AARC Authentication and Authorisation for Research and Collaboration

WP3: Policy and Best Practice Harmonisation

David Groep

Nikhef

AARC2 2018 AL/TL meeting
12-13 September, 2018
Amsterdam

0.4

Policy and best practice activity high-level objectives from our DoW

✓ **“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

Results in our first 12 months

Formal stuff

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

MNA3.3 Define and test a model for organisations to share account compromise information

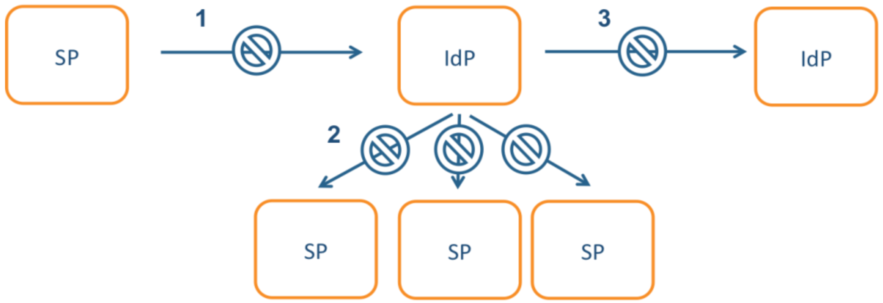
MNA3.5 Inventory of high-assurance identity requirements from the AARC2 use cases

With many other documents and results

… eduGAIN and Sirtfi communications challenge,
community guidance on using Codes of Conduct in the Blueprint Proxies,
REFEDS Assurance Pilot, X-infrastructure assurance expression, social-ID assurance guide,
Community (security) policies in the Policy Development Kit,
FIM4R community engagement, …

Incident response process evolution in federations –Sirtfi

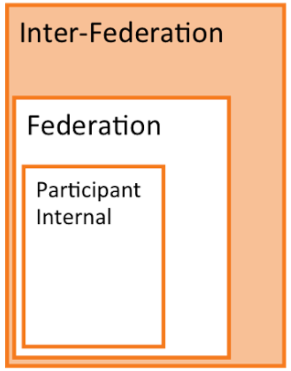
AARC-1 Refresher

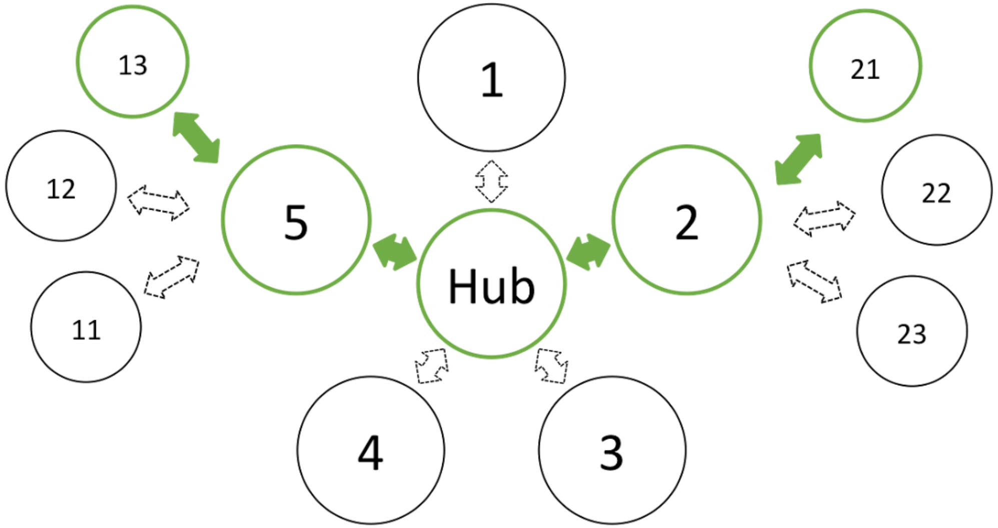


Incident Response Communication, communication blocks

Challenges

- IdP appears outside the service's security mandate
- Lack of contact or lack of trust in the IdP which to the SP is an unknown party
- 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 themselves!

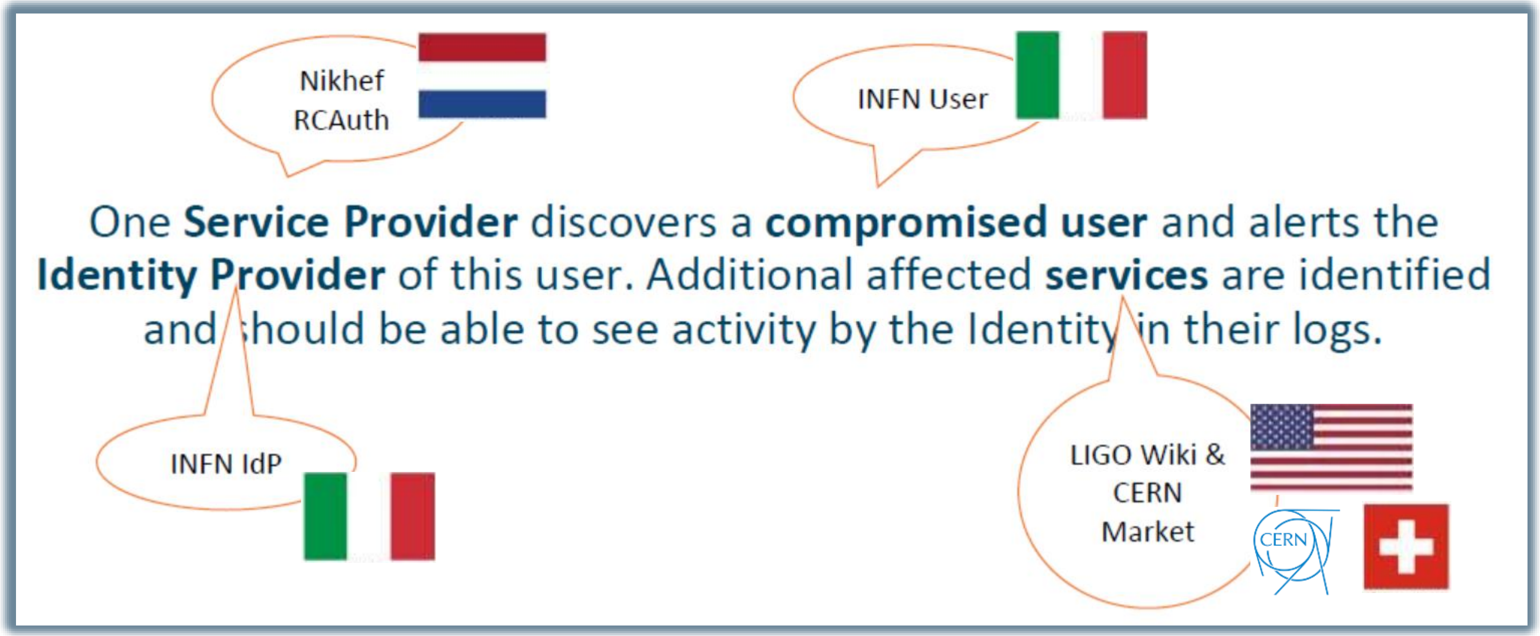




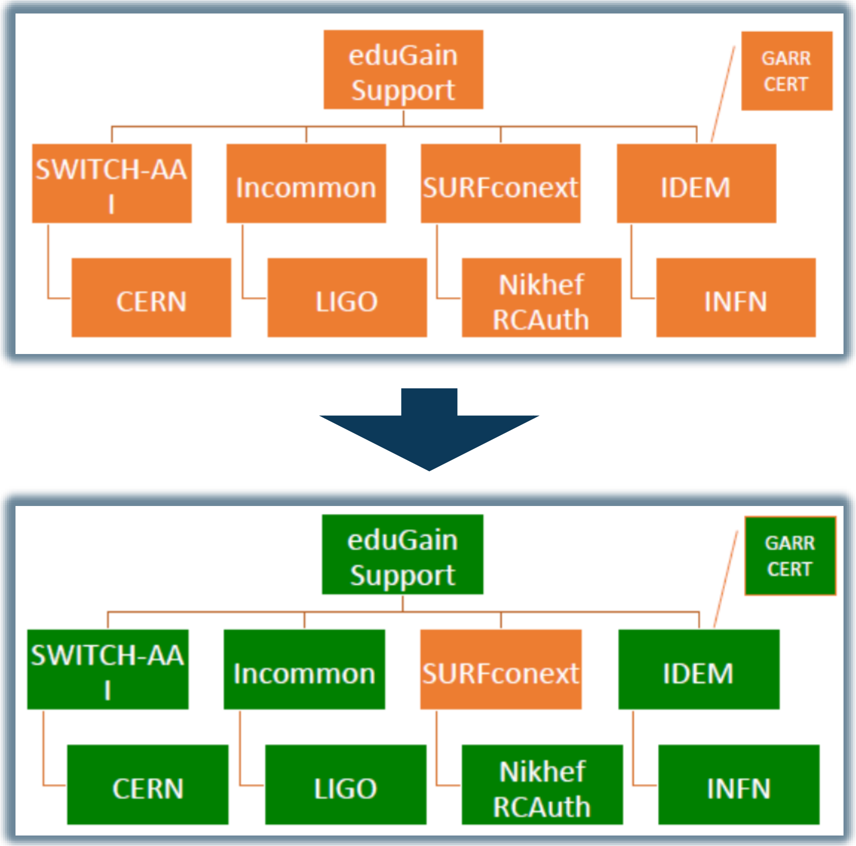
Inter-Federation Incident Response Communication

Test model for incident response (MNA3.3)

- Defines the model actors
- include eduGAIN Support Desk (as per AARC-1 model)
- Exercise the model attack scenario!



One **Service Provider** discovers a **compromised user** and alerts the **Identity Provider** of this user. Additional affected **services** are identified and should be able to see activity by the Identity in their logs.



parties involved in response challenge

Report-out see **https://wiki.geant.org/display/AARC/Incident+Response+Test+Model+for+Organizations**

Main achievements in Operational Security

Sirtfi training and guidance	→	Increased availability of security contact information in eduGAIN globally (167 → 325)
Incident response model test	→	Responsiveness during actual FIM incidents
	→	WISE group (developing) on coordinating security communications challenges
	→	Demonstrated need for federation-level engagement beyond just IdPs and home orgs with an eduGAIN Support Security Team

PY2	Attribute authority operations practice also for Infra proxies
	Trust groups and the exchange of (account) compromise information

GDPR for Infrastructure AAI – both FUD and legitimate concerns

Large discrepancy between practice, perception, and actual risk:

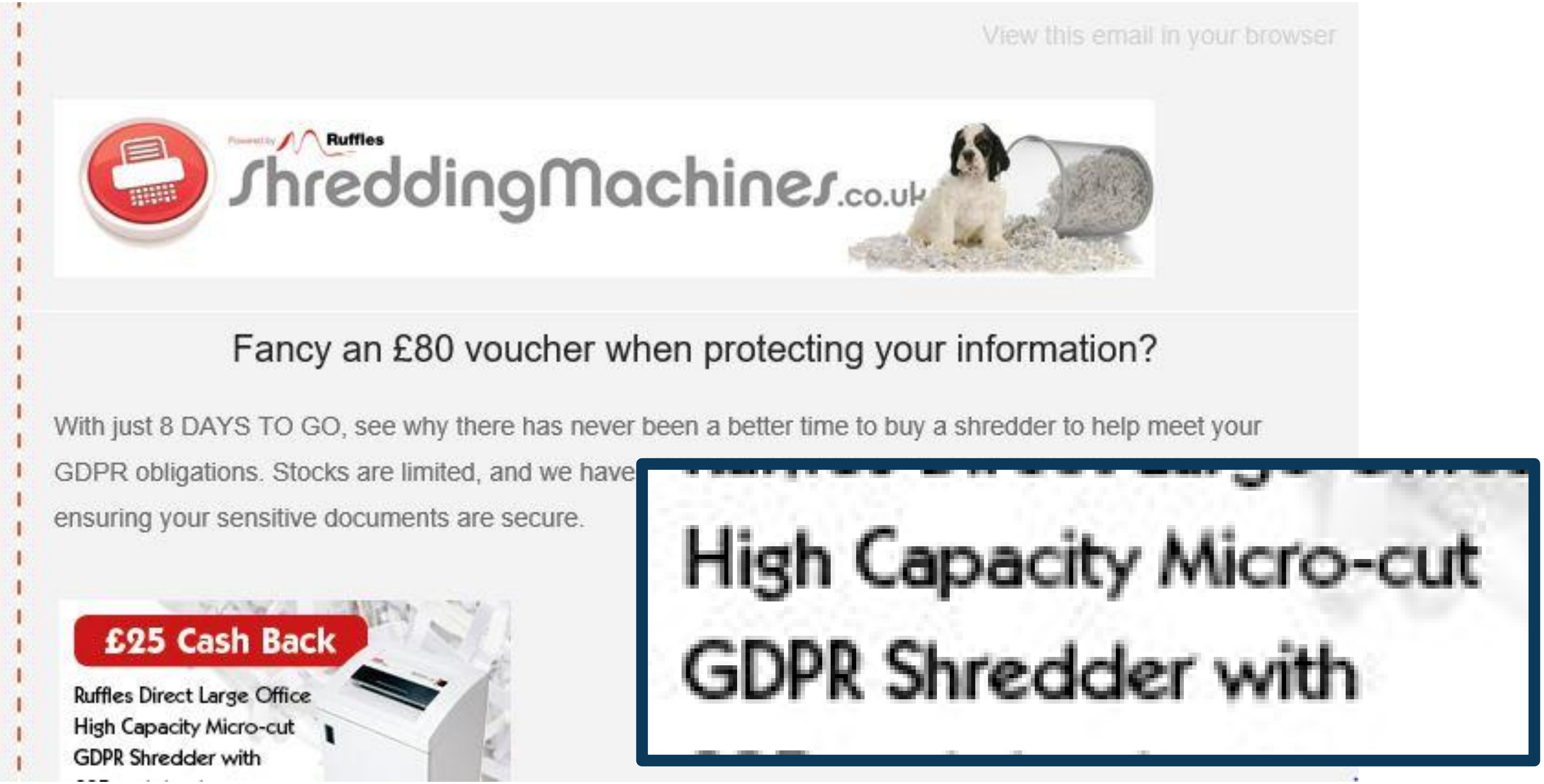
- communities don’t see (or forget) need to protect infrastructure AAI (accounting) data – and don’t even consider our AARC-1 guidance ☹
- others misunderstand the issue, over-state the risks, and fall victim to FUD law firms instead of just reading Andrew Cormack’s blogs
- even ‘simplified’ documents - like the GEANT Data Protection Code of Conduct – considered too complex to be understood and implemented well

DNA3.1 **“assess privacy regulations on [accounting] data needed by service operators**
AARC-G042 **and e/r-infrastructures to ensure smooth and secure service operations”**

specifically purposed to answer the basic questions:

- how much impact does FIM have on your **research infrastructure and accounting data**?
- what guidance is there already from member state regulators to **help you determine risk**?

A solution for our research communities?



View this email in your browser

Fancy an £80 voucher when protecting your information?

With just 8 DAYS TO GO, see why there has never been a better time to buy a shredder to help meet your GDPR obligations. Stocks are limited, and we have

ensuring your sensitive documents are secure.

£25 Cash Back

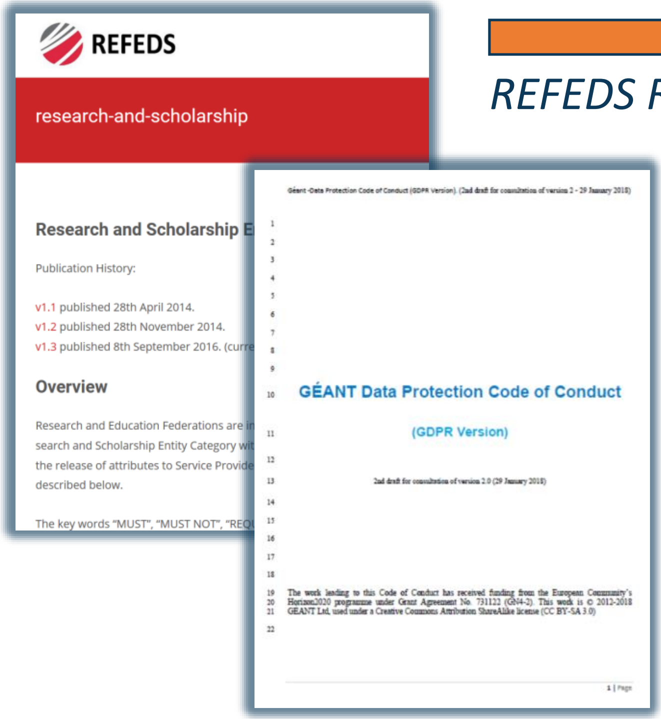
Ruffles Direct Large Office High Capacity Micro-cut GDPR Shredder with

High Capacity Micro-cut GDPR Shredder with

UCE message sent on May 17th to Ian Neilson, and millions more …

https://aarc-project.eu/guidelines/aarc-g040

Implementing *Snctfi*: interpreting generic policies for BPA Proxy use cases



REFEDS

research-and-scholarship

Research and Scholarship E

Publication History:

v1.1 published 28th April 2014.
v1.2 published 28th November 2014.
v1.3 published 8th September 2016. (curre

Overview

Research and Education Federations are i
search and Scholarship Entity Category wi
the release of attributes to Service Provide
described below.

The key words "MUST", "MUST NOT", "REQ

Géant -Data Protection Code of Conduct (GDPR Version). (2nd draft for consultation of version 2 - 29 January 2018)

GÉANT Data Protection Code of Conduct

(GDPR Version)

2nd draft for consultation of version 2.0 (29 January 2018)

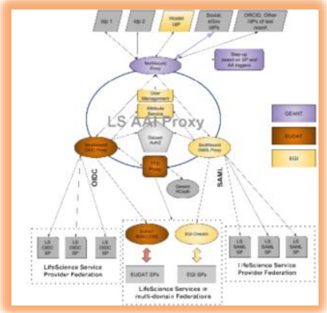
The work leading to this Code of Conduct has received funding from the European Community's Horizon2020 programme under Grant Agreement No. 731122 (GN4-2). This work is © 2012-2018 GEANT Ltd, used under a Creative Commons Attribution ShareAlike license (CC BY-SA 3.0)

1 | Page

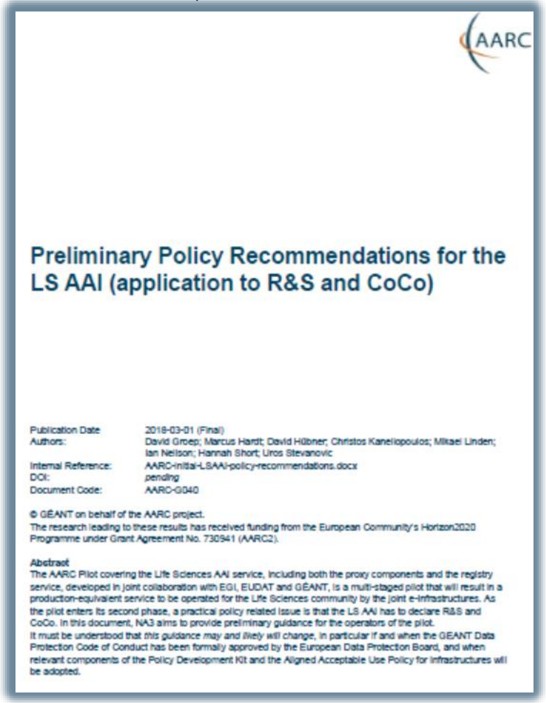
REFEDS R&S: allow attribute flow from the IdPs, express intent and scope

GEANT DPCoCo & GDPR - 'I'll be good with personal data'

Casting policies into implementation and processes is a 'bridging process', requiring **policy and architecture expertise** and **knowledge of the community** use case **– i.e. the ingredients that make AARC!**


LS AAI Proxy
OIDC
SAML
LifeScience Service Provider Federation
LifeScience Services in multi-domain Federations

LSAAI Infrastructures: which components will do what?



AARC

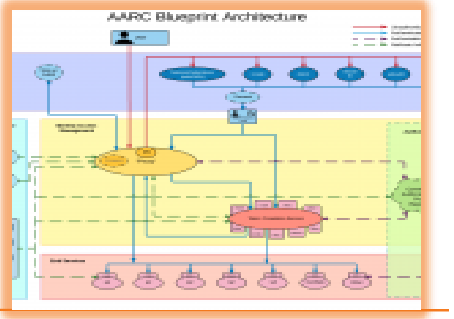
Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)

Publication Date	2018-03-01 (Final)
Authors:	David Groep; Marcus Hardt; David Hübner; Christos Kanellopoulos; Mikael Linden; Ian Neilson; Hannah Short; Uros Stevanovic
Internal Reference:	AARC-initial-LSAAI-policy-recommendations.docx
DOI:	*pending*
Document Code:	AARC-G040

© GÉANT on behalf of the AARC project.
The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract
The AARC Pilot covering the Life Sciences AAI service, including both the proxy components and the registry service, developed in joint collaboration with EGI, EUDAT and GÉANT, is a multi-staged pilot that 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, a practical policy related issue is that the LS AAI has to declare R&S and CoCo. In this document, NA3 aims to provide preliminary guidance for the operators of the pilot.
It must be understood that *this guidance may and likely will change*, in particular if and when the GEANT Data Protection Code of Conduct has been formally approved by the European Data Protection Board, and when relevant components of the Policy Development Kit and the Aligned Acceptable Use Policy for Infrastructures will be adopted.

AARC-G040



AARC BPA: this is how information flows

Accounting and infrastructure-use data protection: a bit of clarification …

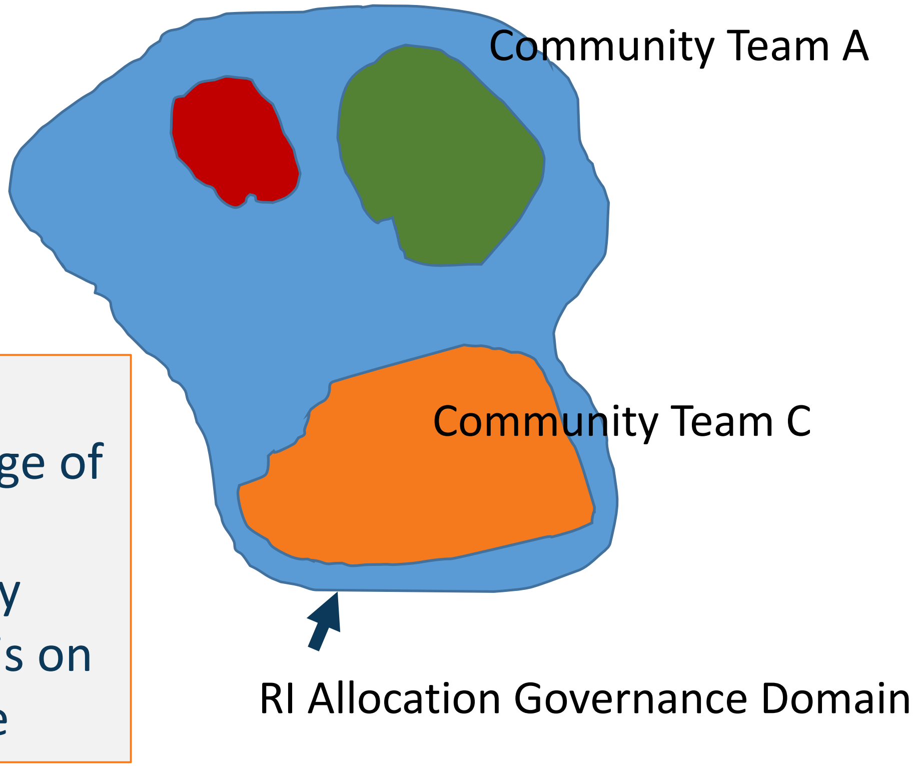
Work on accounting foresaw new communities joining AARC2
processing more sensitive (and: more competitive) work flows,
creating need for sub-structure and protection of accounting data within the community itself

Phased approach

1.
Support communities to deal with general data protection issues
Impact of GDPR for communities

2.
Issue guidance on generic issues, such as assessing impact of infrastructure use

PY2
Depending on stage of community development, may continue emphasis on targeted guidance



Main achievements in Service-Centric Policy

Guidelines model for policy and architecture	→	Clear adoption process for ‘consumers’ of AARC results, including targeted advice
Community Specific Guideline: LSAAI proxy operations (for R&S + DPCoCo)	→	Support the move of LSAAI to full production
Guideline: Data Protection Impact Assessment	→	Reduced complexity for communities and infrastructures handing (accounting) data

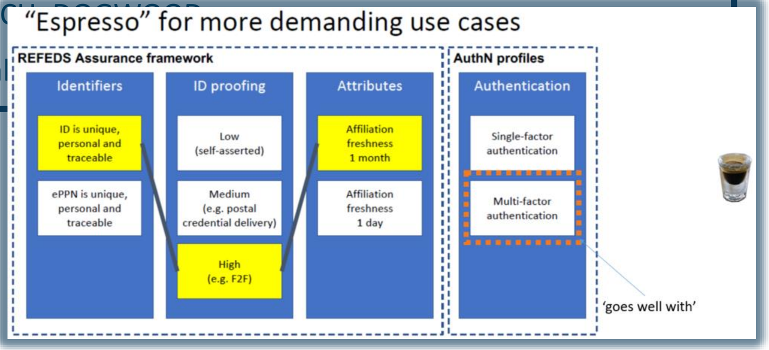
PY2	traceability and accounting data-collection policy framework based on SCI, providing a self-assessment methodology and comparison matrix for infrastructure services
	Evolution of data protection guidance for services – driven by the community needs

Guidance for research communities in the Infrastructure ecosystem

Authentication Assurance

- using both REFEDS RAF components as well as cross Infrastructure profiles
- considering social-ID authenticator assurance, complementing account linking in BPA *in G041*
- alignment with REFEDS SFA/MFA now needs update of *AARC-G021*

- from REFEDS Assurance Framework: Cappuccino, Espresso
- from IGTF Assurance Profiles: BIRCH, DOGWOOD
- from the AARC JRA1 use case anal



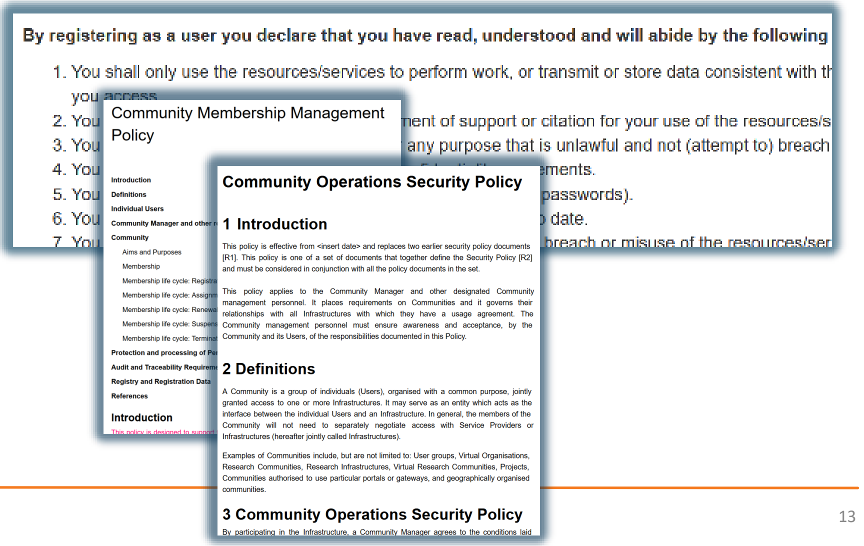
“Espresso” for more demanding use cases

REFEDS Assurance framework
Identifiers
ID is unique, personal and traceable
ePPN is unique, personal and traceable
ID proofing
Low (self-asserted)
Medium (e.g. postal credential delivery)
High (e.g. F2F)
Attributes
Affiliation freshness 1 month
Affiliation freshness 1 day
AuthN profiles
Authentication
Single-factor authentication
Multi-factor authentication
'goes well with'

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

Support **community management using *Snctfi*** easing use of the generic e-Infrastructures

can you show community operations – sufficient to act as a one-stop registration for every Infrastructure?



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 th you access
2. You ment of support or citation for your use of the resources/s
3. You any purpose that is unlawful and not (attempt to) breach
4. You ements.
5. You passwords).
6. You date.
7. You breach or misuse of the resources/ser

Community Membership Management Policy

Introduction
Definitions
Individual Users
Community Manager and other r
Community
Aims and Purposes
Membership
Membership life cycle: Registra
Membership life cycle: Assignm
Membership life cycle: Renewal
Membership life cycle: Suspens
Membership life cycle: Terminat
Protection and processing of Per
Audit and Traceability Requireme
Registry and Registration Data
References

Introduction

This policy is designed to support

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

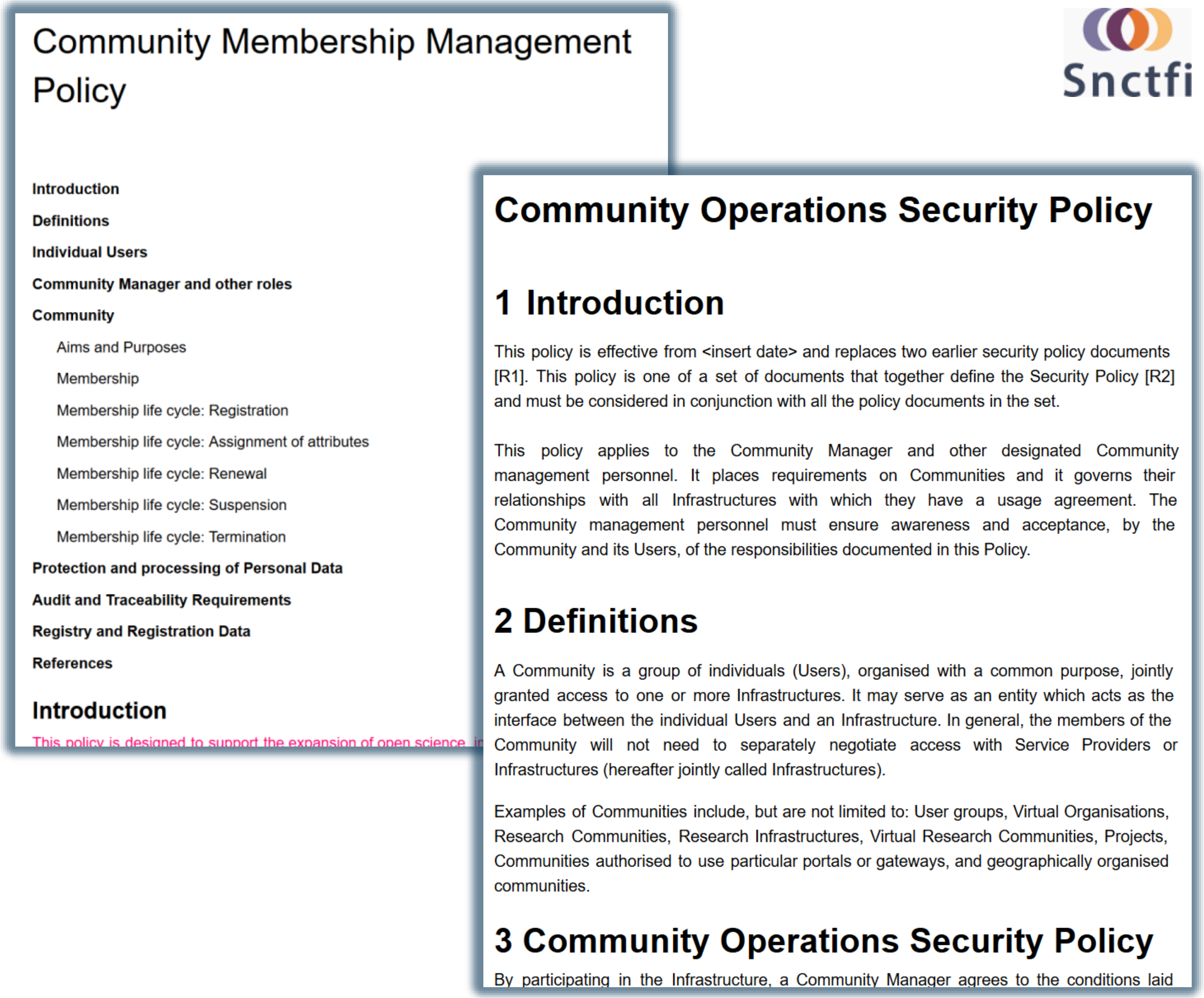
Implementing Snctfi: Community Membership Management and Security

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



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 open science

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

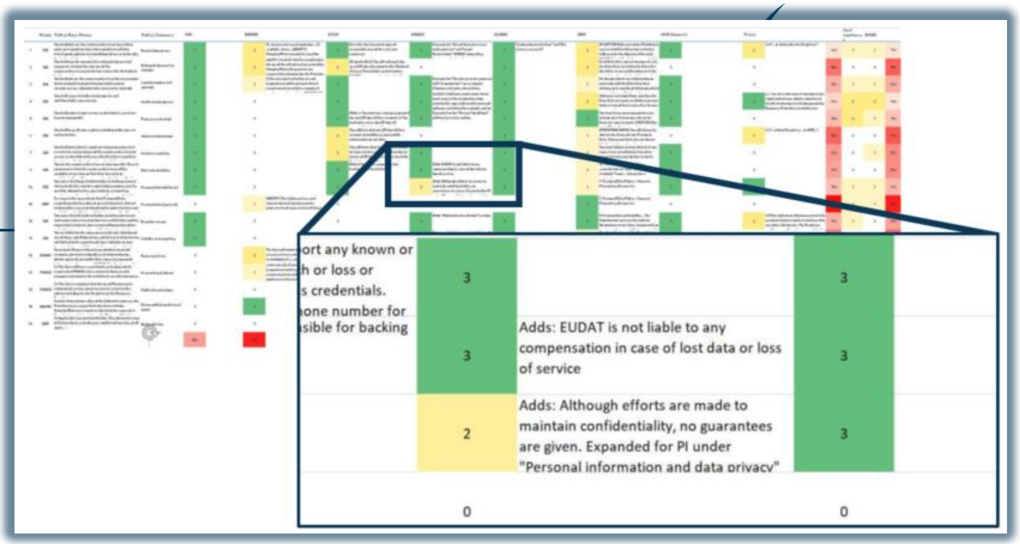
A Community is a group of individuals (Users), organised with a common purpose, jointly granted access to one or more Infrastructures. It may serve as an entity which acts as the interface between the individual Users and an Infrastructure. In general, the members of the Community will not need to separately 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

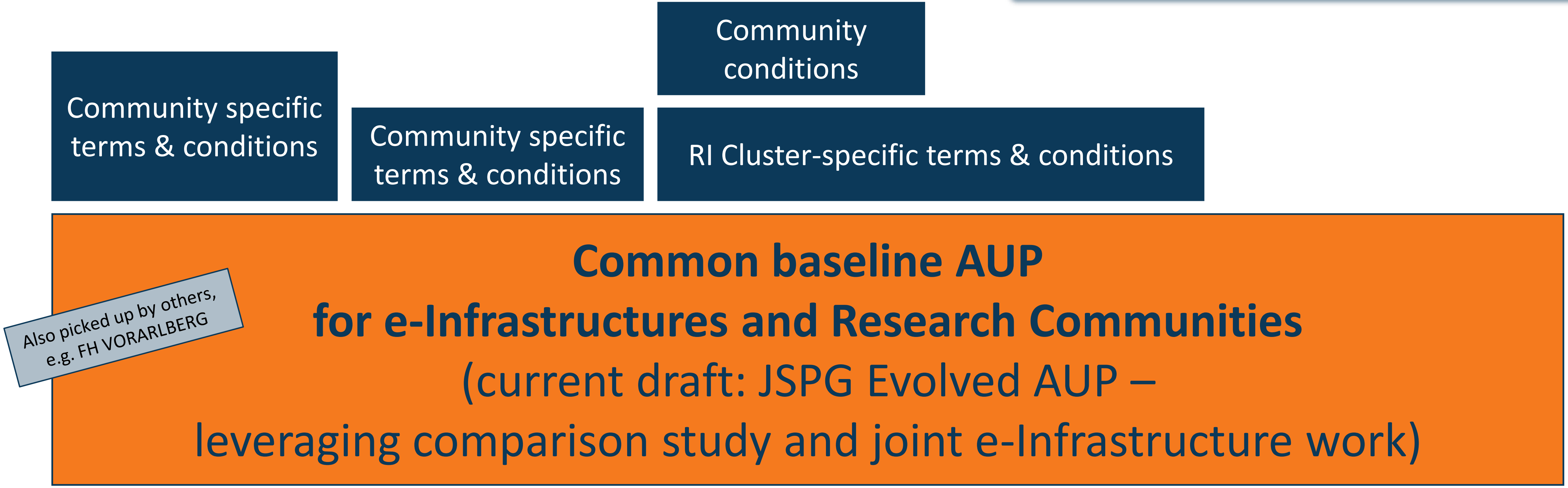
By participating in the Infrastructure, a Community Manager agrees to the conditions laid

Scaling Acceptable Use Policy and data release



ort any known or
h or loss or
s credentials.
one number for
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	Adds: Although efforts are made to maintain confidentiality, no guarantees are given. Expanded for PI under "Personal information and data privacy"	3
	0		0



Community conditions

Community specific terms & conditions

Community specific terms & conditions

RI Cluster-specific terms & conditions

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

Also picked up by others, e.g. FH VORARLBERG

https://wiki.geant.org/x/P4bWBQ

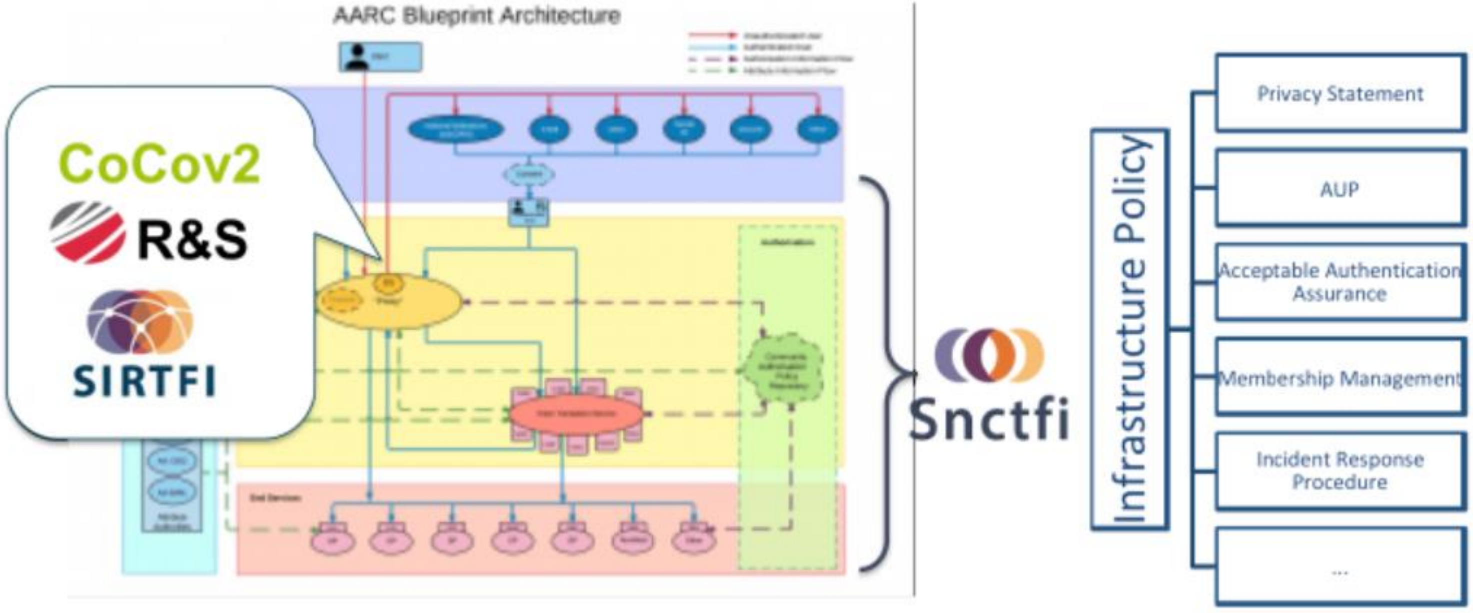
Main achievements in e-Researcher-centric Policy

Assurance Framework alignment	→	REFEDS RAF Pilot with production entities
	→	Profile-driven interop between Infrastructures achieved (AARC-G020)
Guideline: exchange of assurance information	→	Workflows can cross multiple infrastructures
Guideline: social media assurance components	→	Enable collaborative assurance with the community (and guide BPA implementers)
Acceptable Use policy scaling model and baseline	→	*Alignment model* recognized by LSAAI and major e-Infrastructures

PY2	Baseline AUP with major Infrastructures (EGI, EUDAT, PRACE, XSEDE) and communities
	Deployment of assurance guideline and move to high-assurance use cases

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 Blueprint Architecture

CoCov2

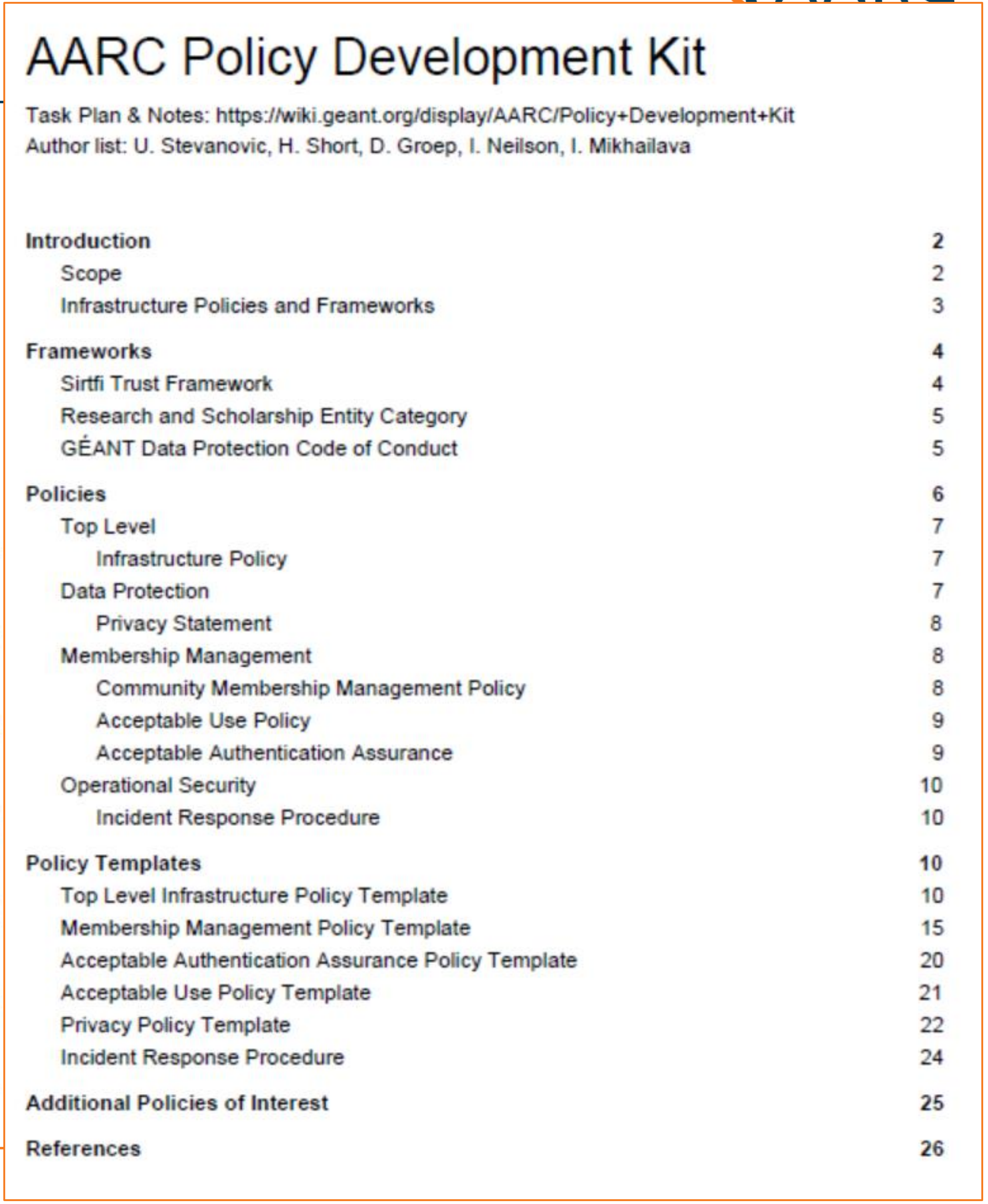
R&S

SIRTFI

Snctfi

Infrastructure Policy

- Privacy Statement
- AUP
- Acceptable Authentication Assurance
- Membership Management
- Incident Response Procedure
- ...



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
GÉANT 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
References 26

Main achievements in Policy Coordination and Engagement

Coordination through IGTF, WISE, REFEDS	→	Involvement with AARC across the globe, including XSEDE, OSG, HPCI, and EU Infra’s (EGI, EUDAT, GEANT, PRACE)
Policy Development Kit	→	Ease implementation of gapless policy set for new communities based on **Snctfi**
FIM4R reinvigoration process	→	FIM4R 2018 paper gives recommendations for Infrastructures, federations operators, and funding agencies
Harmonisation	→	More joint AAI offerings and increased use of the ‘shared service model’

PY2	Evolve Policy Development Kit with a community risk assessment method to guide adoption of appropriate policy
	Support communities and use cases in policy interpretation through Guidelines

Engagement and coordination with the global community

Snctfi

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures

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.

Co-develop

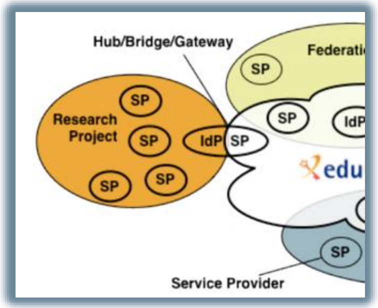
Globally through

- *WISE, SCI*
- *REFEDS*
- *IGTF*
- *joint policy groups (with EGI, EOSC, WLCG)*

/Guidelines

Implement

- ***Adopt** guidelines*
- ***Build on** collective work with EGI, EOSC-Hub, GEANT, and REFEDS*
- ***Consult** with AARC team for targeted guidelines*



Basis for **policy development kit** – *identify gaps in policy suite, coordinate best practice between peer Infrastructures, and leverage AARC templates*

Challenges

- Policy is – still – usually last on the community's priority list, yet we **need community involvement** to develop appropriate policy

provide targeted or bespoke guidance first, and
abstract from it later when possible
though when a policy need arises,
the community wants applicable policy and processes instantly!

- Same small group of experts gets to develop most if not all of the policies – general **lack of distributed skilled expertise**

through e-Infrastructures (alongside AARC2 pilots) and communities aim to identify the people that have policy interest and expertise

The ‘formal’ stuff that is coming up

- MS17/MNA3.4a in M13
  Identify community accepted frameworks to present to the competence centre: draft PDK
- MS18/MNA3.4b in M22
  Identify community accepted frameworks to present to the competence centre: evolved PDK
- MS20/MNA3.7 in M16
  Initial Data protection impact assessment on blueprint architecture
- DNA3.2 in M22
  Report on Security Incident Response and Cybersecurity in Federated Authentication Scenarios
- DNA3.3 in M23
  Accounting and Traceability in Multi-Domain Service Provider Environments
- DNA3.4 in M24
  Recommendations for e-Researcher-Centric Policies and Assurance
  and (including) the document the reviewers requested on assurance framework comparison

Things to do in AARC when you’re still alive by now …

OpSec	Attribute authority operations practice also for Infra proxies (DNA3.2)
	Trust groups and the exchange of (account) compromise information: *Sirtfi+* (DNA3.2)
Infra-centric	traceability and accounting data-collection policy framework based on SCI, providing a self-assessment methodology and comparison matrix for infrastructure services (NA3.3)
	Evolution of data protection guidance for services – driven by the community needs
Researcher-centric	Baseline AUP with major Infrastructures (EGI, EUDAT, PRACE, XSEDE) and communities
	Deployment of assurance guideline and move to high-assurance use cases “DNA3.4”
Engagement	Evolve Policy Development Kit with a community risk assessment method to guide adoption of appropriate policy (MS17/18)
	Support communities and use cases in policy interpretation through Guidelines

Thank you

Any Questions?

davidg@nikhef.nl

AARC

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).