



Authentication and Authorisation for Research and Collaboration

Policy in harmony: our best practice

A Kit List for Communities

David Groep

NA3 Coordinator

Dutch National Institute for Subatomic Physics Nikhef

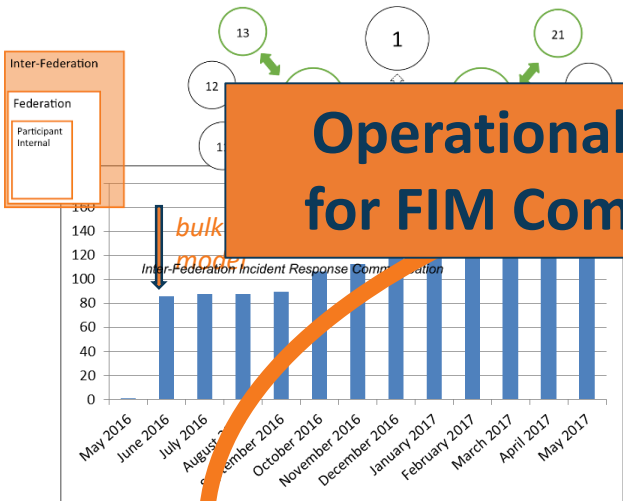


AARC2 AHM3 Athens meeting

April 2018

A tour of the policy space in AARC2

Operational Security for FIM Communities



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
- Ongoing work: text needs to allow for (community) attribute authorities

supporting policies for Infrastructures

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



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.

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 RAE Federation or in another infrastructure, in each case joined via a Service Provider to Identity Provider proxy.

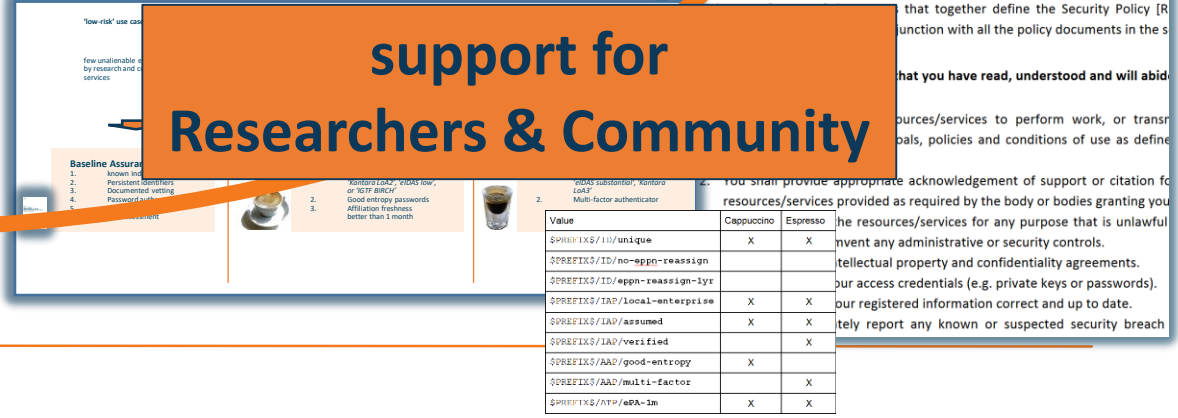
AARC-G021 Exchange of specific assurance information between Infrastructures
Infrastructures and generic e-infrastructure compose an 'effective' assurance profile derived from several sources, yet it is desirable to exchange the resulting assurance assertion obtained between infrastructures so that it need not be re-computed by a requesting infrastructure or infrastructure service provider. This document describes the assurance profiles recommended to be used by the infrastructure AAI Proxies between infrastructures.

3 Community Operations Security Policy

Engagement and Harmonisation



support for Researchers & Community



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 defines the acceptable use of the resources/services provided as required by the body or bodies granting you access to the resources/services for any purpose that is lawful and does not infringe any administrative or security controls, intellectual property and confidentiality agreements, or our access credentials (e.g. private keys or passwords). You must report any known or suspected security breach to the body or bodies granting you access to the resources/services to perform work, or transfer data, policies and conditions of use as defined in this policy.

Value	Cappuccino	Espresso
\$PRFX/ID/unique	X	X
\$PRFX/ID/no-epn-reassign		
\$PRFX/ID/epn-reassign-lyr		
\$PRFX/ID/local-enterprise	X	X
\$PRFX/ID/assumed	X	X
\$PRFX/ID/verified		X
\$PRFX/AA/good-entropy	X	
\$PRFX/AA/multi-factor		X
\$PRFX/ATP/ePA-1m	X	X

Improving operational security readiness for FIM (“T1”)

1. Define & test model for organizations (IdP) to share info on account compromises
2. *Attribute authority operations (security) practices*
3. *Access control, integrity and availability of IdP-SP-Proxies*



Detect, connect, mitigate

- 243 IdPs now support Sirtfi
- and 65 SPs and proxies

What happens when you try the model?

How does this work when you involve community AAs?

How can Sirtfi protect the communities and proxies?

31-01-2018

Incident Response Test Model for Organisations

Deliverable MNA3.3

Contractual Date: 01-02-2018
Actual Date: 31-01-2018
Grant Agreement: 730941
No.:
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)

Hannah Short: before coffee

Service-centric policy support: ‘helping out’ the Infrastructures (“T2”)

- *Develop traceability and accounting data-collection policy framework based on SCI*
 - e.g. why SCI & peer review may more appropriate than trying 27k and audits for Infrastructures?
 - construct (‘service’ part of) a Policy Development Kit for Infrastructures
- **Impact of GDPR and risk assessment guidance**
- *Protection of aggregations of accounting data by (user) communities*
- **Policy recommendations accompanying technical ‘JRA1’ recommendations**

DNA3.1 - Report on the coordination of accounting data sharing amongst Infrastructures

(initial phase)

Abstract	1
Introduction	1
Current legal structure - GDPR	4
Data Protection Impact Assessment - DPIA	4
Risk assessment and DPIA impact on research communities	4
References	4

Uros Stevanovic: after coffee

Researcher-centric policy support (“T3”)

Recommendations for baseline “policy profiles” for FIM Communities & Infrastructures

- for users, communities, identity providers: reducing “policy silos” hindering interoperation
- **commonality between acceptable use policies**

- **through assurance profiles**

Mikael & Jule: Assurance after Coffees

- support community management, also to ease use of the generic e-Infrastructures
- can you support trustworthy community operations? How should a community collaborate in the Infra ecosystem, now that we have very ‘powerful’ communities?*

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 for which you access.
2. You shall acknowledge support or citation for your use of 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 any activity that is prohibited by applicable laws, regulations, or policies.
4. You shall not use the resources/services to perform any activity that is prohibited by applicable laws, regulations, or policies.
5. You shall not use the resources/services to perform any activity that is prohibited by applicable laws, regulations, or policies.
6. You shall not use the resources/services to perform any activity that is prohibited by applicable laws, regulations, or policies.
7. You shall not use the resources/services to perform any activity that is prohibited by applicable laws, regulations, or policies.

Community Membership Management Policy

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

Ian Neilson: after coffee

Policy guidance: generic and community-targeted

Guidelines

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

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


[Architecture Guidelines](#)
[Policy Guidelines](#)
[Targeted Guidelines](#)
[Upcoming Guidance](#)

AARC-G014 Security Incident Response Trust Framework for Federated Identity

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

[... more information ...](#)

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

The Sncffi framework identifies operational and policy requirements to help establish trust between Infrastructures or in another Infrastructure, in each case joined via a Service Provider to Identity Providers.

[... more information ...](#)

AARC-G021 Exchange of specific assurance information between

Infrastructures and generic e-Infrastructures compose an 'effective' assurance profile derived from the 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 ...](#)

[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 EGI, EUDAT and GÉANT, will result in a production-equivalent service to be operated for the Life Sciences community by the joint e-Infrastructures. As the pilot enters its second phase the LS AAI has to declare compliance to R&S and CoCo towards the R&E federations. This document provides preliminary guidance for the operators of the pilot LS AAI.

[... more information ...](#)

Engagement and coordination with the global FIM community (“T4”)



Develop

Through

- *WISE/SCI*
- *REFEDS*
- *IGTF*

... and all willing policy & CSIRT groups



AEGIS

Adopt

In your Community, use

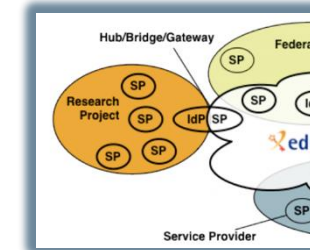
- *Persistent, non-reassigned identifiers*
- *Snctfi*
- *Trusted Community Attributes*

Self-assessment and peer review methods



AARC Engagement & FIM4R
help us progress by adopting results

assessment of SCIV2



Snctfi

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures

- Derived from SCI, the framework on *Security for Collaboration among Infrastructures*
- Structure for the wider policy development kit

Dave Kelsey: FIM4R before coffee

We will need your input today ... and thereafter!

Operational Security and Incident Response

- Beyond *Sirtfi*, involving the proxies and proxy operators: we need volunteers to try (& ‘buy’)
- Cross-domain trust groups spanning Infrastructures & eduGAIN Support Desk to aid resolution

Service-centric policies

- Community Risk Assessment, GDPR, and TF-DPR impact on accounting (and your use cases!)
- Policy framework: what do you need in a policy development kit for Infrastructures?

e-Researcher-Centric Policies

- Assurance profiles: exchanging information between Infrastructures and the ‘Snctfi’ scenario
- Align practices for community policies, and a baseline AUP

Policy Development Engagement and Coordination

- Policy development and engagement ‘kit’ – via existing groups, and trainings, WISE, IGTF, and FIM4R
- Targeted guidance for (AARC) use cases and communities – [‘/guidelines’](#)

Best Practice session

- 10:00-11:00 *10.00 Introduction to the NA3 activities (DavidG)*
 10.15 Operational Security: the Sirtfi Challenge (Hannah)
 10.35 FIM4R and the FIM4R Paper (DaveK)
- 11:00-11:30 **Break**
- 11.30 REFEDS Assurance evolution (Mikael, Jule)*
 11.45 Data Protection and Risk Assessment for communities (Uros)
 and input from the AARC use cases (Uros)
- 11:30- 13:00 *12.15 Acceptable Use Policy alignment study and*
 towards a basic AUP (IanN)
 12.35 Policy Development Kit: supporting communities
 with template policies (Hannah, Uros)

Thank you

Any Questions?

davidg@nikhef.nl



<https://aarc-project.eu>



© GÉANT on behalf of the AARC project.

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