



Authentication and Authorisation for Research and Collaboration

Supporting communities with harmonized policy

as well as best practices, templates, and guidelines

David Groep

NA3 Coordinator

Dutch National Institute for Subatomic Physics Nikhef



I2GS Federated ID Topics

May 2018

Policies and practices to support FIM for Research & Collaboration



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-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 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



guidance 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, together with the Security Policy (R&C), defines the Security Policy (R&C) in conjunction with all the policy documents in the system. You have read, understood and will abide by the terms, conditions, policies and conditions of use as defined in the resources/services provided as required by the body or bodies granting you access to the resources/services for any purpose that is unlawful or in breach of any administrative or security controls. You must report any known or suspected security breach to the appropriate authorities.

Baseline Assurance

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

A Security Incident Response Trust Framework – Sirtfi summary

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



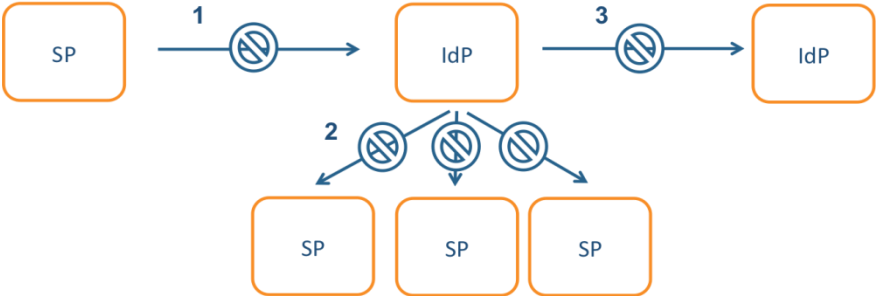
Traceability

- 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

Incident response process evolution in federations – beyond this first step

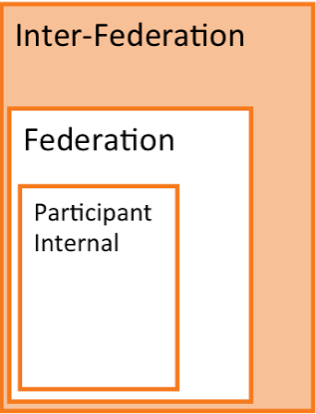


Incident Response Communication, communication blocks



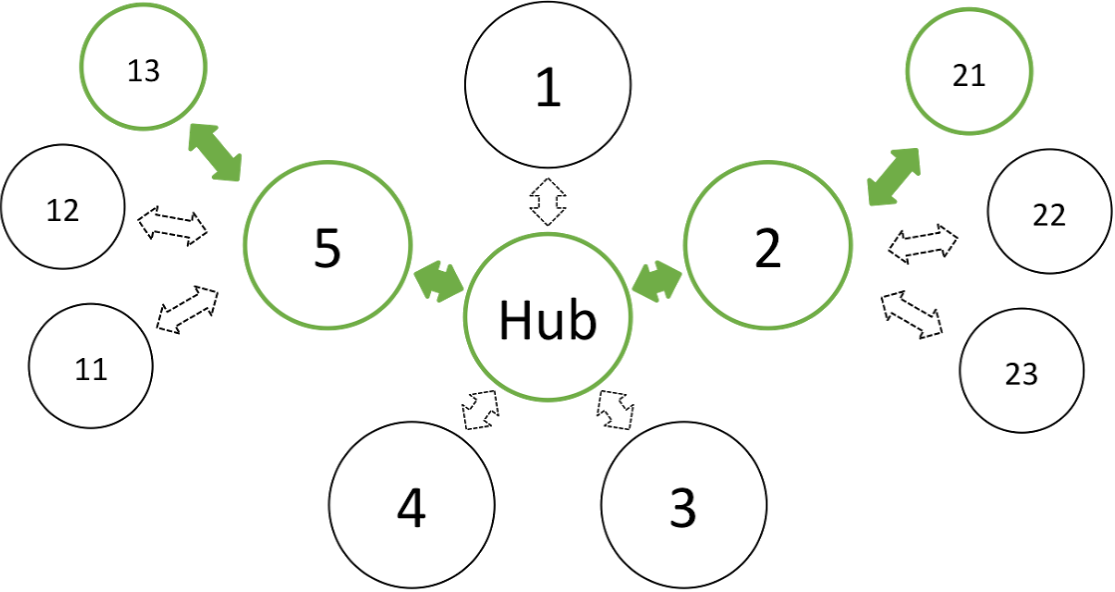
Challenges

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



Solution

- More communications challenges
- Instantly available tooling and defined role for all parties. And: pick a coordinator



Inter-Federation Incident Response Communication

Guidance for research and generic Infrastructures

- **Impact of GDPR and risk assessment guidance**
- *Protection of aggregations of accounting data by (user) communities*
- *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**

Do I Need A DPIA Risk Assessment a guide for communities

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

Guidance for research communities in the Infrastructure ecosystem

- commonality between acceptable use policies using a layered approach
- through assurance profiles
REFEDS RAF, but *also* cross Infrastructure:
- Cappuccino, Espresso
- BIRCH and DOGWOOD
- Assam (social-ID authenticator assurance)
- 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 way you access.
2. Acknowledgement of support or citation for your use of the resources/services for any purpose that is unlawful and not (attempt to) breach confidentiality agreements.
3. Do not attempt to circumvent security controls (e.g. generate keys or passwords).
4. Do not attempt to tamper with or delete data.
5. Do not attempt to tamper with or delete data.
6. Do not attempt to tamper with or delete data.
7. Do not attempt to tamper with or delete data.

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 the Infrastructure ecosystem.

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

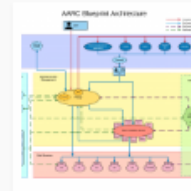
By participating in the Infrastructure, a Community Manager agrees to the conditions laid

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 Federations 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 community

Co-develop

Through

- WISE, SCI
- REFEDS
- IGTF

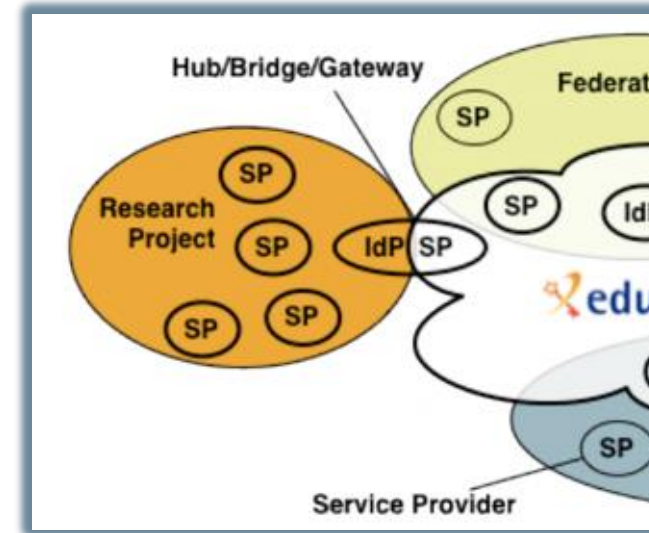
Or drive requirements in

- FIM4R

/Guidelines

In your Community, use

- Unique non-reassigned identifiers
- Snctfi policy structures
- 'Community First' Attributes
- backed with Self-assessment and peer review methods



Snctfi v1.0

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

Licia Florio (GÉANT), David Group (Nikhef), Christos Karatziopoulos (GÉANT), David Kelsey (STFC), Mikael Lindén (CS3), Jan Nilsson (STFC), Stefan Partow (Jisc), Wolfgang Pempe (DFN), Vincent Ribaillier (DRIS-CNRS), Mischa Salle (Nikhef), Hannah Short (CERN), Uros Stevanovic (KIT) and Gerben Venekamp (SURFsaara)

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 its RAE 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.

Snctfi

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures

- Derived from SCI, the framework on *Security for Collaboration in Infrastructures*
- Basis for **policy development kit** – *identify gaps in policy suite and leverage AARC templates*

Thank you Any Questions?

davidg@nikhef.nl



<https://aarc-project.eu>

