Authentication and Authorisation for Research and Collaboration

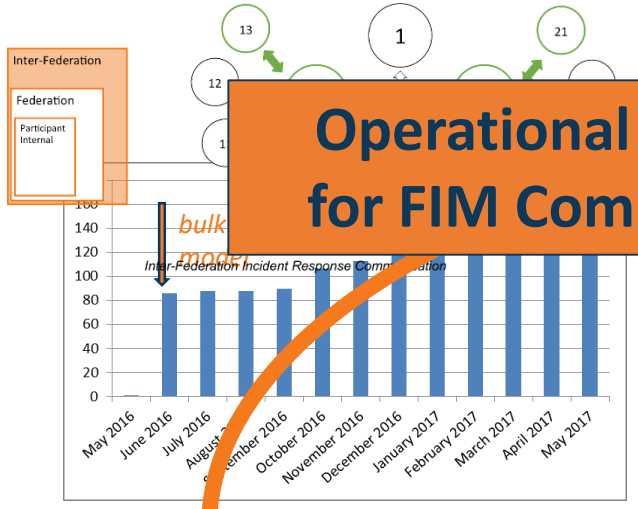
Supporting communities with harmonized policy

as well as best practices, templates, and guidelines

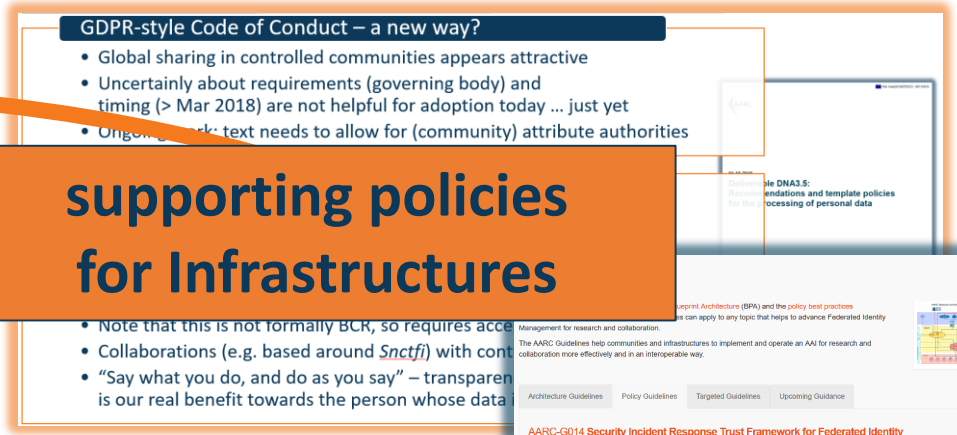
David Groep
NA3 Coordinator
Dutch National Institute for Subatomic Physics Nikhef

I2GS Federated ID Topics
May 2018

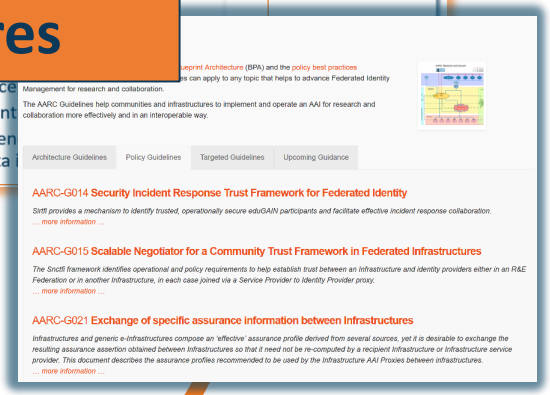
Policies and practices to support FIM for Research & Collaboration



Operational Security for FIM Communities

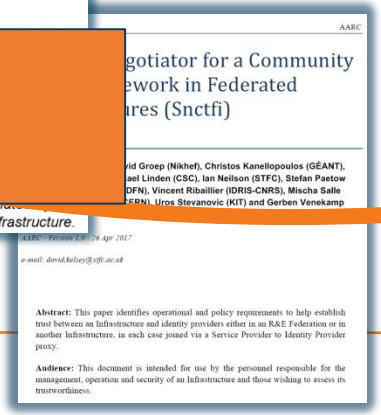


supporting policies for Infrastructures

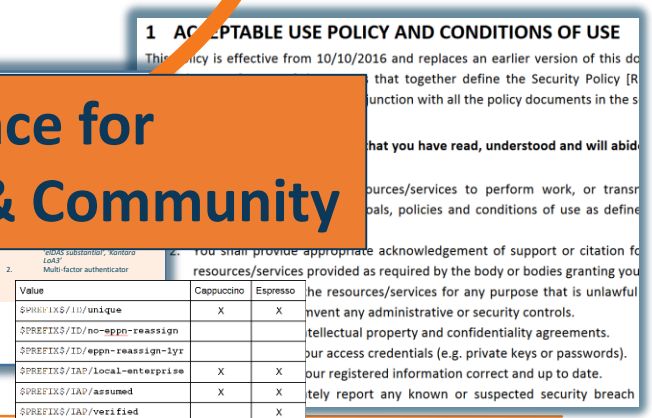


Sctfi

Engagement and Harmonisation



guidance for Researchers & Community



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

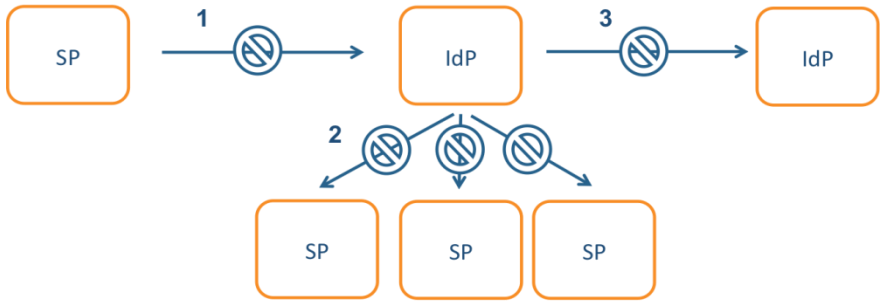
- Improve the usefulness of logs
- Ensure logs are kept in accordance with policy

Participant Responsibilities

- Confirm that end users are aware of an appropriate AUP

see http://refeds.org/sirtfi

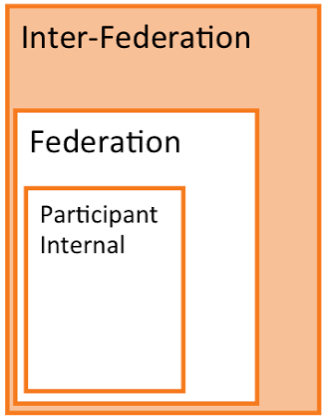
Incident response process evolution in federations – beyond this first step



Incident Response Communication, communication blocks

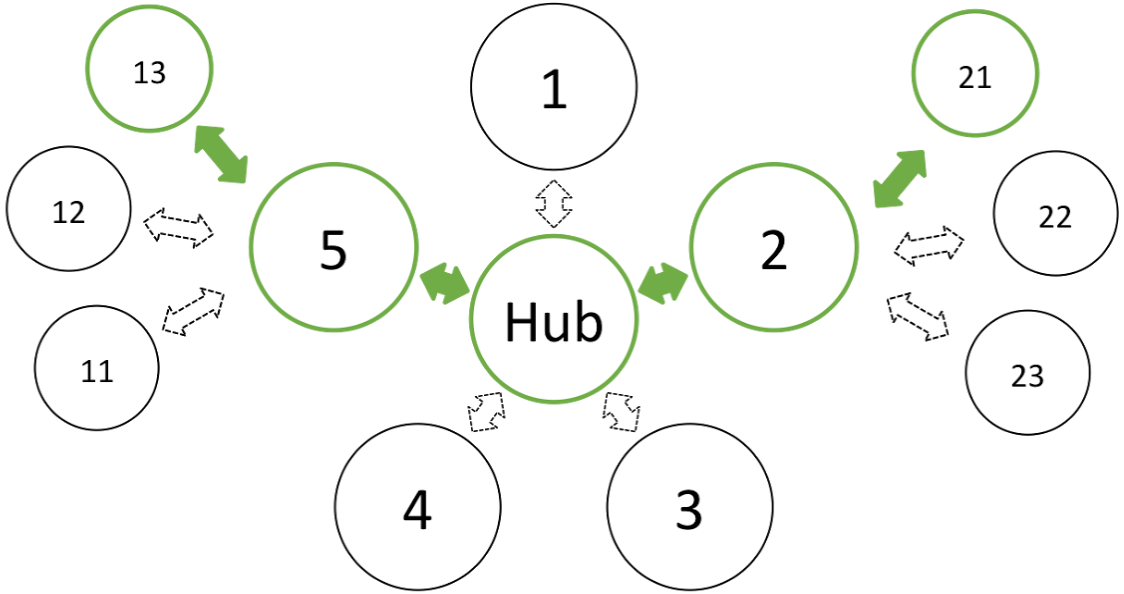
Challenges

- 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

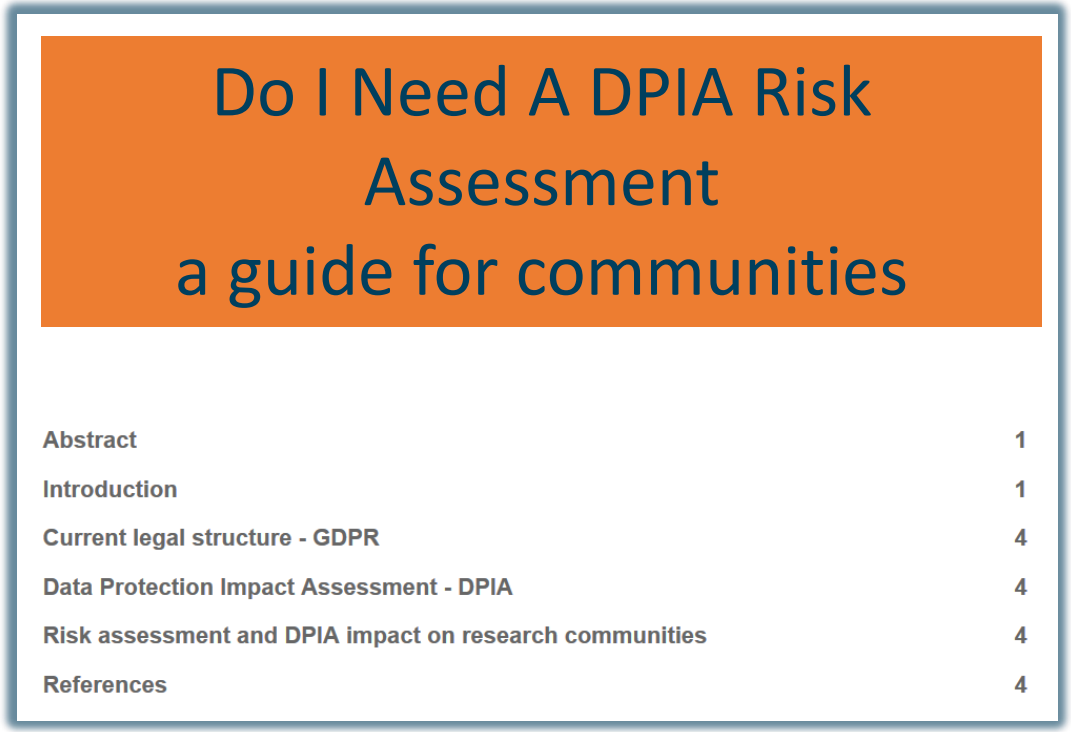
- More communications challenges
- Instantly available tooling and defined role for all parties. And: pick a coordinator



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**

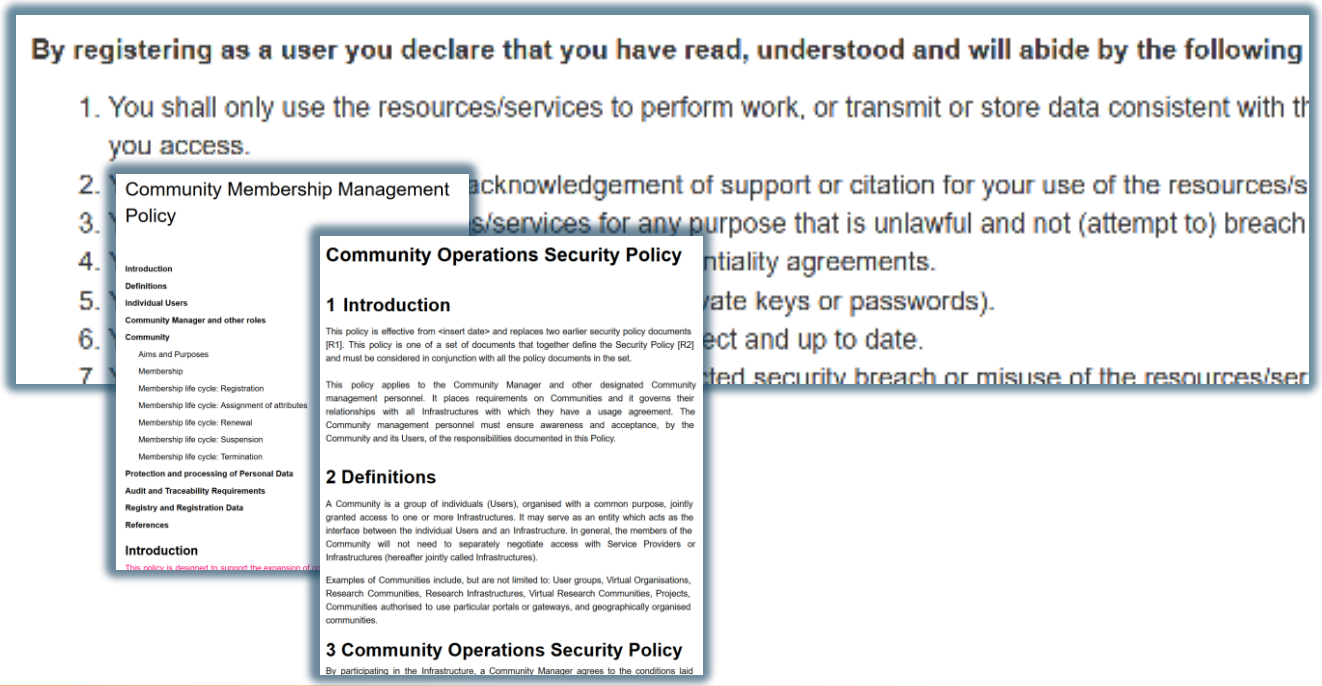


Guidance for research communities in the Infrastructure ecosystem

- **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?



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 Snctfi framework identifies operational and policy requirements to help establish trust be
Federation or in another Infrastructure, in each case joined via a Service Provider to Identity
... more information ...

AARC-G021 Exchange of specific assurance information betwe

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

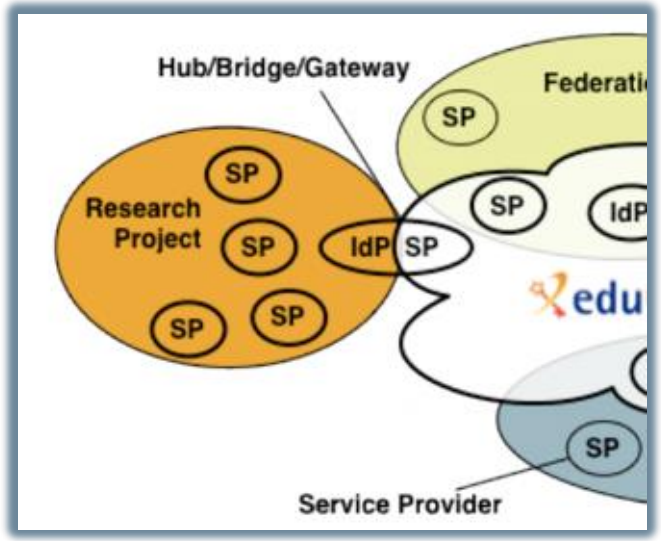
Or drive requirements in

- *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


Snctfi v1.0 AARC

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

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

AARC - Version 1.0 - 26 Apr 2017

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

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

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

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

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).