: allow attribute flow from the IdPs, express intent and scope


Research and Scholarship E

Publication History:

v1.1 published 28th April 2014.
v1.2 published 28th November 2014.
v1.3 published 8th September 2016. (curre

Overview

Research and Education Federations are in
search and Scholarship Entity Category wit
the release of attributes to Service Provide
described below.

The key words "MUST", "MUST NOT", "REQ(

GÉANT Data Protection Code of Conduct

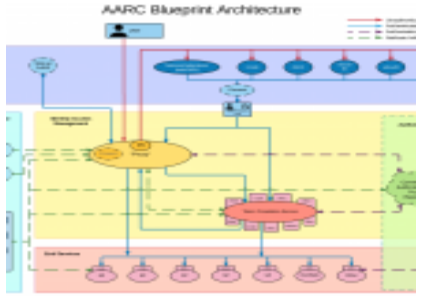
(GDPR Version)

2nd draft for consultation of version 2.0 (29 January 2018)

The work leading to this Code of Conduct has received funding from the European Community's Horizon2020 programme under Grant Agreement No. 731122 (GN4-2). This work is © 2013-2018 GEANT Ltd, used under a Creative Commons Attribution ShareAlike license (CC BY-SA 3.0)

GEANT DPCoCo & GDPR - 'I'll be good with personal data'

Casting policies into implementation and processes is a 'bridging process', requiring **policy and architecture expertise** and **knowledge of the community** use case **– i.e. the ingredients that make AARC!**



LSAAI Infrastructures: which components will do what?

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

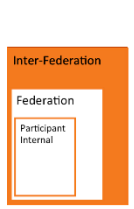
© GÉANT on behalf of the AARC project.
The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

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 GEANT, 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.

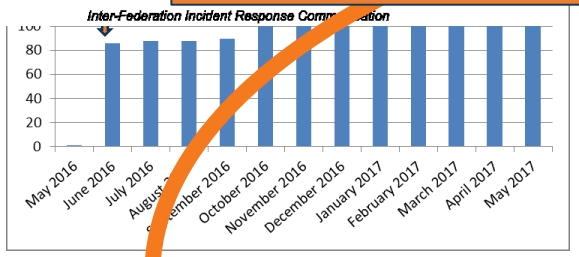
AARC-G040

AARC BPA: this is how information flows

How can policy help you ease collaboration?

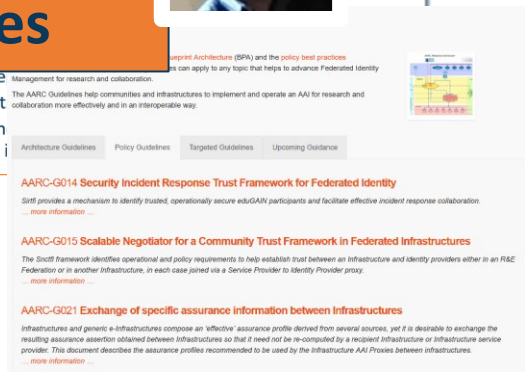


Operational Security for FIM Communities

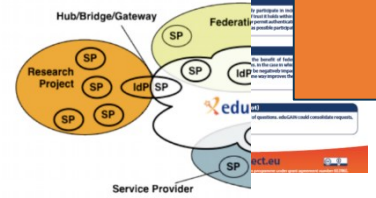


SIRTFI
Security Incident Response Trust Framework for Federated Identity

supporting policies for Infrastructures



Snctfi



engagement and coordination

3 Community Operations Security Policy

a Community
lerated

s Kanellopoulos (GÉANT), son (STFC), Stefan Paetow IRIS-CNRS), Mischa Salle
FERN), Uros Stevanovic (KIT) and Gerben Venekamp

2. The Community shall provide and maintain, in a repository designa
Infrastructure, accurate contact information as specified by the Infrastructure.

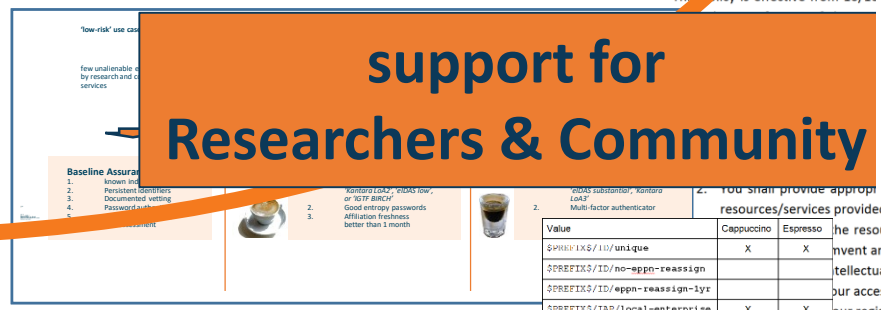
AARC - Version 1.0 - 26 Apr 2017

e-mail: david.kelsey@stfc.ac.uk

Abstract: This paper identifies operational and policy requirements to help establish trust between an Infrastructure and identity providers either in an R&E Federation or in another Infrastructure, in each case joined via a Service Provider to Identity Provider proxy.

Audience: This document is intended for use by the personnel responsible for the management, operation and security of an Infrastructure and those wishing to assess its trustworthiness.

support for Researchers & Community



1 ACCEPTABLE USE POLICY AND CONDITIONS OF USE

This policy is effective from 10/10

ersion of this do
curity Policy [R
cuments in the s

od and will abid

work, or transr
of use as define

ort or citation fo

resources/services provided as required by the body or bodies granting you

he resources/services for any purpose that is unlawful

nvent any administrative or security controls.

ntellectual property and confidentiality agreements.

our access credentials (e.g. private keys or passwords).

our registered information correct and up to date.

tely report any known or suspected security breach

Value	Cappuccino	Espresso
$PREFIX$/ID/unique	X	X
$PREFIX$/ID/no-eppn-reassign		
$PREFIX$/ID/eppn-reassign-1yr		
$PREFIX$/IAP/local-enterprise	X	X
$PREFIX$/IAP/assumed	X	X
$PREFIX$/IAP/verified		X
$PREFIX$/AAD/good-entropy	X	
$PREFIX$/AAD/multi-factor		X
$PREFIX$/ATP/ePA-1m	X	X

Responding to incidents – sharing relevant information

- Sirtfi take-up at proper organizational level

Beyond basic Sirtfi

- federation-level engagement in process
- *Sirtfi+* registry broadens global base
- engagement in trust groups valuable for federated collective response

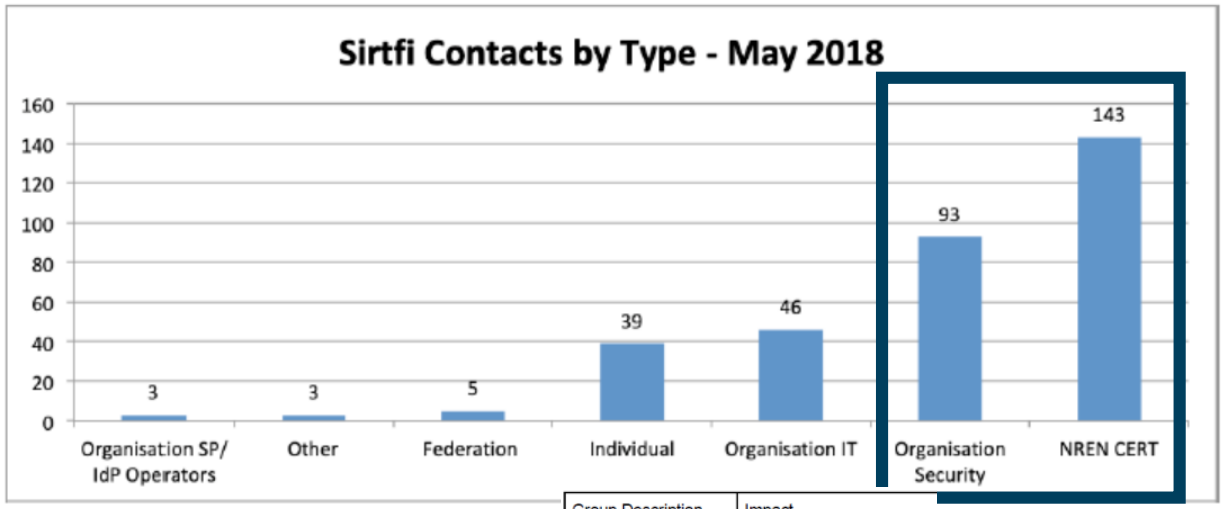


Figure 2: Sirtfi contacts as listed in the edu *d by contact type.*

to the Federated R&E Community given that it is considered unlikely that all Federation Participants would participate in Trust Groups as described above.

Trust Group Benefit	Proposal for the Federated R&E Community
Access to security contacts	Work should continue to promote the Sirtfi framework and identify contacts for Federation Participants. In addition, contacts for Federations and Interfederations

Group Description	Impact
Organisational level membership, Open application	A low degree of trust allow make contact with one ano and facilitates the exchang These groups typically pro additional face-to-face trus
Organisational level membership, Open application with peer vetting	A moderate degree of trust intelligence and vulnerabili groups facilitate the excha These groups typically pro additional face-to-face trus
Individual membership, Invitation only	A high degree of trust lead intelligence sharing and co incident response. Individu play an active role and hav background. Trust is accru meaning that if an employe their job, the benefits are t employer.
Infrastructure group, individuals nominated by participating organisations	These groups facilitate the distributed infrastructures be a single organisation he Individuals are typically no role as a security expert at organisation.

from DNA3.2 *Report on Security Incident Response and Cybersecurity in Federated Authentication Scenarios*

… the rest we test …

In AARC2 we will further the work undertaken in AARC and provide a fram

Month	What	
9	Incident Response Test Model for Organizations **MNA3.3**	
10	Incident Simulation #1 Report	https://aarc-pro
19	Incident Simulation #2 Report	https://aarc-pro
?	Guideline on Incident Response for Federation Participants	Draft at https://
22	Report on Security Incident Response **DNA3.2**	Dr

16-11-2018

Incident Response Test Model for Organisations - Simulation #2

Deliverable MNA3.3.3

Contractual Date:	N/A
Actual Date:	16-11-2018
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	
Lead Partner:	CERN

			Role Test 1
			Identity 1
			IdP1
		org/signi	SP1
		https://fbr.csc.fi/shibboleth	SP3
MWA Telescope Collaboration	AAF	SP https://wiki.mwatelescope.org	SP2
UK Fed		Federation	
Haka		Federation	

Guidelines on Federated Security Incident Response for Research Communities

AARC-G051

https://wiki.geant.org/display/AARC/AARC2+NA3+Task+1+-++Overview
https://aarc-project.eu/guidelines/aarc-i051/

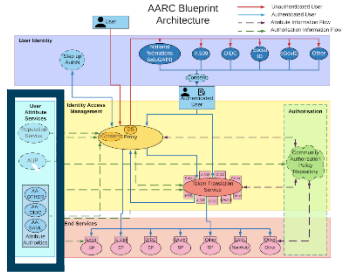
WISE Community: Security Communication Challenges Coordination WG (SCCC-WG)

Introduction and background

Maintaining trust between different infrastructures and domains depends largely on predictable responses by all parties involved. Many frameworks – e.g. SCI and Sirtfi – and groups such as the coordinated e-Infrastructures, the IGTF, and REFEDS, all promote mechanisms to publish security contact information, and have either explicit or implicit expectations on their remit, responsiveness,

Attribute Authority Operations and 'MMS assessment'

Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements



3. Operational Guidelines
3.1. Naming
3.2. Attribute Management and Attribute Release
3.3. Attribute Assertions
3.4. Operational requirements
3.4.1. Key Management
3.4.2. Network Configuration
3.5. Site Security
3.6. Metadata publication
3.7. Assessments and auditability
3.8. Privacy and confidentiality
3.9. Compromise and disaster recovery
4. Relying Party obligations

3.3. Attribute Assertions

Publication Date 2018-11-22
Authors: David Groep;David Kelsey;Hannah Short;Mischa Sallé;Uros Stevanovic;Stefan Paetow;Maarten Kremers
Document Code: AARC-G048

1. Assertions provided by an AA must be integrity-protected. They must be signed by the identified AA, or be transmitted over an integrity-protected channel where the server has been authenticated, and preferably both.

Push model
Where the protocol supports it, enable protection also of the messages conveyed over the established channel. Good examples: SAML Attribute Query should enable message signing and use TLS.

Pull model
As a good example: LDAP should enable TLS protection of the channel

https://aarc-project.eu/guidelines/aarc-g048/
https://www.eugridpma.org/guidelines/aaops/

Service policies: helping peer-reviewed self-assessment in SCI and more

SCI assessment framework is there

mapping to ISO 27k is quite rough, though …

	A	B	C	D
1	**Infrastructure Name:**		<insert name>	
2	**Prepared By:**		<insert name>	
3	**Reviewed By:**		<insert name>	
4				
5	**Operational Security [OS]**		**Maturity**	
6			**Value**	**Σ**
7				
8	**OS1 - Security Person/Team**			#REF!
	- Risk Management Process			#REF!
	- Security Plan (architecture, policies, controls)			2.0
	3.1 - Authentication		3	
	3.2 - Dynamic Response		1	
	3.3 - Access Control			
	3.4 - Physical and Network Security			
	3.5 - Risk Mitigation			
	3.6 - Confidentiality			
	3.7 - Integrity and Availability	Q	1	1.0
	3.8 - Disaster Recovery			
	3.9 - Compliance Mechanisms			
	- Security Patching		1	1.0
	4.1 - Patching Process			
	4.2 - Patching Records and Communication			
	- Vulnerability Mgmt		1	0.7
	5.1 - Vulnerability Process			
	5.2 - Dynamic Response			
	- Intrusion Detection		2	
	- Regulate Access (including suspension)		1	
	- Contact Information			
	8.1 - Contact Users			

	A	B	C	D
	SCI-V1	Completeness in definition in whitepaper	SIRTFI v1.0 (dec 2015)	ISO 27002:2013
			subsections	
	Operational Security [OS]			
	OS1 - Security Model	yes	OS1	9. Access control
	OS1.1 - Authentication			
	OS1.2 - Authorisation			
	OS1.3 - Access Control			
	OS1.4 - Confidentiality			
	OS1.5 - Integrity			
	OS1.6 - Availability			
	OS1.7 - Compliance Mechanisms			
	OS2 - Security Patching	yes	OS2	12.5 Control of operationa
	OS2.1 - Patching Process			
	OS2.2 - Patching Records & Communication			
	OS3 - Vulnerability Mgmt	yes	OS3	12.6 technical vulnerability
	OS3.1 - Vulnerability Process			
	OS3.2 - Dynamic Response			
	OS4 - Intrusion Detection	yes	OS4	13. communication securit
	OS5 - Regulate Access	yes	OS5	9. access control

https://wiki.geant.org/display/WISE/SCIV2-WG+documents

				PKIX RFC 3647 rendering	Persistent registry (community membership) implementation and assessment hints
				1.3.1	specific obligations are put on the registry, so a persistent organisation is needed to take care of these requirements. A community may outsource such obligations to a trusted third party or operator. The (collection of) membership management and assertion-issuing systems and services constitutes the Issuing Authority
				3.2, 4.7, 6.1.1, 6.1.2	The registration process should be such that the apparent applicant enrolled corresponds to the entity that is supposed to be in the registry. The registration data and any issued assertions constitute the 'credential of the user'.
A, B, C	3.1	Sufficient information must be recorded and archived such that the association of the entity and the subject name can be confirmed at a later date.	of custody the process should ensure that any applicant in the future, claiming the same name, is indeed the same entity as the original applicant. This is also needed in order to	3.2, 5.5	The registrar is responsible for all vetting and must record this information for as long as needed (as long as the entity is in the

http://wise-community.org/sci/

https://wiki.eugridpma.org/Main/AssuranceAssessment

Policy Development Kit

introduction video – training – 9 reference templates – continuous 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	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	Infrastructure Management & Data	Research Community	This document defines the obligations on Infrastructure Participants when	Google

https://aarc-project.eu/policies/policy-development-kit/

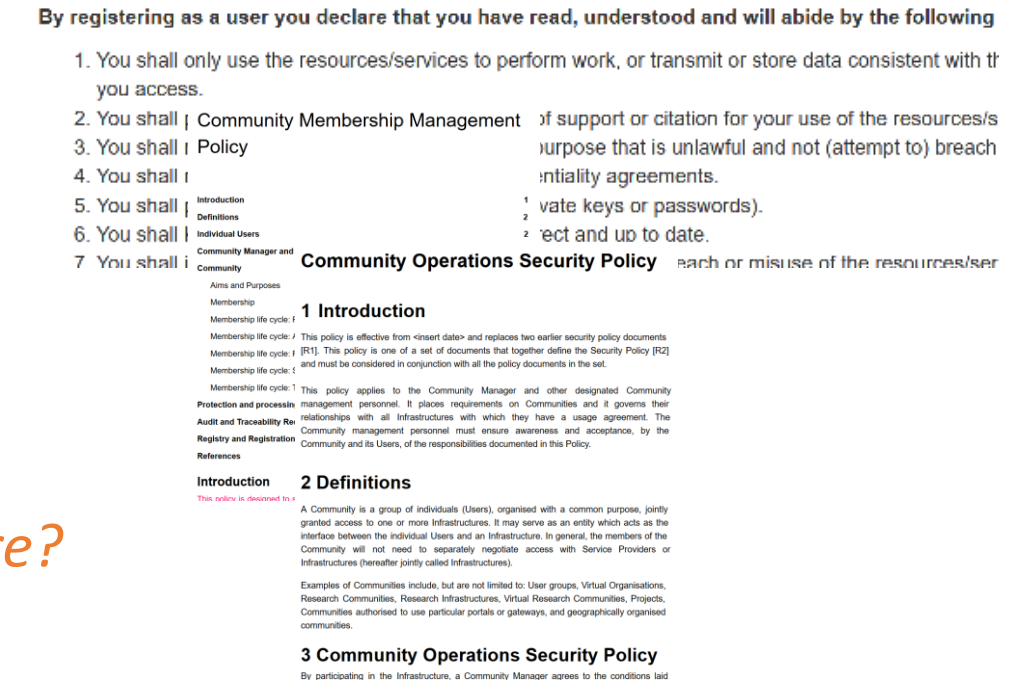
Guidance for research communities in the Infrastructure ecosystem

Authentication Assurance

- using both REFEDS RAF components as well as cross Infrastructure profiles
- considering social-ID authenticator assurance, complementing account linking in BPA

Exploit **commonality between acceptable use policies** to ease cross-infrastructure resource use

Support **community management using *Snctfi*** easing use of the generic e-Infrastructures
can you show community operations – sufficient to act as a one-stop registration for every Infrastructure?


By registering as a user you declare that you have read, understood and will abide by the following

1. You shall only use the resources/services to perform work, or transmit or store data consistent with th
   you access.
2. You shall | Community Membership Management of support or citation for your use of the resources/s
3. You shall r Policy urpose that is unlawful and not (attempt to) breach
4. You shall r ntiality agreements.
5. You shall | vate keys or passwords).
6. You shall | ect and up to date.
7. You shall i each or misuse of the resources/ser

Introduction
Definitions
Individual Users
Community Manager and Community
Aims and Purposes
Membership
Membership life cycle: A
Membership life cycle: M
Membership life cycle: S
Membership life cycle: T
Protection and processin
Audit and Traceability Re
Registry and Registration
References

Community Operations Security Policy

1 Introduction

This policy is effective from <insert date> and replaces two earlier security policy documents [R1]. This policy is one of a set of documents that together define the Security Policy [R2] and must be considered in conjunction with all the policy documents in the set.

This policy applies to the Community Manager and other designated Community management personnel. It places requirements on Communities and it governs their relationships with all Infrastructures with which they have a usage agreement. The Community management personnel must ensure awareness and acceptance, by the Community and its Users, of the responsibilities documented in this Policy.

Introduction

2 Definitions

A Community is a group of individuals (Users), organised with a common purpose, jointly granted access to one or more Infrastructures. It may serve as an entity which acts as the interface between the individual Users and an Infrastructure. In general, the members of the Community will not need to separately negotiate access with Service Providers or Infrastructures (hereafter jointly called Infrastructures).

Examples of Communities include, but are not limited to: User groups, Virtual Organisations, Research Communities, Research Infrastructures, Virtual Research Communities, Projects, Communities authorised to use particular portals or gateways, and geographically organised communities.

3 Community Operations Security Policy

By participating in the Infrastructure, a Community Manager agrees to the conditions laid

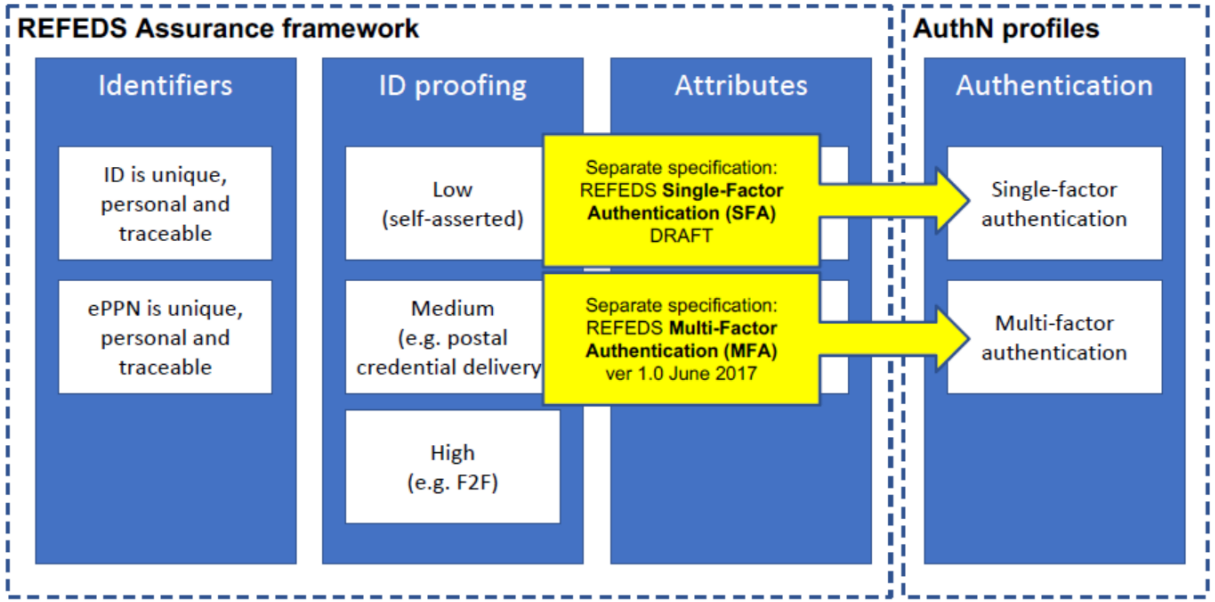
Differentiated Assurance Profile – in eduGAIN and REFEDS

Specific definitive guidance to IdPs and federations

- **Uniqueness** at least ePUID or ePTID/NameID
- **ID proofing**: ‘low’ (good for local use), ‘medium’ (Kantara LoA2, IGTF BIRCH, eIDAS low), or ‘high’ (Kantara LoA3, eIDAS substantial)
- **Authenticator**: devolved to REFEDS single and multi-factor authentication SFA and MFA
- **Freshness**: better than 1 month

Any and all assurance profiles
organisational-level authority, also used locally for ‘real work’, good security practices

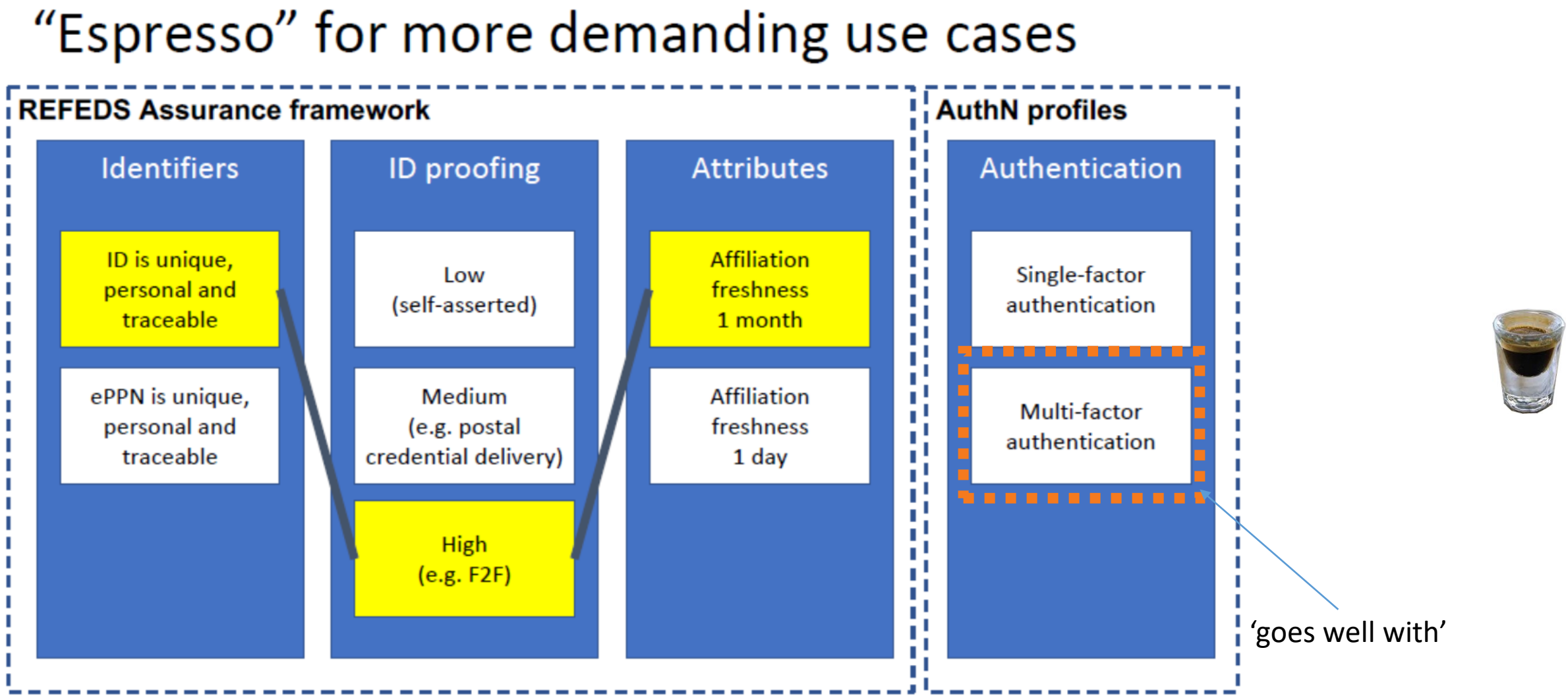
Logical grouping and profiles for the Infrastructures



consolidation depends also on REFEDS SFA (which is not quite AARC…)

https://refeds.org/assurance

Example: “Espresso” profile for demanding use cases



alignment with REFEDS SFA/MFA WG is part of the work programme of AARC2

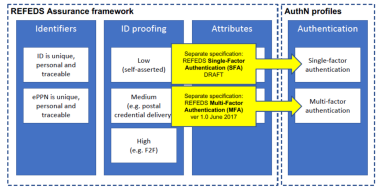
Using the REFEDS Assurance Framework in practice: the RAF Pilot ☺

Goal: gain practical experience with Assurance framework *and* REFEDS Single-factor authentication (SFA) profile, both on specification and in deploying existing SAML products

XSEDE
Extreme Science and Engineering Discovery Environment

CSC-TIETEEN TIETOTEKNIIKAN KESKUS

Aalto University



elixir

EGI

BBMRI-ERIC
Biobanking and BioMolecular resources Research Infrastructure

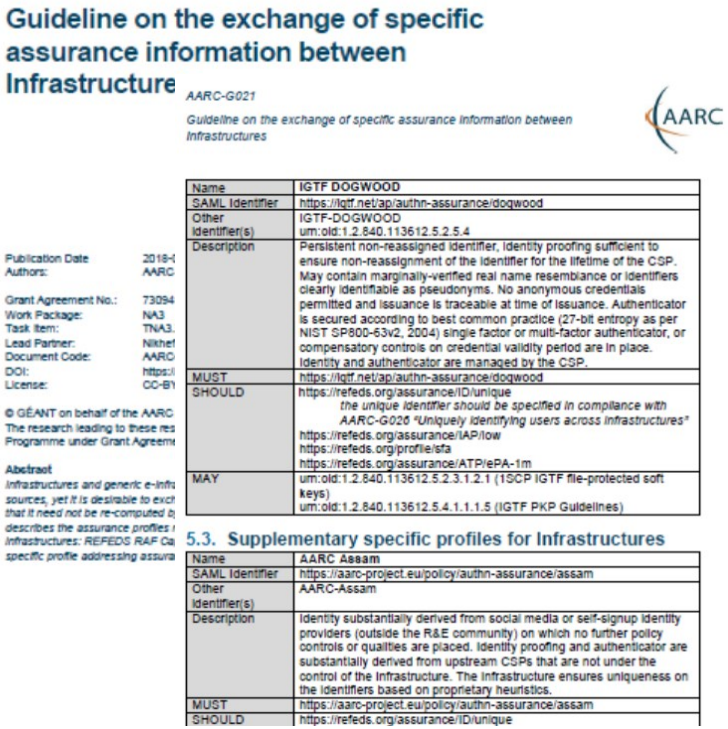
Today: both IdP software (now mostly Shibboleth) can express components and profiles, and use cases can leverage REFEDS assurance profiles (Cappuccino, Espresso) directly

https://wiki.refeds.org/display/GROUPS/Pilot+on+RAF+and+SFA
https://wiki.refeds.org/display/GROUPS/Pilot+resources

Re-usable Assurance between Infrastructures

- BPA (community) proxy constructs identity based on multiple sources: home organisation, attributes, linked identities, authenticators – and process these with (community-specific) heuristics
- resulting assurance level may be different from one in home organization – and may depend on intelligence (components) that are not 'passable' to the next (infrastructure) proxy
- luckily: number of proxies in an exchange limited, and there's explicit trust

AARC-G021



Guideline on the exchange of specific assurance information between Infrastructure

AARC-G021

Guideline on the exchange of specific assurance information between Infrastructures

Name	IGTF DOGWOOD
SAML Identifier	https://igtf.net/ap/authn-assurance/dogwood
Other Identifier(s)	IGTF-DOGWOOD urn:oid:1.2.840.113612.5.2.5.4
Description	Persistent non-reassigned identifier, identity proofing sufficient to ensure non-reassignment of the identifier for the lifetime of the CSP. May contain marginally-verified real name resemblance or identifiers clearly identifiable as pseudonyms. No anonymous credentials permitted and issuance is traceable at time of issuance. Authenticator is secured according to best common practice (27-bit entropy as per NIST SP800-63v2, 2004) single factor or multi-factor authenticator, or compensatory controls on credential validity period are in place. Identity and authenticator are managed by the CSP.
MUST	https://igtf.net/ap/authn-assurance/dogwood
SHOULD	https://refeds.org/assurance/ID/unique *the unique identifier should be specified in compliance with AARC-G026 "Uniquely identifying users across Infrastructures"* https://refeds.org/assurance/IAP/low https://refeds.org/profile/sfa https://refeds.org/assurance/ATP/ePA-1m
MAY	urn:oid:1.2.840.113612.5.2.3.1.2.1 (1SCP IGTF file-protected soft keys) urn:oid:1.2.840.113612.5.4.1.1.1.5 (IGTF PKP Guidelines)

5.3. Supplementary specific profiles for Infrastructures

Name	AARC Assam
SAML Identifier	https://aarc-project.eu/policy/authn-assurance/assam
Other Identifier(s)	AARC-Assam
Description	Identity substantially derived from social media or self-signup identity providers (outside the R&E community) on which no further policy controls or qualities are placed. Identity proofing and authenticator are substantially derived from upstream CSPs that are not under the control of the Infrastructure. The Infrastructure ensures uniqueness on the identifiers based on proprietary heuristics.
MUST	https://aarc-project.eu/policy/authn-assurance/assam
SHOULD	https://refeds.org/assurance/ID/unique

each BPA IdP-SP **proxy should convey its 'established assurance'**

use a **limited number of *profiles*** targeted
at Infrastructure and Services risk levels (not in IdP capabilities)

re-use existing profiles as much as reasonable

AARC-G021: https://doi.org/10.5281/zenodo.1173558

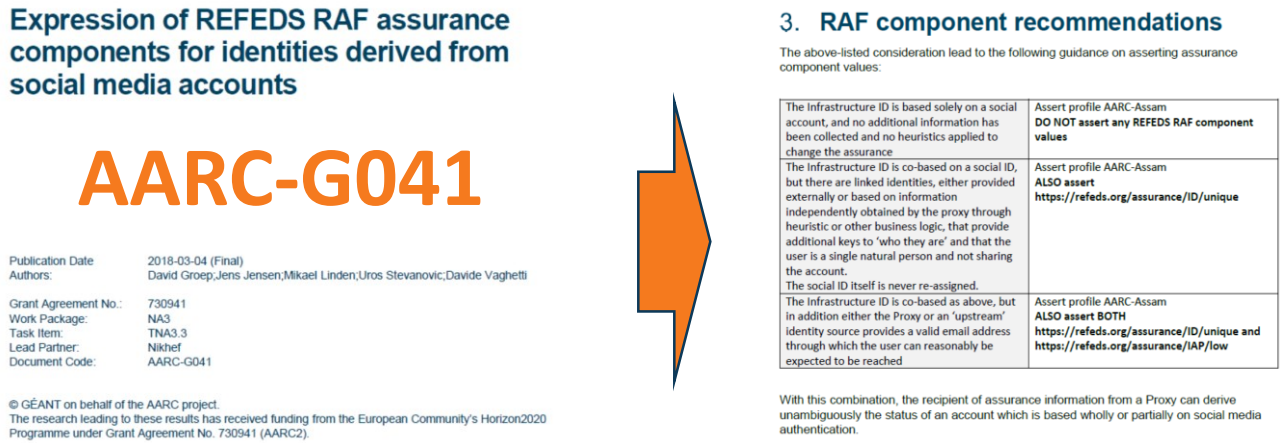
Specific assurance information BETWEEN Infrastructures

- from REFEDS Assurance Framework: Cappuccino, Espresso
- from IGTF Assurance Profiles: BIRCH, DOGWOOD (https://iana.org/assignments/loa-profiles)
- from the AARC JRA1 use case analysis: Assam – derived from a user-held social identity

social identity assurance level is 'unique' to the Infrastructure use case here, since

- home IdPs in eduGAIN are not 'social ID'
- but proxies can use + augment social IDs

so out of REFEDS scope, but needed for AARC Infras



Expression of REFEDS RAF assurance components for identities derived from social media accounts

AARC-G041

Publication Date: 2018-03-04 (Final)
Authors: David Groep;Jens Jensen;Mikael Linden;Uros Stevanovic;Davide Vaghetti

Grant Agreement No.: 730941
Work Package: NA3
Task Item: TNA3.3
Lead Partner: Nikhef
Document Code: AARC-G041

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract
Infrastructure Proxies may convey assurance information derived from multiple sources, one of which may be 'social identity' sources. This guidance explains under which conditions combination of assurance information and augmentation of identity data within the Infrastructure Proxy should result in assertion of the REFEDS Assurance Framework components "unique identifier", and when it may be appropriate to assert the "identity proofing" component value low.

3. RAF component recommendations

The above-listed consideration lead to the following guidance on asserting assurance component values:

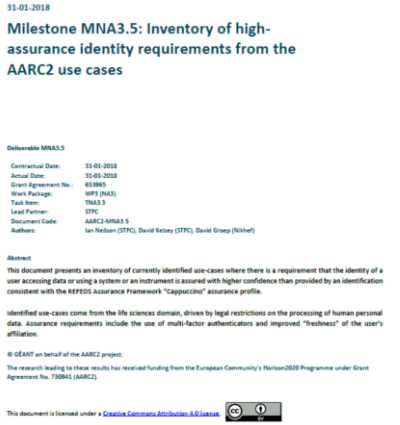
The Infrastructure ID is based solely on a social account, and no additional information has been collected and no heuristics applied to change the assurance	Assert profile AARC-Assam **DO NOT assert any REFEDS RAF component values**
The Infrastructure ID is co-based on a social ID, but there are linked identities, either provided externally or based on information independently obtained by the proxy through heuristic or other business logic, that provide additional keys to 'who they are' and that the user is a single natural person and not sharing the account. The social ID itself is never re-assigned.	Assert profile AARC-Assam **ALSO assert** **https://refeds.org/assurance/ID/unique**
The Infrastructure ID is co-based as above, but in addition either the Proxy or an 'upstream' identity source provides a valid email address through which the user can reasonably be expected to be reached	Assert profile AARC-Assam **ALSO assert BOTH** **https://refeds.org/assurance/ID/unique and** **https://refeds.org/assurance/IAP/low**

With this combination, the recipient of assurance information from a Proxy can derive unambiguously the status of an account which is based wholly or partially on social media authentication.

https://aarc-project.eu/guidelines/aarc-g041/

High-assurance requirements

- REFEDS RAF “Espresso” profile designed to support sensitive use cases
- BBMRI *definitely* known to need it (and in DoW)
  - biobanks by design contain sensitive data
  - need for stringent access control,
    based around reviews and ethics commissions
  - *same* researcher in *different* role
    may have different access rights even


31-01-2018

Milestone MNA3.5: Inventory of high-assurance identity requirements from the AARC2 use cases

Deliverable MNA3.5

Abstract

This document presents an inventory of currently identified use-cases where there is a requirement that the identity of a user accessing data or using a system or an instrument is assured with higher confidence than provided by an identification consistent with the REFEDS Assurance Framework “Cappuccino” assurance profile.

Identified use-cases come from the life sciences domain, driven by legal restrictions on the processing of human personal data. Assurance requirements include the use of multi-factor authenticators and improved “freshness” of the user’s affiliation.

© GÉANT on behalf of the AARC2 project.

The research leading to these results has received funding from the European Community’s Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

This document is licensed under a Creative Commons Attribution 4.0 license.

Use Cases

Community	**ELIXIR AAI**
Contact	Mikael Linden
Description	Some relying services of ELIXIR AAI require MFA when gra Principal issues relate to which attribute is associated with t reliability, usefulness and cost. A pilot has been run to test a token delivered to the user as an SMS.
References	Full discussion of senarios and problems are discussed in t with the pilot roadmap (google doc).

- NA3 survey for more use cases: adds ELIXIR
- survey remains open for new cases –
  community engagement around Policy Dev Kit
  may identify more communities to consider risks
- based on REFEDS RAF pilot and ‘Espresso’,
  NA3 will do full (compliance) review with BBMRI

Community	**BBMRI**
Contact	Petr Holub
Description	Issues identified with the REFEDS AF are related to • lack of prescribed attributes and • timely removal of attributes (1 day required rather than 1 month following termination of employment.)
References	See document (Overleaf doc).

https://wiki.geant.org/x/woXABQ

Combining Assurance source - and policy in EOSC-hub

… just wait for Dave's talk …

Assurance – standard profiles and ‘untangling spaghetti’

- REFEDS RAF profiles (feasible assurance from all over R&E federations – as far as we can!)
- inter-infrastructure profiles and relying-party oriented profiles (IGTF BIRCH, DOGWOOD)
- how to express social media assurance, for citizen science and in support of account linking

AARC-G041

Expression of REFEDS RAF assurance components for identities derived from social media accounts

3. RAF component recommendations

The above-listed consideration lead to the following guidance on asserting assurance component values:

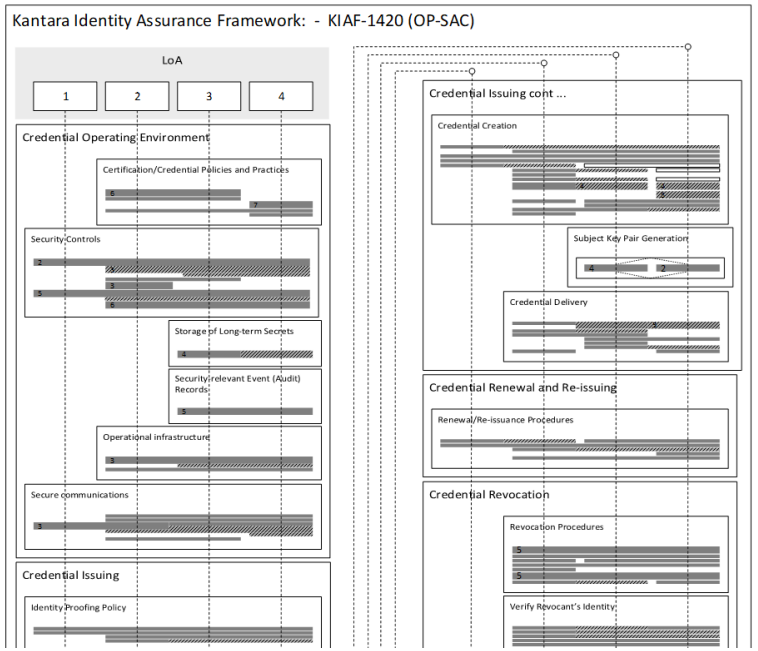
The Infrastructure ID is based solely on a social account, and no additional information has been collected and no heuristics applied to change the assurance	Assert profile AARC-Assam **DO NOT assert any REFEDS RAF component values**
The Infrastructure ID is co-based on a social ID, but there are linked identities, either provided externally or based on information independently obtained by the proxy through	Assert profile AARC-Assam **ALSO assert** **https://refeds.org/assurance/ID/unique**

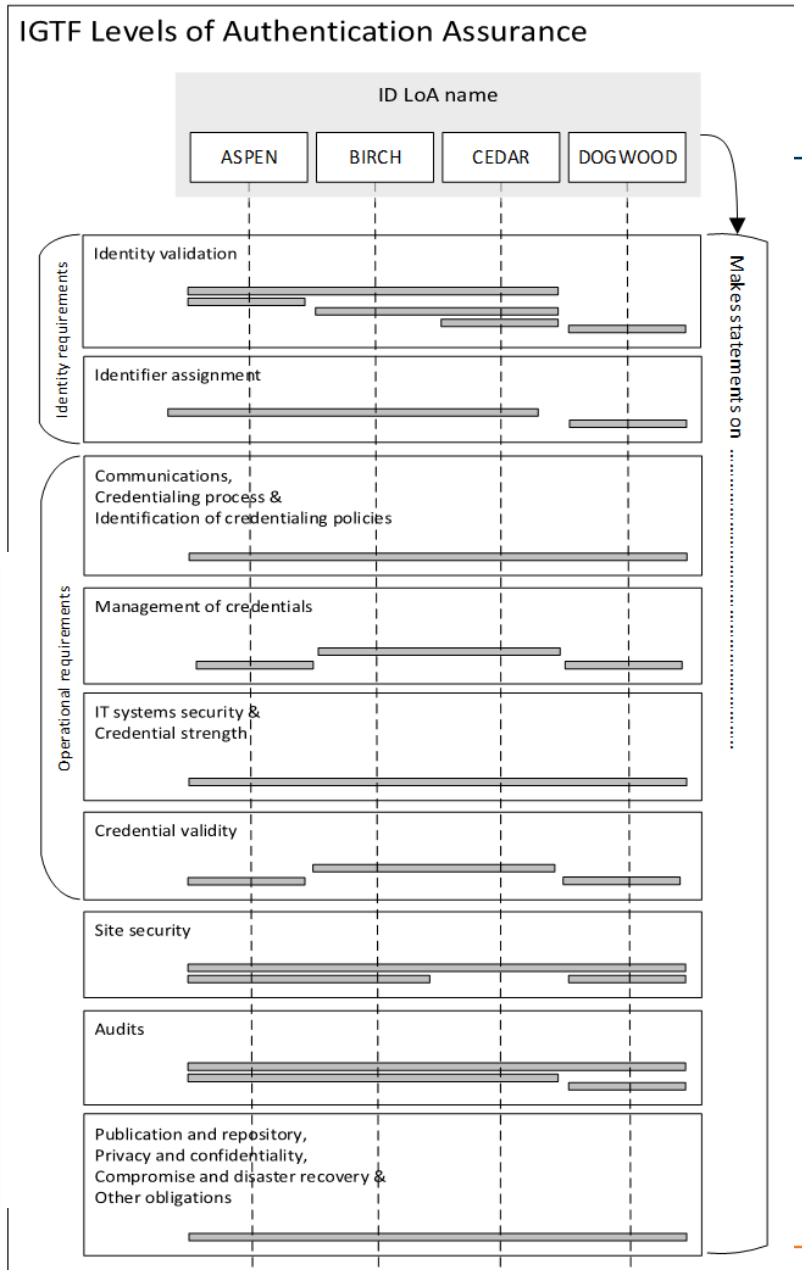
...org/assuranc		
...org/assuranc		
...tion.se/loa/2fa	skolfederation.se-2fa	[https://www.skolfederatio
...d.se/policy/assurance/al1	SWAMID-AL1	[https://www.sunet.se/swa
...d.se/policy/assurance/al2	SWAMID-AL2	[https://www.sunet.se/swa
...sirtfi	Sirtfi	[https://refeds.org/sirtfi]
...authn-assurance/aspen	IGTF-ASPEN	[https://www.igtf.net/ap/au
...authn-assurance/birch	IGTF-BIRCH	[https://www.igtf.net/ap/au
https://igtf.net/ap/authn-assurance/cedar	IGTF-CEDAR	[https://www.igtf.net/ap/au
https://igtf.net/ap/authn-assurance/dogwood	IGTF-DOGWOOD	[https://www.igtf.net/ap/au

https://www.iana.org/assignments/loa-profiles/

Interpreting the graphs

- on context and missing ‘breadcrumbs’
- components vs. profiles
- implicit trust vs. completeness





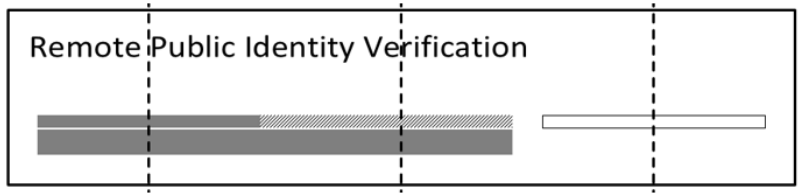


Figure 4.3: Variations of requirement representation

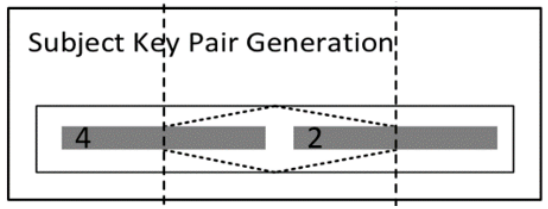
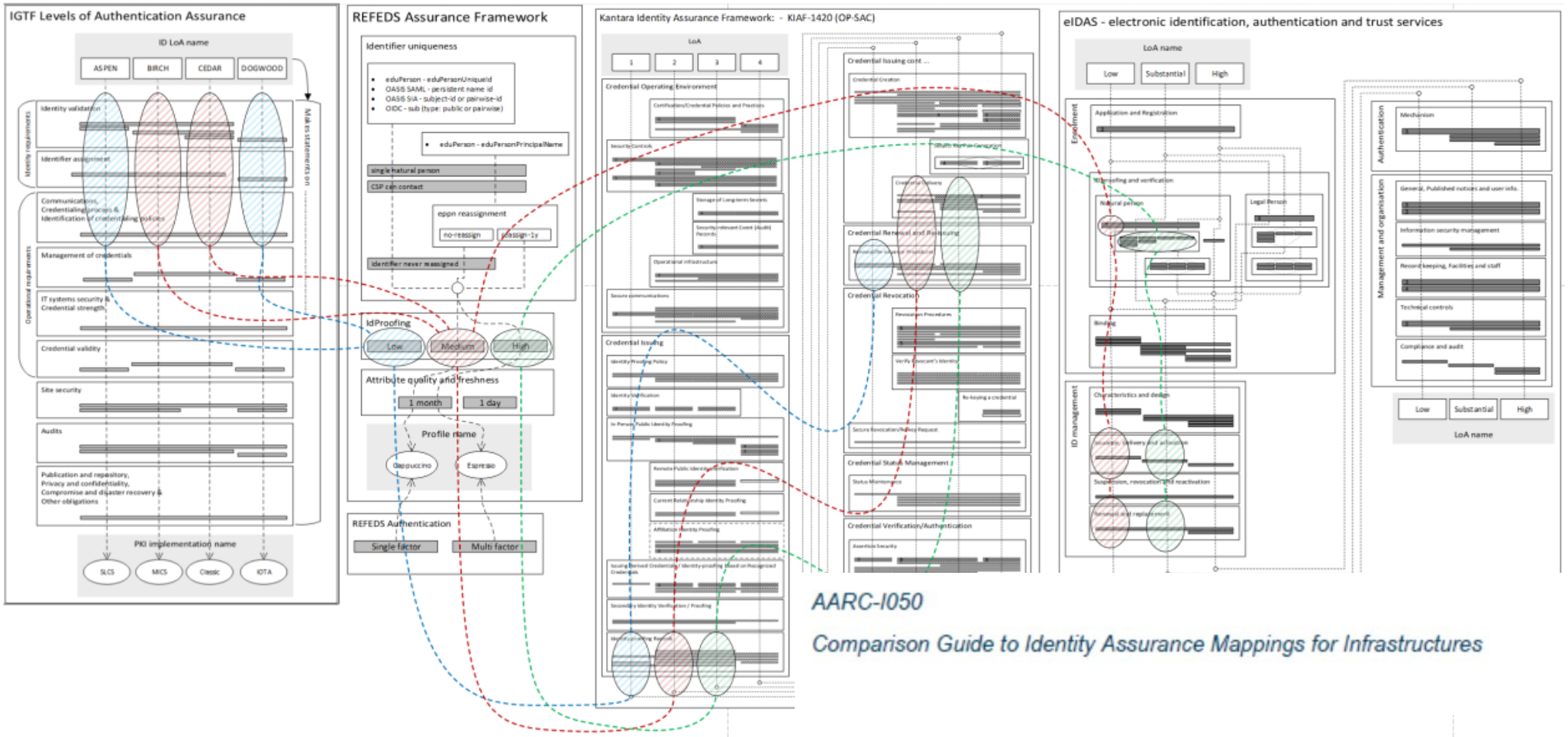


Figure 4.4: Alternate requirement choices

Untangling Assurance Spaghetti:
Comparison Guide to Identity Assurance Mappings for Infrastructures

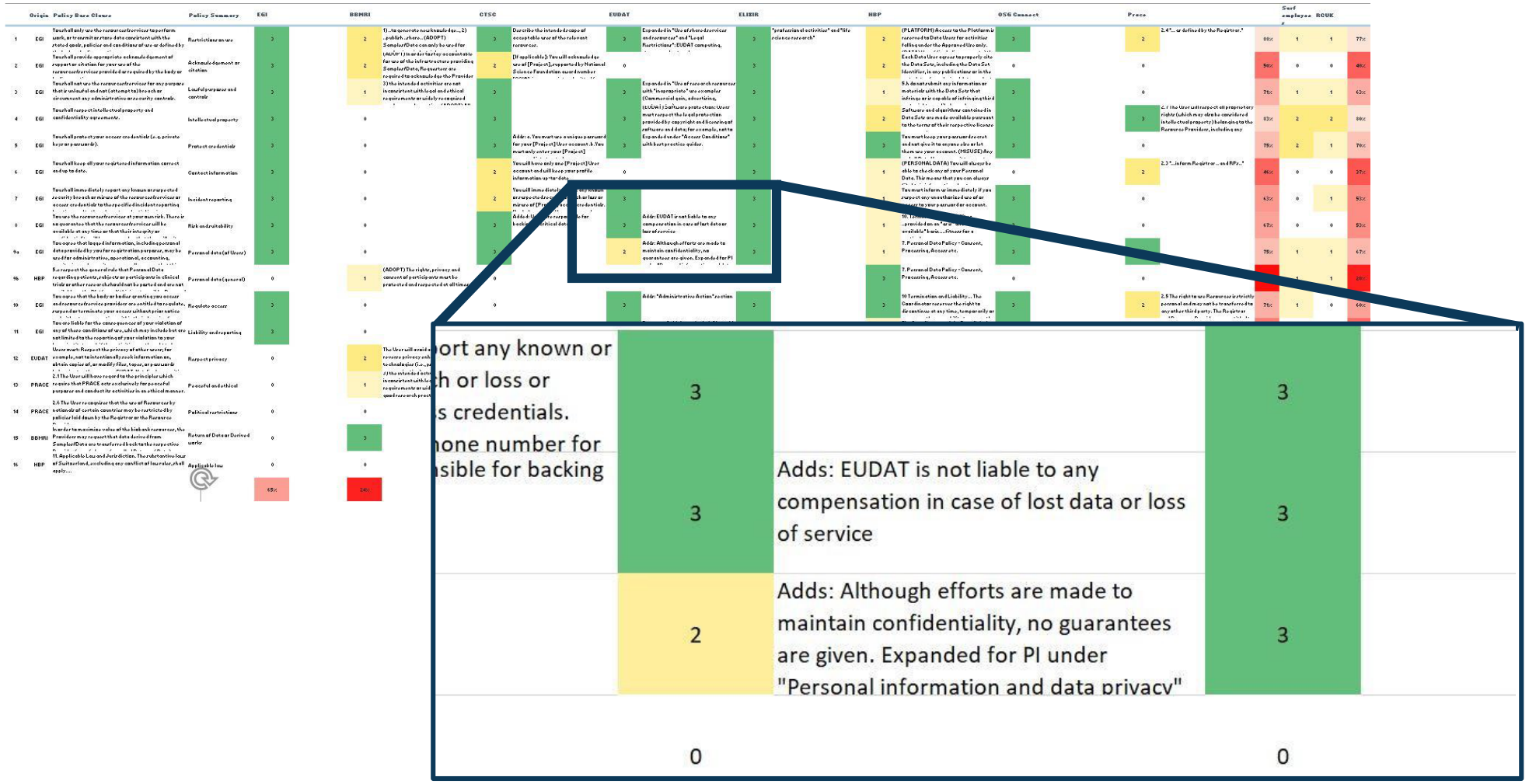


AARC-I050

Comparison Guide to Identity Assurance Mappings for Infrastructures

https://aarc-project.eu/guidelines/aarc-i050/

Divergence and convergence – the AUP Alignment Study



ort any known or h or loss or s credentials. hone number for sible for backing	3	3
	3	Adds: EUDAT is not liable to any compensation in case of lost data or loss of service	3
	2	Adds: Although efforts are made to maintain confidentiality, no guarantees are given. Expanded for PI under "Personal information and data privacy"	3
	0		0

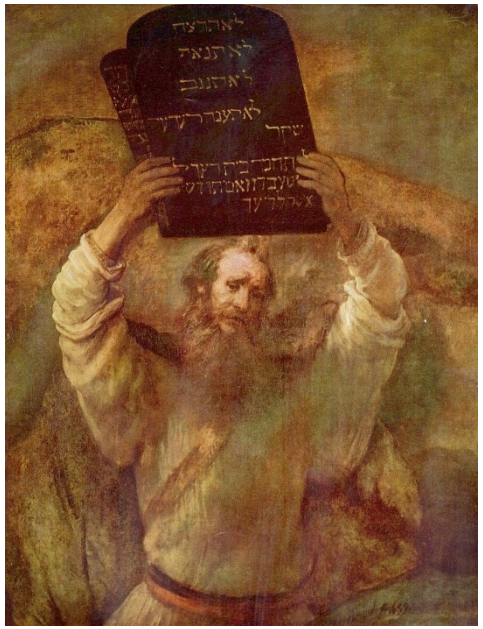


Image: Mozes en de tafelen der Wet, Rembrandt van Rijn, 1659

Scaling Acceptable Use Policy and data release

impractical to present user ‘click-through’ screens on each individual service

This allows a layered approach to the construction of the AUP, where the AUP presented to the end-user (on enrolment or later) comprises both the generic JSPG-evolved version plus the community-specific additions.

The LS AAI shall present an Acceptable Use Policy also on behalf of its connected services and infrastructures.

The LS AAI operators shall present as the AUP:

- the common aims and purposes, i.e. the research or scholarship goals of the Life Sciences Research Infrastructures (in a few high-level sentences) **This text must be supplied by the Life Sciences community.**
- the list of 11 (eleven) items from the Evolved JSPG AUP [JSPGAUP2]
- a notice that enrolment into specific groups or subdivisions may require the user to sign supplementary terms and conditions, and
- that in specific circumstance also specific services *may* ask the user to sign additional conditions of use.

If the Life Sciences community agrees to any joint clauses (‘do not attempt to reverse privacy-enhancing technologies’, for instance), these should be included in the LS AAI AUP.

Community conditions

Community specific terms & conditions

Community specific terms & conditions

RI Cluster-specific terms & conditions

Common baseline AUP
for e-Infrastructures and Research Communities
(current draft: JSPG Evolved AUP –
leveraging comparison study and joint e-Infrastructure work)

Also picked up by others, e.g. FH VORARLBERG

https://wiki.geant.org/x/P4bWBQ

WISE Baseline AUP – and how to apply it for your Infrastructure

AARC-I044

- Includes the final WISE Baseline AUP text
- for both ‘community-first’ and ‘user-first’ MMS services (attribute authorities)
- examples make it concrete

Quick take-up by e-Infras (both global and national)

3. The WISE Baseline AUP

The WISE Baseline AUP[1] in its preamble and final clauses, it given below. The blue text elements should be substituted in-line, whereas the green elements are optional and need to be provided only when needed, e.g. based on the guidance in this document.

Acceptable Use Policy and Conditions of Use

This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services ("Services") as granted by {community, agency, or infrastructure name} for the purpose of {describe the stated goals and policies governing the intended use}.

<To further define and limit what constitutes acceptable use, the community, agency, or infrastructure may optionally add additional information, rules or conditions, or references thereto, here or at the placeholder below. These additions must not conflict with the clauses 1-10 below, whose wording and numbering must not be changed.>

1. You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show consideration towards other users including by not causing harm to the Services; you have an obligation to collaborate in the resolution of issues arising

5.2. Example

The following example shows a co
the appropriate Acceptable Use P

This Acceptable Use Policy and
govern your access to and use (
data) of the resources and servi
the purpose of **studying short-range nucleon-nucleon correlations by means of electron-induced two-proton knockout from Helium-3.**

... follows Baseline AUP standard ten clauses ...

The administrative contact for this AUP is:
he3epp@nikhef.nl
The security contact for this AUP is:
security@nikhef.nl
The privacy statements (e.g. Privacy Notices) are located at:
https://www.nikhef.nl/privacy

Our collective wisdom from AARC2

AARC-I044 **Implementers Guide to the WISE Baseline Acceptable Use Policy**

Applying the Baseline AUP to concrete use cases may appear straightforward, but there are many edge cases and specific circumstances where both achieve the aim of user-friendliness as well as be complete and practical. In this whitepaper, we try to give hints how to use the WISE Baseline community first as well as user first" membership management services

... more information ...

AARC-G048 **Guidelines for Secure Operation of Attribute Authorities and other issuers of a**

These guidelines describe the minimum requirements and recommendations for the secure operation of Attribute Authorities and similar servi purpose of obtaining access to infrastructure services. Stated compliance with these guidelines may help to establish trust between issuers and

... more information ...

AARC-G042 **Data Protection Impact Assessment – an initial guide for communities**

This report presents the results of the desk study on the evaluation of risks to (personal) data protection as considered in the European Regulation (GDPR), for Infrastructures and their service providers that leverage federated identity management (IdM) to connect research

... more information ...

AARC-G041 **Expression of REFEDS RAF assurance components for identities derived from accounts**

Infrastructure Proxies may convey assurance information derived from multiple sources, one of which may be 'social identity' sources. This guid combined combination of assurance information and augmentation of identity data within the Infrastructure Proxy should result in assertion components 'unique identifier', and when it may be appropriate to assert the 'identity proofing' component value low.

... more information ...

AARC-G021 **Exchange of specific assurance information between Infrastructures**

Infrastructures and generic e-Infrastructures compose an 'effective' assurance profile derived from several sources, yet it is desirable to exchange the resulting assurance assertion assumed between Infrastructures so that it need not be re-calculated by a recipient Infrastructure or Infrastructure service provider. This document describes the assurance profiles recommended to be used by the Infrastructure AAI Proxies between Infrastructures.

... more information ...

Description of deliverables

DNA3.1 - Report on the coordination of accounting data sharing amongst Infrastructures (initial phase) - (M12)
DNA3.2 – Report on Security Incident Response and Cybersecurity in Federated Authentication Scenarios (M22)
DNA3.3 –Accounting and Traceability in Multi-Domain Service Provider Environments (M23)
DNA3.4 – Recommendations for e-Researcher-Centric Policies and Assurance (M24)

D3.1 : DNA3.2 - Report on Security Incident Response [22]

Report on Security Incident Response and Cybersecurity in Federated Authentication Scenarios

D3.2 : DNA3.3- Accounting and Traceability in Multi-Domain Service Provider Environments [23]

Accounting and Traceability in Multi-Domain Service Provider Environments

D3.3 : DNA3.4 - Recommendations for e-Researcher-Centric Policies and Assurance [24]

Recommendations for e-Researcher-Centric Policies and Assurance

D3.4 : DNA3.1 - Report on the coordination of accounting data sharing amongst Infrastructures (initial phase) [12]

This document assess privacy
ensure smooth and secure serv

Home › Policies › Policy Development Kit

Policy Development Kit

Accessing, using, and operating services for research in today's world, as a role, is inherently distributed, where users access resources outside their Home Organisations. In this complex environment, the question of trust for users, resource providers, and infrastructures, becomes paramount.

A set of policy documents is necessary to regulate and facilitate this trust. These policies outline the operational measures undertaken by the infrastructure to properly provide services. The policies principally cover security measures, user management and data protection.

What is the Policy Development Kit?

This material is provided to support Research Infrastructures in adopting or enhancing a policy set that regulates the operation and use of an Authentication and Authorisation Infrastructure in line with the AARC Blueprint Architecture. The policies are there to provide a starting point, so that Research Infrastructures do not have to re-invent the wheel!

Get Started with Policies

AARC-I050 **Comparison Guide to Identity Assurance Mappings for Infrastructures**

With a wide range of identity assurance frameworks to choose from, the most appropriate choice of assurance profile for a use case (or the social and community context in which the assurance is needed) may be viewed as confusing. The choice of Cappuccino or Espresso Assam from the AARC social media assurance, Birch and Dogwood from the Interoperable Global Trust Federation, Silver and Bronze fr... from both Kantara and NIST SP800-63 – all of these merit a policy mapping and comparison framework. In this whitepaper, we identify the implicit trust assumptions (in research and collaboration frameworks, the R&E identity federations, general private sector frameworks and e-government schemes) and present a way of comparing these frameworks.

... more information ...

plus all our AARC1 wisdom!

and the AARC-G051 incident response process

Thank you

Any Questions?

davidg@nikhef.nl

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agre