Authentication and Authorisation for Research and Collaboration

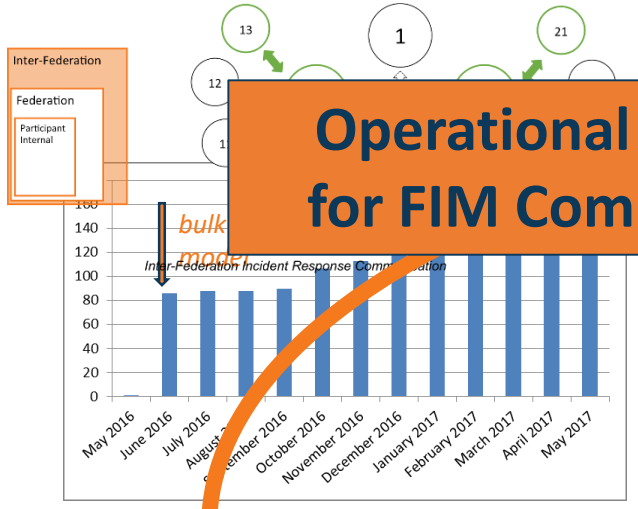
You ain’t seen nothing yet in **Policy and Best Practice Harmonisation** *where we are and where we go …*

David Groep *for the entire AARC Policy Team*

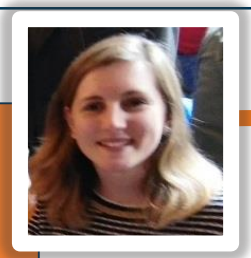
Nikhef

AARC2 AHM4 meeting
19 November 2018
Milano, IT

How can policy help you ease collaboration? A holistic view



Operational Security for FIM Communities



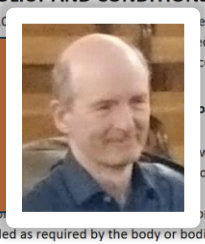
SIRTFI
Security Incident Response Trust Framework for Federated Identity

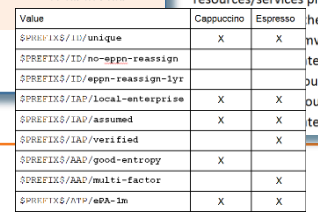
Sctfi

supporting policies for Infrastructures

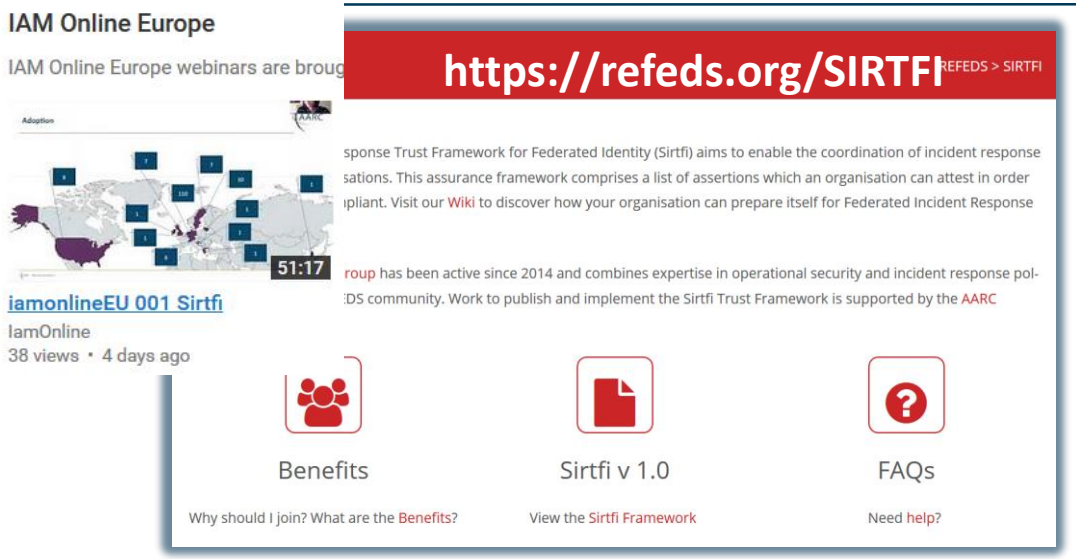
engagement and coordination

support for Researchers & Community





Sirtfi – presentation, training, adoption in AARC2



Services increasingly **demand and use Sirtfi**

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

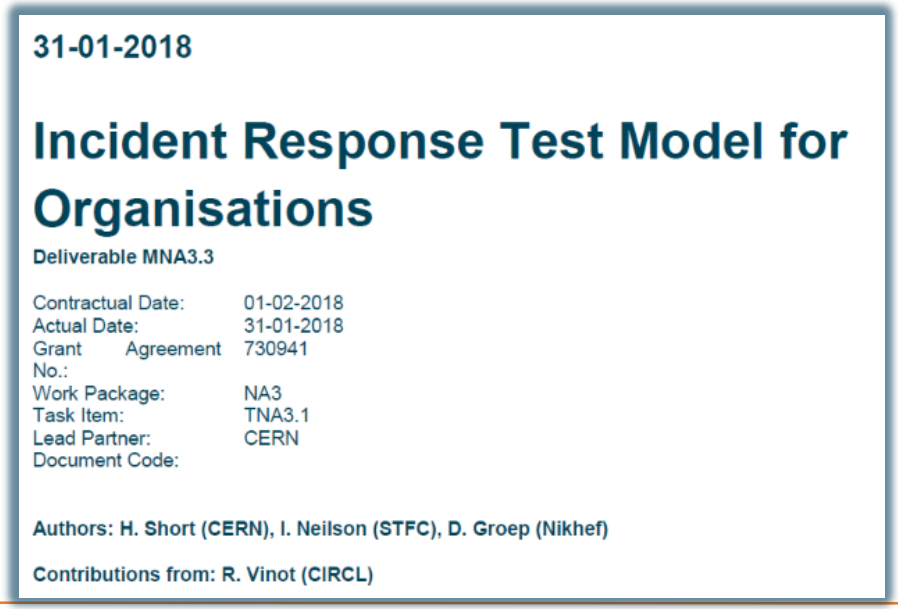
and

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

Promotional activities successful

- REFEDS, Internet2 TechX, ISGC Taipei, TNC, TF-CSIRT, FIM4R, Kantara webinars, …
- **Now 427 entities** (but inly in 25 federations)

- Ready to move to the next phase:


31-01-2018

Incident Response Test Model for Organisations

Deliverable MNA3.3

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

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

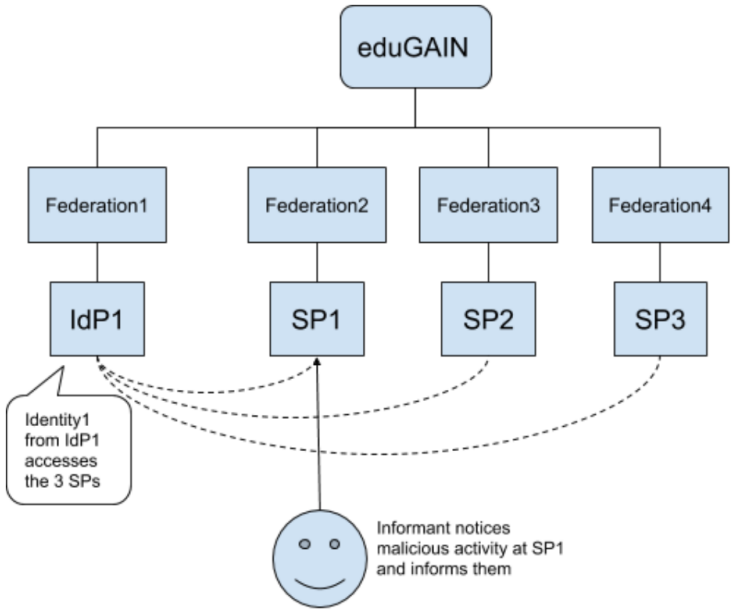
Contributions from: R. Vinot (CIRCL)

'I Need Sirtfi Right Now™'

statistics: technical.edugain.org, visited 2018-10-16

Test model for incident response – a continuing process …

- 2nd Sirtfi Communications Challenge
- include eduGAIN Support Desk
- Exercise the model attack scenario … ☺



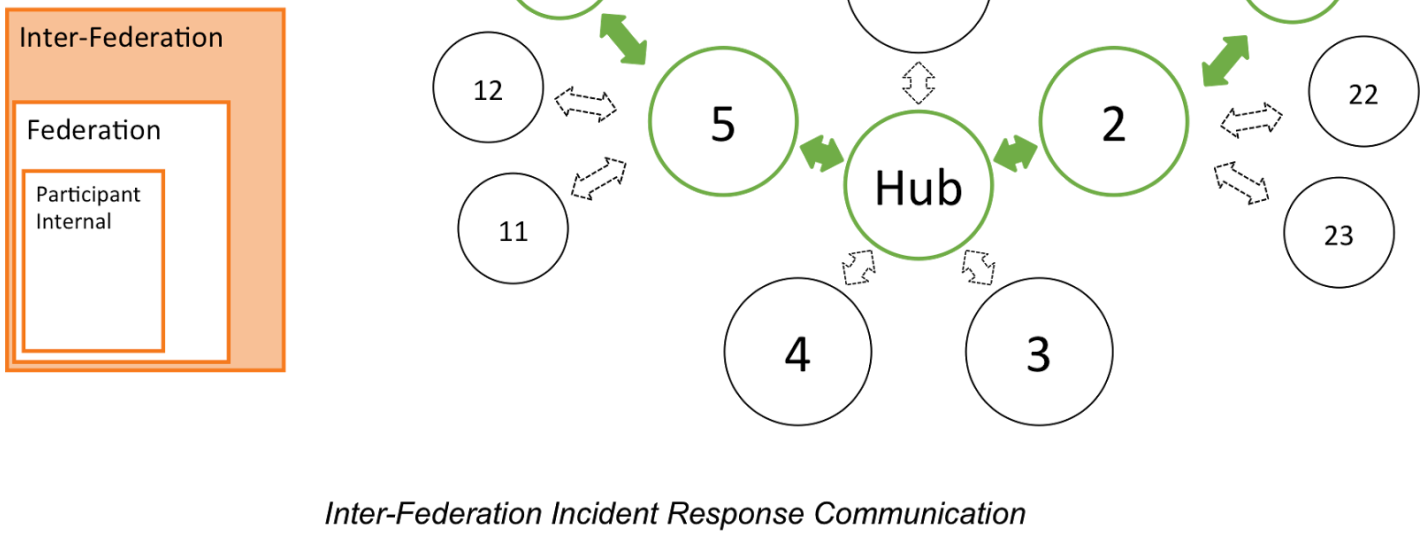
Participants

Participant	Federation	IdP/SP	Role Test 1
User	UK Fed	Jisc	Identity 1
Jisc	UK Fed	IdP	IdP1
ORCID	Incorrectly identified as Incommon (registrar is actually SURFconext)	SP https://orcid.org/signin	SP1
CSC	Haka	SP https://lbr.csc.fi/shibboleth	SP3
MWA Telescope Collaboration	AAF	SP https://wiki.mwatelescope.org	SP2
UK Fed		Federation	
Haka		Federation	
AAF		Federation	
Incommon		Federation	
eduGAIN		Interfederation	

parties involved in response challenge

See **https://aarc-project.eu/wp-content/uploads/2018/11/Incident-Response-Test-Model-for-Organisations-Simulation-2.pdf**

Incident response process evolution in federations – beyond basic Sirtfi



Inter-Federation Incident Response Communication

Continuing Challenges

- IdP **fails to inform other affected** SPs, for fear of leaking data, of reputation, or just lack of interest and knowledge
- **No established channels** of communication, esp. not **to federations** or eduGAIN

Can we evolve operational security in our federated academic environment?
Expand Sirtfi in places where there is no federation support (Sirtfi+ Registry)
And extend the concept of trust groups and facilitate exchanging incident information?

Guidance for research AAIs in the Infrastructure ecosystem

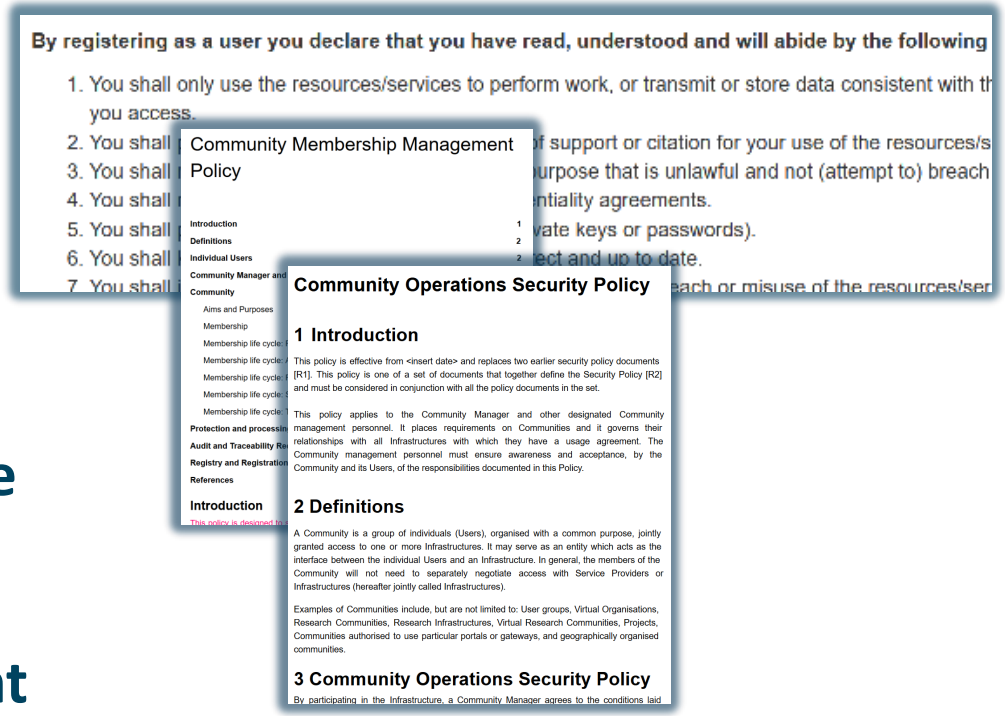
Authentication Assurance – a truly joint exercise

- using both REFEDS RAF components  as well as cross Infrastructure profiles 
- considering social-ID authenticator assurance, complementing account linking in BPA

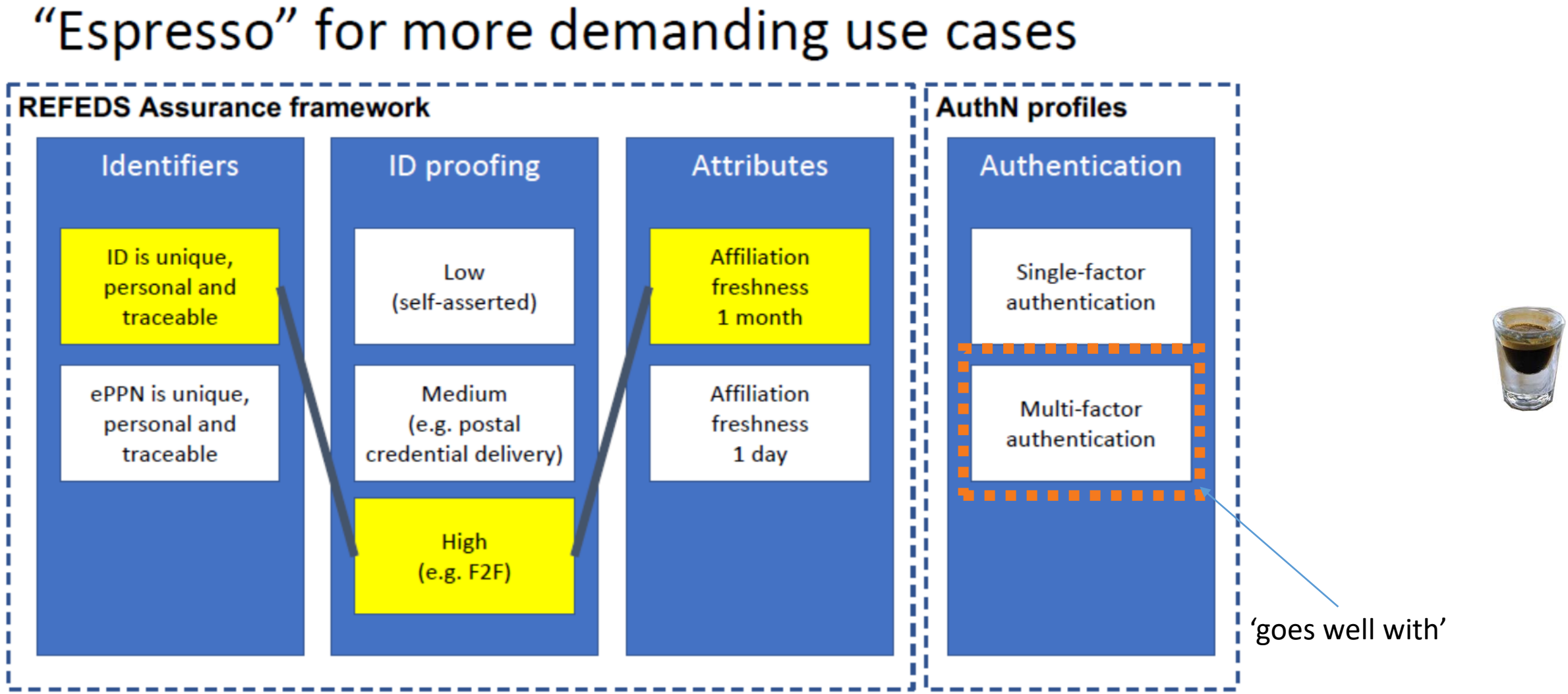
Protecting personal data from infrastructure use

Exploit **commonality between acceptable use policies** to ease cross-infrastructure resource use

Support **community management and a policy suite** using ***Snctfi*** to ease use of generic e-Infrastructures and interoperability
with the **Policy Development Kit** and **SCI assessment**

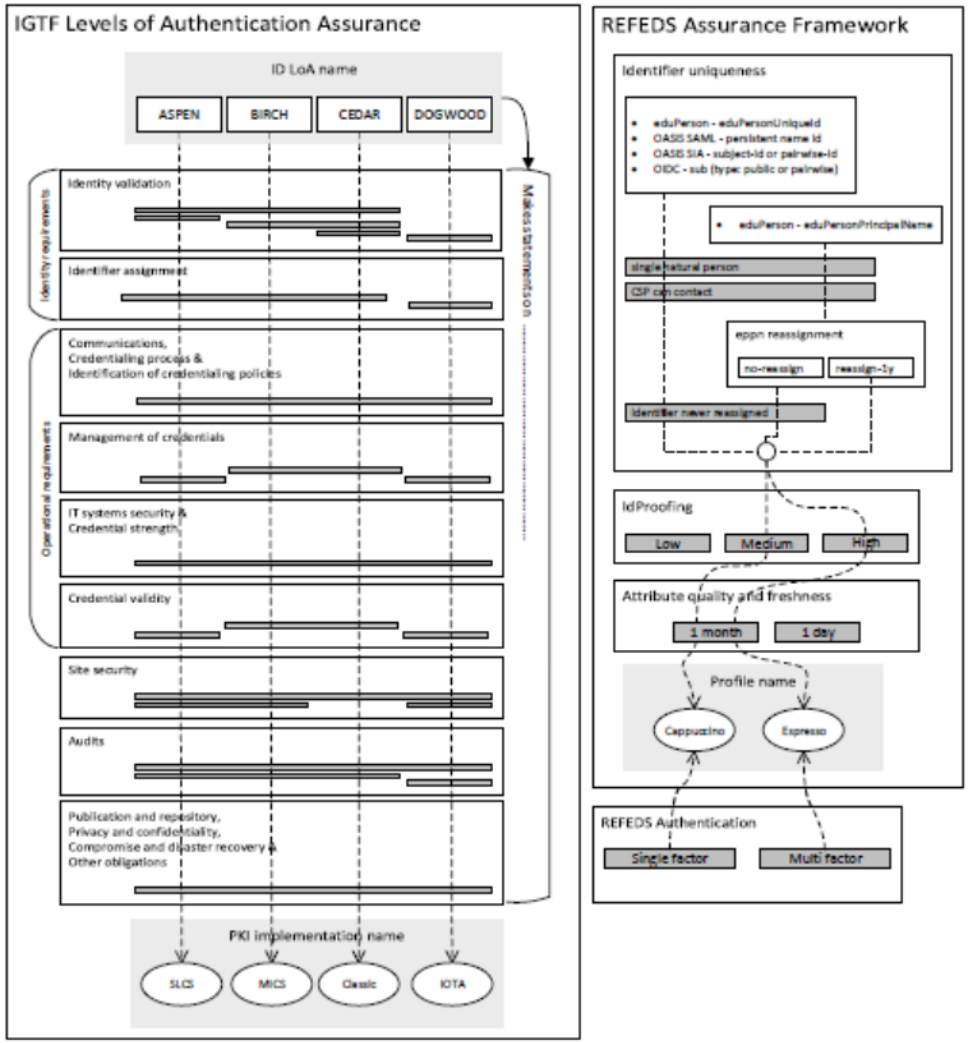


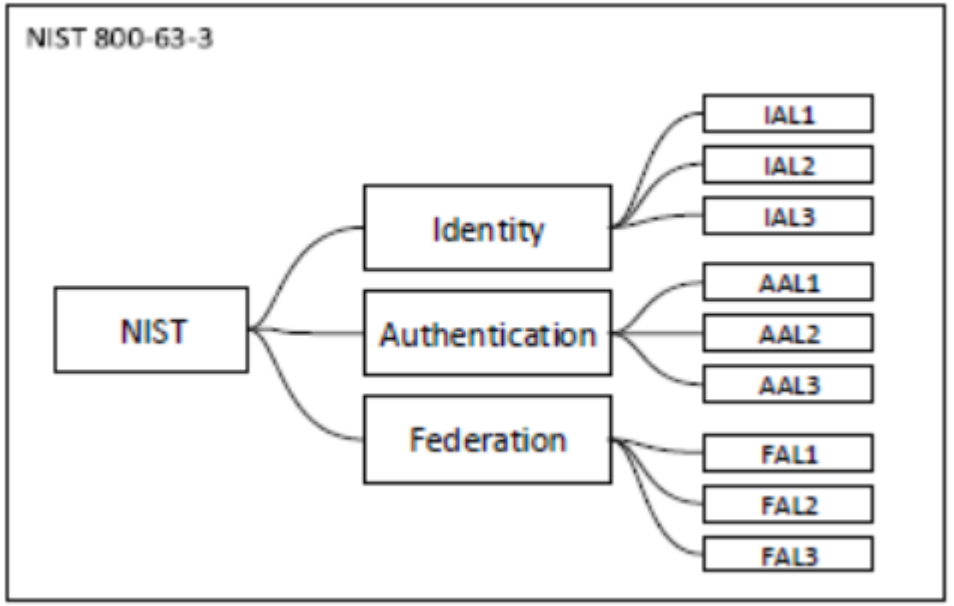
Example: “Espresso” profile for demanding use cases



REFEDS RAF, SFA, and MFA now endorsed – supplementary inter-infrastructure profiles in G021 and G041

Many assurance frameworks – how do they compare?





EIDAS

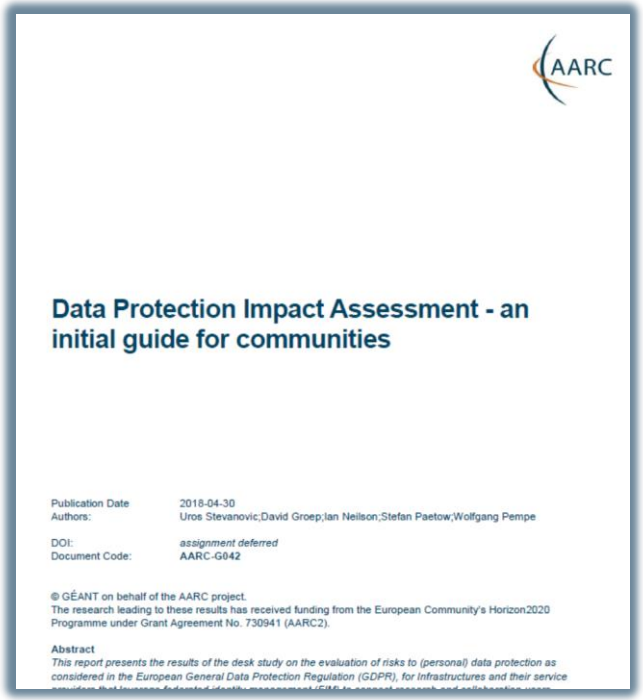
KANTARA

Protection of Personal Data and PII for Infrastructure AAIs – there is both FUD but also legitimate concerns

Large discrepancy between practice, perception, and actual risk:

- communities themselves don't see need to protect *infrastructure* AAI (accounting) data – and don't even consider existing AARC guidance ☹
- misunderstanding issue, over-stating risk, falling victim to FUD law firms
- even 'simplified' documents - like the GEANT Data Protection Code of Conduct – considered too complex to be understood

help determine risk and impact of FIM on **research infrastructure**



https://aarc-project.eu/guidelines/aarc-g042/

Difference to commonality in the Baseline AUP – sign once, use everywhere

ort any known or h or loss or s credentials. hone number for sible for backing	3	3
Adds: EUDAT is not liable to any compensation in case of lost data or loss of service	3	3
Adds: Although efforts are made to maintain confidentiality, no guarantees are given. Expanded for PI under "Personal information and data privacy"	2	3
	0	0

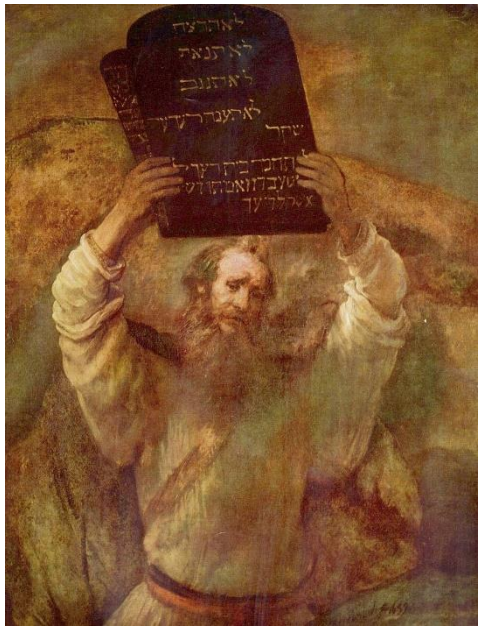
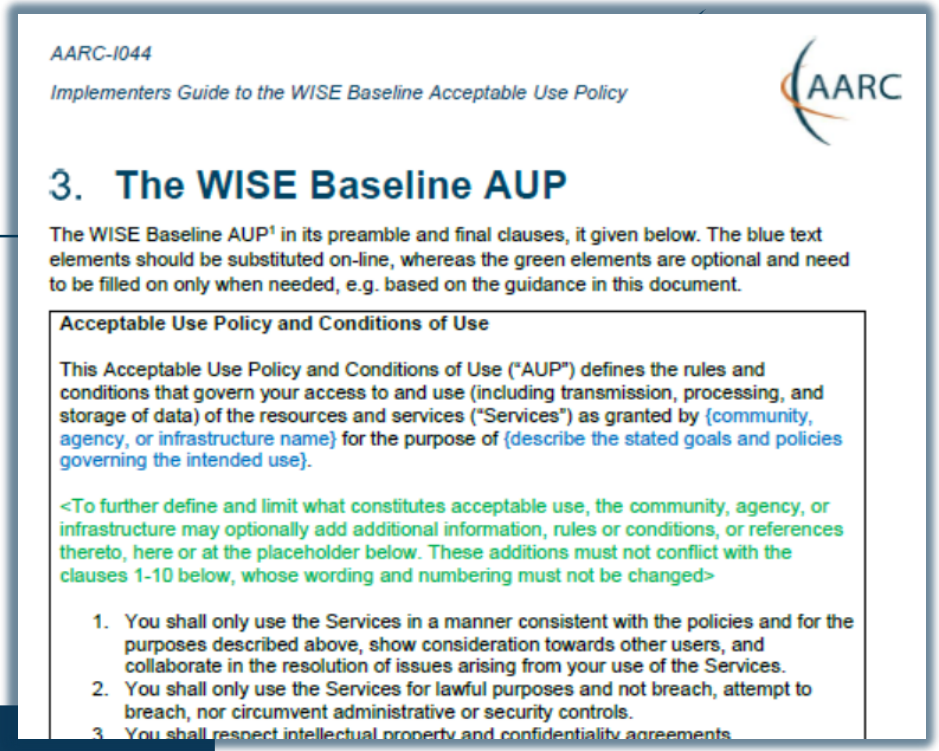


Image: Mozes en de tafelen der Wet, Rembrandt van Rijn, 1659

Scaling Acceptable Use Policy and data release

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



AARC-I044

Implementers Guide to the WISE Baseline Acceptable Use Policy

AARC

3. The WISE Baseline AUP

The WISE Baseline AUP[1] in its preamble and final clauses, it given below. The blue text elements should be substituted on-line, whereas the green elements are optional and need to be filled on 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 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

Community conditions

Community specific terms & conditions

Community specific terms & conditions

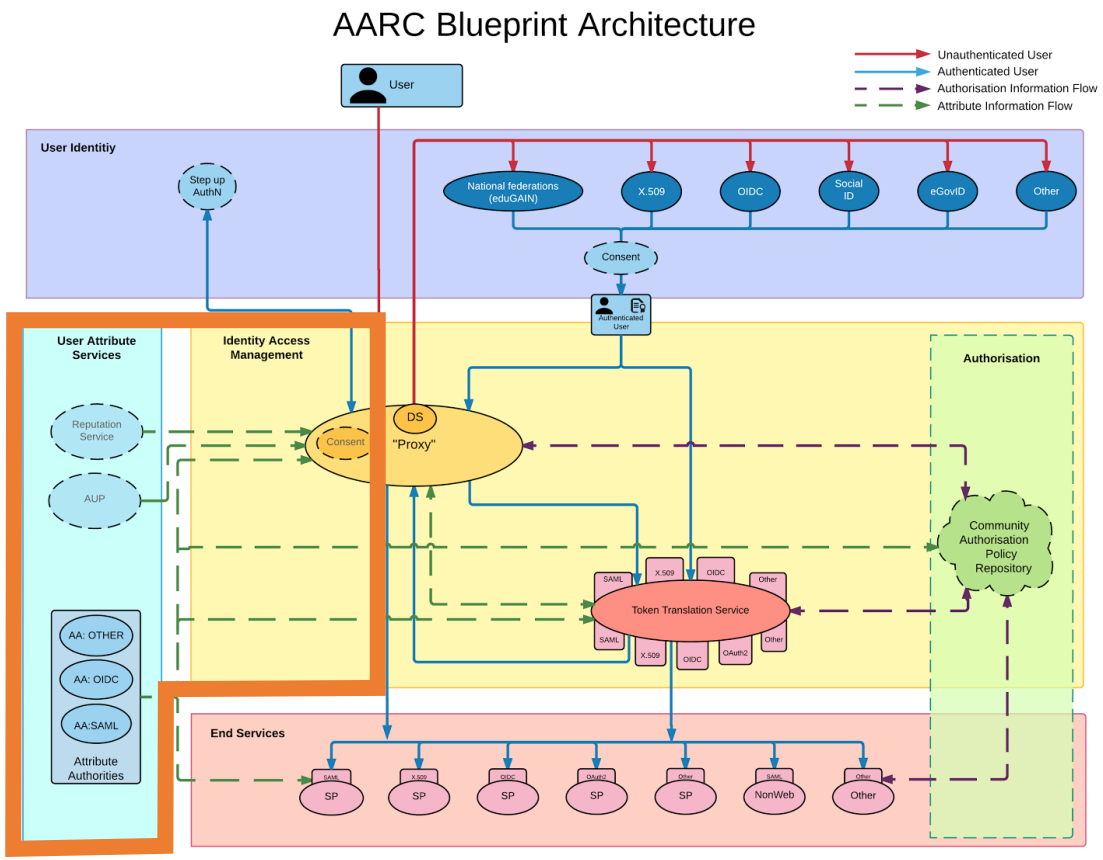
RI Cluster-specific terms & conditions

AARC-I044 Implementers Guide

Common baseline AUP
for e-Infrastructures and Research Communities
(current draft Baseline AUP –
leveraging comparison study and joint e-Infrastructure work)

https://aarc-project.eu/guidelines/aarc-i044/

Beyond just identity providers, services, and Federations: AA security



BPA Proxy and connected sources of trusted attributes critical to infrastructure security


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

Sctfi **igtf.net/sctfi**

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures

- **Help AA operators with operational security**
- requisite processes and traceability support
- secure operation and deployment
- protected transport
- for different attribute distribution models

Derived from **SCI**, the framework on *Security for Collaboration in Infrastructures*

WISE **I**nformation **S**ecurity for **E**-infrastructures got global endorsement SCI in June 2017

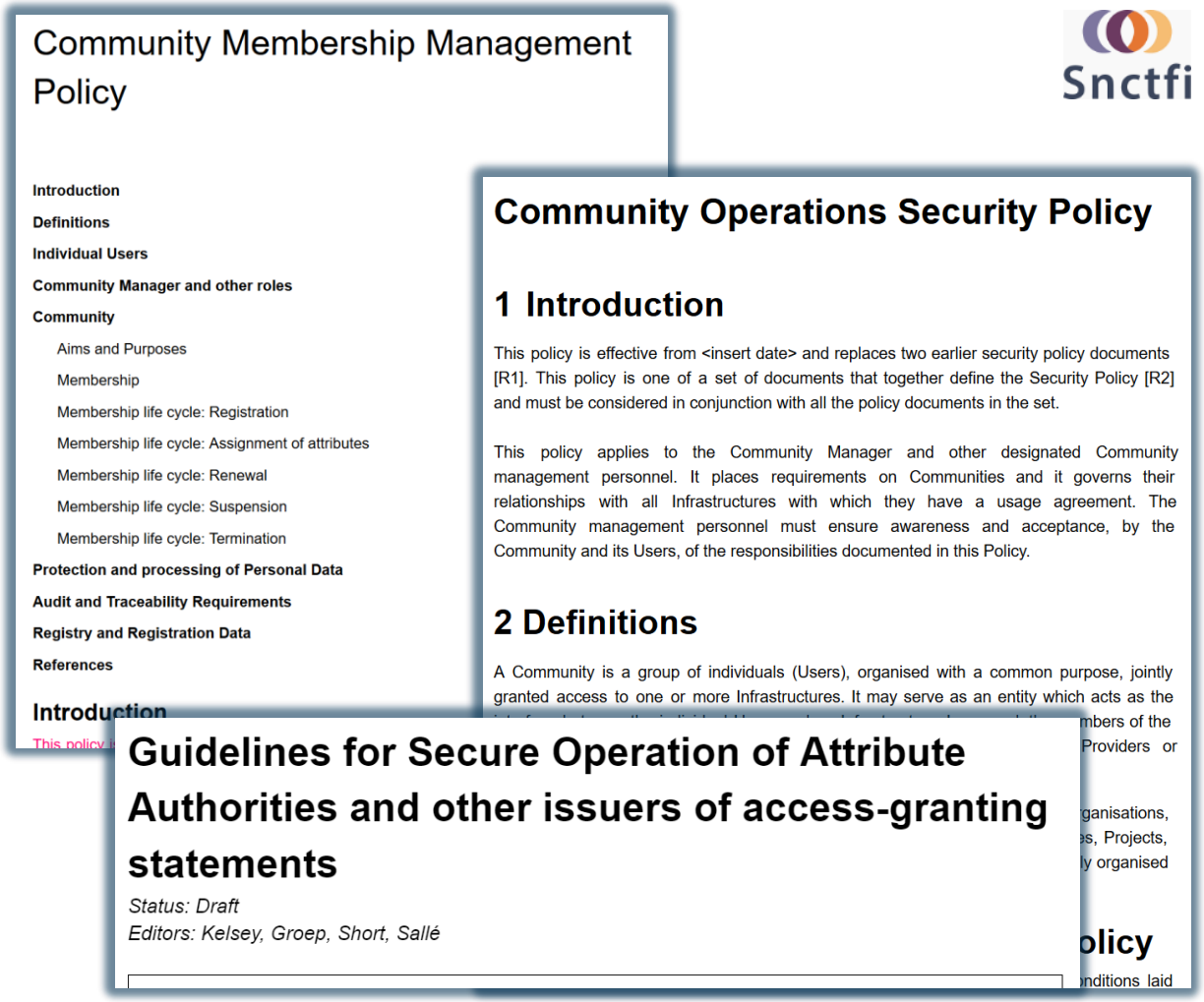
Implementing Snctfi:
Community Management and Security, AA Operations Security, …

Relevant to communities and e-Infrastructures both

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

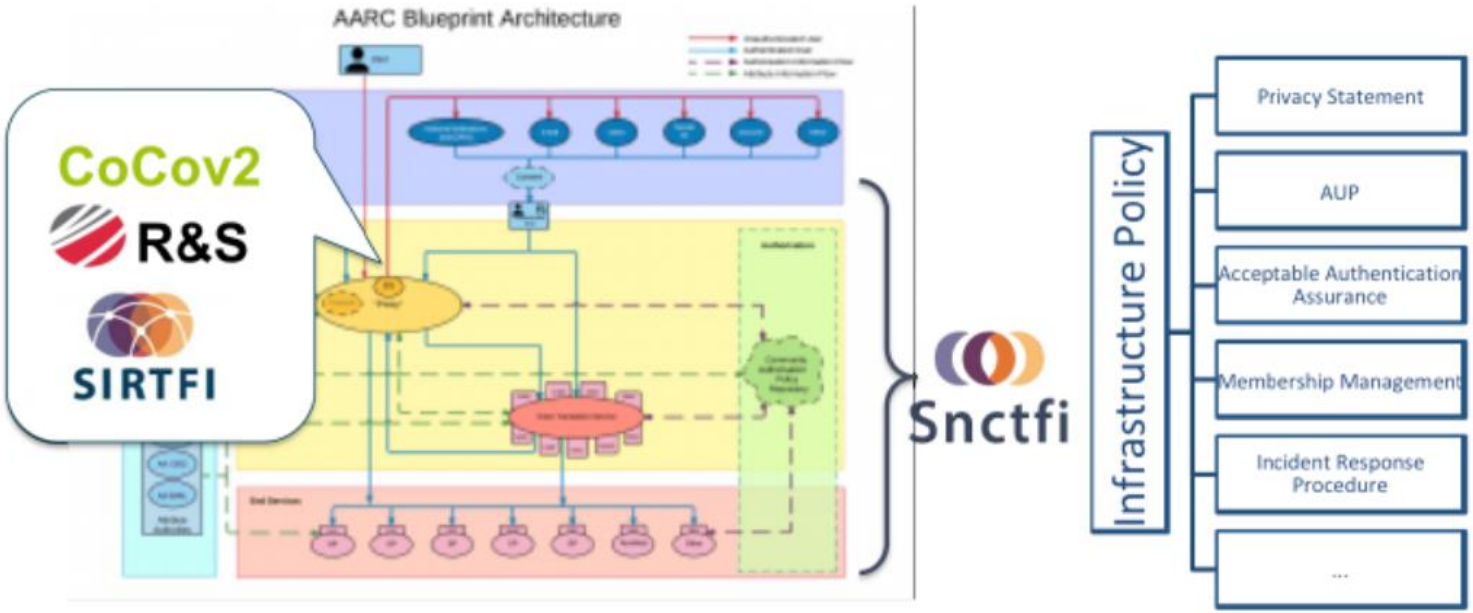
joint work with EGI-ENGAGE and EOSC-Hub projects and the EGI, PRACE, HBP, EUDAT communities

ENGAGE EOSC-hub



Policy Development Engagement and the 'Kit'

- Bring together a consistent suite of policies & guidance
- based on e-Infrastructure best practices
  from advanced operational infrastructures today

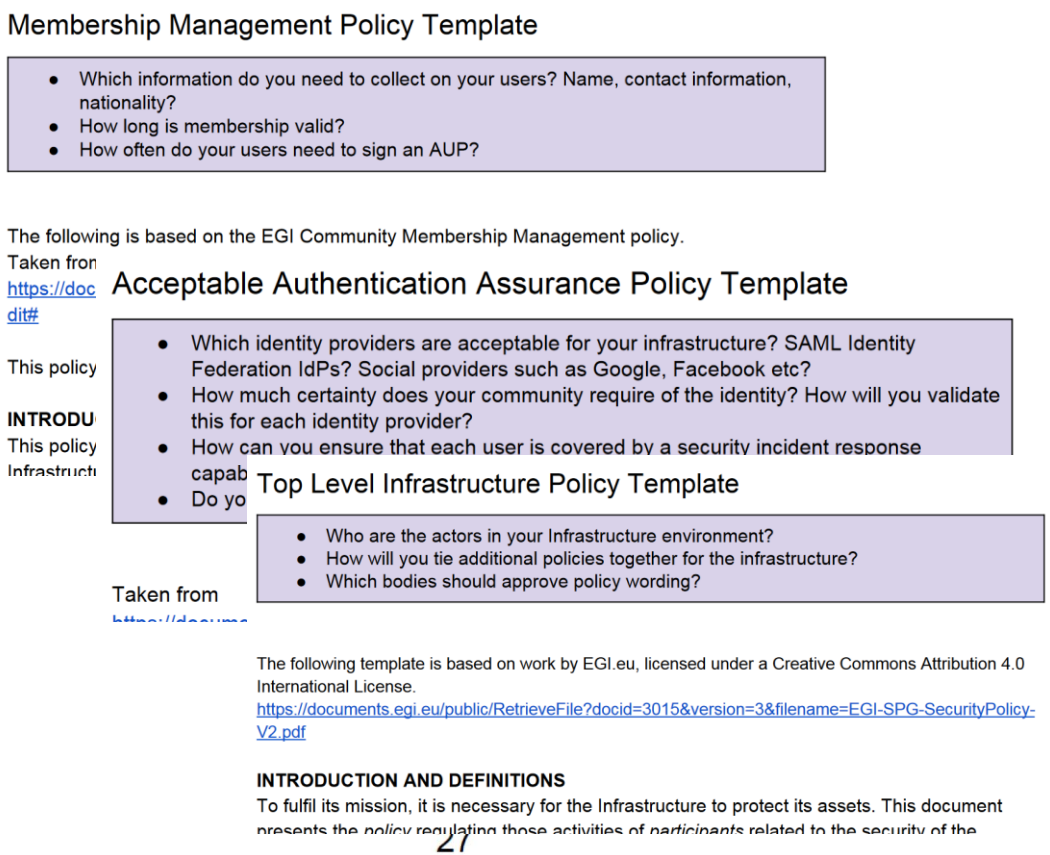


AARC Policy Development Kit

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

https://wiki.geant.org/display/AARC/Policy+Development+Kit

Helping you towards SCI and Snctfi: templates in the PD Kit



Membership Management Policy Template

- Which information do you need to collect on your users? Name, contact information, nationality?
- How long is membership valid?
- How often do your users need to sign an AUP?

The following is based on the EGI Community Membership Management policy.
Taken fron
https://doc
dit#

This policy

INTRODU
This policy
Infrastructu

Acceptable Authentication Assurance Policy Template

- 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? How will you validate this for each identity provider?
- How can you ensure that each user is covered by a security incident response capab
- Do yo

Top Level Infrastructure Policy Template

- Who are the actors in your Infrastructure environment?
- How will you tie additional policies together for the infrastructure?
- Which bodies should approve policy wording?

Taken from

The following template is based on work by EGI.eu, licensed under a Creative Commons Attribution 4.0 International License.
https://documents.egi.eu/public/RetrieveFile?docid=3015&version=3&filename=EGI-SPG-SecurityPolicy-V2.pdf

INTRODUCTION AND DEFINITIONS
To fulfil its mission, it is necessary for the Infrastructure to protect its assets. This document presents the *policy* regulating those activities of *participants* related to the security of the

27

The SCI Trust Framework – globally comparable structure in Security Policy

Endorsement of SCI Version 2 at TNC17 (Linz)

- 1st June 2017
- *Infrastructures endorse the governing principles and approach of SCI, as produced by WISE, as a medium of building trust between infrastructures, to facilitate the exchange of security information in the event of a cross-infrastructure incident, and the collaboration of e-Infrastructures to support the process. These Infrastructures welcome the development of an information security community for the Infrastructures, and underline that the present activities by the research and e-Infrastructures should be continued and reinforced*
- Endorsements have been received from the following infrastructures; EGI, EUDAT, GEANT, GridPP, MYREN, PRACE, SURF, WLCG, XSEDE, HBP
- https://www.geant.org/News_and_Events/Pages/supporting-security-for-collaborating-infrastructures.aspx

Kelsey/SCI Trust Framework 24 Sep 2018 30

see the SCI Webinar by David Kelsey on Sept 24th! https://www.youtube.com/watch?v=vZvfRvMQfFg

SCIv2 – beyond its endorsement to self-assessment and review

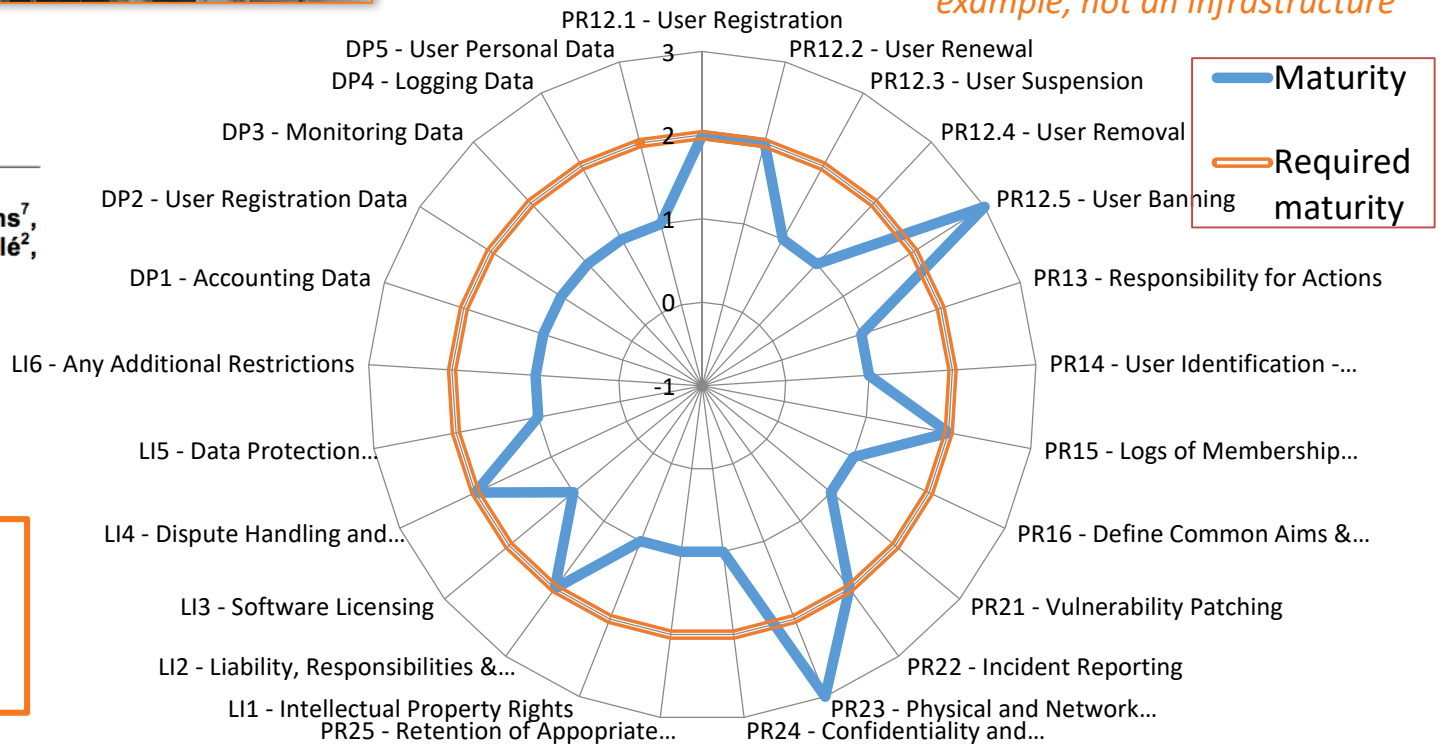
A Trust Framework for Security Collaboration among Infrastructures

SCI version 2.0, 31 May 2017

L Florio[1], S Gabriel[2], F Gagadis[3], D Groep[2], W de Jong[4], U Kaila[5], D Kelsey[6], A Moens[7], I Neilson[6], R Niederberger[8], R Quick[9], W Raquel[10], V Ribaillier[11], M Sallé[2], A Scicchitano[12], H Short[13], A Slagell[10], U Stevanovic[14], G Venekamp[4] and R Wartel[13]

The WISE SCIv2 Working Group - e-mail: david.kelsey@stfc.ac.uk, sci@lists.wise-community.org

example, not an infrastructure



AARC may help by supporting evolving the peer review self-assessment model for SCI
and how that compares to e.g. ISO-based audits

http://wise-community.org/sci

Things to do in AARC's last 6 mo and beyond when you're still alive by now …

OpSec	**Attribute authority operations** practice … also for Infra proxies
	Trust groups and the exchange of (account) compromise information: ***beyond Sirtfi***
Infra-centric	traceability and accounting data-collection policy framework based on **SCI, providing a self-assessment methodology** and comparison matrix for infrastructure services
	Evolution of **data protection guidance** for services
Researcher-centric	**Baseline AUP** with major Infrastructures (EGI, EUDAT, PRACE, XSEDE) and communities
	Deployment of **assurance guidelines** and assess high-assurance use cases (BBMRI)
Engagement	Evolve **Policy Development Kit** and a simpler top-level security policy with a community 'assessment method' or 'guide' to the adoption of appropriate policy
	Support communities and use cases in policy interpretation through Guidelines

Thanks to the AARC2 policy collaborators: David Kelsey, Hannah Short, Ian Neilson, Uros Stevanovic, Mikael Linden, Ralph Niederberger, Petr Holub, Wolfgang Pempe, Stefan Paetow, and many contributions from across the AARC project, REFEDS, IGTF, and WISE!
Selected policy work performed in collaboration with the EOSC-HUB WP4.4 ISM activity

Thank you

Any Questions?

davidg@nikhef.nl

http://aarc-project.eu/

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