Authentication and Authorisation for Research and Collaboration

WP3: Policy and Best Practice Harmonisation

David Groep

Nikhef

AARC2 Y1 EC Review
26-27 June, 2016
Lëtzebuerg

https://g.nikhef.nl/aarc2na3py1

Agenda “NA3” Policy and Best Practice Harmonisation

Team and partners

Objectives

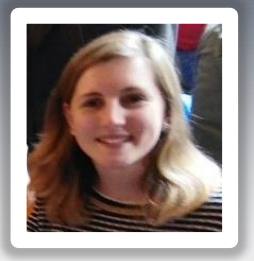
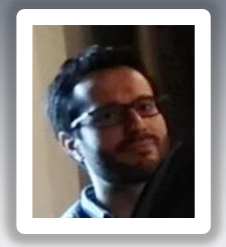
Resource Use and Deliverables

Achievements

security, service- and researcher-centric policy,
and community engagement

Challenges, **Status,** and **Outlook**

Activity Structure

	T1	T2	T3	T4
Activity Lead	Incident Response Trust	Service-centric Policy Support	Researcher-centric Support	Enagement & Development
				
David Groep Nikhef (NWO-I)	**Hannah Short** CERN	**Uros Stevanovic** KIT	**Ian Neilson** STFC RAL	**David Kelsey** STFC-RAL

Partners

Nikhef

CSC – TIETEEN TIETOTEKNIIKAN KESKUS

Science & Technology Facilities Council

CERN

BBMRI-ERIC®

JÜLICH FORSCHUNGSZENTRUM

KIT Karlsruhe Institute of Technology

in collaboration with: DFN Deutsches Forschungsnetz, Jisc

Policy and best practice activity high-level objectives from our DoW

“Minimise the number of divergent AAI policies and **empower** identity providers, service providers and research communities to **identify interoperable policies”**

Define a **reference framework** to enable different parties to compare policies and assess policy compatibility

Create (**baseline**) **policy requirements**, driven by the explicit needs of the research communities

Identify all necessary policy elements and **develop guidelines and assessment models to support communities** in establishing, adopting, or evolving their own policies

Resources (1 May 2017 – 30 April 2018) and deliveries

Effort Used	PY1:	*23 PM foreseen in PY1*	***26 PM used in PY1***
	Total:	*47 PM for the entire duration*	*26 PM used in total*
		approx. 2 FTE average	***113% of forecast resources***

1 of 1 deliverable in PY1

DNA3.1 – Report on the coordination of accounting data sharing amongst Infrastructures (initial phase)

3 milestones in PY1

3 plans and periodic activity reports (MS12, MS13, MS14)

MNA3.3 Define and test a model for organisations to share account compromise information

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

With many other documents and results

… Community (security) policies in the Policy Development Kit, community guidance on using Codes of Conduct in the Blueprint Proxies, REFEDS Assurance Pilot, FIM4R community engagement, eduGAIN Sirtfi communications challenge, X-infrastructure assurance expression, social-ID assurance guide, …

Deliverable submission status

DNA3.1 Report on the coordination of accounting data sharing amongst Infrastructures (initial)

In this (initial) phase focussing on giving guidance to the community on GDPR DPIA

communities and pilots not yet ready at this stage to consider composite accounting use cases
2nd phase evolution (DNA3.4) will depend on advancement of actual need

MNA3.3 Define and test model for organisations to share account compromise information

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

An evolving role for policy and best practices

Strengthened use case & community focus in AARC2

- **Policy Development Kit** as requested by the pilots
- **Consultancy role** for Communities & Infrastructures
- generalize guidance with **SCI and *Snctfi* structure**

- work items address policy aspects of the architecture & its envisioned implementation

  AARC-G041

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

- or address pilots in SA1, communities, or Infrastructures

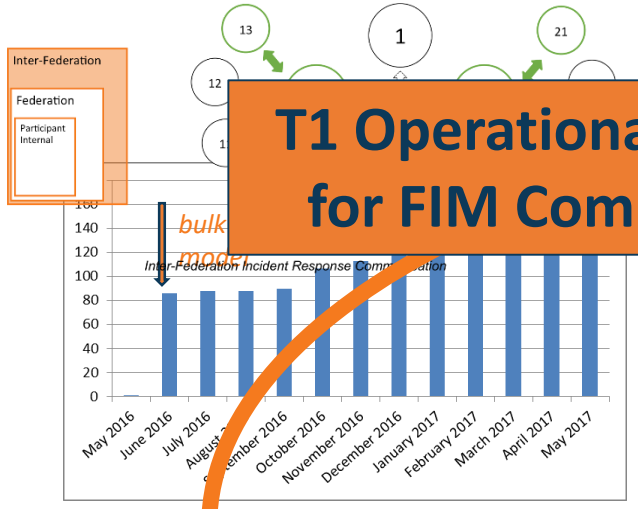
  AARC-G040

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

+ ever closer **collaboration with Infrastructures** applying harmonization to their operations

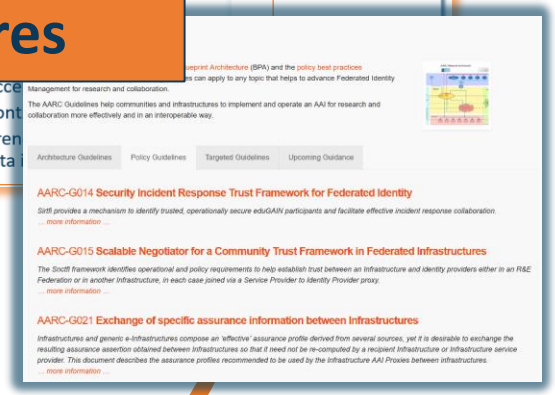
By construction NA3 work 'homed' in sustained fora: WISE, IGTF, REFEDS, FIM4R

A tour of the policy space in AARC2



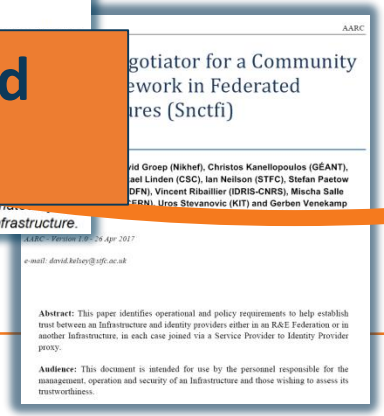
T1 Operational Security for FIM Communities

T2 supporting policies for Infrastructures



Sctfi

T4 Engagement and Coordination



T3 support for Researchers & Community

Policy and Best Practices Harmonisation

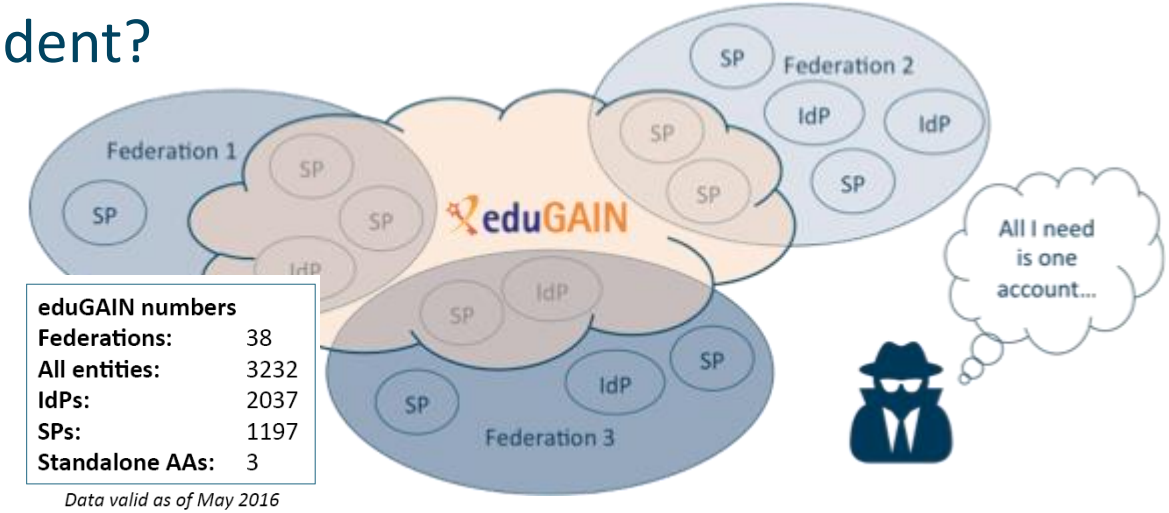
Task 1

Operational Security and Incident Response

Security Incident Response in the Federated World

AARC-1 Refresher

- How could we determine the scale of the incident?
  - Do useful logs exist?
  - Could logs be shared?
- Who should take responsibility for resolving the incident?
- How could we alert the identity providers and service providers involved?



eduGAIN numbers	
Federations:	38
All entities:	3232
IdPs:	2037
SPs:	1197
Standalone AAs:	3

Data valid as of May 2016

- Could we ensure that information is shared confidentially, and reputations protected?

Security Incident Response Trust Framework for Federated Identity

Sirtfi – *based on Security for Collaborating Infrastructures (SCI) & FIM4R Recommendations*

A Security Incident Response Trust Framework – Sirtfi summary

AARC-1 Refresher

Operational Security

- Require that a security incident response capability exists with sufficient authority to mitigate, contain the spread of, and remediate the effects of an incident.

Incident Response

- Assure confidentiality of information exchanged
- Identify trusted contacts
- Guarantee a response during collaboration

Traceability

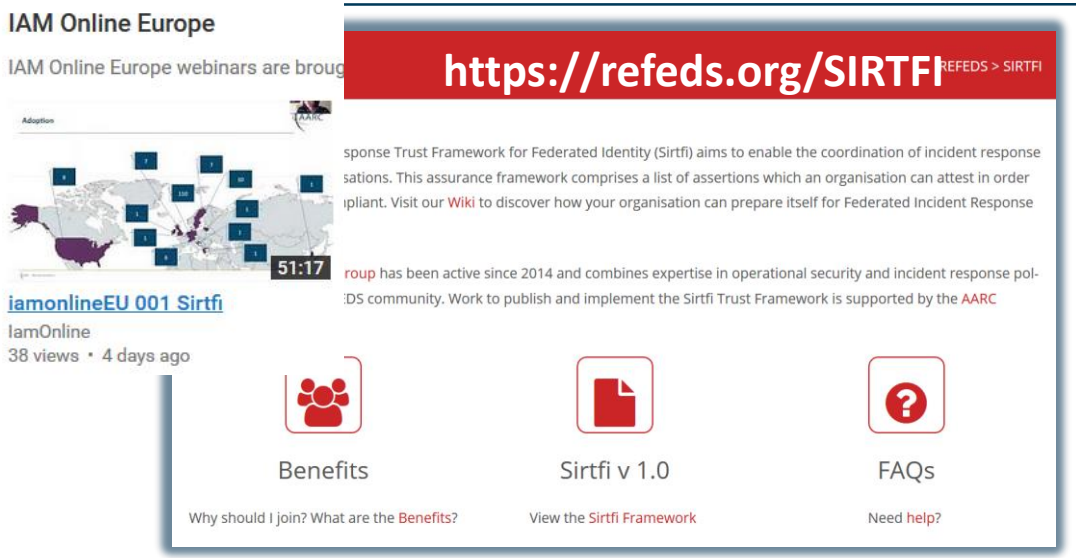
- Improve the usefulness of logs
- Ensure logs are kept in accordance with policy

Participant Responsibilities

- Confirm that end users are aware of an appropriate AUP

SIRTFI
Security Incident Response Trust Framework for Federated Identity

Sirtfi – presentation, training, adoption in AARC2



Services increasingly **demand and use Sirtfi**

- *CERN & LCG, CILogon (US), RCauth.eu, IGTF-to-eduGAIN bridge*

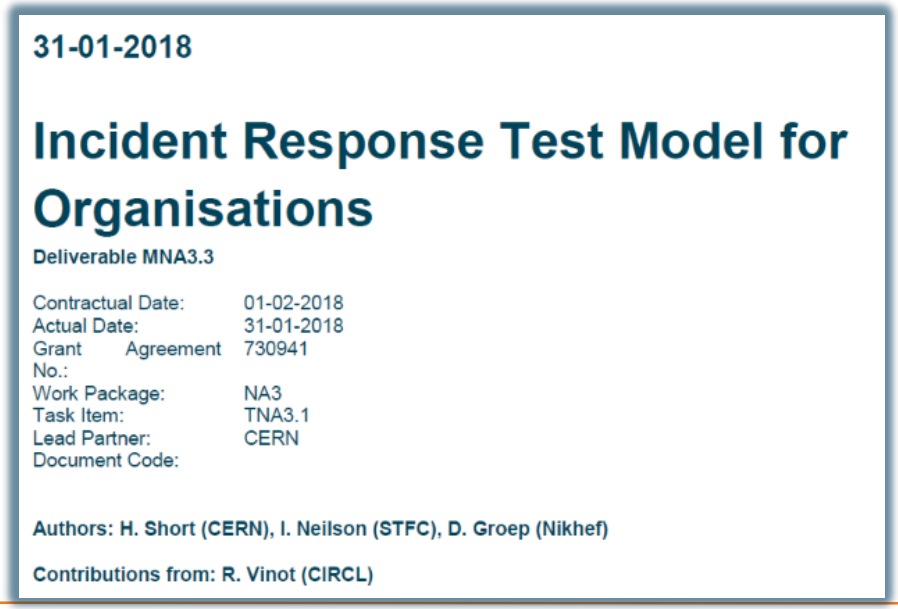
and

Sirtfi is included verbatim in the (GN4) DPCoCo version 2 to be submitted to EDPB

Promotional activities successful

- REFEDS, Internet2 TechX, ISGC Taipei, TNC, TF-CSIRT, FIM4R, Kantara webinars, …
- **Now 325 entities** (from 167 at start of AARC2)

- Ready to move to the next phase:


31-01-2018

Incident Response Test Model for Organisations

Deliverable MNA3.3

Contractual Date:	01-02-2018
Actual Date:	31-01-2018
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	TNA3.1
Lead Partner:	CERN
Document Code:	

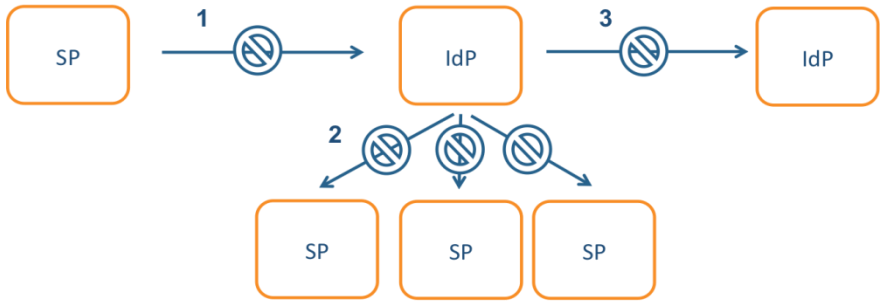
Authors: H. Short (CERN), I. Neilson (STFC), D. Groep (Nikhef)

Contributions from: R. Vinot (CIRCL)

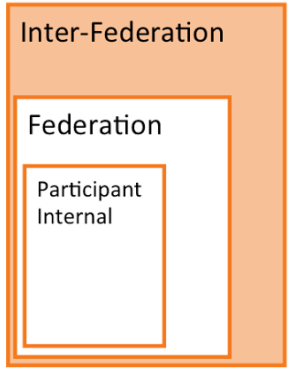
MNA3.3

statistics: technical.edugain.org, visited 2018-05-27

Incident response process evolution in federations –Sirtfi

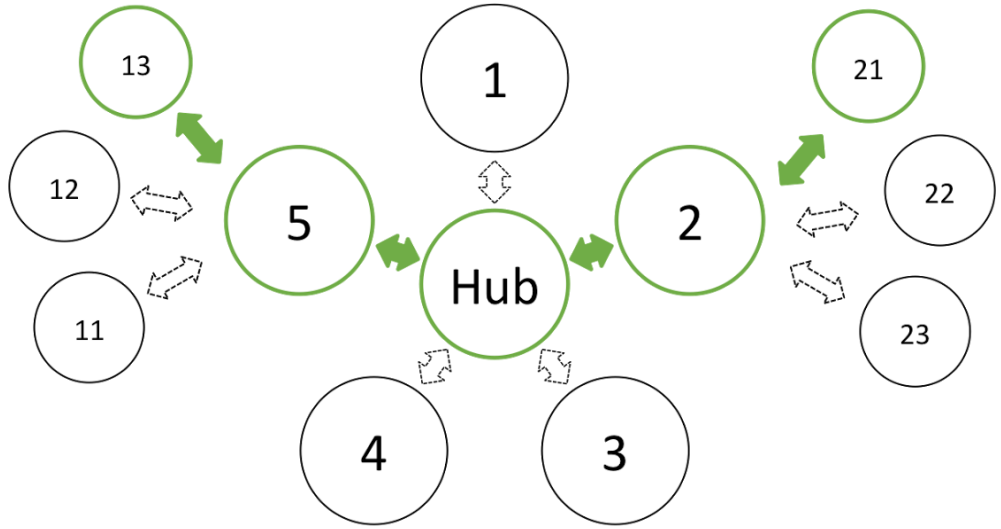


Incident Response Communication, communication blocks



Challenges

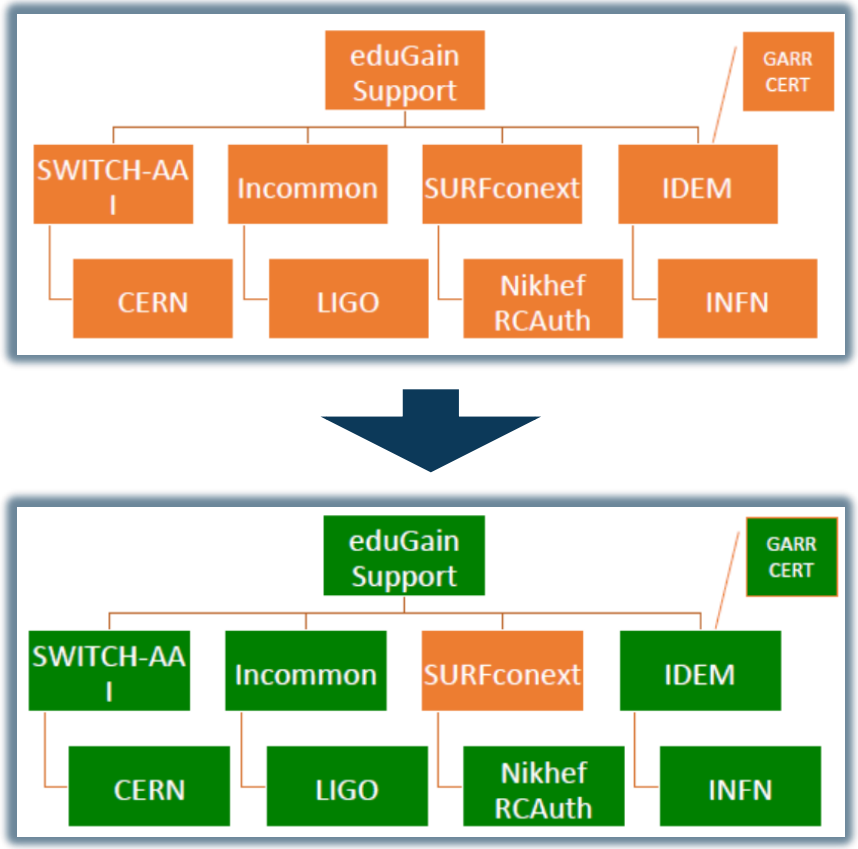
- IdP appears outside the service's security mandate
- Lack of contact or lack of trust in the IdP which to the SP is an unknown party
- IdP **fails to inform other affected** SPs, for fear of leaking data, of reputation, or just lack of interest and knowledge
- No established channels of communication, esp. not to federations themselves!



Inter-Federation Incident Response Communication

Test model for incident response (MNA3.3)

- Defines the model actors
- include eduGAIN Support Desk (as per AARC-1 model)
- Exercise the model attack scenario!



parties involved in response challenge

Report-out see **https://wiki.geant.org/display/AARC/Incident+Response+Test+Model+for+Organizations**

Post Simulation Interviews

Question	Response summary (9 responses received)
What went well?	The initial investigation was quick and responsive and Sirtfi contacts largely worked. eduGAIN support was helpful and included federation operators.
What didn't go well?	Lack of coordination. Delay in official alert. It was unclear who should be contacted. eduGAIN was brought in too late. The incident trigger was too vague. Investigation incomplete.

Planned progress

- More exercises, coordinated via WISE
- Improve available tooling
- Set defined roles, including a *coordinator*, and promote eduGAIN security capability GN4-*

Main achievements in Operational Security

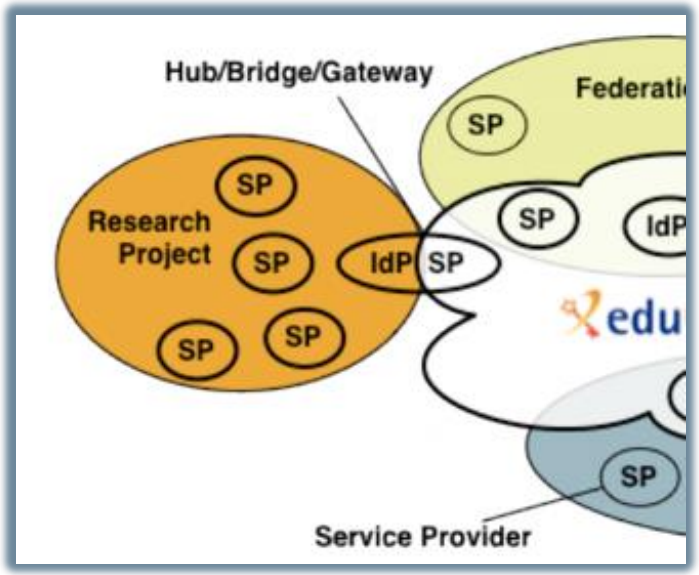
Sirtfi training and guidance	→	Increased availability of security contact information in eduGAIN globally (167 → 325)
Incident response model test	→	Responsiveness during actual FIM incidents
	→	WISE group (developing) on coordinating security communications challenges
	→	Demonstrated need for federation-level engagement beyond just IdPs and home orgs with an eduGAIN Support Security Team
PY2	Attribute authority operations practice also for Infra proxies - in collaboration with IGTF	
	Trust groups and the exchange of (account) compromise information	

Task 2
Service Centric Policies

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.

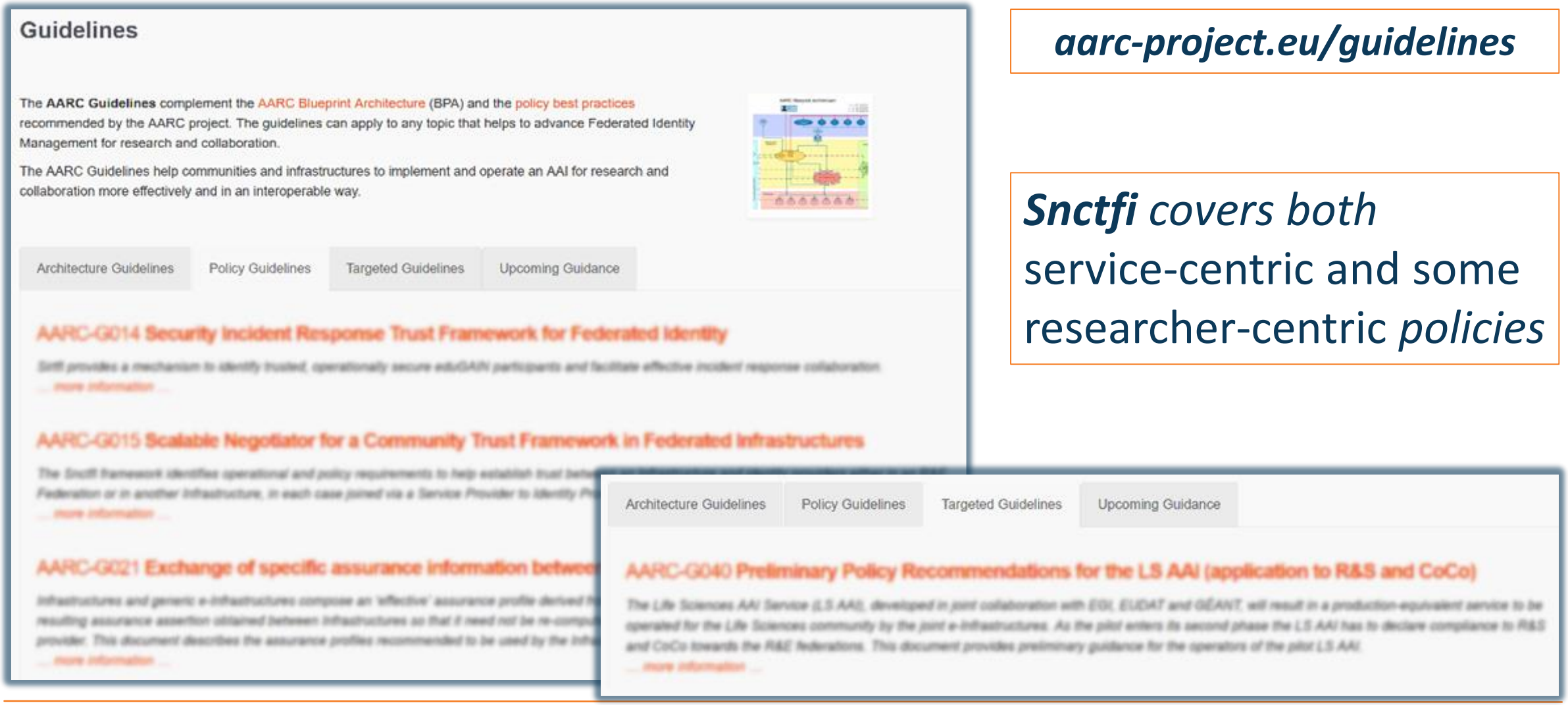
Audience: This document is intended for use by the personnel responsible for the management, operation and security of an Infrastructure and those wishing to assess its trustworthiness.

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

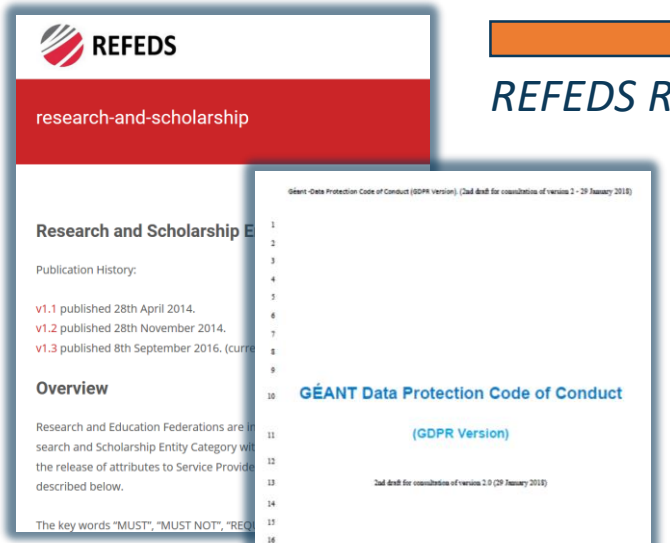
Filling the framework: generic and community-targeted guidance



aarc-project.eu/guidelines

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

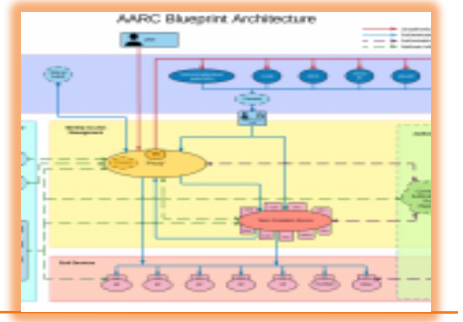
Implementing *Snctfi*: interpreting generic policies for BPA Proxy use cases

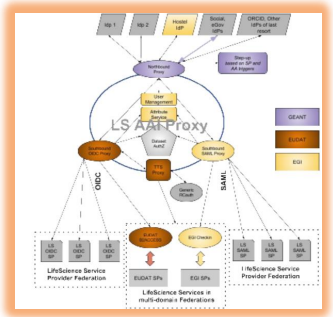


REFEDS R&S: allow attribute flow from the IdPs, express intent and scope

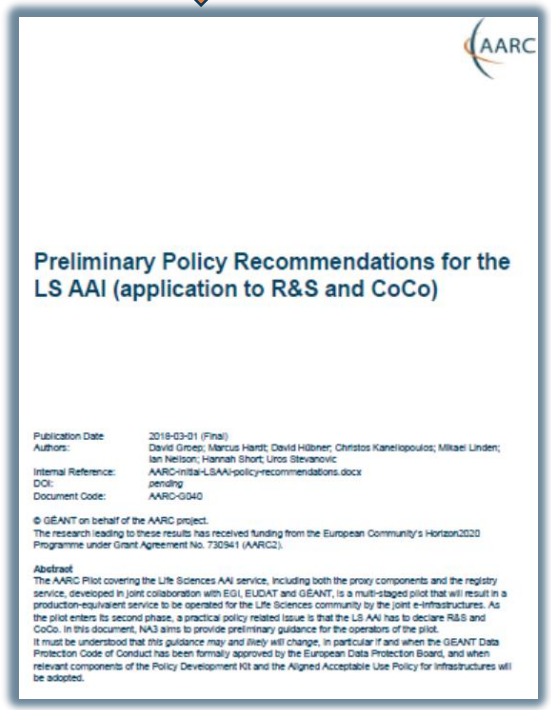
GEANT DPCoCo & GDPR - 'I'll be good with personal data'

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?



AARC-G040

AARC BPA: this is how information flows

AARC-G040: from generic Snctfi and DPCoCo to actionable statements

consent as per DPCoCo version 2. This is addressed by Snctfi RC1, which must be implemented by the LS AAI registry service. This information is also needed to effectuate collective incident response (RC4, RC5).

The LS AAI operators shall record for all end-users enough information to contact the user directly in case of security incidents, and to inform these users in case the acceptable use policy or data transfers to third parties change in a way that must be communicated to the users.

The LS AAI must not store personal data for any longer than necessary for the proper functioning of the LS AAI (which includes good incident response and similar duties, of course). It must define a data retention period for all personal data stored in the registry service, and have effective mechanisms to remote stale and obsolete data. The Code of Conduct version 2 draft suggests 18 months in absence of any more specific requirements

https://aarc-project.eu/guidelines/aarc-g040

Accounting and infrastructure-use data protection: a bit of clarification …

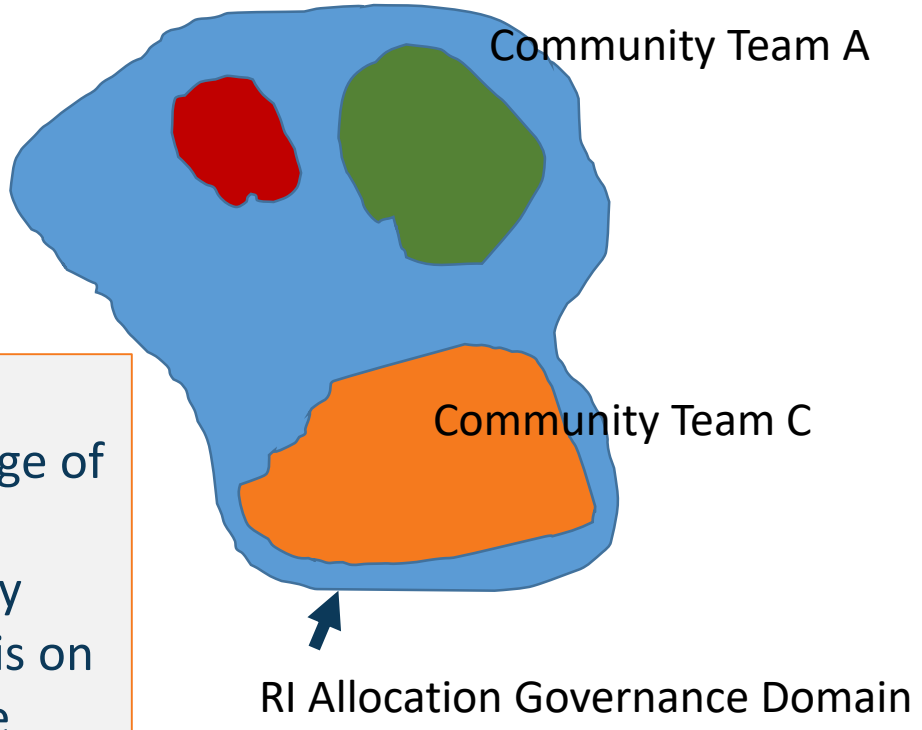
Work on accounting foresaw new communities joining AARC2
processing more sensitive (and: more competitive) work flows,
creating need for sub-structure and protection of accounting data within the community itself

Phased approach

1.
Support communities to deal with general data protection issues
Impact of GDPR for communities

2.
Issue guidance on generic issues, such as assessing impact of infrastructure use

PY2
Depending on stage of community development, may continue emphasis on targeted guidance



GDPR for Infrastructure AAI – both FUD and legitimate concerns

Large discrepancy between practice, perception, and actual risk:

- communities don't see (or forget) need to protect infrastructure AAI (accounting) data – and don't even consider our AARC-1 guidance ☹
- others misunderstand the issue, over-state the risks, and fall victim to FUD law firms
- even 'simplified' documents - like the GEANT Data Protection Code of Conduct – considered too complex to be understood and implemented well

DNA3.1 **"assess privacy regulations on [accounting] data needed by service operators and e/r-infrastructures to ensure smooth and secure service operations"**

specifically purposed to answer the basic questions:

- how much impact does FIM have on your **research infrastructure and accounting data**?
- what guidance is there already from member state regulators to **help you determine risk**?

A solution for our research communities?

View this email in your browser

Ruffles ShreddingMachines.co.uk

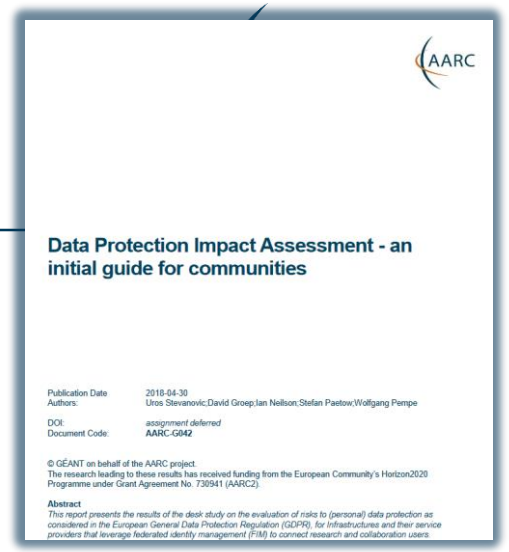
Fancy an £80 voucher when protecting your information?

With just 8 DAYS TO GO, see why there has never been a better time to buy a shredder to help meet your GDPR obligations. Stocks are limited, and we have
ensuring your sensitive documents are secure.

High Capacity Micro-cut
GDPR Shredder with

UCE message sent on May 17th to Ian Neilson, and millions more …

Guidance for research and generic Infrastructures – what is the risk?



AARC-G042

Initial phase: 'impact of GDPR' on community AAI risk assessments

Interpretation of WP29 guidance is complex for average user. Example:

- research is global, so: *"cross-border transfer"*
- infrastructures have many users: *"processed on a large scale?"*

→EDPB says *"in most cases, when meeting two or more criteria the data controller should conduct a DPIA"*

but how is a research community or Infrastructure to judge if this indeed applies to them?

DNA3.1 – released as AARC Guideline G042 to give concrete help for communities

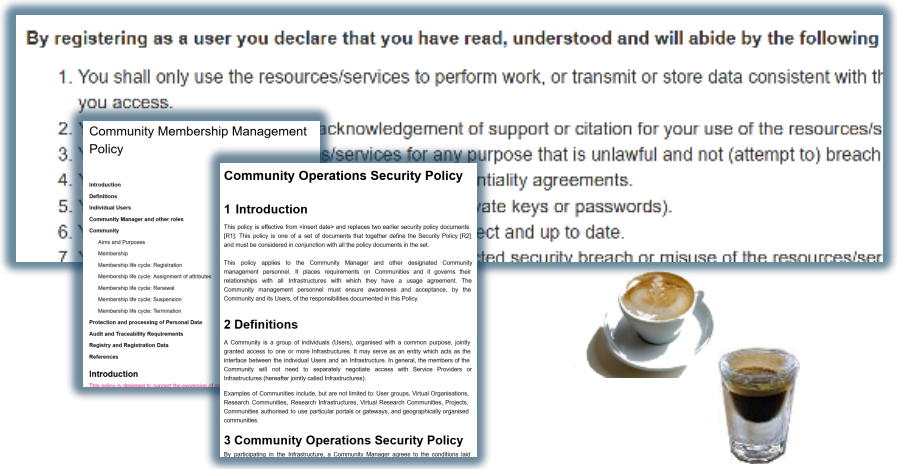
- desk study of regulator and expert opinions scoped to research and collaboration
- guidance still evolving, national regulatory bodies not yet synced, but best available now!

Main achievements in Service-Centric Policy

Guidelines model for policy and architecture	→	Clear adoption process for 'consumers' of AARC results, including targeted advice
Community Specific Guideline: LSAAI proxy operations (for R&S + DPCoCo)	→	Support the move of LSAAI to full production
Guideline: Data Protection Impact Assessment	→	Reduced complexity for communities and infrastructures handing (accounting) data

PY2	traceability and accounting data-collection policy framework based on SCI, providing a self-assessment methodology and comparison matrix for infrastructure services
	Evolution of data protection guidance for services – driven by the community needs

Policy and Best Practices Harmonisation



Task 3

e-Researcher Centric Policies

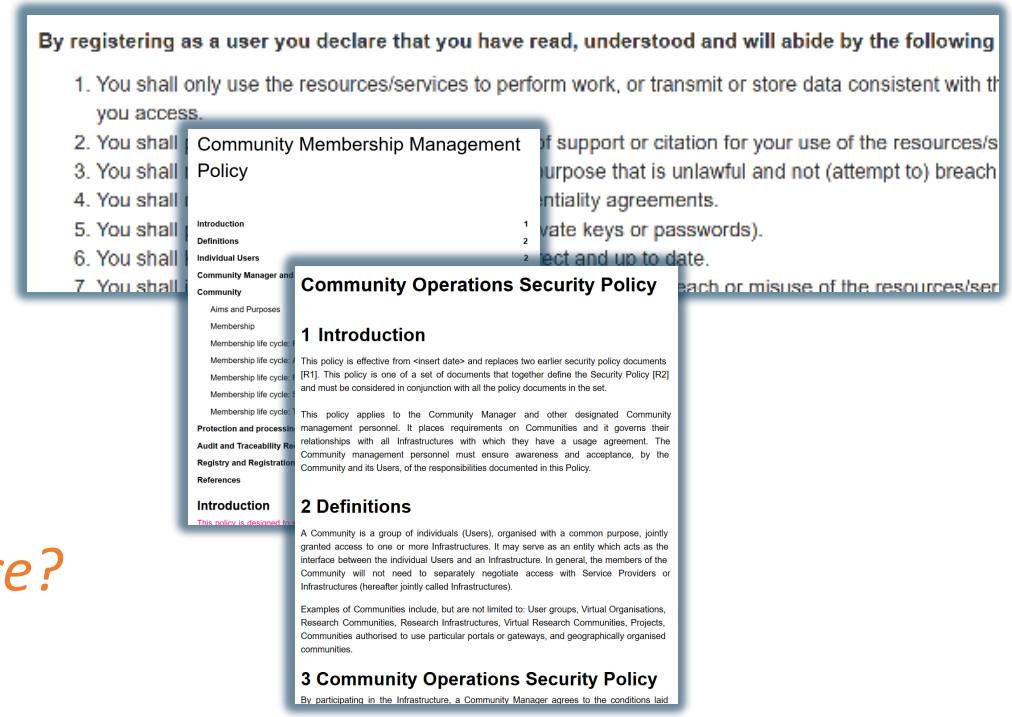
Guidance for research communities in the Infrastructure ecosystem

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?



Differentiated Assurance Profile – in eduGAIN and REFEDS

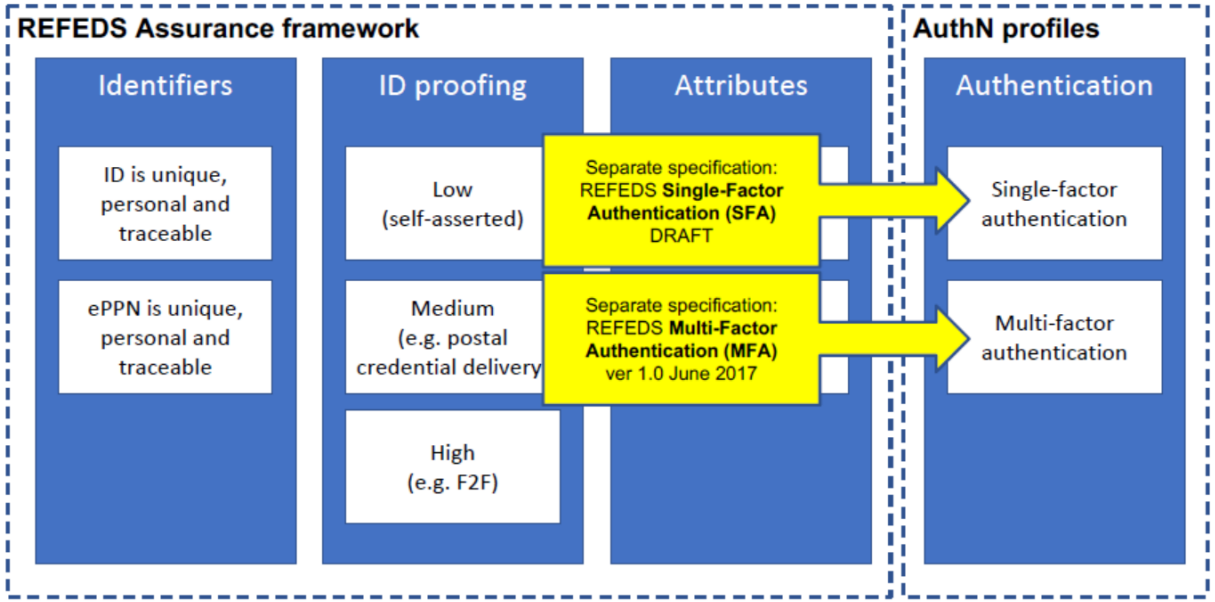
AARC-1 Refresher

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

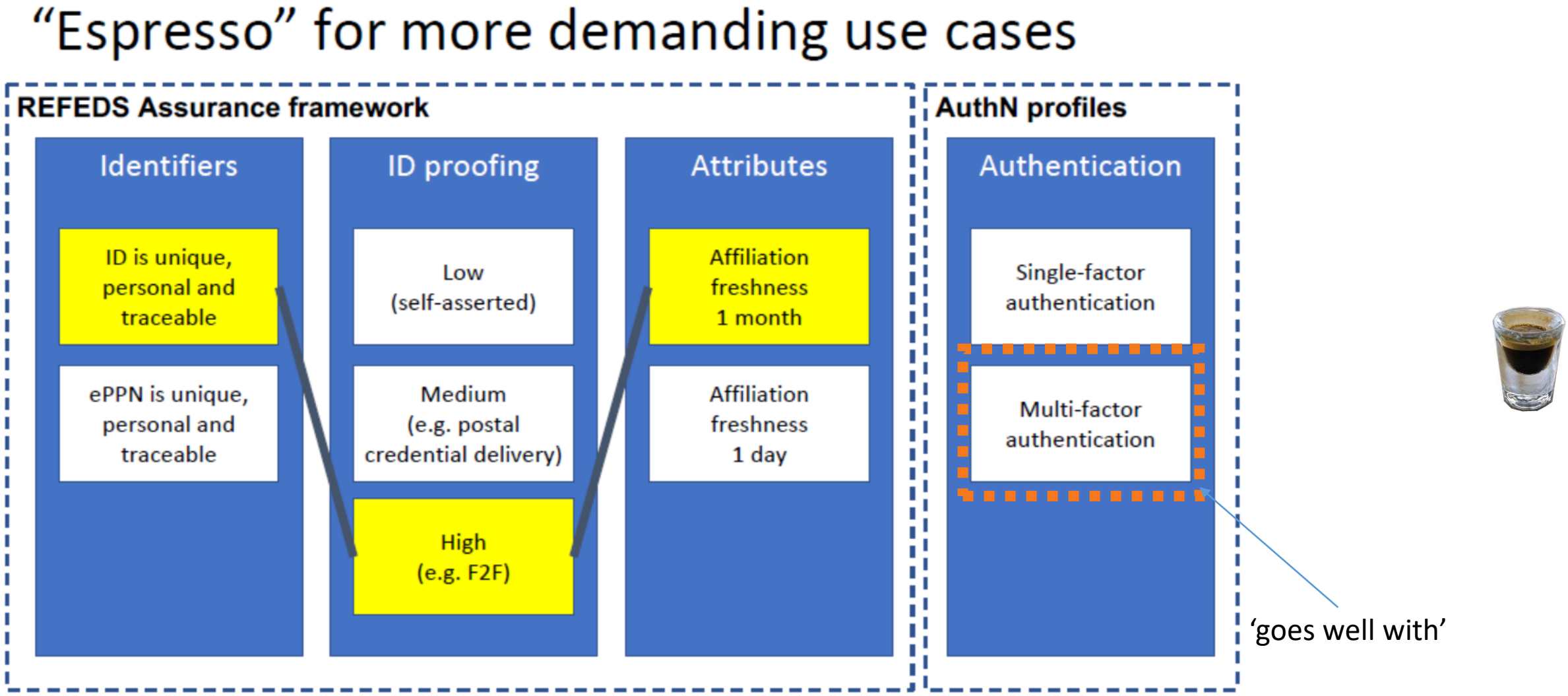
Logical grouping and profiles for the Infrastructures



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

https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+Assurance+Framework+round+2

Example: “Espresso” profile for demanding use cases



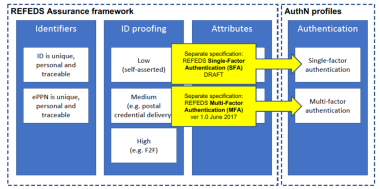
Using the REFEDS Assurance Framework in practice: the RAF Pilot ☺

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



eli r

EGI

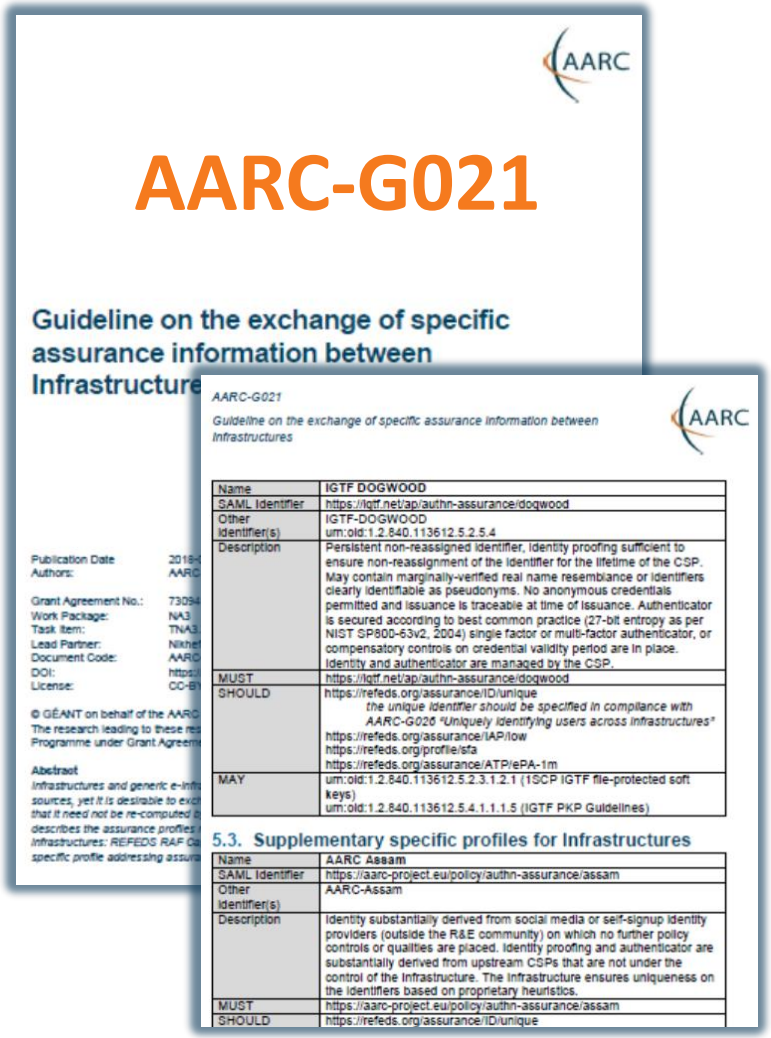
BBMRI-ERIC
Biobanking and BioMolecular resources Research Infrastructure

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



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

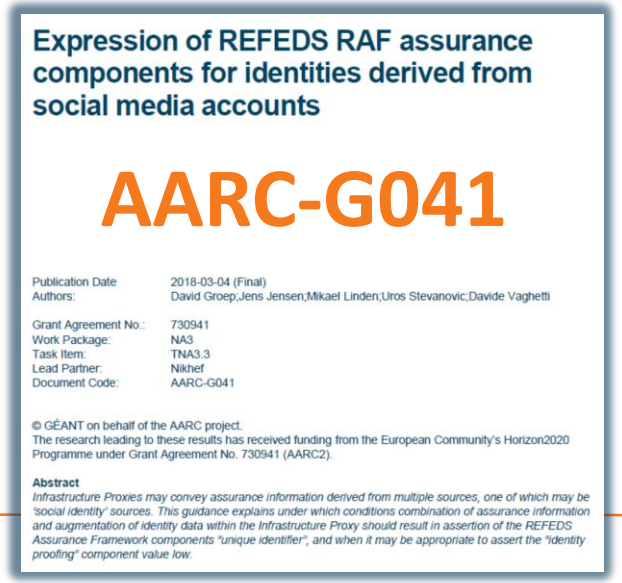
Specific assurance information BETWEEN Infrastructures

- 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

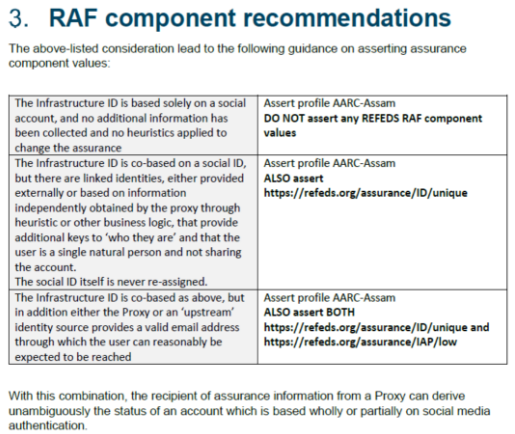
AARC-G041

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**

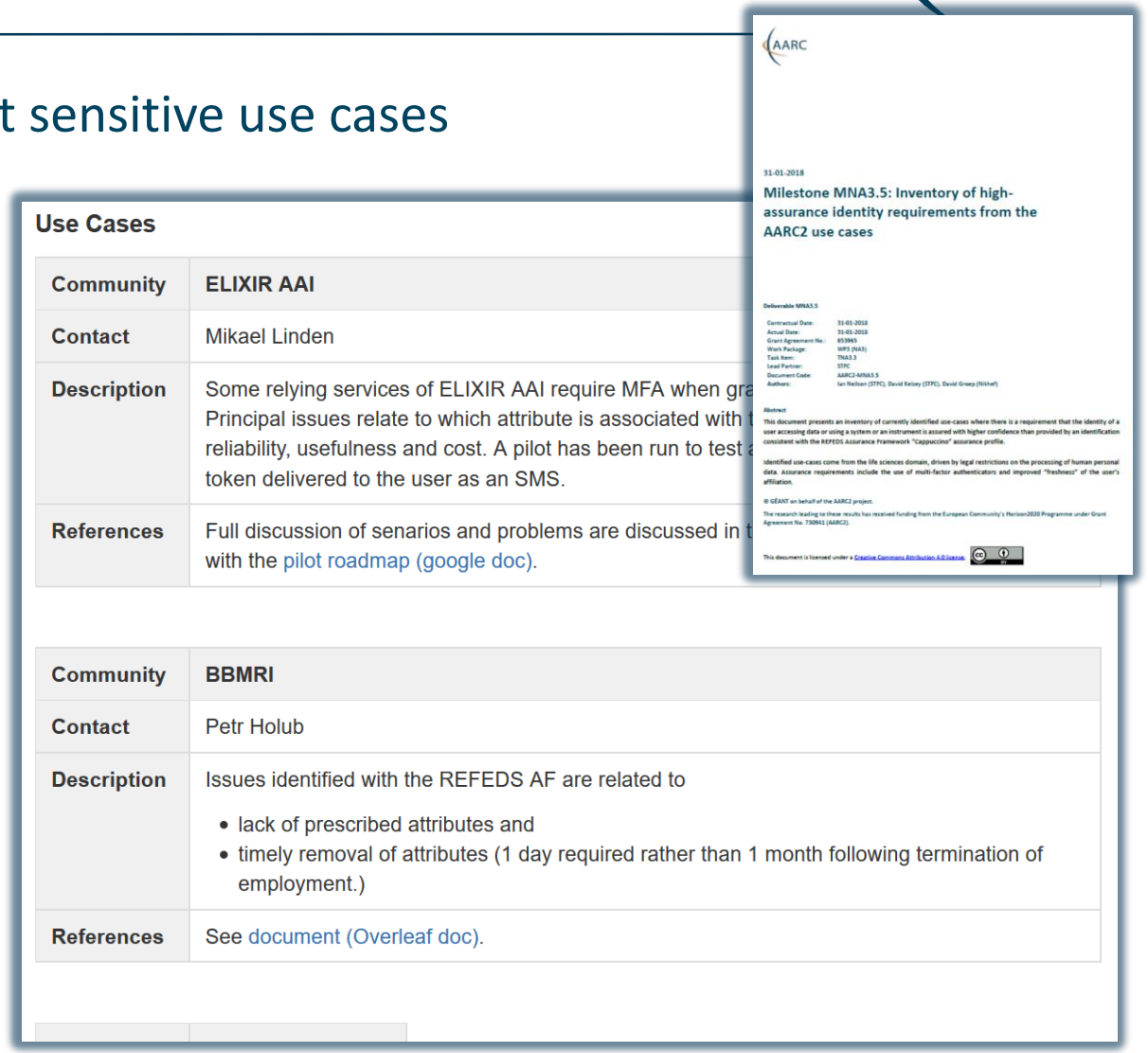
With this combination, the recipient of assurance information from a Proxy can derive unambiguously the status of an account which is based wholly or partially on social media authentication.

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

High-assurance requirements – MNA3.5

- REFEDS RAF “Espesso” 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

- 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



31-01-2018

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

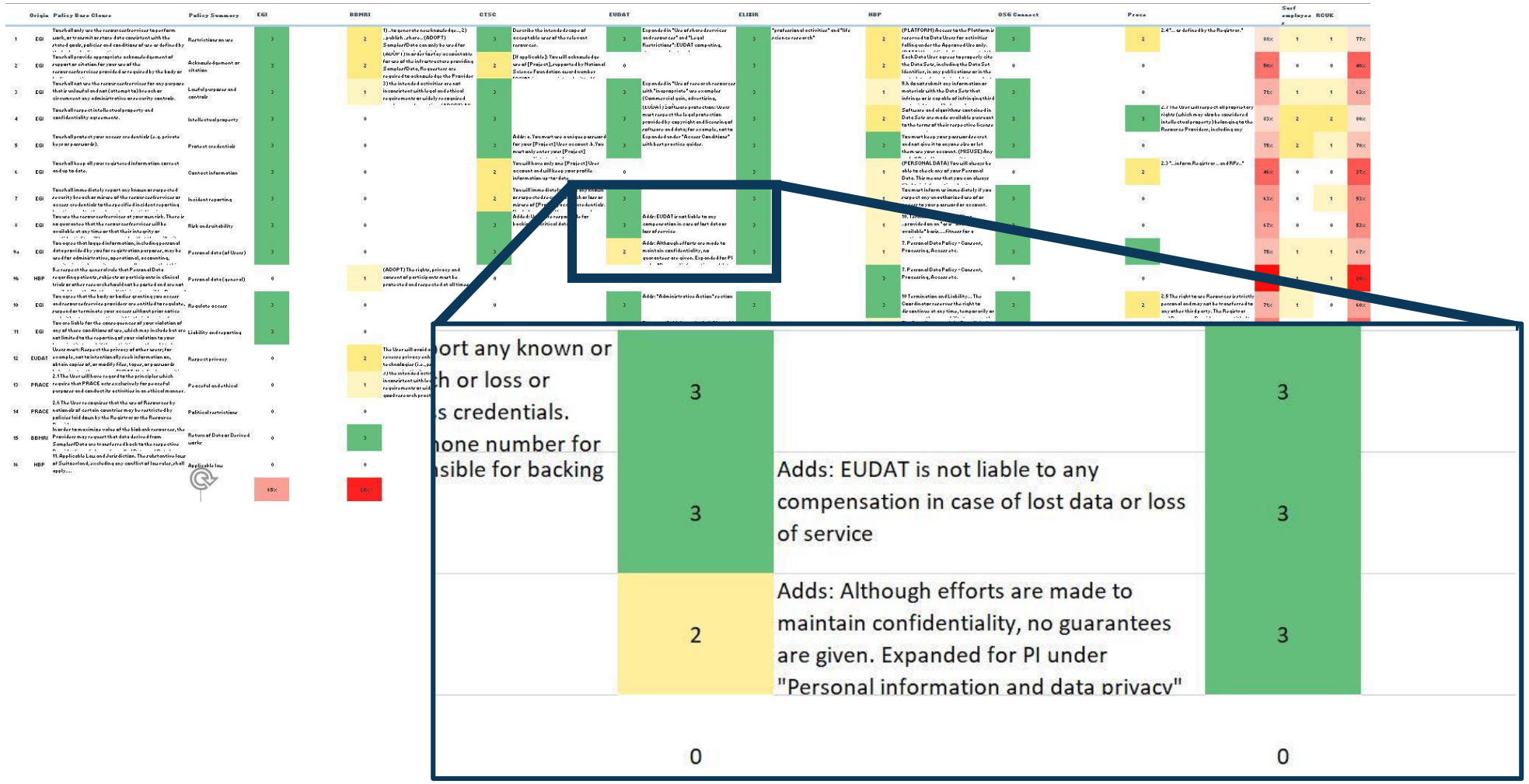
Use Cases

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).

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

Divergence and convergence – the AUP Alignment Study



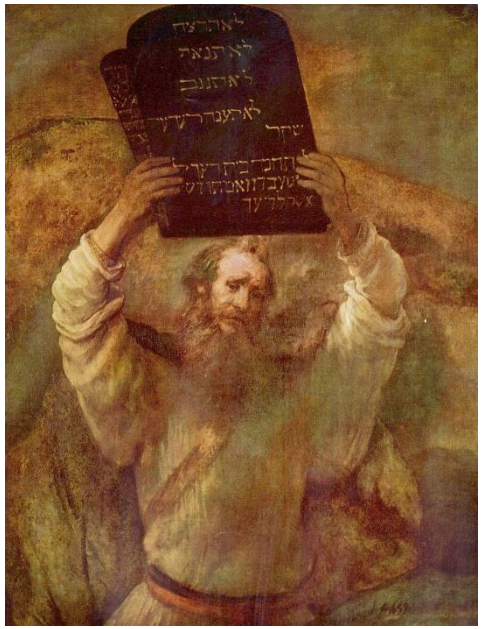
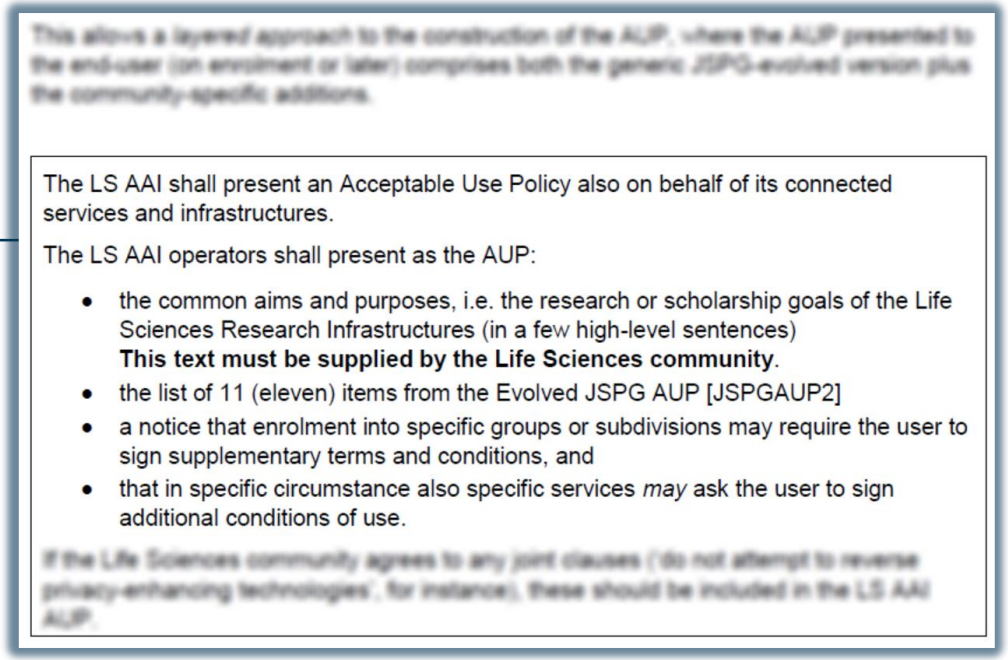


Image: Mozes en de tafelen der Wet, Rembrandt van Rijn, 1659

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

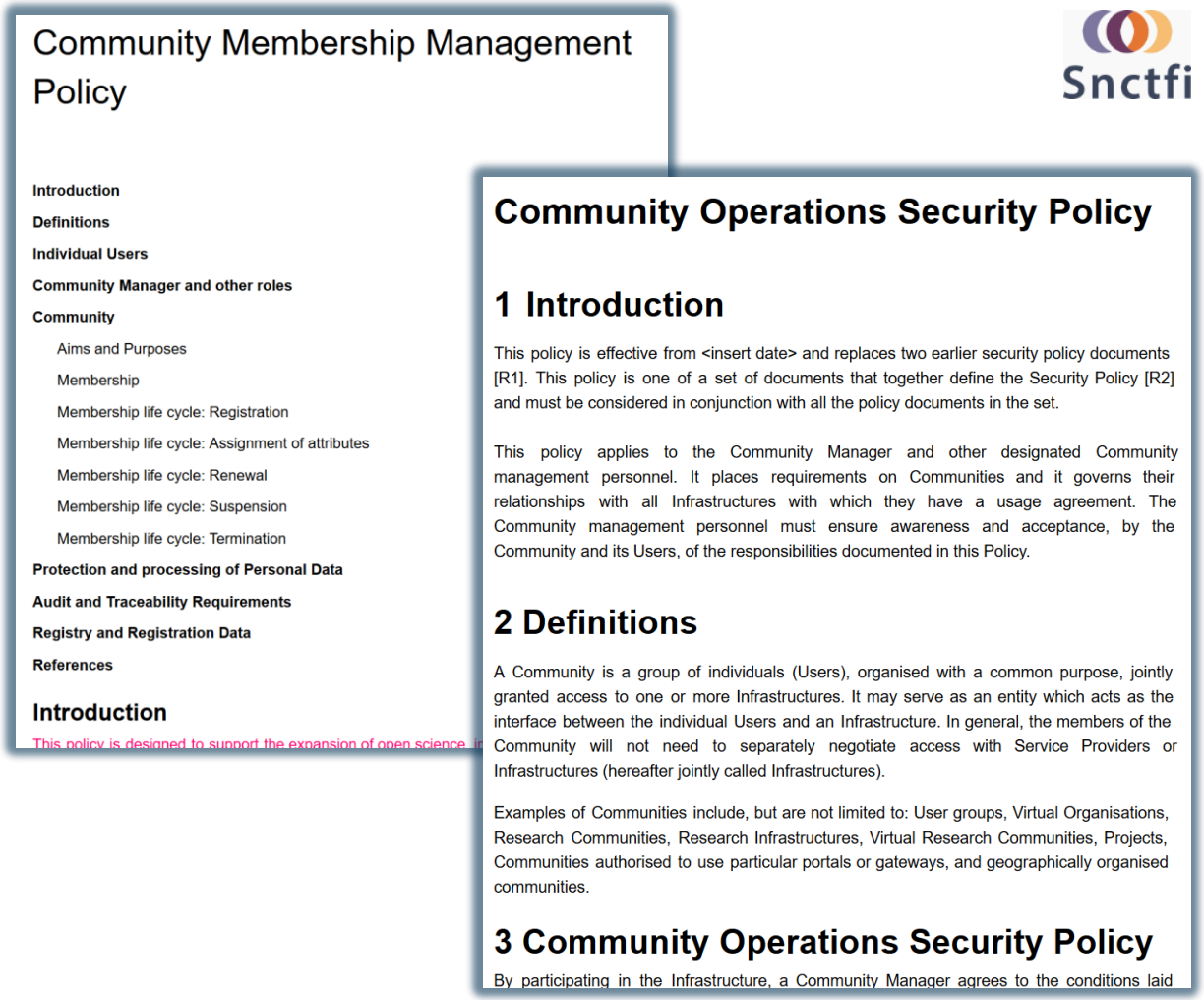
Implementing Snctfi: Community Membership Management and Security

Relevant to communities and e-Infrastructures both

- what are the requisite policy elements and processes you need to define to manage a structured community?
- which of these are required to access general-purpose e-Infrastructures?
- which roles and responsibilities lie with the community 'management' to that the BPA proxy model will scale out?

joint work with EGI-ENGAGE and EOSC-Hub projects and the EGI, PRACE, HBP, EUDAT communities

ENGAGE EOSC-hub



Community Membership Management Policy

Introduction
Definitions
Individual Users
Community Manager and other roles
Community
- Aims and Purposes
- Membership
- Membership life cycle: Registration
- Membership life cycle: Assignment of attributes
- Membership life cycle: Renewal
- Membership life cycle: Suspension
- Membership life cycle: Termination

Protection and processing of Personal Data
Audit and Traceability Requirements
Registry and Registration Data
References

Introduction

This policy is designed to support the expansion of open science in

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.

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.

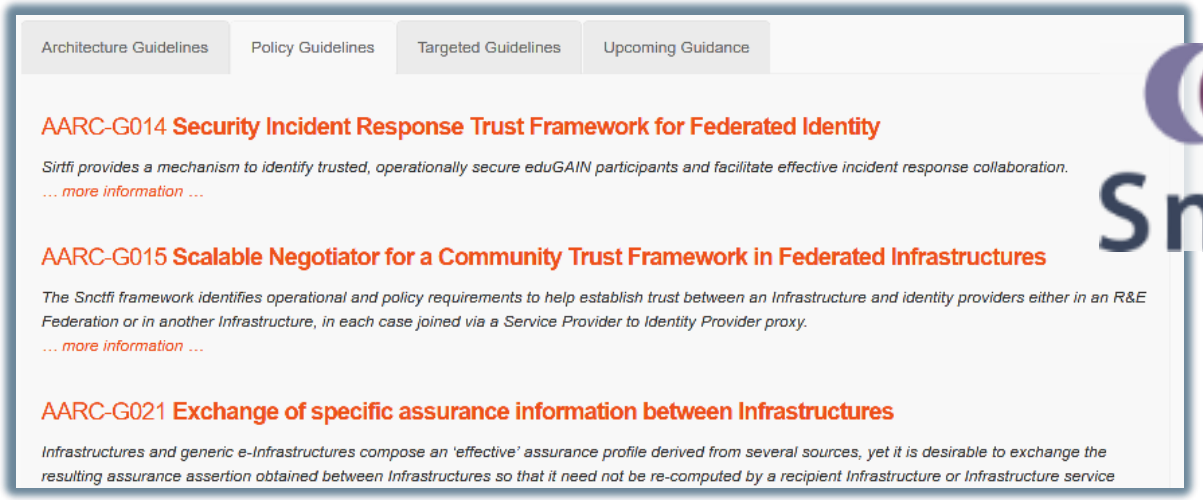
3 Community Operations Security Policy

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

Main achievements in e-Researcher-centric Policy

Assurance Framework alignment	→	REFEDS RAF Pilot with production entities
	→	Profile-driven interop between Infrastructures achieved (AARC-G020)
Guideline: exchange of assurance information	→	Workflows can cross multiple infrastructures
Guideline: social media assurance components	→	Enable collaborative assurance with the community (and guide BPA implementers)
Acceptable Use policy scaling model and baseline	→	*Alignment model* recognized by LSAAI and major e-Infrastructures
PY2	Baseline AUP with major Infrastructures (EGI, EUDAT, PRACE, XSEDE) and communities	
	Deployment of assurance guideline and move to high-assurance use cases	

Policy and Best Practices Harmonisation



Snctfi

excluding the FIM4R engagement work that was already described in the AEGIS & CEF presentation

Task 4

Policy Development Engagement and Coordination

Engagement and coordination with the global community

Sctfi

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures


Sctfi v1.0 AARC

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

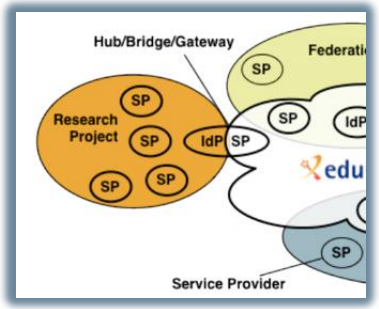
Licia Florio (GÉANT), David Groep (Nikhef), Christos Kanellopoulos (GÉANT), David Kelsey (STFC), Mikael Linden (CSC), Ian Neilson (STFC), Stefan Paetow (Jisc), Wolfgang Pempe (DFN), Vincent Ribaillier (IDRIS-CNRS), Mischa Salle (Nikhef), Hannah Short (CERN), Uros Stevanovic (KIT) and Gerben Venekamp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



Co-develop

Globally through

- *WISE, SCI*
- *REFEDS*
- *IGTF*
- *joint policy groups (with EGI, EOSC, WLCG)*

/Guidelines

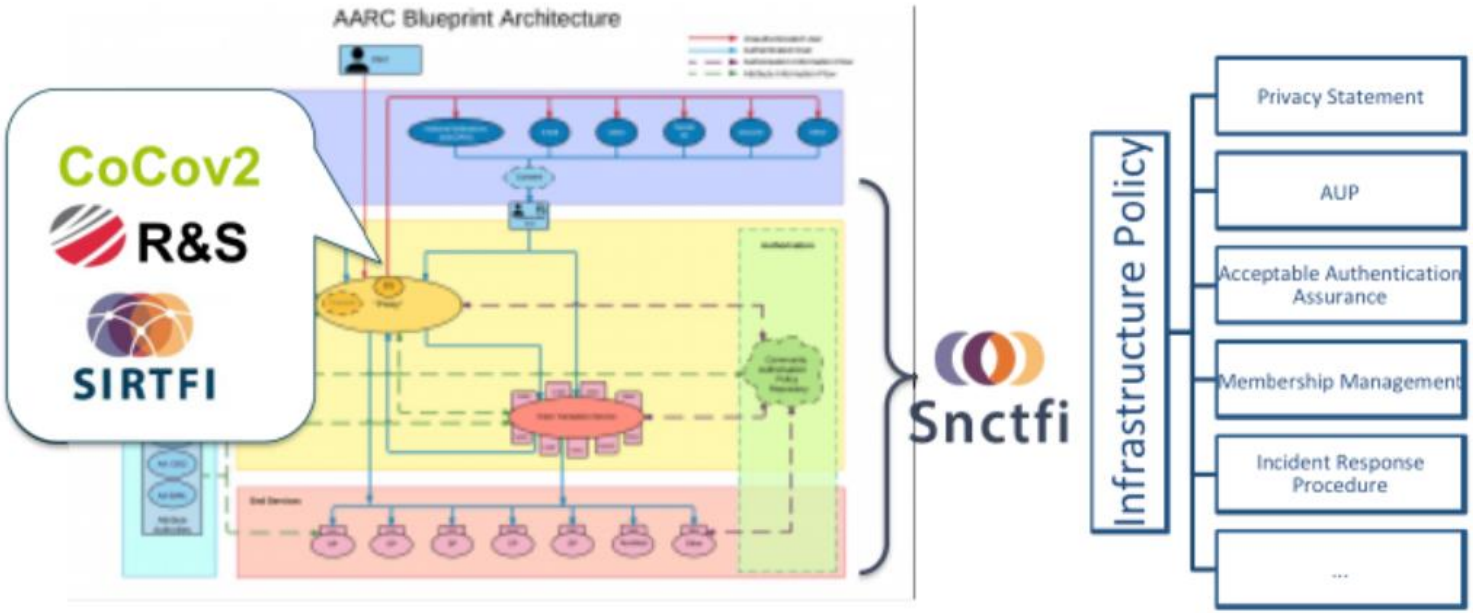
Implement

- ***Adopt** guidelines*
- ***Build on** collective work with EGI, EOSC-Hub, GEANT, and REFEDS*
- ***Consult** with AARC team for targeted guidelines*

Basis for **policy development kit** – *identify gaps in policy suite, coordinate best practice between peer Infrastructures, and leverage AARC templates*

Policy Development Kit

- Bring together a consistent suite
- based on e-Infrastructure best practices in particular EGI-ENGAGE and the JSPG



AARC Policy Development Kit

Task Plan & Notes: https://wiki.geant.org/display/AARC/Policy+Development+Kit
Author list: U. Stevanovic, H. Short, D. Groep, I. Neilson, I. Mikhailava

Introduction	**2**
Scope	2
Infrastructure Policies and Frameworks	3
Frameworks	**4**
Sirtfi Trust Framework	4
Research and Scholarship Entity Category	5
GÉANT Data Protection Code of Conduct	5
Policies	**6**
Top Level	7
Infrastructure Policy	7
Data Protection	7
Privacy Statement	8
Membership Management	8
Community Membership Management Policy	8
Acceptable Use Policy	9
Acceptable Authentication Assurance	9
Operational Security	10
Incident Response Procedure	10
Policy Templates	**10**
Top Level Infrastructure Policy Template	10
Membership Management Policy Template	15
Acceptable Authentication Assurance Policy Template	20
Acceptable Use Policy Template	21
Privacy Policy Template	22
Incident Response Procedure	24
Additional Policies of Interest	**25**
References	**26**

Polity harmonisation

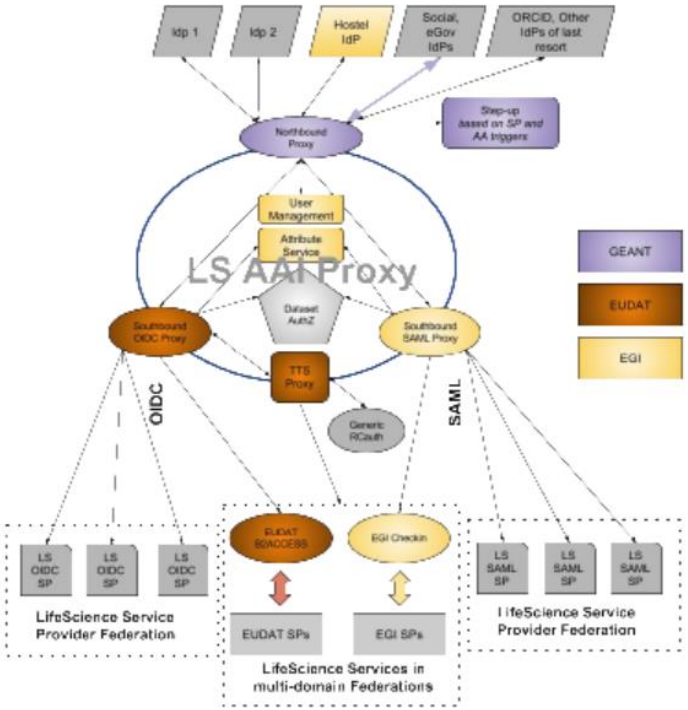
- Alignment and integration of e-Infrastructure AAI service offerings for (AARC-2) communities

  → **encouraging harmonisation**
  → **communities are converging on more limited number of options**

- AARC has a **unique position in providing neutral guidance**

  and **maintaining community focus** across-infrastructure

LSAAI is an example, but of course not the sole reference composition – each community will have its own characteristics and most appropriate technology and service match



Joint e-Infrastructure service for supporting the Life Sciences AAI

In response to the request for proposals by the Life Sciences Research Infrastructures, the joint e-Infrastructures (in alphabetical order EGI, EUDAT, and GÉANT) would like to propose the following solution suite for use in the AARC2 pilot and in support of the initiative by the LS RIs to obtain funding for a sustained LS AAI to be proposed in January 2018.

enabled by the Power of AARC

Main achievements in Policy Coordination and Engagement

Coordination through IGTF, WISE, REFEDS	→	Involvement with AARC across the globe, including XSEDE, OSG, HPCI, and EU Infra's (EGI, EUDAT, GEANT, PRACE)
Policy Development Kit	→	Ease implementation of gapless policy set for new communities based on **Snctfi**
FIM4R reinvigoration process	→	FIM4R 2018 paper gives recommendations for Infrastructures, federations operators, and funding agencies
Harmonisation	→	More joint AAI offerings and increased use of the 'shared service model'
PY2	Evolve Policy Development Kit with a community risk assessment method to guide adoption of appropriate policy	
	Support communities and use cases in policy interpretation through Guidelines	

Challenges

- Policy is – still – usually last on the community's priority list, yet we **need community involvement** to develop appropriate policy

  provide targeted or bespoke guidance first, and
  abstract from it later when possible
  though when a policy need arises,
  the community wants applicable policy and processes instantly!

- Same small group of experts gets to develop most if not all of the policies – general **lack of distributed skilled expertise**

  through e-Infrastructures (alongside AARC2 pilots) and communities
  aim to identify the people that have policy interest and expertise,
  e.g. by pushing it out alongside other thematic service interaction
  with the communities

Conclusions - Where We Are and Where We Go!

Operational Security and Incident Response

- Increased adoption of Sirtfi now permits real-life exercise of the procedures
- PY2: *Extension of OpSec concept to attribute authority operations security for communities*

Service-centric policies

- Policy guidelines, support for AAI proxy operations, and GDPR risk assessment for communities
- PY2: *Develop assessment model based on SCI – to compare against audit based model for trust*

e-Researcher-Centric Policies

- Assurance framework in pilot, cross-infrastructure interop profiles defined, AUP study complete
- PY2: *Move to agreement on a layered AUP and a matching baseline common to Infrastructures*

Policy Development Engagement and Coordination

- Policy Development Kit under way, reinvigorated FIM4R for strategic directions, polities alignment
- PY2: *Risk assessment methodology for communities, targeted guidance policy for communities*

Thank you

Any Questions?

davidg@nikhef.nl

http://aarc-project.eu/

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