



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*

Nik|hef

AARC2 AHM4 meeting

19 November 2018

Milano, IT

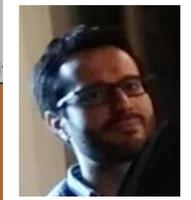
How can policy help you ease collaboration? A holistic view

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 authority



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
SIRTFI 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 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 recipient 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 coordination



2. The Community shall provide and maintain, in a repository designed for this purpose, accurate contact information as specified by the Infrastructure.

Abstract: This paper 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.

Address: 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.

1 ACCEPTABLE USE POLICY AND CONDITIONS OF USE

support for Researchers & Community



Baseline Assurance

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

resources/services provided as required by the body or bodies granting you access to the resources/services for any purpose that is unlawful or inconsistent with any administrative or security controls, intellectual property and confidentiality agreements, your access credentials (e.g. private keys or passwords), your registered information correct and up to date, and promptly report any known or suspected security breach.

Sirtfi – presentation, training, adoption in AARC2

IAM Online Europe

IAM Online Europe webinars are brought to you by AARC



iamonlineEU 001 Sirtfi

IamOnline
38 views · 4 days ago

<https://refeds.org/SIRTFI>

REFEDS > SIRTFI

sponse Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response sations. This assurance framework comprises a list of assertions which an organisation can attest in order pliant. Visit our [Wiki](#) to discover how your organisation can prepare itself for Federated Incident Response

roup has been active since 2014 and combines expertise in operational security and incident response pol- DS community. Work to publish and implement the Sirtfi Trust Framework is supported by the [AARC](#)



Benefits

Why should I join? What are the **Benefits**?



Sirtfi v 1.0

View the **Sirtfi Framework**



FAQs

Need **help**?

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:

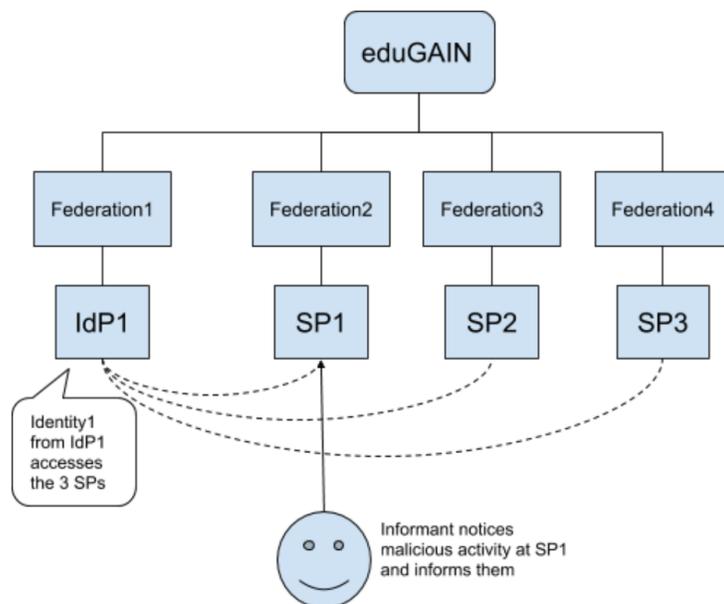
Authors: H. Short (CERN), I. Neilson (STFC), D. Groep (Nikhef)

Contributions from: R. Vinot (CIRCL)

'I Need Sirtfi Right Now™'

Test model for incident response – a continuing process ...

- 2nd Sirtfi Communications Challenge
- include eduGAIN Support Desk
- Exercise the model attack scenario ... 😊



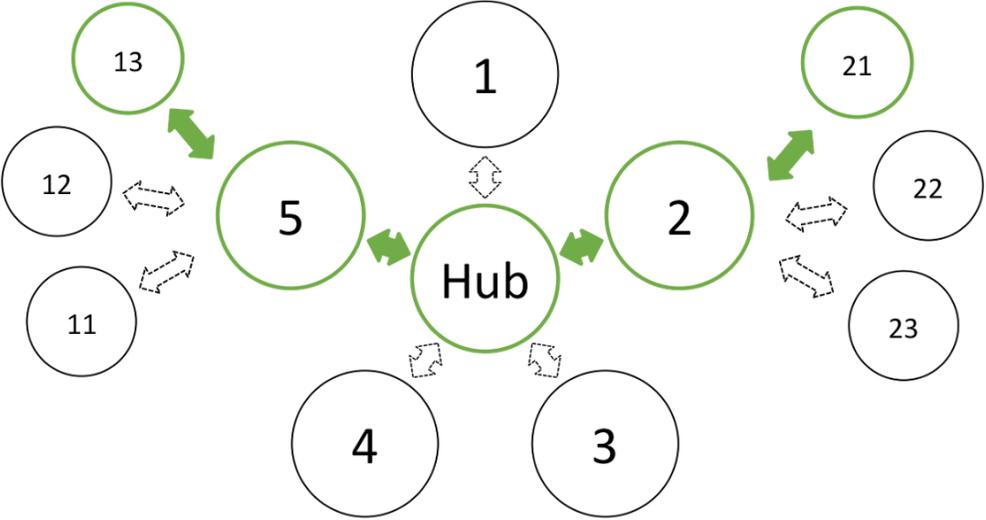
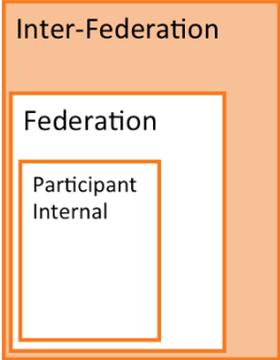
Participants

| 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



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

Inter-Federation Incident Response Communication

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 AAls 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

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 that you access.
2. You shall not use the resources/services for support or citation for your use of the resources/services.
3. You shall not use the resources/services for any purpose that is unlawful and not (attempt to) breach confidentiality agreements.
4. You shall not use the resources/services to store or transmit private keys or passwords).
5. You shall not use the resources/services to defame or libel any person or entity.
6. You shall not use the resources/services to defame or libel any person or entity.
7. You shall not use the resources/services to defame or libel any person or entity.

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).

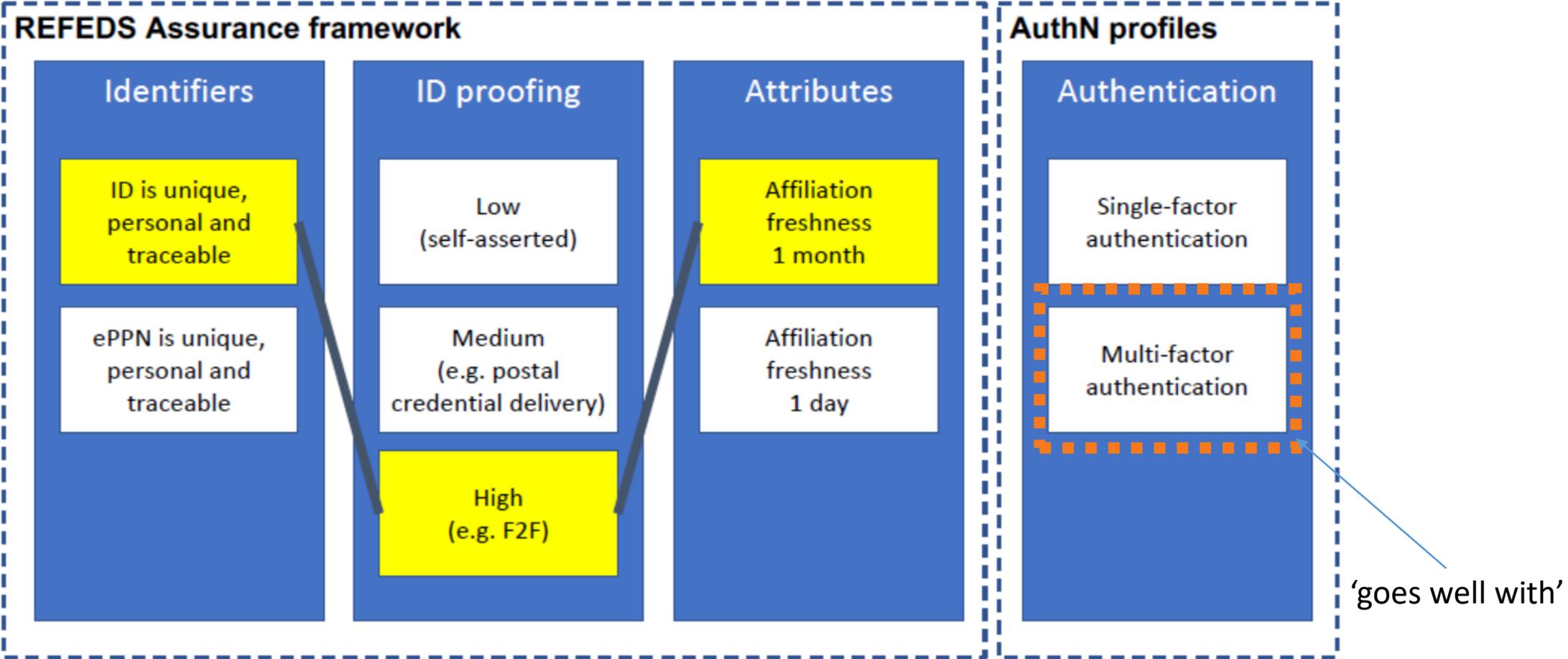
Examples of Communities include, but are not limited to: User groups, Virtual Organisations, Research Communities, Research Infrastructures, Virtual Research Communities, Projects, Communities authorised to use particular portals or gateways, and geographically organised communities.

3 Community Operations Security Policy

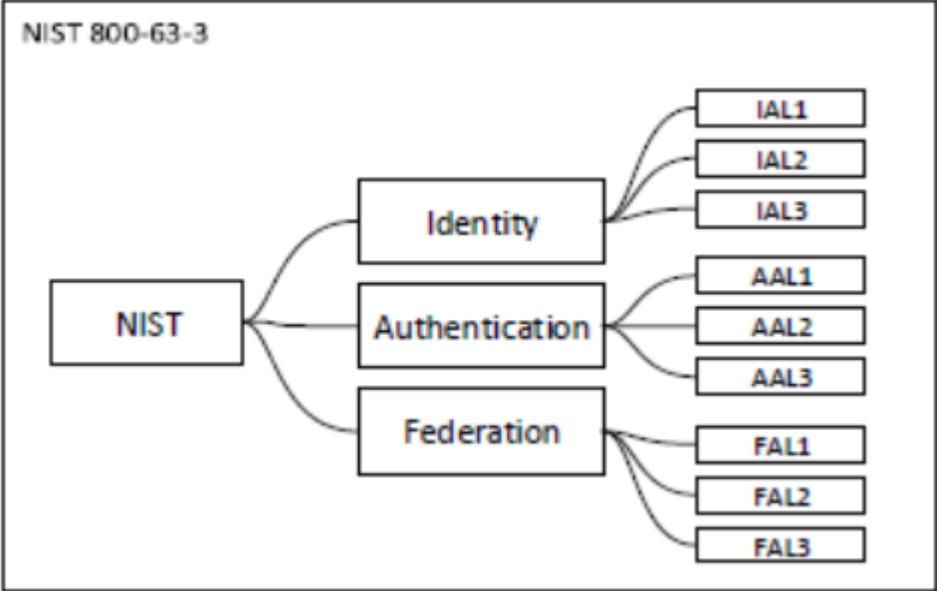
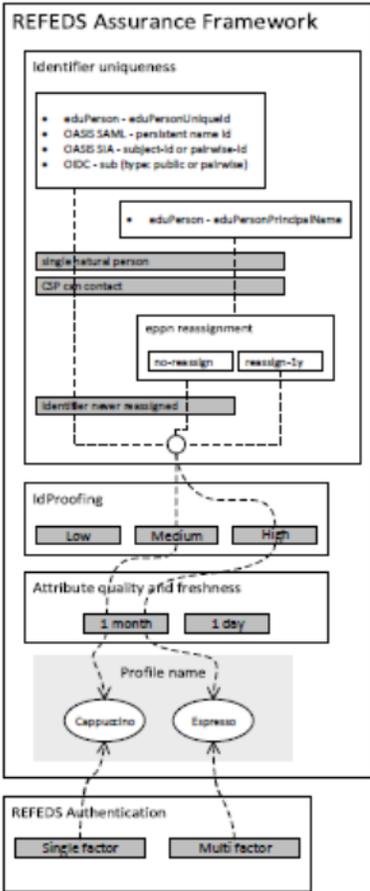
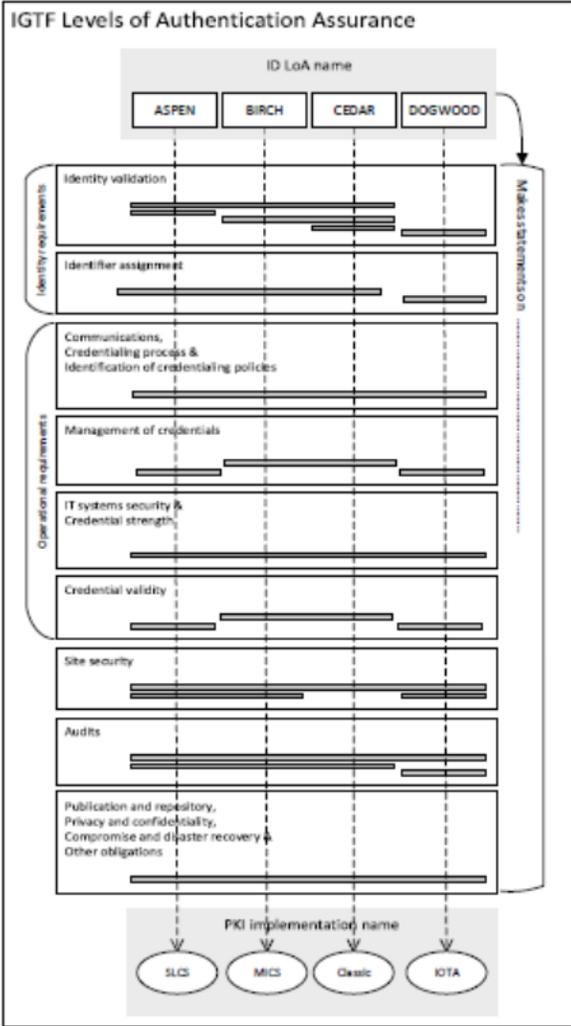
By participating in the Infrastructure, a Community Manager agrees to the conditions laid

Example: “Espresso” profile for demanding use cases

“Espresso” for more demanding use cases



Many assurance frameworks – how do they compare?



Protection of Personal Data and PII for Infrastructure AAls

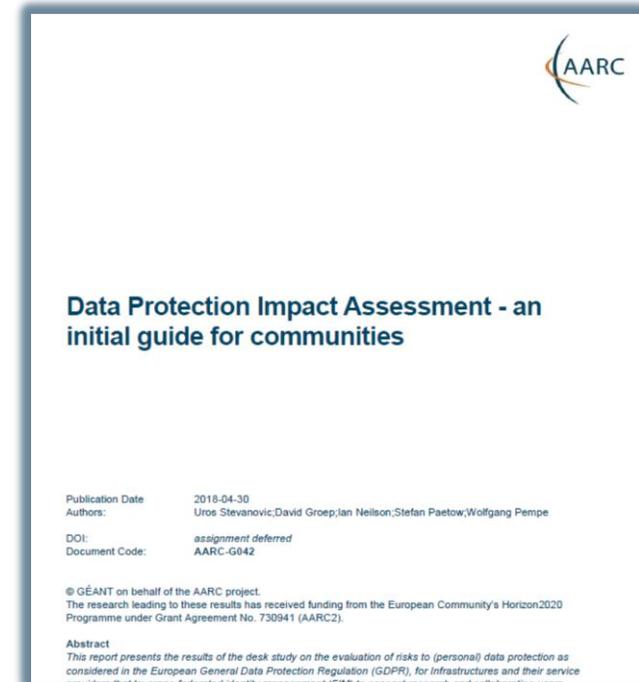
– there is both FUD but also legitimate concerns

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



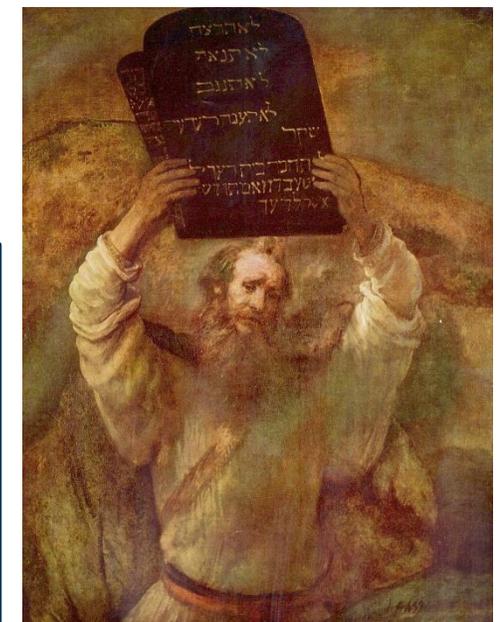
Difference to commonality in the Baseline AUP – sign once, use everywhere



| Origin | Policy Base Owner | Policy Summary | EGI | BBMRI | OTSO | EUDAT | ELIRIR | HBP | OSG Comment | Price | Self employee | RCUK |
|--------|-------------------|---|-----|-------|------|-------|--------|-----|--|-------|------------------|------|
| 1 | EGI | You will allow us the researcher to perform work, to transmit your data consistent with the data transfer policy and conditions of use of the data... | 3 | 2 | 3 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 2 | 850 | 1 |
| 2 | EGI | You will provide appropriate acknowledgment of support for your use of the data... | 3 | 2 | 3 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 0 | 850 | 0 |
| 3 | EGI | You will not use the research results for any purpose that is unlawful and/or (attempts to) breach or circumvent any administrative or security controls... | 3 | 1 | 3 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 0 | 750 | 1 |
| 4 | EGI | You will not use the research results for any purpose that is unlawful and/or (attempts to) breach or circumvent any administrative or security controls... | 3 | 0 | 3 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 0 | 850 | 2 |
| 5 | EGI | You will not use the research results for any purpose that is unlawful and/or (attempts to) breach or circumvent any administrative or security controls... | 3 | 0 | 3 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 0 | 750 | 2 |
| 6 | EGI | You will allow us to register information correct and up-to-date. | 3 | 0 | 2 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 2 | 450 | 0 |
| 7 | EGI | You will immediately report any known or suspected security breach or incident to the appropriate person... | 3 | 0 | 2 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 0 | 450 | 0 |
| 8 | EGI | You use the research results in your own work, there is no guarantee that the research results will be available at any time or that they will be available in the future... | 3 | 0 | 3 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 0 | 450 | 0 |
| 9 | EGI | You agree that these information, including personal data provided by you for registration purposes, may be used for administrative, operational, accounting, or research purposes... | 3 | 0 | 3 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 0 | 750 | 1 |
| 10 | HBP | Regarding privacy, you or a participant in clinical trial will not be asked to provide personal data... | 0 | 1 | 0 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 0 | 1 | 1 |
| 11 | EGI | You will not use the research results for any purpose that is unlawful and/or (attempts to) breach or circumvent any administrative or security controls... | 3 | 0 | 3 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 2 | 750 | 1 |
| 12 | EUDAT | You must respect the privacy of other users for example, not to disclose their information to, obtain copies of, or modify files, reports or records of other users... | 0 | 2 | 3 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 0 | 3 | 3 |
| 13 | PRACE | The User will not use the personal data which is provided for the purposes of the activities in an official manner... | 0 | 1 | 3 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 0 | 3 | 3 |
| 14 | PRACE | The User will not use the personal data which is provided for the purposes of the activities in an official manner... | 0 | 0 | 3 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 0 | 3 | 3 |
| 15 | BBMRI | Provider may request that data during from SimpleQuery are transferred to the appropriate legal and jurisdictional authorities... | 0 | 3 | 3 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 0 | 3 | 3 |
| 16 | HBP | of Switzerland, including any conflict of law rules, shall apply... | 0 | 0 | 3 | 3 | 3 | 3 | Expanded: "Use of personal data for research purposes" and "Data protection" | 0 | 3 | 3 |

Support any known or lost or loss or credentials. Add: EUDAT is not liable to any compensation in case of lost data or loss of service

Support any known or lost or loss or credentials. Add: Although efforts are made to maintain confidentiality, no guarantees are given. Expanded for PI under "Personal information and data privacy"



Scaling Acceptable Use Policy and data release

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

Community specific terms & conditions

Community specific terms & conditions

Community conditions

RI Cluster-specific terms & conditions

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

AARC-I044 Implementers Guide

AARC-I044
Implementers Guide to the WISE Baseline Acceptable Use Policy



3. The WISE Baseline AUP

The WISE Baseline AUP¹ 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

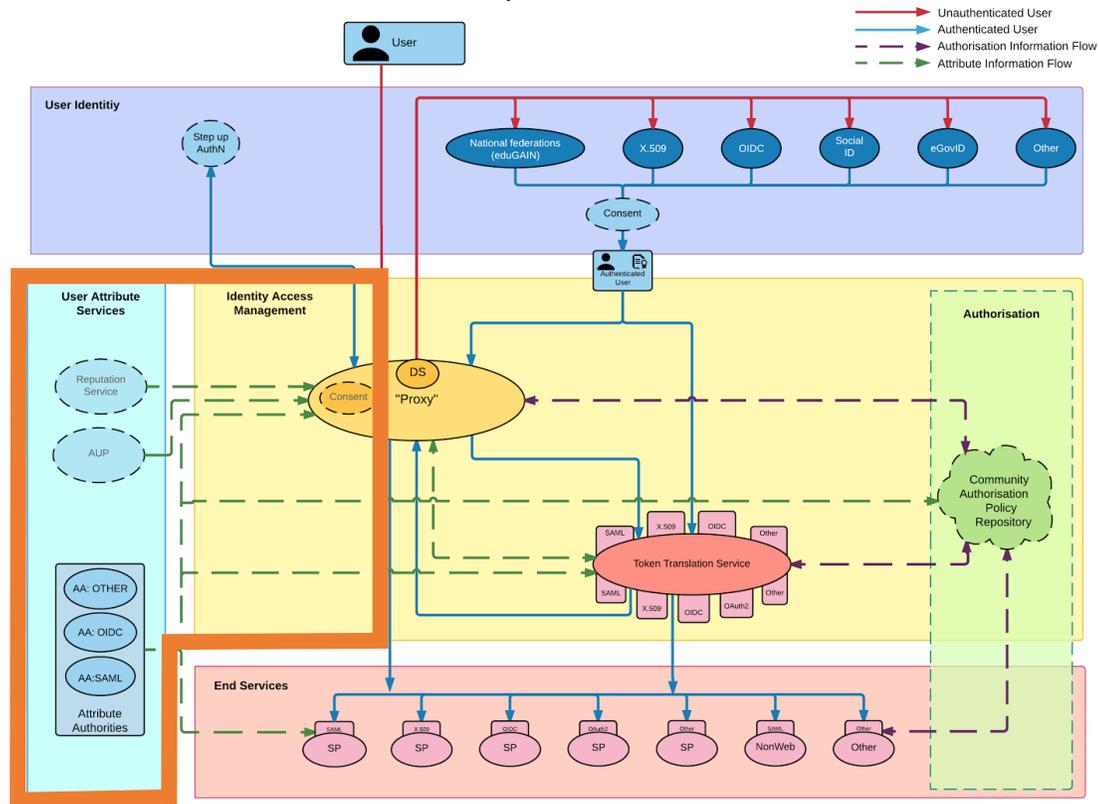
This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services ("Services") as granted by {community, agency, or infrastructure name} for the purpose of {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.

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

AARC Blueprint Architecture



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



Snctfi

igtf.net/snctfi

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 Information Security 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



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

Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements

Status: Draft

Editors: Kelsey, Groep, Short, Sallé

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

Policy Development Engagement and the 'Kit'

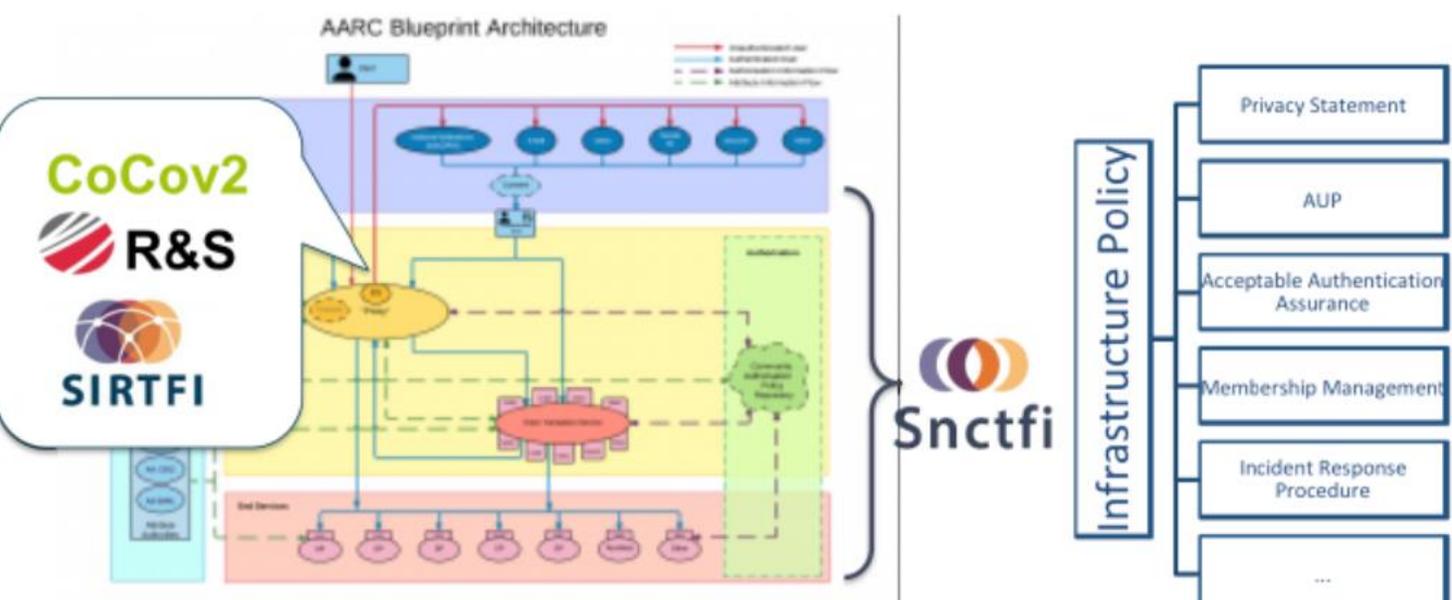
- Bring together a consistent suite of policies & guidance
- based on e-Infrastructure best practices from advanced operational infrastructures today

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

| | |
|---|-----------|
| 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 |
| | 26 |



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

| | |
|--|----------|
| Policies | 7 |
| Top Level | 7 |
| Infrastructure Policy | 7 |
| Data Protection | 8 |
| Privacy Statement | |
| Risk Assessment | |
| Membership Management | |
| Community Membership Management Policy | |
| Acceptable Use Policy | |
| Acceptable Authentication Assurance | |
| Operational Security | |
| Incident Response Procedure | |

| |
|---|
| Policy Templates |
| Top Level Infrastructure Policy Template |
| Membership Management Policy Template |
| Acceptable Authentication Assurance Policy Template |
| Acceptable Use Policy Template |
| Privacy Policy Template |
| Risk Assessment |
| Incident Response Procedure |

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.

Acceptable Authentication Assurance Policy Template

- Taken from <https://doc.dit#>
- This policy
- 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

Top Level Infrastructure Policy Template

- INTRODU
This policy
Infrastruct
- 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 <https://documents.egi.eu/public/RetrieveFile?docid=3015&version=3&filename=EGI-SPG-SecurityPolicy-V2.pdf>

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

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

SCIv2 – beyond its endorsement to self-assessment and review



A Trust Framework for Security Collaboration among Infrastructures

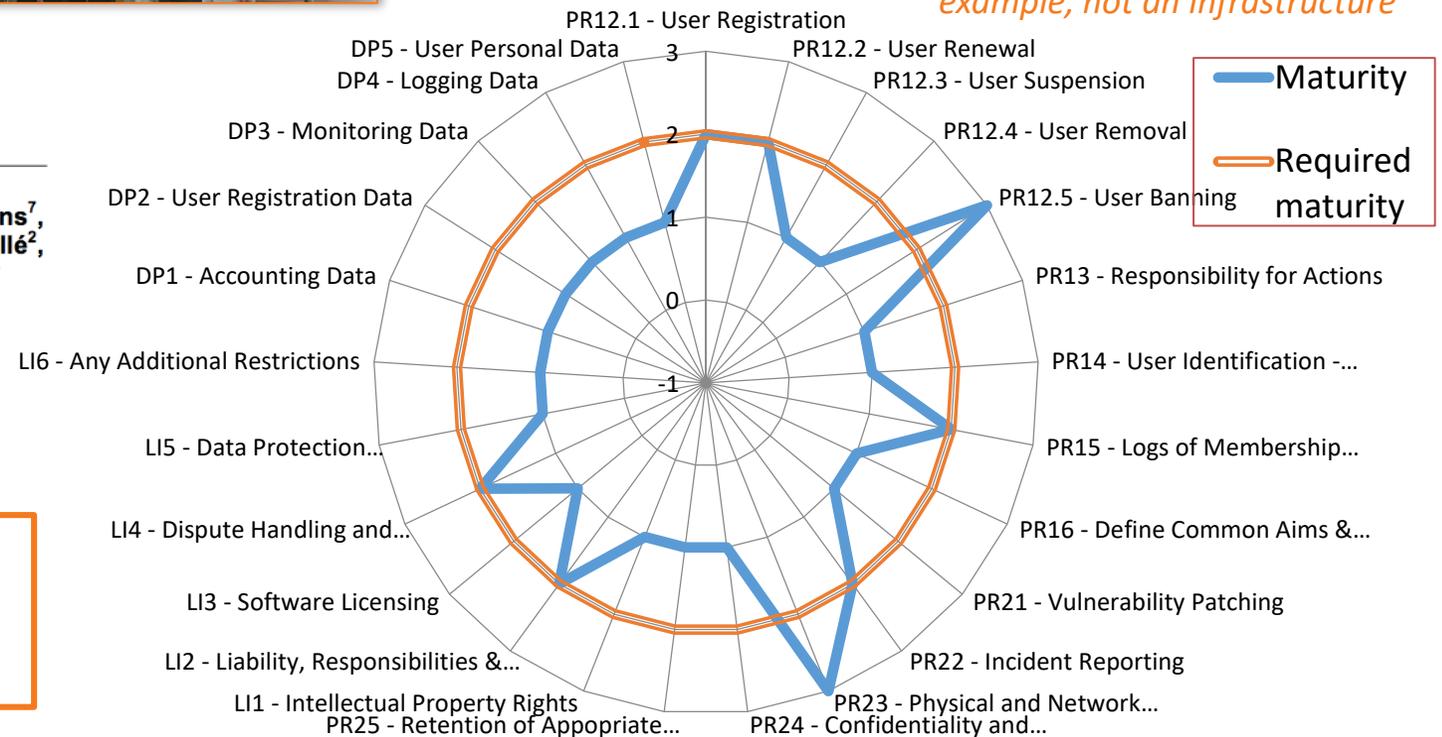
SCI version 2.0, 31 May 2017

L Florio¹, S Gabriel², F Gagadis³, D Groep², W de Jong⁴, U Kaila⁵, D Kelsey⁶, A Moens⁷, I Neilson⁶, R Niederberger⁸, R Quick⁹, W Raquel¹⁰, V Ribailier¹¹, M Sallé², A Scicchitano¹², H Short¹³, A Slagell¹⁰, U Stevanovic¹⁴, G Venekamp⁴ and R Wartel¹³

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

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

example, not an infrastructure



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

Resear- cher- centric

Baseline AUP with major Infrastructures (EGI, EUDAT, PRACE, XSEDE) and communities

Deployment of **assurance guidelines** and assess high-assurance use cases (BBMRI)

Engage- ment

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/>

