



Authentication and Authorisation for Research and Collaboration

Things to do in
Policy and Best Practice Harmonisation
when you're in Orlando ... and thereafter

David Groep *for the entire AARC Policy Team*



I2TechEX18 meeting

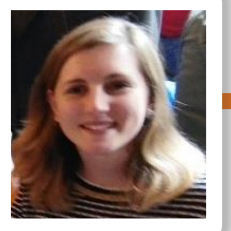
17 October 2018

Orlando

How can policy help you ease collaboration? A holistic view



Operational Security for FIM Communities

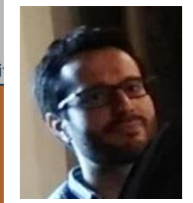


GDPR-style Code of Conduct – a new way?

- 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 context
- "Say what you do, and do as you say" – transparency is our real benefit towards the person whose data



3 Community Operations Security Policy

engagement and coordination



1 ACCEPTABLE USE POLICY AND CONDITIONS OF USE

support for Researchers & Community



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.

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

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:

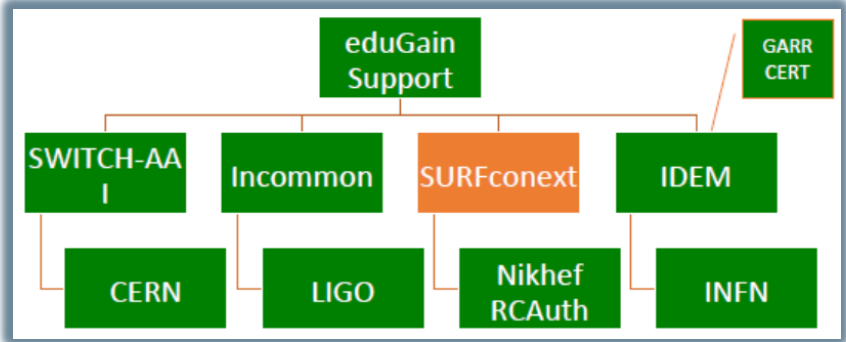
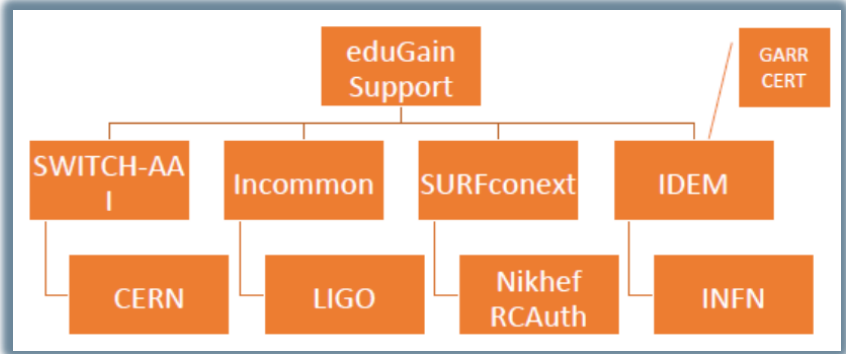
Authors: H. Short (CERN), I. Neilson (STFC), D. Groep (Nikhef)

Contributions from: R. Vinot (CIRCL)

'I Need Sirtfi Right Now™'

Test model for incident response – a continuing process from now on ...

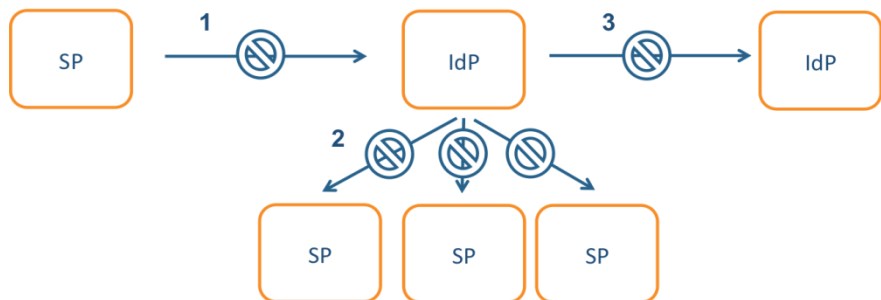
- Defines the model actors
- include eduGAIN Support Desk
- Exercise the model attack scenario ... 😊



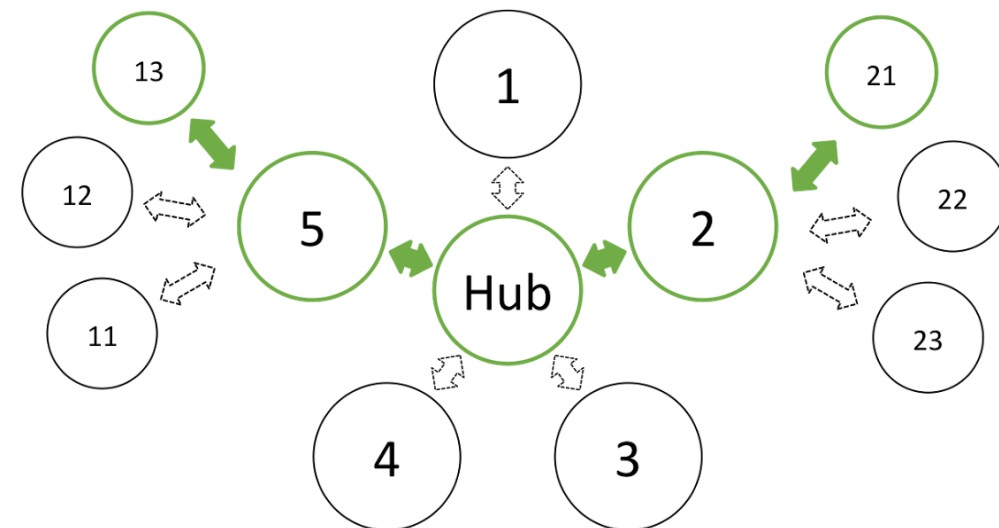
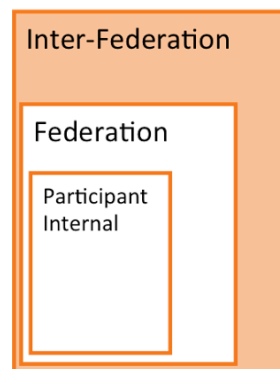
parties involved in response challenge

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

Incident response process evolution in federations – beyond Sirtfi



Incident Response Communication, communication blocks



Inter-Federation Incident Response Communication

Challenges

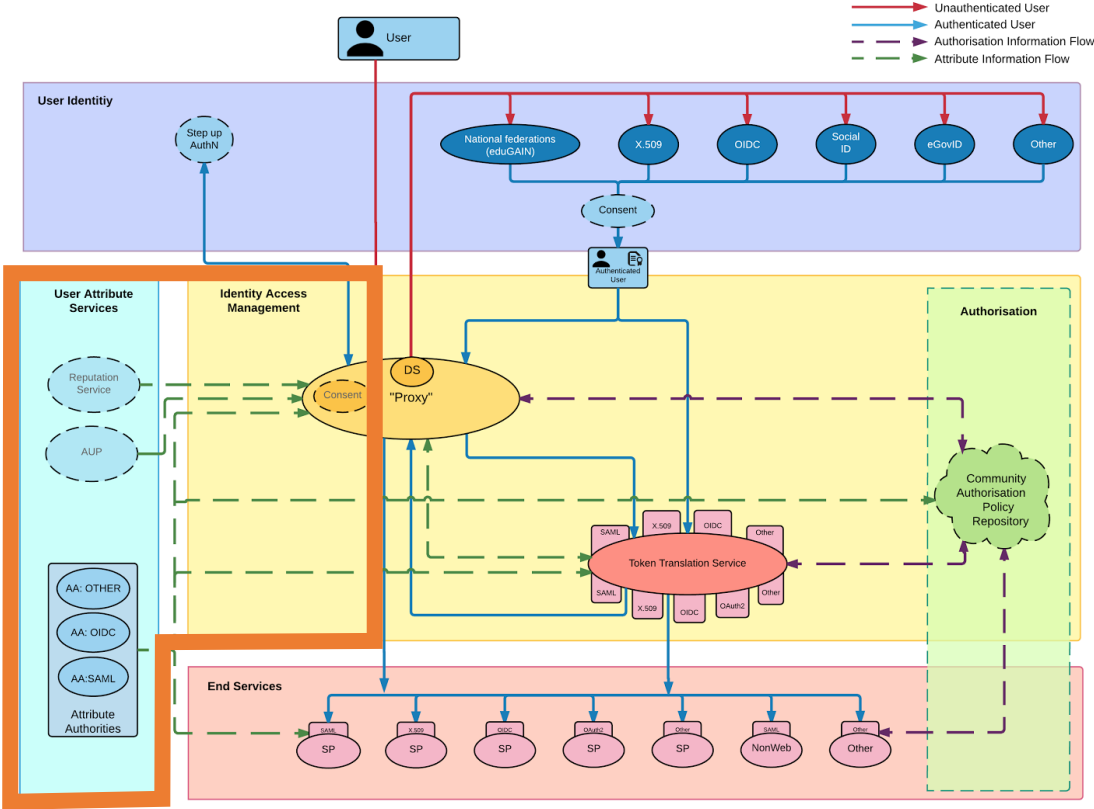
- **IdP fails to inform other affected SPs**, for fear of leaking data, of reputation, or just lack of interest and knowledge
- **No established channels** of communication, esp. not **to federations** themselves!

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?



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

AARC Blueprint Architecture



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



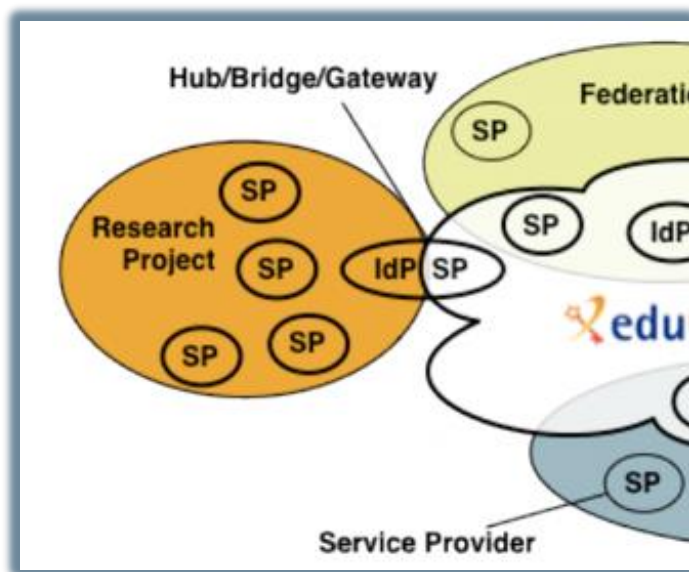
Snctfi
Scalable Negotiator for a Community Trust Framework in Federated Infrastructures

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

A policy framework for service providers groups and proxies in the BPA

Snctfi

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures



graphic IdP-SP bridge: Lukas Hammerle and Ann Harding, SWITCH

igtf.net/snctfi



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

WISE Information Security for **E**-infrastructures got global endorsement SCI in June 2017

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

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 is lawful and not (attempt to) breach confidentiality agreements.
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 for any purpose that is unlawful and not (attempt to) breach confidentiality agreements.
5. You shall not use the resources/services for any purpose that is unlawful and not (attempt to) breach confidentiality agreements.
6. You shall not use the resources/services for any purpose that is unlawful and not (attempt to) breach confidentiality agreements.
7. You shall not use the resources/services for any purpose that is unlawful and not (attempt to) breach confidentiality agreements.

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

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



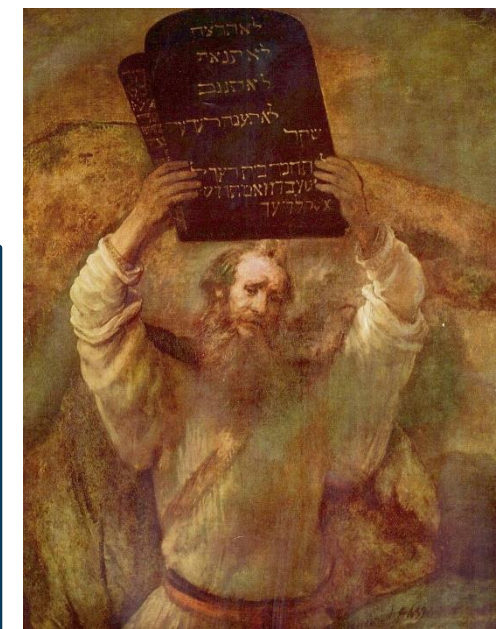
Origin	Policy Base Owner	Policy Summary	EGI	BBMRI	OTSO	EUDAT	ELIRIR	HBP	OSG Comment	Price	Self employee	RCUK		
1	EGI	You will allow us the researcher to perform work, to transmit your data consistent with the data transfer policy and conditions of use of the data...	3	2	3	3	3	3	Expanded: "Use of personal data for research purposes" and "Data protection"	2	850	1	1	770
2	EGI	You will provide appropriate acknowledgment of reporter citation for your use of the research resources provided for you by us...	3	2	2	2	2	2	Expanded: "Use of research resources with 'inappropriate' use of data" (Commercial data, advertising, (LDD)) Software protection. User must respect the data protection provided by copyright and license of software and data for example, with Expanded under "Accuser Conditions" with best practice update.	0	850	0	0	400
3	EGI	You will not use the research resources for any purpose that is unlawful and not (attempt) to such or circumvent any administrative or security controls.	3	1	3	3	3	3	Expanded: "Use of research resources with 'inappropriate' use of data" (Commercial data, advertising, (LDD)) Software protection. User must respect the data protection provided by copyright and license of software and data for example, with Expanded under "Accuser Conditions" with best practice update.	0	750	1	1	420
4	EGI	You will not use the research resources and confidentiality agreements.	3	0	3	3	3	3	Expanded: "Use of research resources with 'inappropriate' use of data" (Commercial data, advertising, (LDD)) Software protection. User must respect the data protection provided by copyright and license of software and data for example, with Expanded under "Accuser Conditions" with best practice update.	3	850	2	2	800
5	EGI	You will not allow your account credentials to be shared with a second user.	3	0	3	3	3	3	You must keep your account secure and not share the account details with any other user. (NB: USE) Any other user must use your account.	0	750	2	1	700
6	EGI	You will allow us all your registered information correct and up-to-date.	3	0	2	2	2	2	You will have only one (Profile) User account and will have your profile information up-to-date.	2	400	0	0	350
7	EGI	You will immediately report any known or suspected security breach involving the research resources or account credentials to the specific data protection officer.	3	0	2	2	2	2	You will immediately report any known or suspected security breach involving the research resources or account credentials to the specific data protection officer.	0	450	0	1	500
8	EGI	You are the owner of the research resources. There is no guarantee that the research resources will be available at any time or that they will last.	3	0	3	3	3	3	Add: EUDAT is not liable to any compensation in case of lost data or loss of service.	0	470	0	0	530
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	Add: Although efforts are made to maintain confidentiality, no guarantees are given. Expanded for PI under "Personal information and data privacy".	3	750	1	1	420
10	HBP	Regarding privacy, you are a participant in clinical trials and your personal data will be processed and stored in a secure and confidential manner.	0	1	1	1	1	1	7. Personal Data Policy - Consent, Preserving, Accuser, etc.	0	1	1	1	100
11	EGI	You are liable for the consequences of your violation of any of these conditions of use, which may include but not limited to the reporting of your violation to your institution.	3	0	3	3	3	3	10. Limitation and Liability - The Contributor reserves the rights for inclusion in any trial, temporary or otherwise.	2	750	1	0	400
12	EUDAT	You must respect the privacy of other users for example, not to disclose their information, or obtain copies of, or modify files, reports or source code.	0	2	2	2	2	2	Add: "Administrative Action" section.	0	3	3	3	3
13	PRACE	The User will have regard to the principles which govern the processing of personal data for the purposes and conduct the activities in an ethical manner.	0	1	1	1	1	1	Add: "Administrative Action" section.	0	3	3	3	3
14	PRACE	The User understands that the use of Resources by individuals at certain centres may be restricted by policies laid down by the Register or the Resource Provider.	0	0	0	0	0	0	Add: "Administrative Action" section.	0	3	3	3	3
15	BBMRI	Resource Provider may request that data during from SampleData are transferred to back the respective PI.	0	3	3	3	3	3	Add: "Administrative Action" section.	0	3	3	3	3
16	HBP	Application Law and Jurisdiction. The applicable law will be that of the United Kingdom. The applicable law will be that of the United Kingdom.	0	0	0	0	0	0	Add: "Administrative Action" section.	0	3	3	3	3

Support any known or lost or loss of credentials.

Phone number for backup

Adds: EUDAT is not liable to any compensation in case of lost data or loss of service

Adds: 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)

Look ahead to an ACAMP session on a global baseline AUP

This allows a layered approach to the construction of the AUP, where the AUP presented to the end-user (on enrolment or later) comprises both the generic JSPG-evolved version plus the community-specific additions.

The LS AAI shall present an Acceptable Use Policy also on behalf of its connected services and infrastructures.

The LS AAI operators shall present as the AUP:

- the common aims and purposes, i.e. the research or scholarship goals of the Life Sciences Research Infrastructures (in a few high-level sentences)
This text must be supplied by the Life Sciences community.
- the list of 11 (eleven) items from the Evolved JSPG AUP [JSPGAUP2]
- a notice that enrolment into specific groups or subdivisions may require the user to sign supplementary terms and conditions, and
- that in specific circumstance also specific services *may* ask the user to sign additional conditions of use.

If the Life Sciences community agrees to any joint clauses (do not attempt to reverse privacy-enhancing technologies, for instance), these should be included in the LS AAI AUP.

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 designed to support the expansion of open science in



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

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



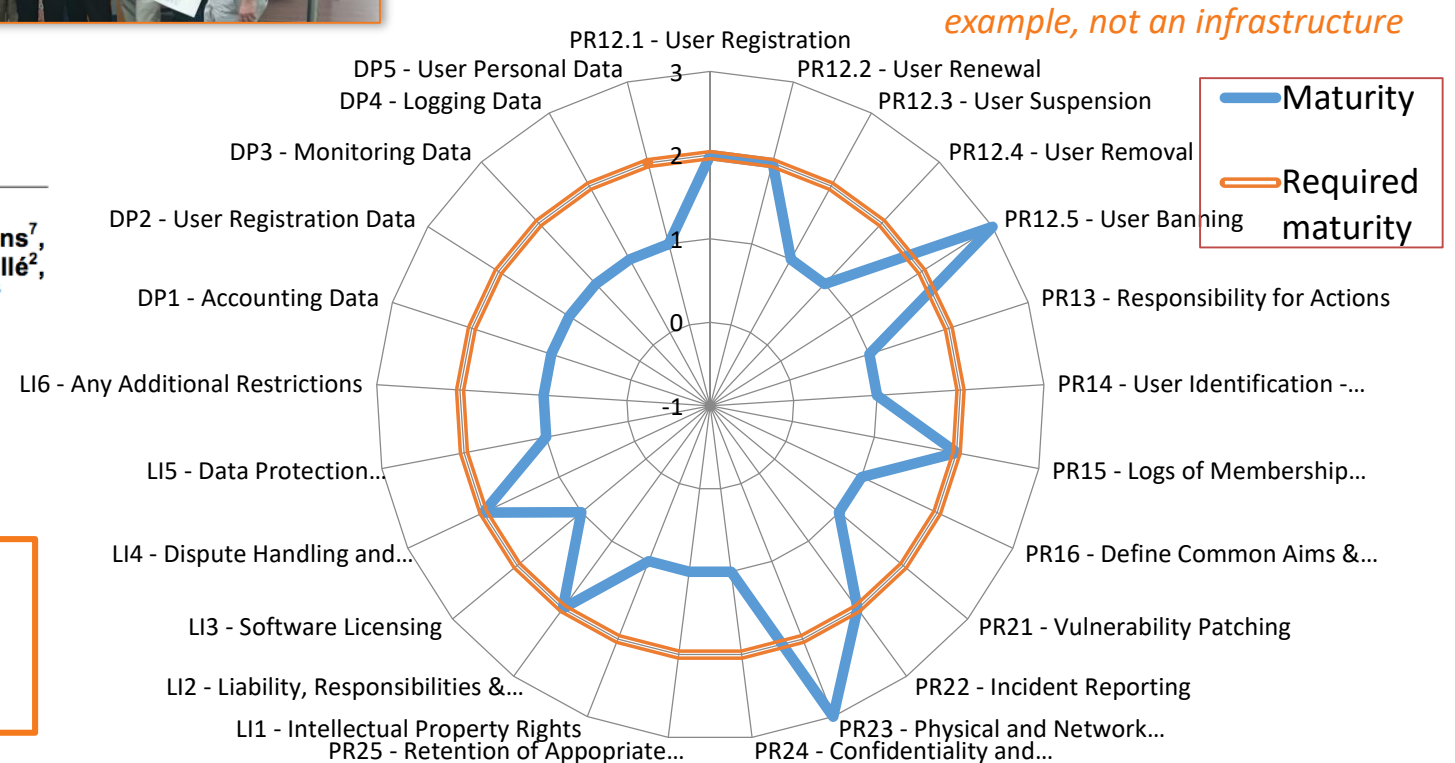
A Trust Framework for Security Collaboration among Infrastructures

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



Policy Development Engagement and the 'Kit'

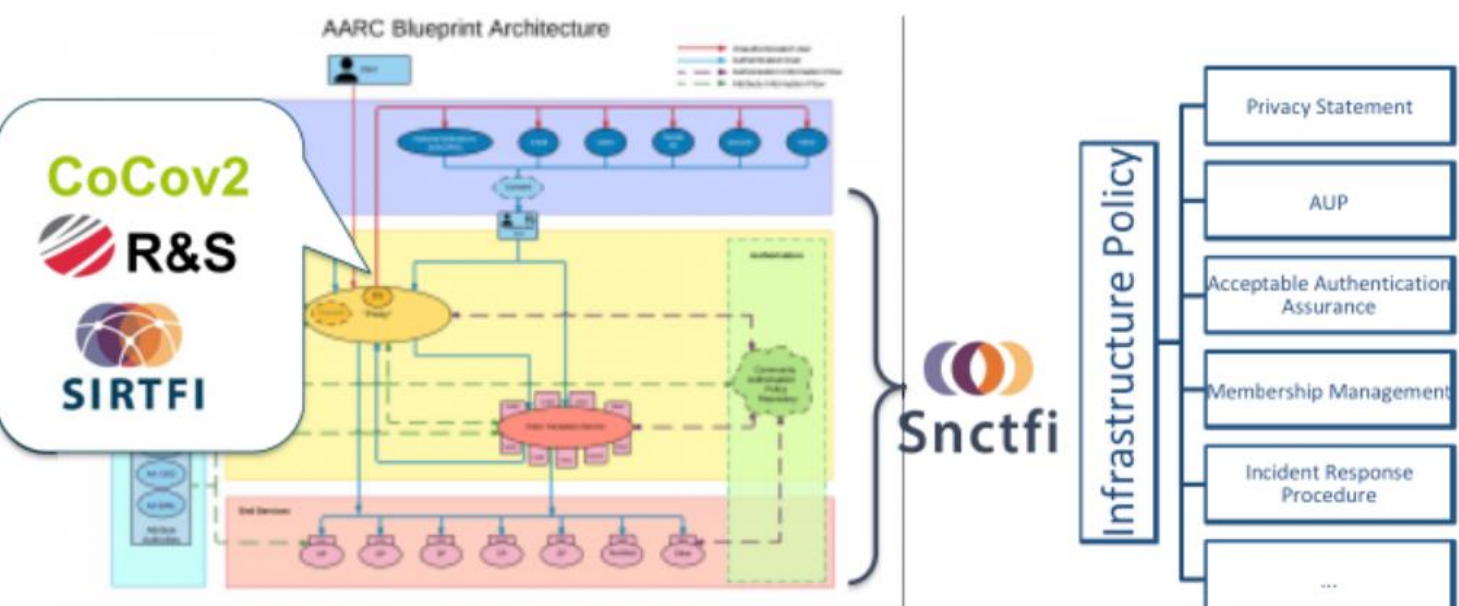
- Bring together a consistent suite of policies & guidance
- based on e-Infrastructure best practices from advanced operational infrastructures today

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

INTRODU
This policy
Infrastruct

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 <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

Things to do in AARC's last year 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

Research-centric

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

Deployment of **assurance guidelines** and move to high-assurance use cases


Engagement

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

If we don't: there is also commercial GDPR guidance for research and collaboration

View this email in your browser



shreddingMachines.co.uk

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**

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!

Thank you Any Questions?

davidg@nikhef.nl



<http://aarc-project.eu/>

