



Authentication and Authorisation for Research and Collaboration



[go.nikhef.nl/aarc2na3py2](https://go.nikhef.nl/aarc2na3py2)

## **WP3: Policy and Best Practice Harmonisation**

*the policy side of AARC*

**David Groep**

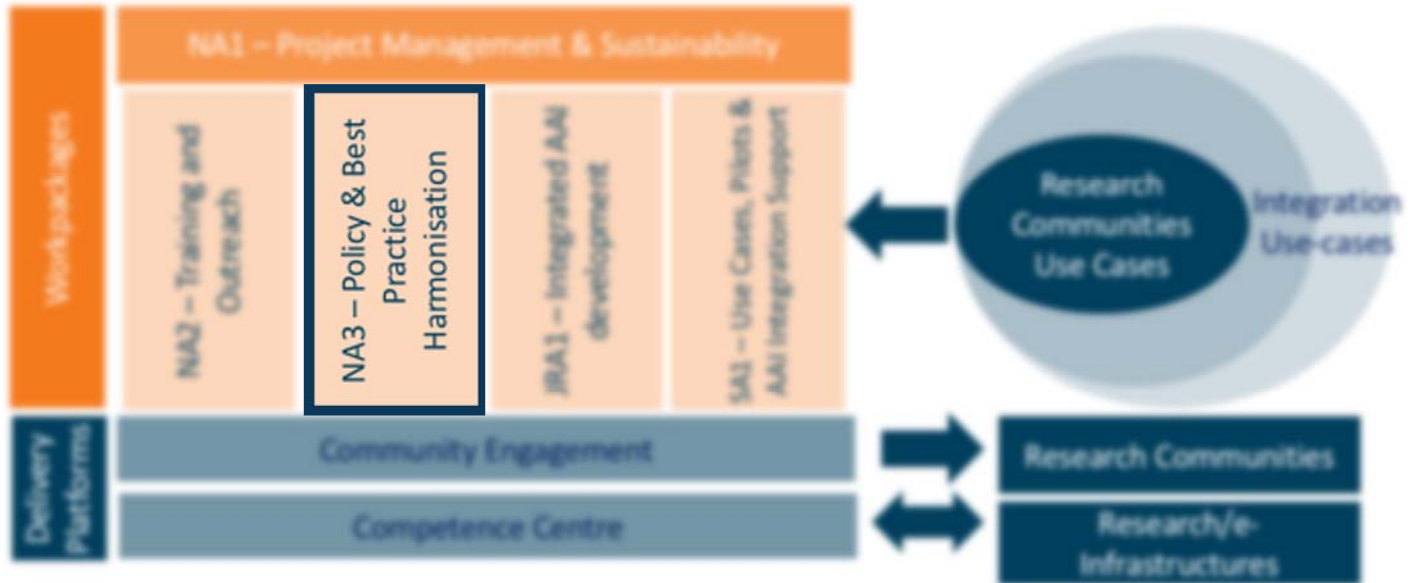
Nik|hef

AARC2 Y2 EC Review

June, 2019

Lëtzebuerg, LU

# WP3: Policy and Best Practice Harmonisation



## Agenda “NA3” Policy and Best Practice Harmonisation

### Organisation

- Team and partners
- Objectives
- Use of Resources

### Achievements

- Operational Security and Incident Response
- Service-centric activities
- Researcher-centric activities
- Engagement and consultation

### Beyond the project

- Leveraging persistent structures for sustainability
- e-Infrastructure support and collaboration



“**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

	T1	T2	T3	T4
<b>Activity Lead</b>	<b>Incident Response Trust</b>	<b>Service-centric Policy Support</b>	<b>Researcher-centric Support</b>	<b>Engagement &amp; Development</b>
				
<b>David Groep</b> Nikhef (NWO-I)	<b>Hannah Short</b> CERN	<b>Uros Stevanovic</b> KIT	<b>Ian Neilson</b> STFC RAL	<b>David Kelsey</b> STFC-RAL

## Partners



CSC-TIETEEN TIETOTEKNIIKAN KESKUS



Science & Technology  
Facilities Council



BBMRI-ERIC®



JÜLICH  
FORSCHUNGSZENTRUM



Karlsruhe Institute of Technology

## Resources (1 May 2017 – 30 April 2018 – 30 April 2019) and deliveries



Cumulative: *47 PM foreseen*  
Total: *approx. 2 FTE average*

*> 38 PM used*  
*of which 26 PM used in PY1*  
*> 81% of forecast personnel resources*

**3 of 3 deliverables in PY2**



DNA3.2 – Report on Security Incident Response  
DNA3.3 – Accounting and Traceability in Multi-Domain Service Provider Environments  
DNA3.4 – Recommendations for e-Researcher-Centric Policies and Assurance

**With many other documents and results**

**7 Guidelines and Informational documents (topical white papers) in AARC2**

... the Policy Development Kit, WISE Baseline AUP implementation guide, guidance on using DPCoCo in proxies, REFEDS Assurance Pilot, secure attribute authority operations, FIM4R community engagement, eduGAIN Sirtfi communications challenge, reference incident response process, X-infrastructure assurance expression, social-ID assurance guide, Data Protection Impact Assessment hints, untangling spaghetti ...

## Deliverable submission status



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

*Initial phase in PY1 focussed on giving guidance to the community on GDPR DPIA*



Report on Security Incident Response (in FIM): **DNA3.2 / D3.1**

*Operational security processes for R&E federations and protection of (BPA) proxies Sirtfi readiness, and how trust groups can support federated incident response*



Accounting and Traceability in Multi-Domain Service Provider Environments: **DNA3.3 / D3.2**

*Supporting proxies and infrastructures in service delivery with privacy guidance on traceability and accounting, policy suites, and frameworks to interwork at a global level for research infras*



Recommendations for e-Researcher-Centric Policies and Assurance: **DNA3.4 / D3.3**

*Complementing policies centering on research communities and involving end-researchers: assurance sourced from R&E federations and peer infrastructures, a global common Baseline AUP to prevent interrupting research workflows, and engaging through the FIM4R v2 process*

## The evolved role for policy and best practices in AARC2

AARC2's stronger use case driven & community focus



- **Policy Development Kit**
- **Consultancy role** for *communities & infrastructures*

- work items address policy aspects of the architecture & implementation, *e.g.*,

**AARC-G041** *Assurance derived from social media*

**AARC-G048** *Secure Operation of Attribute Authorities ...*

- address pilots in SA1, communities, or Infrastructures, *e.g.*

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

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

& **ever closer collaboration with infrastructures** in applying this harmonization

by construction NA3 work 'homed' in sustained forums: WISE, IGTF, REFEDS, FIM4R



# A tour of the policy space in AARC2

**T1 Operational Security for FIM Communities**

**T2 supporting policies for Infrastructures**

**T4 Engagement and Coordination**

**T3 support for Researchers & Community**



**3 Community Operations Security Policy**

**T4 Engagement and Coordination**

GDPR-style Code of Conduct – a new way?

- Global sharing in controlled communities appears attractive
- Uncertainty about requirements (governing body) and timing (> Mar 2018) are not helpful for adoption today ... just yet
- Original text needs to allow for (community) attribute authorities

- Note that this is not formally SICT, so requires sc...
- Collaborations (e.g. based around Snctfi) with com...
- "Say what you do, and do as you say" – transparency is our real benefit towards the person whose data...

**1 ACCEPTABLE USE POLICY AND CONDITIONS OF USE**

This policy is effective from 10/10/2016 and replaces an earlier version of this document. It is intended to be used in conjunction with all the policy documents in the SICT Policy Framework. It is intended to be read together with all the policy documents in the SICT Policy Framework. It is intended to be read together with all the policy documents in the SICT Policy Framework. It is intended to be read together with all the policy documents in the SICT Policy Framework.

## Policy and Best Practices Harmonisation



*Security Incident Response Trust Framework  
SCCC: Security Service Challenge Coordination  
Attribute Authority Security, in the BPA model and beyond*

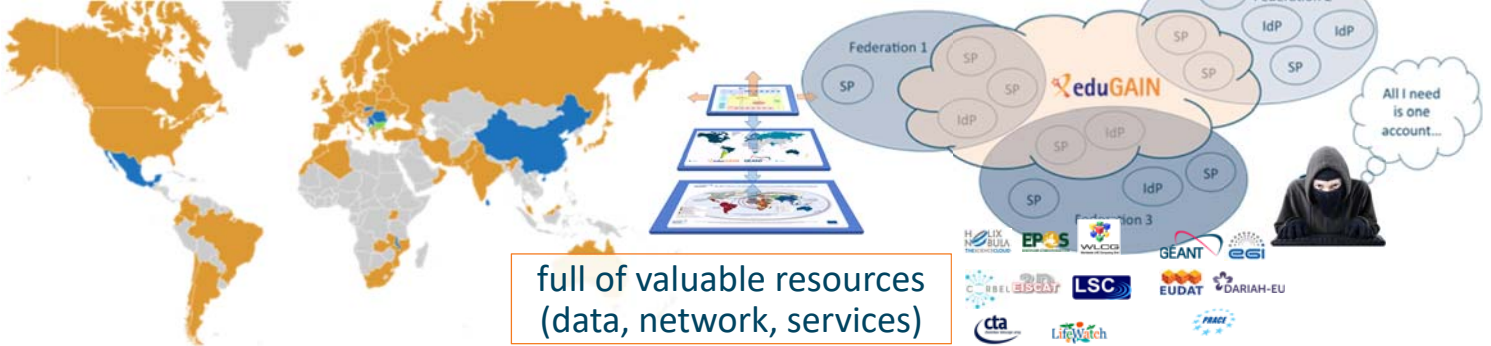
## Task 1

# Operational Security and Incident Response

# Security Incident Response in the Federated World

AARC-1 Refresher

many countries & economic regions with an R&E identity federation



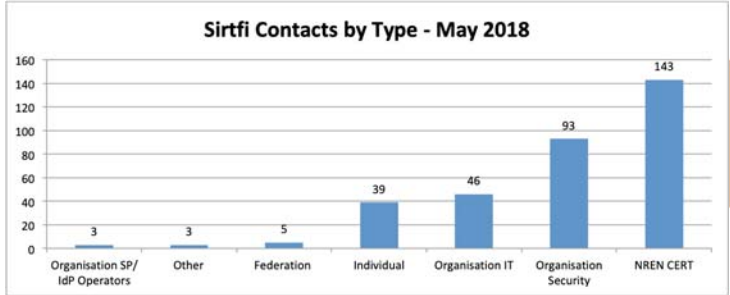
full of valuable resources (data, network, services)

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

## Security Incident Response Trust Framework for Federated Identity

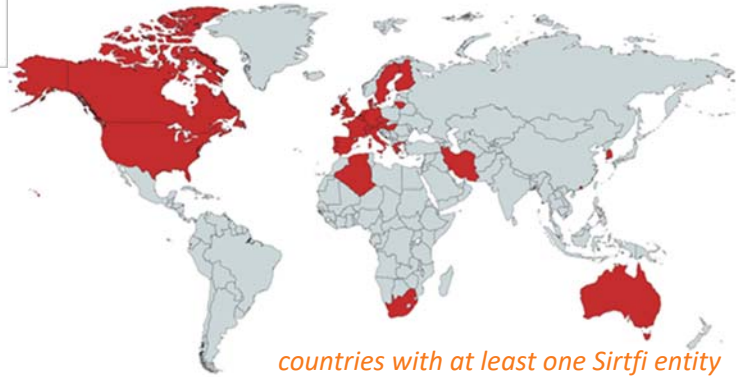
Sirtfi – based on Security for Collaborating Infrastructures (SCI) & FIM4R Recommendations

# Sirtfi is there today – 575 parties (420 IdPs) joined, in 28 federations



## Incident Response

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



### IAM Online Europe

IAM Online Europe webinars are brought to you by



[IAMonlineEU 001 Sirtfi](#)  
IAMonline  
38 views • 4 days ago

<https://refeds.org/SIRTFI> REFEDS > SIRTFI

Incident response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response situations. This assurance framework comprises a list of assertions which an organisation can attest in order to be compliant. Visit our [Wiki](#) to discover how your organisation can prepare itself for Federated Incident Response.

Group has been active since 2014 and combines expertise in operational security and incident response policies community. Work to publish and implement the Sirtfi Trust Framework is supported by the AARC.



Benefits

[http://aarc.org/Why should I join? What are the Benefits?](#)



Sirtfi v 1.0

[View the Sirtfi Framework](#)



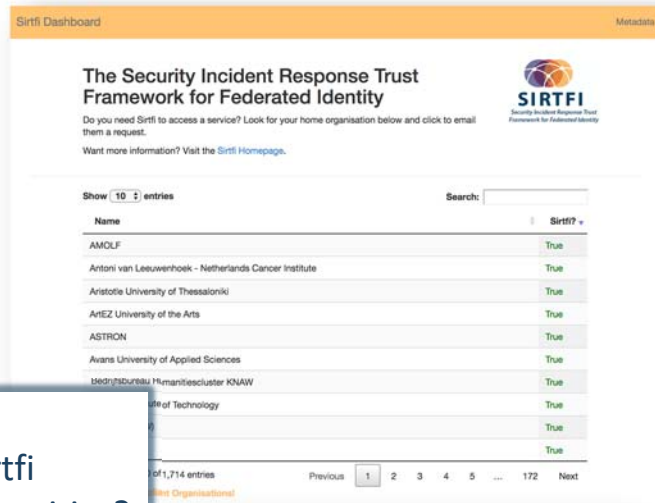
FAQs

[Need help?](#)

## The sociology of checking Sirtfi enablement ...


### Sirtfi 'encouragement'

- the tool certainly raises attention 😊
- lack-of-Sirtfi (and R&S) is non-trivial to diagnose – other causes may interfere



Sirtfi Dashboard Metadata

**The Security Incident Response Trust Framework for Federated Identity**

 **SIRTFI**  
Security Incident Response Trust Framework for Federated Identity

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

Want more information? Visit the [Sirtfi Homepage](#).

Show  entries Search:

Name	Sirtfi?
AMOLF	True
Antoni van Leeuwenhoek - Netherlands Cancer Institute	True
Aristotle University of Thessaloniki	True
ArtEZ University of the Arts	True
ASTRON	True
Avans University of Applied Sciences	True
Medi@Bureau Humanitiescluster KNAW	True
... of Technology	True
...	True
...	True

of 1,714 entries Previous  2 3 4 5 ... 172 Next

[View Organisations!](#)

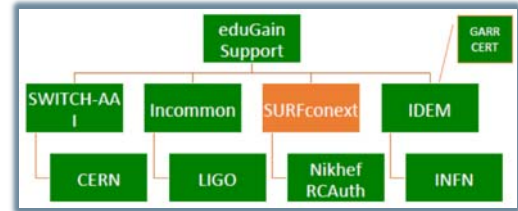
### Sirtfi+ registry

- enabling more entities to express Sirtfi
- sharing implicit trust between communities?
- tool requirement

# Testing incident response coordination

As seen in PY1

- Can we coordinate our collective R&E response?
- Communication guidelines to help timely resolution?
- Two 'challenges': **March 2018** and **December 2018**

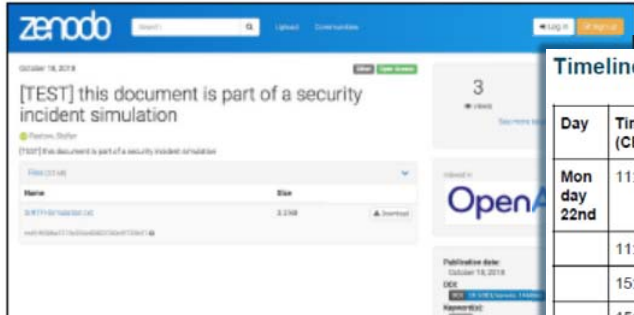


parties involved in response challenge

Report-outs see <https://wiki.geant.org/display/AARC/Sirtfi+Communications+Challenges%2C+AARC2-TNA3.1>

## 2<sup>nd</sup> challenge, December 2018: using the draft response templates

### Malicious content hosted on Zenodo, uploaded with an ORCID account



#### Timeline

Day	Time (CEST)	Action (orange text indicates entity's first action within day)
Monday 22nd	11:00	CERN Computer Security informed Zenodo about malicious content [CERN: RQF1143915]
	11:54	Zenodo identifies that the user was authenticated through ORCID
	15:00	Zenodo contacts ORCID with account identifier
	15:44	ORCID replies <ul style="list-style-type: none"> <li>Disables the ORCID account</li> </ul>



- time delay between 'malicious act' and request for investigation (+3 days)
- spread over all time zones (.au, .ch, .nl, .uk, .us,
- new set of participant IdPs and federations
- initial mitigation within 4 hrs, but eduGAIN support desk gets it only on the 3<sup>rd</sup> day ...
- contact with affected user effective and appreciated
- TLP classification not used throughout, some entities initially missed

# Preparing the ground for REFEDS Sirtfi procedures: AARC-I051

Acknowledging that only reviewers read deliverables, response process from DNA3.2 issued as ...  
**AARC-I051 Guide to Federated Security Incident Response for Research Collaboration**

## Be Prepared

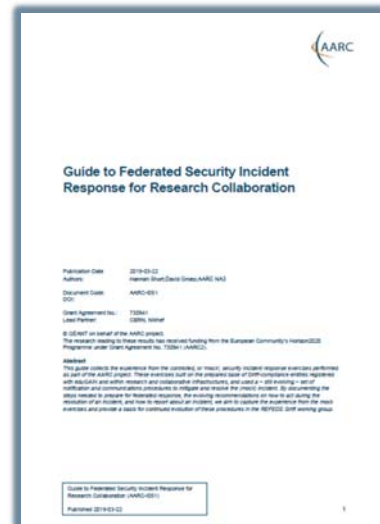
- Federated Entities Should Support Sirtfi
- Community Proxies Should Adopt Interoperable Policies & Procedures
- Federations and Interfederations Should Adopt Common Procedures
- Leverage Templated Emails
- Establish Secure Communication Channels in Advance

## Act

- Scope
- Goals
- Responsibilities
- **Procedures:** for IdPs & SPs, for coordinators, for eduGAIN

## Report and Share

*informational document and not a guideline since Sirtfi WG still needs to get global endorsement, yet we need practical guidance right now!*

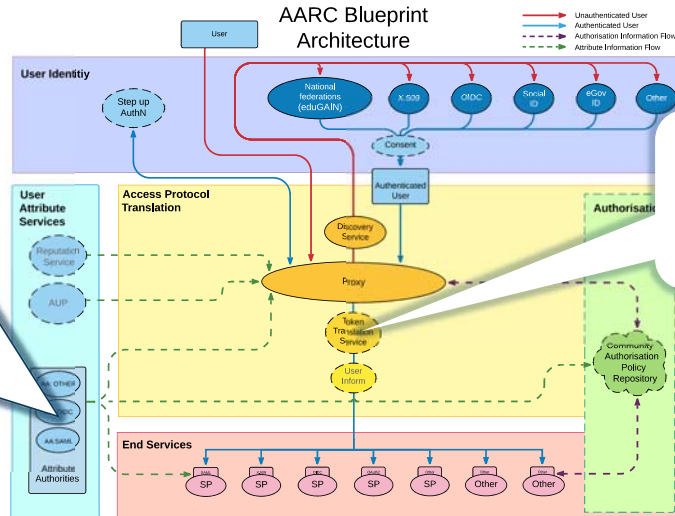




# Operational security focus in the BPA: beyond just the IdPs

## Community membership management directories and attribute authorities

- integrity of membership
- identification, naming and traceability
- site and service security
- protection on the network
- assertion integrity



Store and manage ephemeral user credentials

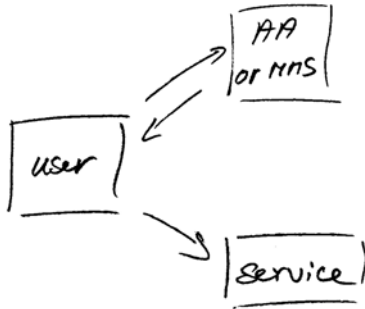
- trusted credential stores
- protection at rest

IGTF Guidelines on Trusted Credential Stores (pre-existing)

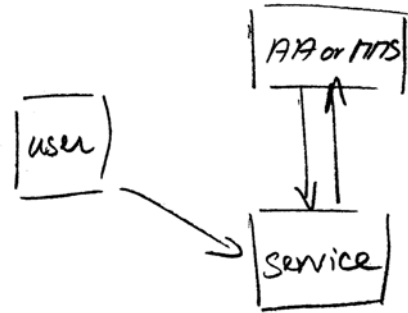
Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements (AARC-I048, in collaboration with IGTF AAOPS)

## Protecting the community membership data and its proxy

- Intentionally targeted broader than just BPA-style communities, since operational security spans data centres and infrastructures using other forms of AA membership management
- PRACE: ‘pull model’ directory-based communities
- BPA: encourages ‘push model’ attribute-carrying service requests



*push model – the common BPA method  
(e.g. SAML AttributeStatement, VOMS AC)*



*pull model – common when using directories  
(e.g. LDAP in PRACE, GUMS in OSG)*

# AARC-G048: keeping users & communities protected, moving across models

trusted delegation of response from communities to operators, and from services to communities in recognizing their assertions

Structured around concept of “**AA Operators**”, operating “**Attribute Authorities**” (technological entities), on behalf of, one or more, **Communities**

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

Publication Date: 2016-11-22  
 Authors: David Groep, David Kiersma, Pieter-Jan Maarten Kiersma  
 Document Code: AARC-G048



## 3.3. Attribute Assertions

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

## 3.4.1. Key Management

1. A key used to protect assertions should be dedicated to assertion protection functions.

### Push model

If the AA both signs assertions and provides functionality over protected channels, the keys used to sign assertions shall be different from those protecting those channels.

### Pull model

The key of the AA must be used solely for protecting connections to its protocol endpoint and ensure an integrity protected and mutually authenticated channel.

## Main achievements in Operational Security

Sirtfi framework adoption and promotion	➔	Sirtfi checking tool, and the <i>Sirtfi+</i> Registry Much increased awareness (and some beneficial annoyance as well)
Sirtfi incident exercises and training	➔	Improved incident response in eduGAIN Response guidelines on readiness and action
Communications challenge coordination	➔	Commitment beyond WISE or Sirtfi for challenge coordination in SIGISM & REFEDS
Attribute Authority Operations guidance	➔	Better protected community management in the provisioning of data form BPA proxies

**After  
AARC**

WISE Security Communication Challenge Coordination JWG

REFEDS Sirtfi, eduGAIN Security Capability, EGI CSIRT, EOSChub ISM, and the IGTF

## Policy and Best Practices Harmonisation



*Snctfi contributions to the Policy Development Kit*  
*Data Minimisation at the proxy for access to services*  
*Security for Collaboration among Infrastructures SCI: assessment and peer review methodology*

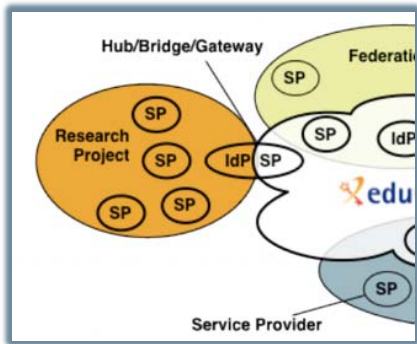
## Task 2

# 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*




derived from **SCIV2**: framework on *Security for Collaboration in Infrastructures* via **WISE** reference policies supporting *Snctfi* fulfilment in the Policy Development Kit

# Filling the framework: generic and community-targeted guidance

**Guidelines**

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

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



Architecture Guidelines   Policy Guidelines   Targeted Guidelines   Upcoming Guidance

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

*Swift provides a mechanism to identify trusted, operationally secure eduGAIN participants and facilitate effective incident response collaboration.*

... more information ...

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

*The Swift framework identifies operational and policy requirements to help establish trust between Federation or in another infrastructure, in each case joined via a Service Provider to Identity Provider.*

... more information ...

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

*Infrastructures and generic e-infrastructures compose an 'effective' assurance profile derived from resulting assurance assertion obtained between infrastructures so that it need not be re-computed by the provider. This document describes the assurance profiles recommended to be used by the infrastructures.*

... more information ...

[aarc-project.eu/guidelines](http://aarc-project.eu/guidelines)

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

Architecture Guidelines   Policy Guidelines   Targeted Guidelines   Upcoming Guidance

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

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

... more information ...

## Service-centric policies – key elements to our ‘PDK’

**more on the Policy Development Kit when we get to task 4!**



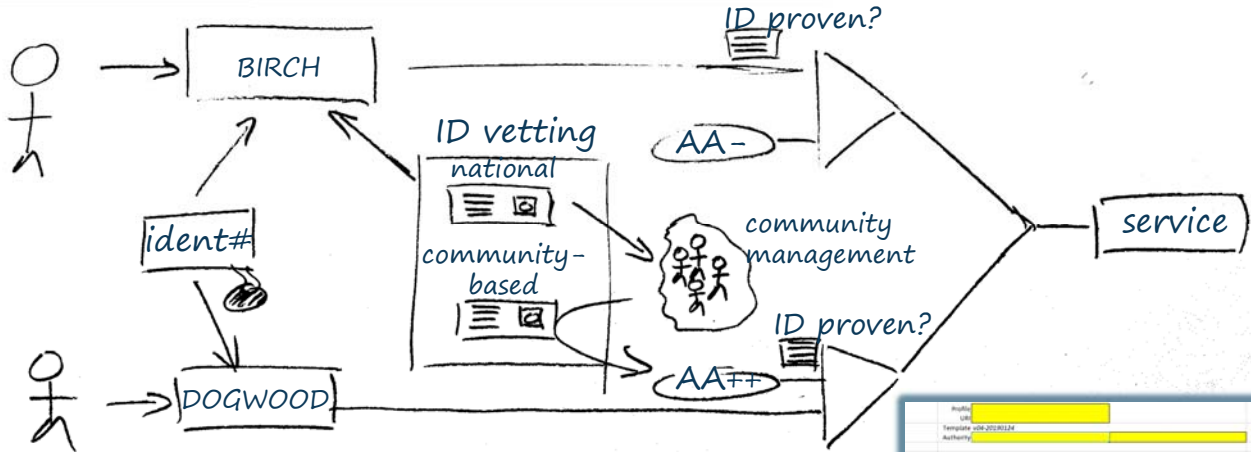
Document	Why should complete the template?	Audience	Description
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template provides a step-by-step breakdown of the actions to be taken following a security incident.
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines the rules for Research Communities to manage their members, including expiration.
Acceptable Assurance	Infrastructure Management	Research Community	This is a placeholder for the acceptable assurance profiles of user credentials.
			This table can be used as a starting point for identifying when a Protection Impact Assessment is required.
			This document defines the obligations on Infrastructure Participants when processing personal data.
			This can be used to define the requirements for data collected and processed within the infrastructure and the service in the infrastructure to be used in the template.
Service Operations Security Policy	Infrastructure Management	Services (abide by)	This policy defines the requirements for running a service within the infrastructure.
Acceptable Use Policy	Infrastructure Management (for Research Communities) & Research Communities (for community specific restrictions)	Users (abide by)	This is a template for a policy that users must agree to when using the infrastructure, augmented by Research Communities.

Showing 1 to 9 of 9 entries

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
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.
Policy on the Processing of Personal Data	Infrastructure Management & Data Protection Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.
Service Operations Security Policy	Infrastructure Management	Services (abide by)	This policy defines requirements for running a service within the Infrastructure.
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.



# Example: Acceptable Authentication Assurance – enabling flexible user communities by mapping assurance elements



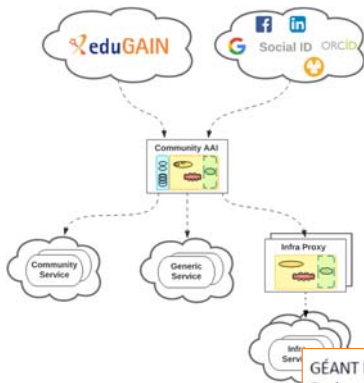
Identity vetting can be done

- when credentialing the user
- on enrolling the user in a community

e.g. *LIGO LSC* always does researcher vetting, and Assurance Policy accommodates linkage in either place – still meeting SP trust needs

Profile	AP source	Description	Method	AP to BIRCH?	Remarks
1	2, line 1	operated as a long term commitment	contact data should refer to an organisation, not a project, and the description should (implicitly) address sustainability	3.1.3	Persistent registry (community membership) implementation and assessment being specific obligations are put on the registry, as 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 assessment systems and services constitutes the Issuing Authority.
2	3.1, line 1	credentials bound to act of setting	description of the proof of possession of key material (improving private keys, symmetric passwords or pin codes, authentication devices delivered or associated with users). The process must ensure that the writing and issuance of the credential are linked, and there are no insecure elements to the chain of custody.	3.2, 4.1, 6.1.1, 6.1.2	The registration process should be such that the applicant-issued credential corresponds to the entity that is supposed to be in the registry. The registration data and any issued assertions constitute the 'literal of the user'. 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
AARC	5.1	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.	the process should ensure that any applicant in the future, stating the same name, is indeed the same entity as the original applicant. This is also needed in order to	3.2, 5.5	

# GDPR for BPA and multi-BPA proxy scenarios



*Snctfi and DPCoCo jointly provide the transitive trust model*  
 Common attributes 'enabling End User to access the Service(s)' behind a BPA proxy (and its omnidirectional attributes) in Snctfi is scoped to enable access – in conjunction with DPCoCo *allows release of attributes by IdPs and MMS services*

**DNA3.3 (D3.2) Accounting and Traceability in Multi-Domain Service Provider Environments**  
*in fact collecting service-centric policy support also for the BPA proxy privacy implications*

GÉANT Data Protection Code of Conduct  
 Explanatory memorandum 16

The Code of Conduct aims to provide guidance on how to process such personal data for online management purposes in compliance with the requirements provided by the GDPR.

However, it is limited to the processing of Attributes which are released for enabling the End User to access the Service. That means processing activities of personal data for purposes other than enabling the End User to access the Service are not covered by the Code of Conduct. Nevertheless, Service Provider Organisation can decide to commit to the GDPR also for other Attributes.

**4.3 Protection and processing of Personal Data [DP]**

*Infrastructure Constituents* and, where necessary Collections of users, must have policies and procedures addressing the protection of the privacy of individual users, i.e. members of the Collections, with regard to the processing of their personal data (also known as Personally Identifiable Information or PII) collected as a result of their access to services provided by the *Infrastructure*.

The *Infrastructure* must:

[DP1] have a Data Protection Policy binding those *Constituents* and Collections of Users who process personal data to an appropriate policy framework, e.g. the GÉANT Data Protection Code of Conduct [6] or, for example, as recommended by AARC [7].

[DP2] ensure that all *Constituents* must provide, in a visible and accessible way, a Privacy Policy covering their processing of personal data for purposes that are necessary for the safe and reliable operation of their service, compliant with the *Infrastructure* policy (or policy framework). The availability of a Privacy Policy template for the *Constituents* to follow, provided by the *Infrastructure*, would help the easier production of such a policy.

# SCIV2 assessment and peer review – do you want to work with your peer?

## SCIV2 proposed assessment model

**Level 0:** Not implemented for critical services;

**Level 1:** Implemented for all critical services, but not documented;

**Level 2:** Implemented and documented for all critical services;

**Level 3:** Implemented, documented & reviewed by a collaborating infrastructure or by an independent external body;

**“Justifiable exclusion”:** feature not relevant for infrastructure.

## Conclusions

- self-assessment feasible, SCI model emphasises proper elements for *federated* access
- peer-review extends trust across similar organisations
- transparency needed: infrastructures weigh sub-elements differently! (no global consensus yet on any weighting method ...)

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

	A	B	C	D	E	F
1	Infrastructure Name:			<insert name>		
2	Prepared By:			<insert name>		
3	Operational Security (OS)					
4				maturity		
5				Value	Σ	
6						
7						
8	OS1 - Security Person/Team			#REF!	#	
9	OS2 - Risk Management Process			#REF!	#	
10	OS3 - Security Plan (architecture, policies, controls)			2.0	●	
11	OS3.1 - Authentication		●	3		
12	OS3.2 - Dynamic Response		●	1		
13	OS3.3 - Access Control					
14	OS3.4 - Physical and Network Security					
15	OS3.5 - Risk Mitigation					
16	OS3.6 - Confidentiality					
17	OS3.7 - Integrity and Availability	Q	●	1	1.0	●
18	OS3.8 - Disaster Recovery					
19	OS3.9 - Compliance Mechanisms					
20	OS4 - Security Patching		●	1	1.0	●
21	OS4.1 - Patching Process					
22	OS4.2 - Patching Records and Communication					
23	OS5 - Vulnerability Mgmt		●	1	0.7	●
24	OS5.1 - Vulnerability Process					
25	OS5.2 - Dynamic Response					
26	OS6 - Intrusion Detection		●	2		
27	OS7 - Regulate Access (including suspension)		●	1		
28	OS8 - Contact Information					
29	OS8.1 - Contact Users					

## Main achievements in Service-Centric Policy

Policy templates and guidance for infrastructures and services	➔	Increased interoperability by adoption of <i>Snctfi</i>
Guidance in data protection in proxies for infrastructures for research	➔	Ease attribute release by communities in BPA scenarios
SCIv2 Assessment <i>Security Collaboration among Infrastructures</i>	➔	Developed assessment model and gained adoption in global WISE-community
Assessment model based on peer review	➔	Increased trust between infrastructures for a broader community at lower cost

<b>After AARC</b>	AEGIS (and WISE SCI WG & IGTF): supporting interworking infrastructures
	GN4-3 EnCo: support communities in data protection & policy development kit

# Policy and Best Practices Harmonisation

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 the purpose that is lawful and not (attempt to) breach confidentiality agreements.
2. You shall not use the resources/services for any purpose that is unlawful and not (attempt to) breach confidentiality agreements.
3. You shall not use the resources/services to perform work, or transmit or store data consistent with the purpose that is unlawful and not (attempt to) breach confidentiality agreements.
4. You shall not use the resources/services to perform work, or transmit or store data consistent with the purpose that is unlawful and not (attempt to) breach confidentiality agreements.
5. You shall not use the resources/services to perform work, or transmit or store data consistent with the purpose that is unlawful and not (attempt to) breach confidentiality agreements.
6. You shall not use the resources/services to perform work, or transmit or store data consistent with the purpose that is unlawful and not (attempt to) breach confidentiality agreements.
7. You shall not use the resources/services to perform work, or transmit or store data consistent with the purpose that is unlawful and not (attempt to) breach confidentiality agreements.



*Identity Assurance and Assurance Framework Mapping  
Baseline Acceptable Use Policy and WISE  
Policies for the Development Kit*

## Task 3 e-Researcher Centric Policies

# 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 <b>DO NOT</b> 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 <b>ALSO</b> assert <a href="https://refeds.org/assurance/ID/unique">https://refeds.org/assurance/ID/unique</a>

5. Profiles.....	5
5.1. REFEDS RAF Profiles .....	5
5.2. Supplementary IGTF profiles for Infrastructures.....	6
5.3. Supplementary specific profiles for Infrastructures.....	7
5.4. Attribute freshness assurance component .....	<b>AARC-G021</b> 8
5.5. Implementation notes.....	<b>inter-infrastructure adoption</b> 8

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

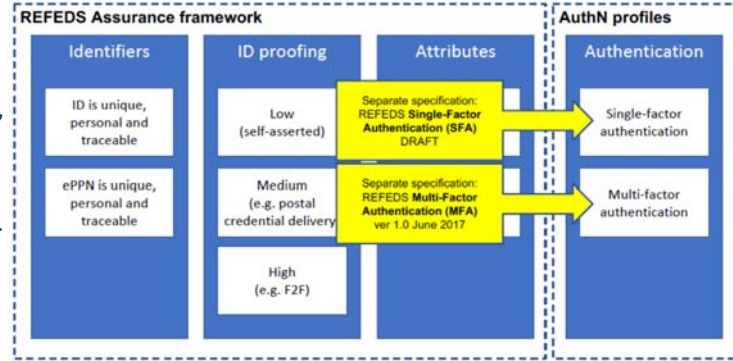
# Differentiated Assurance Profile – in eduGAIN and REFEDS



## Specific definitive guidance to IdPs and federations

- **Uniqueness:** at least ePUIID or NameID
- **ID proofing:** ‘low’ (good for local use), ‘medium’ (Kantara LoA2, IGTF BIRCH, eIDAS low), or ‘high’ (Kantara LoA3, eIDAS substantial)
- **Authenticator:** in REFEDS separate profiles, single (SFA) and multi-factor (MFA) authenticator
- **Freshness:** better than 1 month

## Logical grouping and profiles for the Infrastructures



All assurance profiles assume organizational-level authority, also used *by the IdP* for ‘real work’, good security practices

# e-Infra & Research Infra: high-assurance use cases – does it stand the test?

## Two representative use cases from the AARC Pilots

Sensitive data – assurance must stand up to scrutiny, and seen in conjunction with other standards

- Retrieval of data from medical data repository  
*BBMRI-ERIC Colorectal Cancer Cohort study data*
- Processing personal data on secure computing infrastructures  
*BioBankCloud, TSD Trusted Sensitive Data, MOSLER platform*

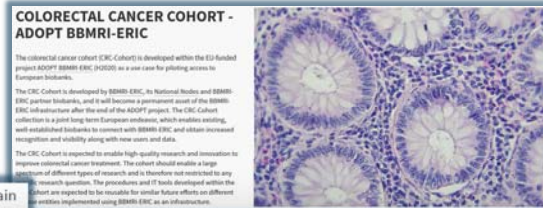


Table 8: Minimum requirements for basic data types. Non-personal data is used to denote data that does not contain any traces of privacy-sensitive data (e.g., data about operation of the biobank storage systems).

	raw (non-deidentified)	pseudonymous	practically anonymous	non-personal
<i>Authentication and authorization</i>				
Identity verification	LoA $\geq 2$	LoA $\geq 2$	LoA $\geq 0$	op
Authentication instance	LoA $\geq 3$	LoA $\geq 2$	LoA $\geq 0$	op
Assessing project & informed consent compliance	not available for research	MANDATORY	RECOMMENDED	
Restricted access	high security	high security	medium-low security	op
DTA/MTA	REQUIRED	REQUIRED	RECOMMENDED	op
<i>Authentication and authorization</i>				
Access log archive since last access	$\geq 10$ years	$\geq 10$ years	$\geq 3$ years	
<i>Data transfers and storage</i>				
Encrypted storage	REQUIRED	REQUIRED		
Encrypted transfers	REQUIRED	REQUIRED		

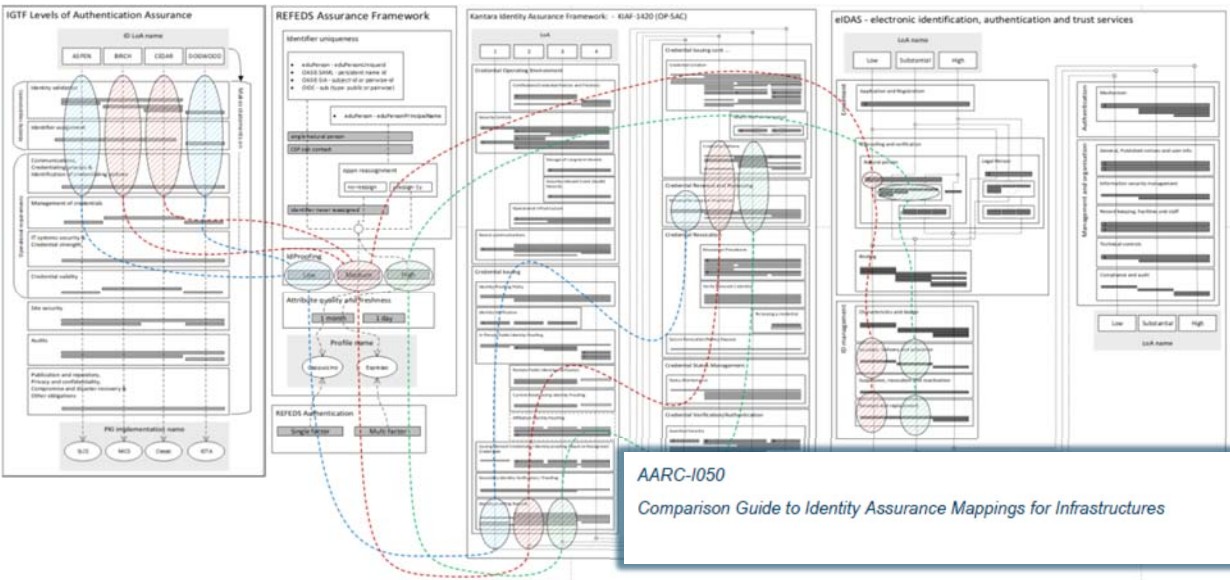
raw (non-deidentified)	pseudonymous
<i>Authentication and authorization</i>	
LoA $\geq 2$	LoA $\geq 2$
LoA $\geq 3$	LoA $\geq 2$



## REFEDS RAF Assurance in relation to Kantara, eIDAS, and IGTF profiles

		raw (non-deidentified)	pseudonymous
		<i>Authentication and authorization</i>	
		LoA $\geq 2$	LoA $\geq 2$
		LoA $\geq 3$	LoA $\geq 2$
Value	Description		
\$PREFIX\$/IAP/low	<p>Identity proofing and credential issuance, renewal, and replacement qualify to any of</p> <ul style="list-style-type: none"> <li>sections 5.1.2-5.1.2.9 and section 5.1.3 of Kantara assurance level 1 [Kantara SAC]</li> <li>IGTF level DOGWOOD [IGTF]</li> <li>IGTF level ASPEN [IGTF]</li> </ul> <p>Example: self-asserted identity together with verified e-mail address, following sections sections 5.1.2-5.1.2.9 and section 5.1.3 of [Kantara SAC].</p>		
\$PREFIX\$/IAP/medium	<p>Identity proofing and credential issuance, renewal, and replacement qualify to any of</p> <ul style="list-style-type: none"> <li>sections 5.2.2-5.2.2.9, section 5.2.2.12 and section 5.2.3 of Kantara assurance level 2 [Kantara SAC]</li> <li>IGTF level BIRCH [IGTF]</li> <li>IGTF level CEDAR [IGTF]</li> <li>section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level low [eIDAS LoA]</li> </ul> <p>Example: the person has sent a copy of their government issued photo-ID to the CSP and the CSP has had a remote live video conversation with them, as defined by [IGTF].</p>		
\$PREFIX\$/IAP/high	<p>Identity proofing and credential issuance, renewal, and replacement qualifies to any of</p> <ul style="list-style-type: none"> <li>section 5.3.2-5.3.2.9, section 5.3.2.12 and 5.3.3 of Kantara assurance level 3 [Kantara SAC]</li> <li>section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level substantial [eIDAS LoA]</li> </ul> <p>Example: the person has presented an identity document that is checked to be genuine and represent the claimed identity and steps have been taken to minimise the risk of a lost, stolen, suspended, revoked or expired document, following sections 2.1.2, 2.2.2 and 2.2.4 of eIDAS assurance level substantial [eIDAS LoA].</p>		

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



# Interpreting the graphs

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

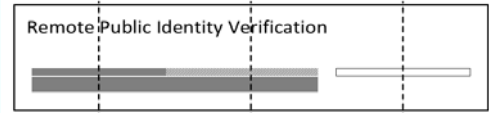
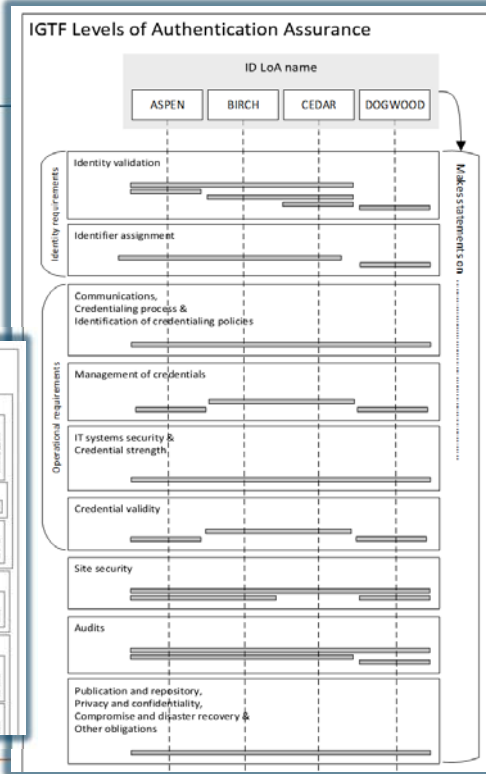
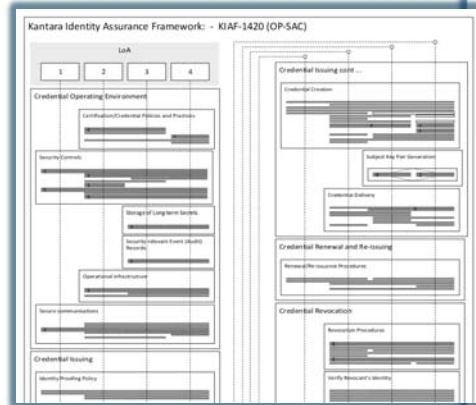


Figure 4.3: Variations of requirement representation

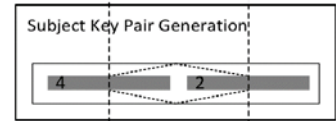


Figure 4.4: Alternate requirement choices

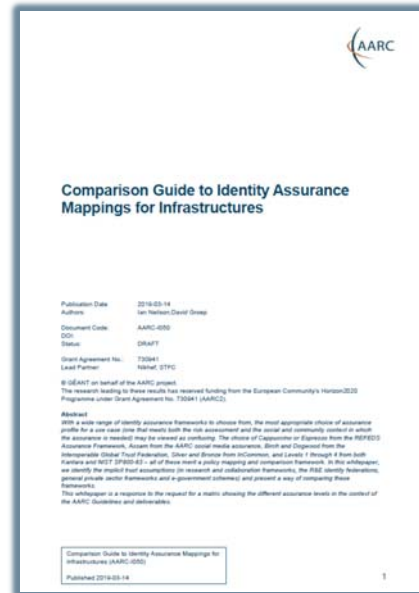
## About the mapping exercise – the AARC-I050 white paper

### Answering the questions

- why are there so many Assurance Frameworks
- why are the academic and research ones different
- why is there more than one for each
- how do they compare? what are the unique features

We attempted to answer your request ... at TIIME and in **AARC-I050!**

- addressing different audiences:  
IdP feasibility vs SP minimal requirements
- orthogonality vs component-suite approach (profiles)
- completeness vs community-focused:  
leveraging common understanding,  
*... and forgetting the grains of rice on how we got there*



# Divergence and convergence – the AUP Alignment Study

As seen in PY1

Article	Public Good Issues	Public Interests	EU	EU/EEA	EEA	EEA/IS	IS	IS/EEA	IS/EEA/IS	IS/EEA/IS/IS	IS/EEA/IS/IS/IS	IS/EEA/IS/IS/IS/IS	IS/EEA/IS/IS/IS/IS/IS	IS/EEA/IS/IS/IS/IS/IS/IS
1	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
2	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
3	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
4	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
5	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
6	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
7	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
8	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
9	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
10	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
11	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
12	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
13	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
14	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
15	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
16	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
17	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
18	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
19	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
20	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
21	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
22	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
23	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
24	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
25	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
26	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
27	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
28	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
29	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
30	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
31	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
32	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
33	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
34	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
35	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
36	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
37	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
38	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
39	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
40	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
41	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
42	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
43	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
44	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
45	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
46	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
47	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
48	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
49	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
50	...	...	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green

Support any known or	3	
ch or loss or	3	
s credentials.	3	
none number for		3
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	3
Adds: Although efforts are made to maintain confidentiality, no guarantees are given. Expanded for PI under "Personal information and data privacy"		3
	0	0



# Scaling Acceptable Use Policy and data release

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

Community specific terms & conditions

Community specific terms & conditions

Community conditions

RI Cluster-specific terms & conditions

**Common baseline AUP  
for e-Infrastructures and Research Communities**

***WISE Baseline Acceptable Use Policy and Conditions of Use***

Also picked up by e.g. SURF SCZ, eduTEAMS, CheckIn, Vorarlberg, ...

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.

## Baseline AUP at WISE SCI



### The WISE Baseline Acceptable Use Policy and Conditions of Use

Version 1.0.1 (draft), 25 Feb 2019

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

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

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

DRAFT WISE Baseline AUP template v1.0.1

When using the baseline AUP text below, curly brackets "1" (coloured blue) indicate text

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

### Other information shown to user during registration

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

# 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<sup>1</sup> 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 complete AUP for the appropriate Acceptable Use Policy and Conditions of Use.

This Acceptable Use Policy and Conditions of Use govern your access to and use (including transmission, processing, and storage of data) of the resources and services (“Services”) as granted by **studying short 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:

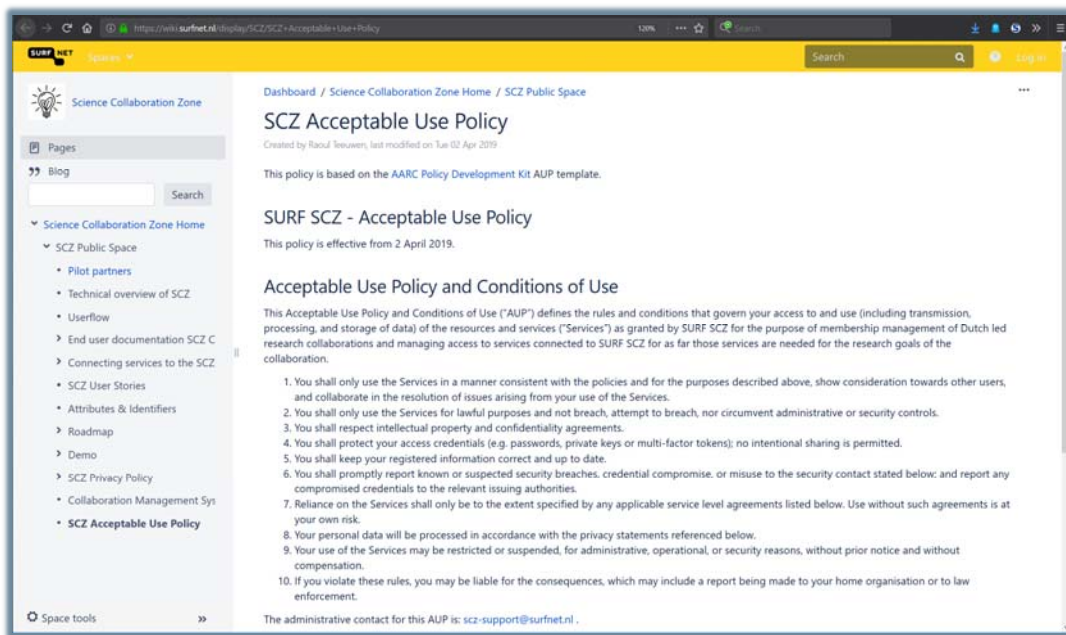
**security@nikhef.nl**

The privacy statements (e.g. Privacy Notices) are located at:

**https://www.nikhef.nl/privacy**



# Examples in action: SURF Science Collaboration Zone, eduTEAMS, ...



The screenshot shows a web browser displaying the SURF Science Collaboration Zone (SCZ) website. The page title is "SCZ Acceptable Use Policy". The breadcrumb trail is "Dashboard / Science Collaboration Zone Home / SCZ Public Space". The page was created by Raoul Teuwen and last modified on Tue 02 Apr 2019. It states that the policy is based on the AARC Policy Development Kit AUP template. Below this, there is a section for "SURF SCZ - Acceptable Use Policy" which is effective from 2 April 2019. The main content is titled "Acceptable Use Policy and Conditions of Use" and defines the rules for using services. A list of 10 conditions is provided, covering topics like consistent use, lawful purposes, intellectual property, access credentials, information accuracy, security breaches, service level agreements, privacy, and liability. The administrative contact for this AUP is scz-support@surfnet.nl.

Dashboard / Science Collaboration Zone Home / SCZ Public Space

## SCZ Acceptable Use Policy

Created by Raoul Teuwen, last modified on Tue 02 Apr 2019

This policy is based on the AARC Policy Development Kit AUP template.

### SURF SCZ - Acceptable Use Policy

This policy is effective from 2 April 2019.

### 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 SURF SCZ for the purpose of membership management of Dutch led research collaborations and managing access to services connected to SURF SCZ for as far those services are needed for the research goals of the collaboration.

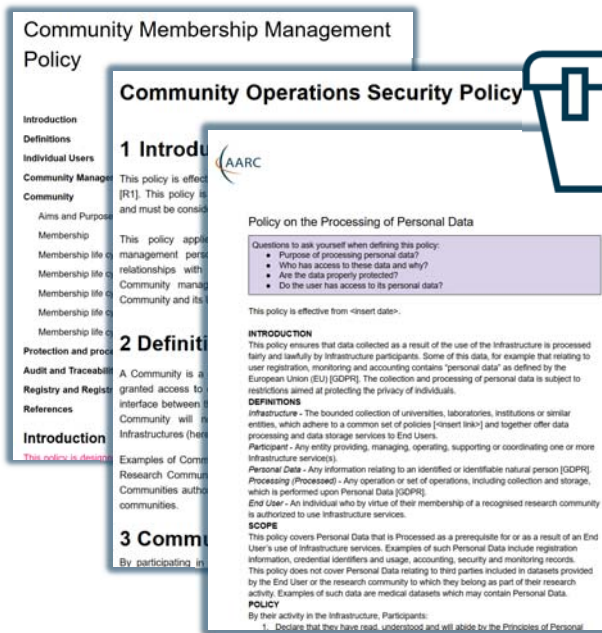
1. You shall only use the Services in a manner consistent with the policies and for the purposes described above, show consideration towards other users, and collaborate in the resolution of issues arising from your use of the Services.
2. You shall only use the Services for lawful purposes and not breach, attempt to breach, nor circumvent administrative or security controls.
3. You shall respect intellectual property and confidentiality agreements.
4. You shall protect your access credentials (e.g. passwords, private keys or multi-factor tokens); no intentional sharing is permitted.
5. You shall keep your registered information correct and up to date.
6. You shall promptly report known or suspected security breaches, credential compromise, or misuse to the security contact stated below; and report any compromised credentials to the relevant issuing authorities.
7. Reliance on the Services shall only be to the extent specified by any applicable service level agreements listed below. Use without such agreements is at your own risk.
8. Your personal data will be processed in accordance with the privacy statements referenced below.
9. Your use of the Services may be restricted or suspended, for administrative, operational, or security reasons, without prior notice and without compensation.
10. If you violate these rules, you may be liable for the consequences, which may include a report being made to your home organisation or to law enforcement.

The administrative contact for this AUP is: [scz-support@surfnet.nl](mailto:scz-support@surfnet.nl).

# Implementing Snctfi in community policies

## 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' so that the BPA proxy model will scale out?



**Community Membership Management Policy**

**Community Operations Security Policy**

**Policy on the Processing of Personal Data**

Questions to ask yourself when defining this policy:

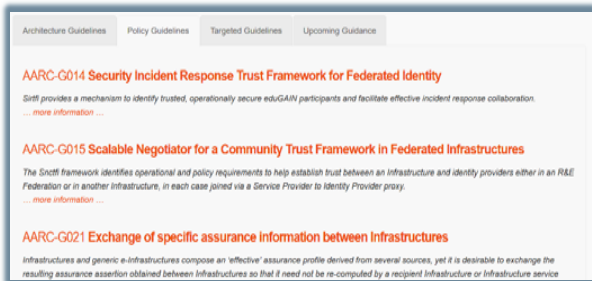
- Purpose of processing personal data?
- Who has access to these data and why?
- Are the data properly protected?
- Do the user has access to its personal data?

**PDK**

## Main achievements in Researcher-Centric Policy

<p>Interoperable authentication assurance across federations also for high-assurance use cases</p>	<p>➔</p>	<p>REFEDS RAF adoption shown to work &amp; <i>e.g.</i> adopted in lieu of complex frameworks by CILogon Silver</p>
<p>'1050' white paper on assurance frameworks</p>	<p>➔</p>	<p>Untangled some assurance spaghetti</p>
<p>WISE Baseline Acceptable Use Policy</p>	<p>➔</p>	<p>Directly supported eduTEAMS and CheckIn, adopted in other places, both nationally and thematically</p>
<p>Snctfi-compatible community policies</p>	<p>➔</p>	<p>Fill the need of research communities for a complete Policy Development Kit</p>
<p><b>After AARC</b></p>	<p>WISE and REFEDS committed to supporting research communities in development</p> <p>EOSCH ISM and GN43-EnCo: support communities in policy adoption and design</p>	

## Policy and Best Practices Harmonisation



Architecture Guidelines | Policy Guidelines | Targeted Guidelines | Upcoming Guidance

**AARC-G014 Security Incident Response Trust Framework for Federated Identity**  
Snctfi provides a mechanism to identify trusted, operationally secure eduGAIN participants and facilitate effective incident response collaboration.  
... more information ...

**AARC-G015 Scalable Negotiator for a Community Trust Framework in Federated Infrastructures**  
The Snctfi framework identifies operational and policy requirements to help establish trust between 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.  
... 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 obtained between Infrastructures so that it need not be re-computed by a recipient Infrastructure or Infrastructure service



*Policy Development Kit*

*FIM4R version 2*

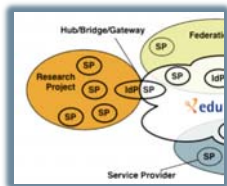
*WISE SCI and SCCC-JWG*

## Task 4

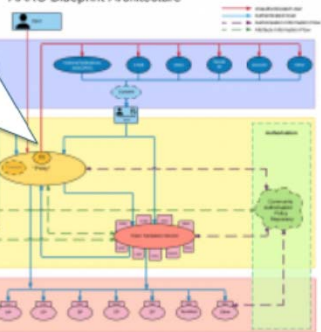
# Policy Development Engagement and Coordination

# Policy Development Kit

- Bring together a consistent suite
- based on e-Infrastructure best practices in particular EGI, WLCG, and the JSPG
- cover all of the *Snctfi* requirements



AARC Blueprint Architecture



## 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
GEANT 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

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

### Get Started with Policies

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

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

Supporting documents are available below for download.

### Download Material

Show 100 entries

Search:

Document	Who should complete the template?	Audience	Description	Link
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together	<a href="#">Google Doc</a>
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template procedure provides a step-by-step breakdown of actions to take following a security incident.	<a href="#">Google Doc</a>
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.	<a href="#">Google Doc</a>
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.	<a href="#">Google Doc</a>
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.	<a href="#">Google Doc</a>
Deliver on the	Infrastructure Management & Data	Research Community	This document defines the obligations on Infrastructure Participants when	<a href="#">Google</a>

joint work  
with peers in



# Templates and guidance on how to implement

## Questions to ask yourself when defining this policy:

- Which identity providers are acceptable for your infrastructure? SAML Identity Federation IdPs? Social providers such as Google, Facebook etc?
- How much certainty does your community require of the identity? Review each of the elements (personal accounts, uniqueness, freshness, vetting quality and

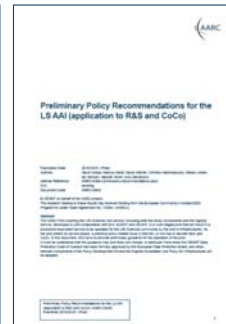
capability at their home organisation?

- Do your services, or a subset, require step-up (multi-factor) authentication?

The following chart can be used to help determine an appropriate assurance profile for you. Refer also to [AARC Guideline 21](#):

Should identifiers be unique, personal and traceable?	Should identifiers be unique across the infrastructure?	How fresh do attributes need to be?	What kind of ID Proofing is required?	Is Multi-Factor Authentication required?
Unspecified	Unspecified	Unspecified	Unspecified	Unspecified
Yes	Yes	1 month	Low (self asserted)	Single factor authentication
			Medium (e.g. postal credential delivery)	Multi-factor authentication
			High (e.g. face to face)	

AARC Assam  
 IGTF Dogwood  
 RAF Cappuccino  
 IGTF Birch  
 RAF Espresso



## Adoption – by new (national) proxies, and: PDK seen as a ‘neutral go-to’



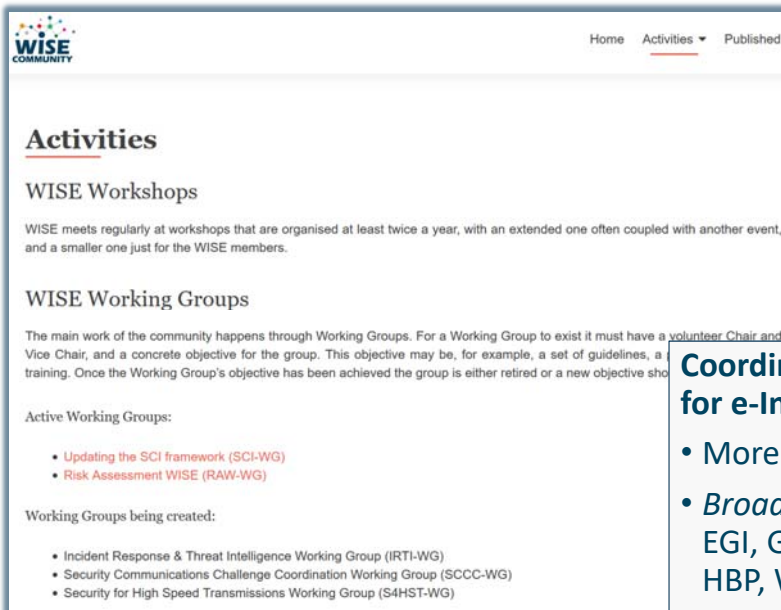
Policy Development Kit showing up without me prompting in a Dutch collaborative science presentation ...  
(slides: Raoul Teeuwen, January 2019)

And much more (do we want a list?):

- PDK adoption: by HDF, WLCG
- MMS services adopting AUP
- LSAAI R&S+DPCoCo
- EOSC-HUB and WLCG policy framework revision
- AUP by many (even by a FH)
- FIM4R impact
- ...



# Bringing Infrastructures Together – the WISE road



Home Activities Published

## Activities

### WISE Workshops

WISE meets regularly at workshops that are organised at least twice a year, with an extended one often coupled with another event, and a smaller one just for the WISE members.

### WISE Working Groups

The main work of the community happens through Working Groups. For a Working Group to exist it must have a volunteer Chair and Vice Chair, and a concrete objective for the group. This objective may be, for example, a set of guidelines, a training. Once the Working Group's objective has been achieved the group is either retired or a new objective shown.

Active Working Groups:

- Updating the SCI framework (SCI-WG)
- Risk Assessment WISE (RAW-WG)

Working Groups being created:

- Incident Response & Threat Intelligence Working Group (IRTI-WG)
- Security Communications Challenge Coordination Working Group (SCCC-WG)
- Security for High Speed Transmissions Working Group (S4HST-WG)

## Coordinating Information Security for e-Infrastructures

- More than just the home of SCI
- *Broad collaboration:* steering group with EGI, GEANT, EUDAT, PRACE, XSEDE, OSG, TrustedCI, HBP, WLCG, LIGO, SURF, CERN, CSC, JSC, & Nikhef.



# Example of WISE coordination – evolving the *Sirtfi* challenges



*The first Sirtfi challenges were run 'by AARC' to establish the guidelines*

**But: many 'logical' candidates that could all run the test**

**... and all have an interest in knowing the result so to establish trust!**

- eduGAIN
- GEANT.org
- any EOSC-HUB and e-Infrastructure CSIRT teams
- the IGTF (as it leverages federated identity in RCauth, TCS, CILogon)
- each of the e-Infrastructures XSEDE, EGI, EUDAT, PRACE, OSG, HPCI, ...
- every research infra with an interest: WLCG, LSAI, BBMRI, ELIXIR, ...

```
## AARC Information - Limited Distribution ##
## see https://www.us-cert.gov/ftp for distribution restrictions ##
Summary of Incident (eduGAIN-201810243400027)
-----
A compromise account was detected by an SP registered in eduGAIN. The incident
was handled by the user's IAP who blocked the user and notified the SPs that
were used by the offender to check their systems and possibly suspend the user
during the incident resolution.

The incident is closed now. The user's credentials have been re-set and the
user account shall be activated on systems that decided to suspend it before.

Details
-----
On 23rd of Oct 2018 an SP (identified as https://orcis.org/saml2/sp/1, from
[SPName]) alerted the Jisc IAP (https://isp.jisc.ac.uk/dp/vhobolath, UK
Federation) about unauthorized access by an account from the IAP. In response
to the alert the IAP suspended the user account and identified the SPs that
were accessed by the offender. The SPs and corresponding federations were
subsequently contacted by the IAP who shared details about the users and
accesses.

Three SPs were involved:
https://proy.mnatelescope.org/sp (AARF)
- provided detailed response, including activities, access times and IP
  addresses used by the offender
- suspended the user account

https://orcis.org/saml2/sp/1 (SURFconext)
- reported initially the incident
- suspended the user account

https://ibr.usc.fj/akobolath (SPN-A&I / HMAA)
- logs checked, simulated suspension

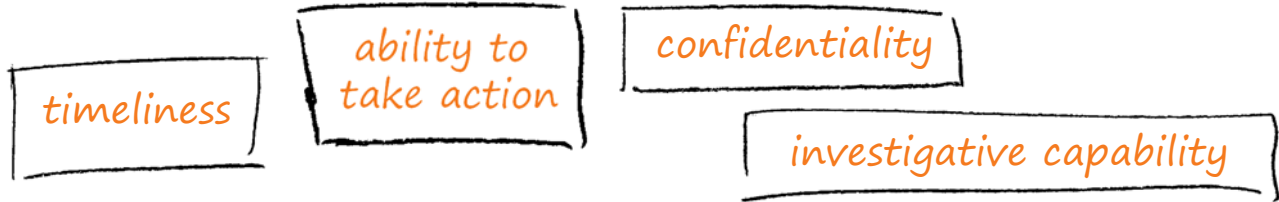
Timeline (as per DTR)
-----
2018-10-23 Compromised account detected by ORCID SP, reported to Jisc IAP. Jisc
  contacts affected SP.
2018-10-23 13:32 [UTC] User suspended at ORCID SP
2018-10-23 14:01 [UTC] User suspension (incomplete) at ibr_eur.fj SP
2018-10-23 20:09 [UTC] UK Federation warns MNATelescope SP about compromised
  account.
2018-10-24 00:53 [UTC] MNATelescope responds, notifying eduGAIN, too.
2018-10-24 00:53 [UTC] User suspended at MNATelescope.
2018-10-24 13:12 [UTC] Details provided by Jisc to eduGAIN (user suspended at
  IAP, confirmed SPs that were contacted)
2018-10-24 15:21 - 15:48 [UTC] Jisc informs Federations of affected SP about
  the incident
2018-10-26 User's credentials reset, user unblocked at IAP
```

and any institution (or person) with access to <https://mds.edugain.org/> can run them, of course!

*'so in a short while, all the email in the world will be on Sirtfi Incident Response tests??'*

## Challenge elements – what is valued or expected might differ ...

A single test and challenge can answer one **or more** of these questions



- when data available: infrastructure can set its *own level* of expectancy and gives *deep trust*
- assessment supported with community controls (suspension) gives a *baseline compliance*

### Communications challenges build ‘confidence’ and trust – an important social aspect!

- different tests bring complementary results: responsiveness vs. ability act , or do forensics
- unless you run the test yourself, you may not be growing more trust in the entities tested
- for a ‘warm and fuzzy feeling of trust’, share results: but this is sociologically still challenging ...

# 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, and level of confidentiality maintained. However, it is a well-recognised fact that data that is not

**WISE**  
**SIG-ISM**  
**REFEDS**  
**IGTF**

## Main achievements in Policy Development Coordination

Policy Development Kit	→	Lasting resource for both emerging and established communities
	→	Supports alignment also of e-Infrastructures
	→	Continuous evolution happening in practice: security policy for WLCG, LIGO, and EOSCH
WISE and SCCC JWG coordination (SIG-ISM, REFEDS, EOSCH-ISM)	→	AARC brought together security coordination and articulated need across many domains

### **After AARC**

WISE: new working groups like the SCCC JWG, and evolution in SCI

FIM4R, GN4-3 EnCo, EOSCHUB-WP44, AEGIS, REFEDS, GN4-EOSCH-CA!



*WISE SCI and SCCC*

*IGTF*

*REFEDS*

*SIG-ISM*

*FIM4R*

*[aarc-community.org](http://aarc-community.org)*



*Beyond AARC*

**The Community Beyond the Project**

- *Sirtfi & the Registry*
- *Communications Challenges*
- *Attribute Authority operations*
- *SCI evolution and its assessment to support trust*
- *Acceptable Use Policy*
- *Assurance profiles: adoption & suitability in high-risk cases*
- *Policy Development Kit evolution*
- *Data Protection guidance for global research collaboration*

WISE-community

IGTF

REFEDS

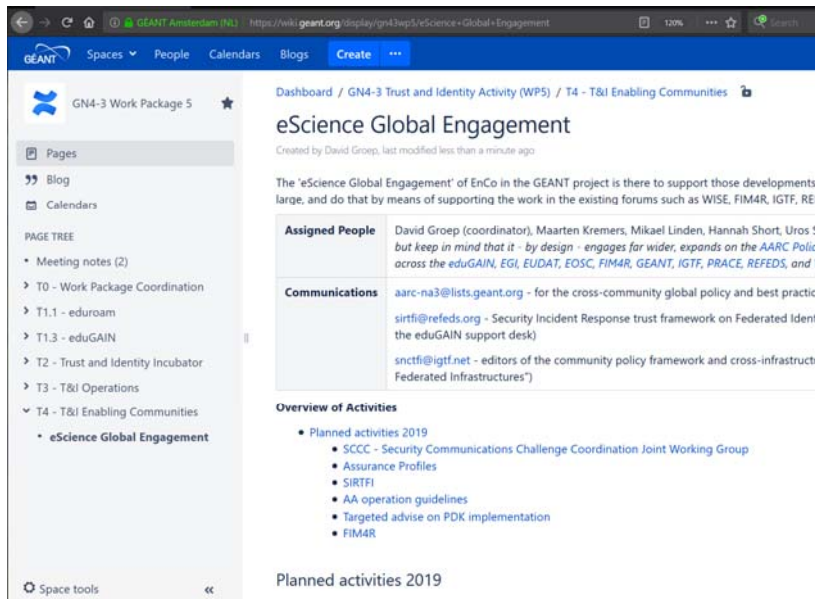
FIM4R

AEGIS

Collaboration EOSCH-GN4

national, domain and community groups

# AARC Community – towards EOSChub, GEANT4-3, and the Research Infra's



Dashboard / GN4-3 Trust and Identity Activity (WP5) / T4 - T&I Enabling Communities

## eScience Global Engagement

Created by David Groep, last modified less than a minute ago

The 'eScience Global Engagement' of EnCo in the GEANT project is there to support those developments in large, and do that by means of supporting the work in the existing forums such as WISE, FIM4R, IGTf, REFEDS

<b>Assigned People</b>	David Groep (coordinator), Maarten Kremers, Mikael Linden, Hannah Short, Uros St but keep in mind that it - by design - engages far wider, expands on the AARC Policy across the eduGAIN, EGI, EUDAT, EOSC, FIM4R, GEANT, IGTf, PRACE, REFEDS, and W
<b>Communications</b>	<p>aarc-na3@lists.geant.org - for the cross-community global policy and best practice</p> <p>sirtfi@refeds.org - Security Incident Response trust framework on Federated Identity the eduGAIN support desk)</p> <p>snctfi@igtfnet.net - editors of the community policy framework and cross-infrastructure Federated Infrastructures")</p>

**Overview of Activities**

- Planned activities 2019
  - SCCC - Security Communications Challenge Coordination Joint Working Group
  - Assurance Profiles
  - SIRTFI
  - AA operation guidelines
  - Targeted advise on PDK implementation
  - FIM4R

Planned activities 2019



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

[wiki.geant.org/display/AARC/AARC+Policy+Harmonisation](https://wiki.geant.org/display/AARC/AARC+Policy+Harmonisation)

# Thank you Any Questions?

davidg@nikhef.nl



<http://aarc-project.eu/>



© GEANT on behalf of the AARC project.

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 7318941 (AARC2).