

Enabling Communities Building trust for research and collaboration.

Maarten Kremers, SURF

ISGC 2023
23rd March 2023
Taipei



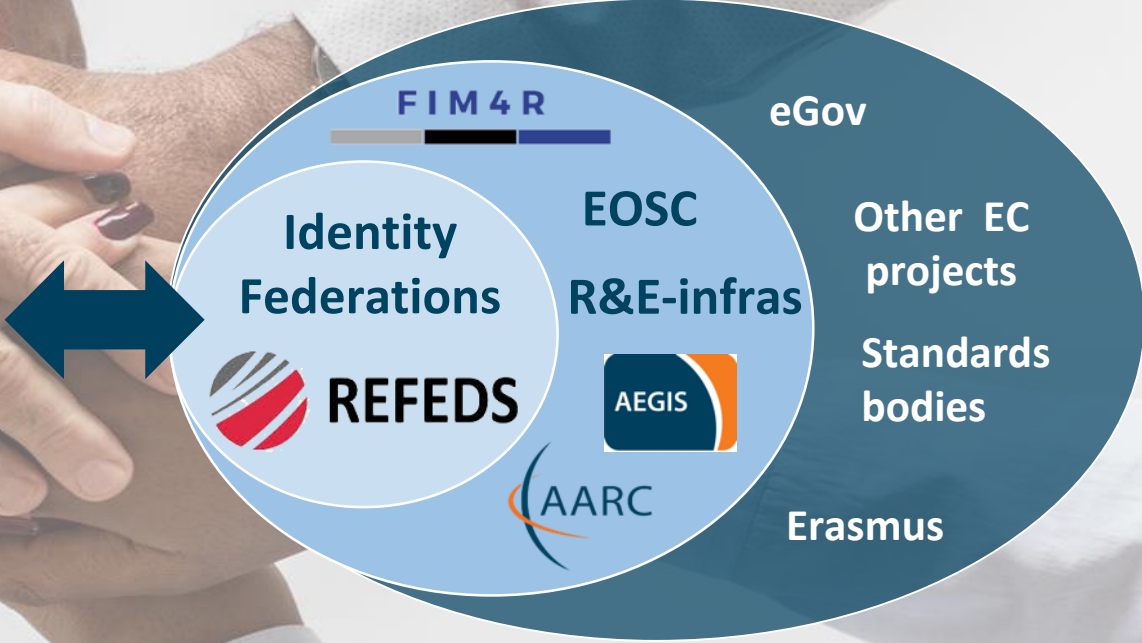
GN5-1 T&I Team and Key Collaborations

WP 5



Marina Adomeit SUNET
Maarten Kremers SURF

| | | | |
|----|------------------------|--|------|
| T1 | | Paul Dekkers SURF | |
| T2 | | Davide Vagheti GARR | |
| T3 | Core AAI Platform | Christos Kanellopoulos GÉANT | |
| T4 | | Michelle Williams GÉANT | |
| T5 | | Niels van Dijk SURF Michael Schmidt LRZ | |
| T6 | Enabling Communities | Maarten Kremers SURF | |
| T7 | Distributed Identities | Christoph Graph, SWITCH | |



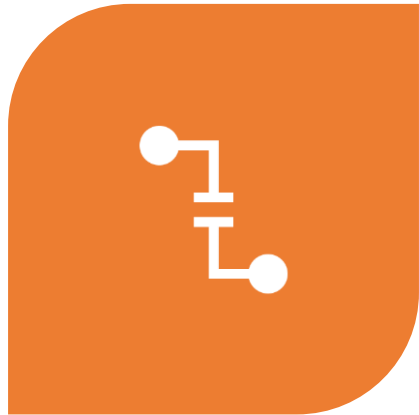
Enabling Communities

T&I eScience Global Engagement

The 'eScience Global Engagement' of EnCo in the GEANT project is there to support those developments in **the policy and best practice areas** that would benefit **the community at large**, and do that by means of **supporting** the work in the **existing forums** such as WISE, FIM4R, IGTF, REFEDS, AARC-community, and the research and e-Infra communities directly



T&I Enabling Communities



INTEROPERABILITY



TRUST

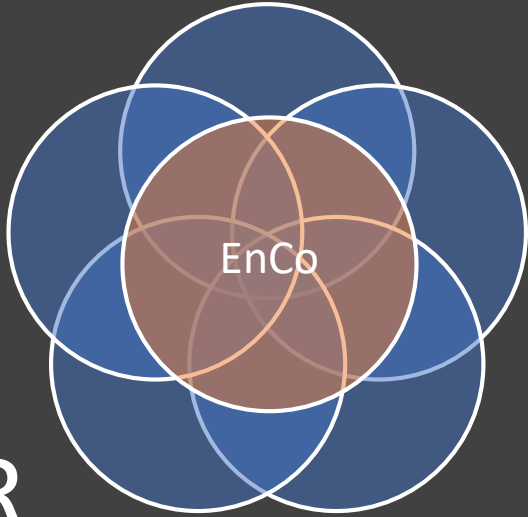


SECURITY

REFEDS



IGTF

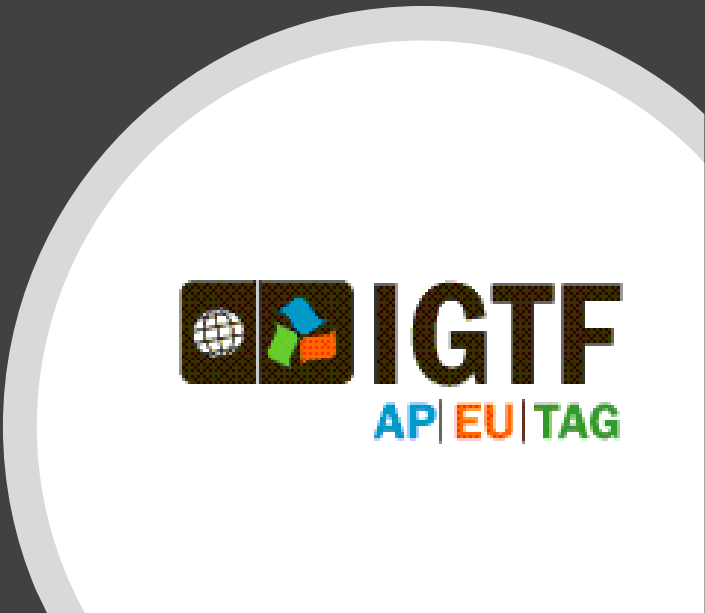


AARC



FIM4R

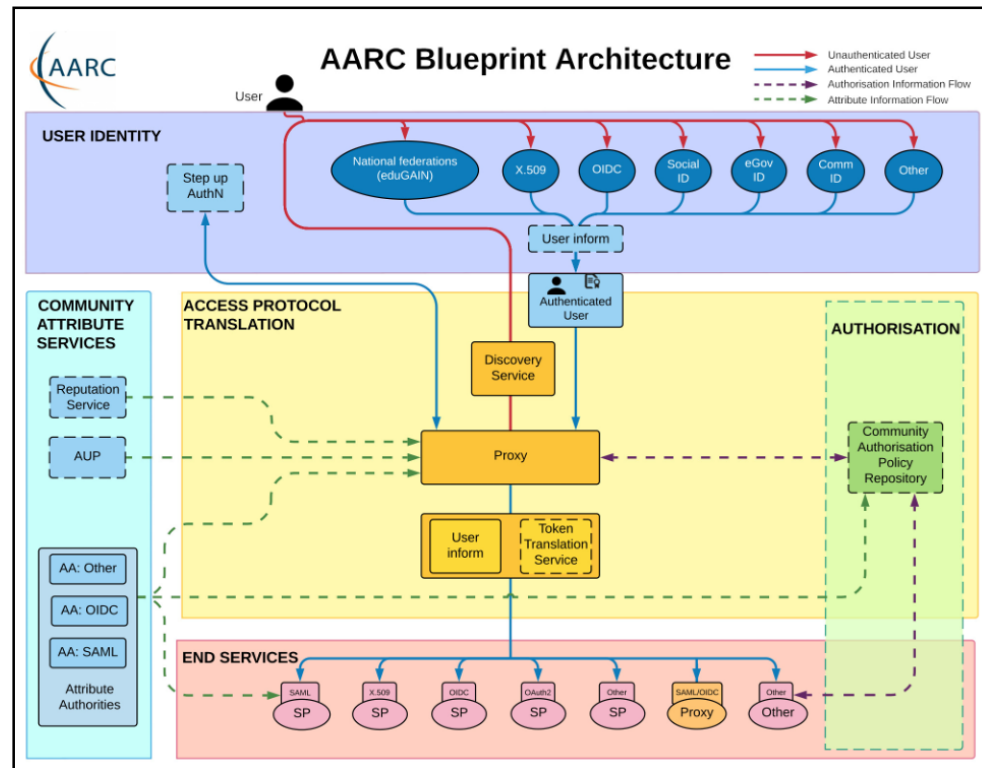
WISE





Interoperability, sustainability, integration and compatibility: **Authentication and Authorisation for Research and Collaboration (AARC)** – a set of turn-key AAI solutions bringing research collaborations closer together.

T&I Enabling Communities



The AARC Blueprint Architecture (BPA)

is a set of software building blocks that can be used to implement federated access management solutions for international research collaborations.

T&I Enabling Communities



Harmonising rules for a common infrastructure: The **Policy Development Kit (PDK)**
Harmonising the rules that organisations apply to identity management is essential for achieving an integrated AAI framework.

T&I Enabling Communities

Not sure how to begin with the AARC Blueprint Architecture? There are plenty of [guidelines](#) available but it can be a minefield at first. Here you can find common questions matched to the relevant Blueprint Architecture component, along with links to guidelines that can help.

Getting Started:

- How should I design my infrastructure? What is the AARC Blueprint Architecture? [AARC-G045](#)
- How should I approach performing a Data Protection Impact Assessment? [AARC-G042](#)
- How should my infrastructure support Federated Security Incident Response? [AARC-I051](#)

Access Protocol Translation:

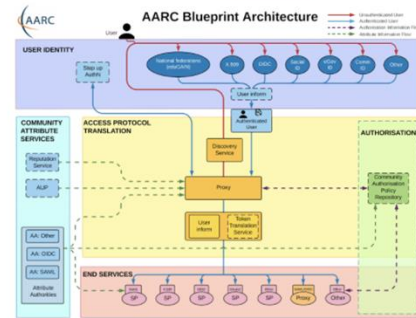
- Which best practices should I follow for my Token Translation Services? [AARC-G004](#)
- How should I translate from Identity Federation information to X.509 certificates? [AARC-G010](#)

Proxies:

- How can I ensure that my proxy is able to accurately claim that it supports best practices in Identity Federation? [AARC-G015](#)
- How should I express assurance information for users when interacting with another proxy? [AARC-G021](#)

Community Attribute Services:

- How should attributes from multiple sources be aggregated? [AARC-G003](#)
- How should I express the home institute of a user? [AARC-G025](#)
- What are the best practices for running my Attribute Authorities securely? [AARC-G048](#)
- Which Acceptable Use Policy should I use to facilitate interoperability? [AARC-I044](#)



End Services:

- My service needs to act on behalf of the user - how should I handle credential delegation and impersonation? [AARC-G005](#)
- My services are not web based, how can I use identities from the proxy? [AARC-G007](#)
- How should Services hint which IdP they would like users to use? [AARC-G049](#)
- Which Security practices should I follow? [AARC-G014](#)

User Identity:

- How should I integrate Social Media Identity Providers? [AARC-G008](#)
- How should users link accounts, and how does that affect Assurance? [AARC-G009](#)
- How should services indicate that they would like users to authenticate with multifactor authentication, and how should my proxy forward that information? [AARC-G029](#)

Assurance:

- How should assurance information of external identities be calculated? [AARC-G031](#)
- What can I say about assurance of identities from social media accounts? [AARC-G041](#)
- How is assurance impacted by account linking? [AARC-G009](#)
- How should assurance information be shared with other infrastructures? [AARC-G021](#)
- Which Assurance Profiles should I use, there are so many! [AARC-I050](#)

Authorisation:

- How should I manage authorisation information from multiple sources? [AARC-G006](#)
- How should group and role information be expressed to facilitate interoperability? [AARC-G002](#)
- How should resource capabilities be expressed? [AARC-G027](#)

What next? Are you looking for a kick start with your policies? Take a look at the [Policy Development Toolkit](#) which provides a set of templates.

Certain guidelines are being adopted by the AEGIS community to support interoperability between infrastructures - consider prioritising [these best practices](#).

Linking Guidelines, BPA and PDK

<https://aarc-project.eu/aarc-hitecture/>

<https://edu.nl/h3dm4>



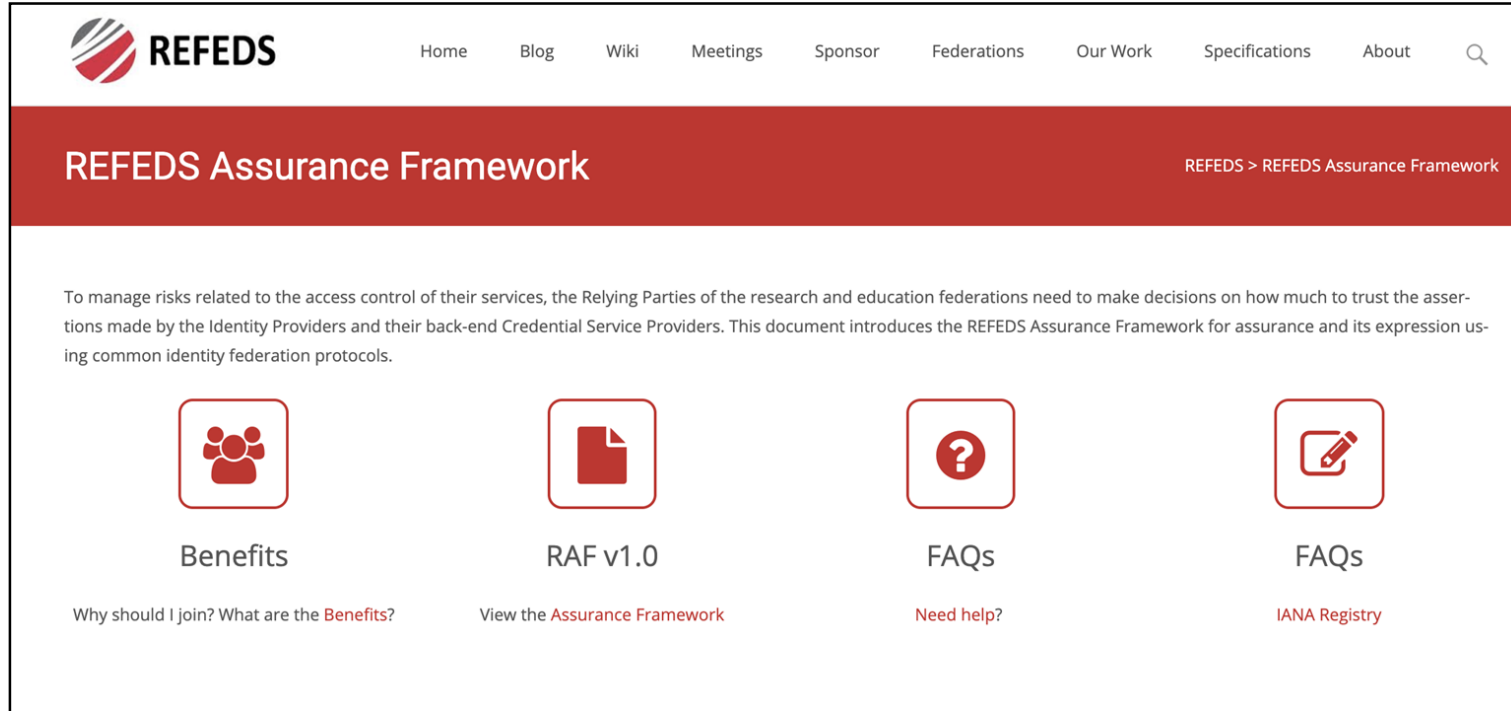
The **AARC Engagement Group for Infrastructures (AEGIS)** brings together global representatives from AAI operators in **research infrastructures and e-infrastructures**, which are **implementing authentication and authorisation** services that support **federated access**, to discuss **adoption of policy and technical best practices** that facilitate interoperability across e-infrastructures and research infrastructures.





REFEDS (the Research and Education FEDerations group) is to be the voice that articulates the mutual needs of research and education identity federations worldwide.

T&I Enabling Communities



The screenshot shows the REFEDS Assurance Framework page. At the top, there is a navigation menu with links for Home, Blog, Wiki, Meetings, Sponsor, Federations, Our Work, Specifications, and About. The main heading is "REFEDS Assurance Framework" with a breadcrumb trail "REFEDS > REFEDS Assurance Framework". Below the heading, there is a paragraph explaining the purpose of the framework: "To manage risks related to the access control of their services, the Relying Parties of the research and education federations need to make decisions on how much to trust the assertions made by the Identity Providers and their back-end Credential Service Providers. This document introduces the REFEDS Assurance Framework for assurance and its expression using common identity federation protocols." Below this text are four icons representing different sections: "Benefits" (group of people), "RAF v1.0" (document), "FAQs" (question mark), and "FAQs" (document with pencil). Each icon has a corresponding text label and a link below it: "Benefits" (Why should I join? What are the Benefits?), "RAF v1.0" (View the Assurance Framework), "FAQs" (Need help?), and "FAQs" (IANA Registry).

REFEDS Assurance Profile (v1.0)

- Consisting of **three individual specifications**:
 - [REFEDS Assurance Framework](#) (RAF), ver 1.0, published 2018
 - [REFEDS Single Factor Authentication Profile](#) (SFA), ver 1.0, 2018
 - [REFEDS Multi Factor Authentication Profile](#) (MFA), ver 1.0, 2017
- Component-based approach
- Two identity assurance profiles: Espresso (high assurance) and Cappuccino (moderate assurance)

v2.0 in progress





PROCEEDINGS
OF SCIENCE

Making Identity Assurance and Authentication Strength Work for Federated Infrastructures

Jule Anna Ziegler,^{a,*} Uros Stevanovic,^b David Groep,^c Ian Neilson,^d David P. Kelsey^d
and Maarten Kremers^e

^aLeibniz Supercomputing Centre, Garching near Munich, Germany

^bKarlsruhe Institute of Technology (KIT), Karlsruhe, Germany

^cNikhef, Amsterdam, the Netherlands

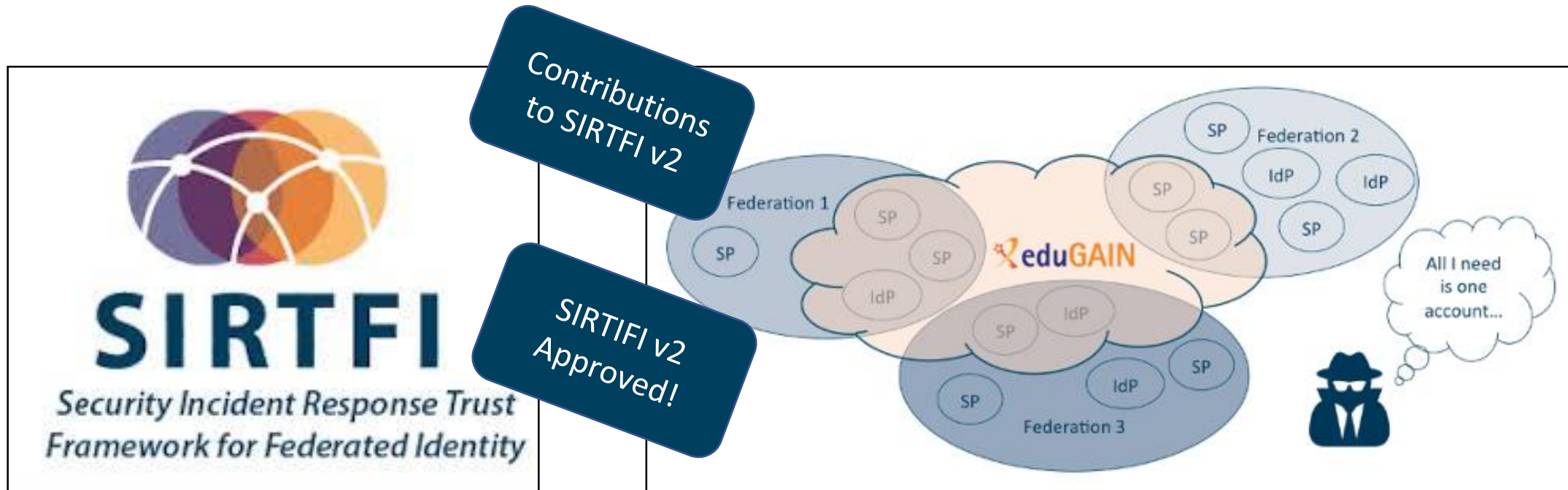
^dUKRI STFC Rutherford Appleton Laboratory, Didcot, United Kingdom

^eSURF, Utrecht, the Netherlands

Full paper
published

[https://doi.org/10.22323/
1.378.0029](https://doi.org/10.22323/1.378.0029)

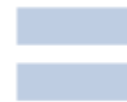
T&I Enabling Communities



Inviting new vector of attack



Uncertainty in security capability of participants



Lack of trust



Source and more information: https://refeds.org/wp-content/uploads/2016/02/Why_Sirtfi.pdf

eduGAIN Security Incident Response Handbook

| | |
|--|----------|
| Preface | 1 |
| Chapter 1. Understanding Your Role and Responsibilities | 2 |
| Introduction | 2 |
| Roles | 2 |
| Scope | 3 |
| Responsibilities | 3 |
| Federation Participants | 4 |
| Federation Operators | 4 |
| eduGAIN Security Team | 4 |
| Chapter 2. Security Incident Response Procedures | 5 |
| Federation Participants | 5 |
| Federation Operators | 6 |
| eduGAIN Security Team | 7 |

Contributions to the
eduGAIN security
incident Handbook



Preface



As with products of any REFEDS Working Group, in this instance the SIRTFI Working Group, this document is a community-developed Best Practice Recommendation. However, as with the SIRTFI Trust Framework itself, these Best Practice Recommendations are most effective when all parties it addresses agree to follow it. Organisations such as Federation Operators or eduGAIN may decide to incorporate adoption of these Best Practice Recommendations into their own policies, as many have done with the SIRTFI Trust Framework.

This document is based on previous work conducted in the AARC2 project¹.





The Interoperable Global Trust Federation (IGTF) is a body to establish common policies and guidelines that help establish interoperable, global trust relations between providers of e-Infrastructures and e-Research, identity providers, and other qualified relying parties.



Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities

Publication Date: 2022-02-24

Authors: Members of the IGTF and the AARC Community; David Groep; Ian Collier, Tom Dack; Jens Jensen; David Kelsey; Maarten Kremers; Ian Neilson; Stefan Paetow; Hannah Short; Mischa Sallé; Uros Stevanovic

With feedback from: Marina Adomeit; Sander Apweiler; Jim Basney; Christos Kanellopoulos; Johannes Reetz

AARC Document Code: **AARC-G071**

AA Operations Security
Guideline 2022 (AARC-G071)

<https://www.eugridpma.org/guidelines/aaops/>





The Wise Information Security for Collaborating e-Infrastructures (WISE) community enhances best practice in information security for IT infrastructures for research.

SCI (Security for Collaboration among Infrastructures) Workgroup focusses on best practices, trust and policy standards for collaboration with the aim of managing cross-infrastructure security risks

SCI Trust Framework

- Enable interoperation of collaborating Infrastructures in managing cross-infrastructure operational security risks.
- Builds trust between Infrastructures by adopting policy standards for collaboration especially in cases where identical security policy documents cannot be shared.



T&I Enabling Communities

SCI

Security for Collaborating Infrastructures Trust Framework

Introduction

Research and e-Infrastructures recognise that controlling information security is crucial for providing continuous and trustworthy services for the communities. The Security for Collaborating Infrastructures (SCI) working group is a collaborative activity within the Wise Information Security for e-Infrastructures (WISE) trust community. The aim of the SCI trust framework is to enable interoperation of collaborating Infrastructures in managing cross-infrastructure operational security risks. It also builds trust between Infrastructures by adopting policy standards for collaboration especially in cases where identical security policy documents cannot be shared. Governing principles of the SCI framework are incident containment, ascertaining the causes of incidents, identifying affected parties, addressing data protection and risk management and understanding measures required to prevent an incident from reoccurring. The original **SCI version 1** Framework was produced in 2013.

The SCI Working Group has produced a second version of the framework, to reflect changes in technology, culture and to improve its relevance to a broad range of infrastructures.

[Access the SCI version 2 Framework here](#)




| | A | B | C | D | E | F | G |
|----|--|---------------|---|-----|----------|---|----------------------------|
| 1 | Infrastructure Name: | <insert name> | | | | | |
| 2 | Prepared By: | <insert name> | | | | | |
| 3 | Reviewed By: | <insert name> | | | | | |
| 4 | | | | | | | |
| 5 | Operational Security [OS] | Maturity | | | Evidence | | |
| 6 | | Value | Σ | | | | (Document Name and/or URL) |
| 7 | | | | | | | |
| 8 | OS1 - Security Person/Team | | | | | | |
| 9 | OS2 - Risk Management Process | | | | | | |
| 10 | OS3 - Security Plan (architecture, policies, controls) | | | 2.0 | | | |
| 11 | OS3.1 - Authentication | | 3 | | | | |
| 12 | OS3.2 - Dynamic Response | | 1 | | | | |
| 13 | OS3.3 - Access Control | | | | | | |
| 14 | OS3.4 - Physical and Network Security | | | | | | |
| 15 | OS3.5 - Risk Mitigation | | | | | | |
| 16 | OS3.6 - Confidentiality | | | | | | |
| 17 | OS3.7 - Integrity and Availability | Q | 1 | 1.0 | | | |
| 18 | OS3.8 - Disaster Recovery | | | | | | |
| 19 | OS3.9 - Compliance Mechanisms | | | | | | |
| 20 | OS4 - Security Patching | | 1 | 1.0 | | | |
| 21 | OS4.1 - Patching Process | | | | | | |
| 22 | OS4.2 - Patching Records and Communication | | | | | | |
| 23 | OS5 - Vulnerability Mgmt | | 1 | 0.7 | | | |
| 24 | OSS.1 - Vulnerability Process | | | | | | |

Self Assessment Tool

Guidance Doc





Top Level Infrastructure Policy Template

Questions to ask yourself when defining the policy:

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

This policy is effective from <insert date>.

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 Infrastructure.

Definitions

Infrastructure All of the IT hardware, software, networks, data, facilities, processes and any other elements that together are required to develop, test, deliver, monitor, control or support *services*.

Service An *infrastructure* component fulfilling a need of the *users*, such as computing, storage, networking or software systems.

Revision PDK
in progress
based on
feedback and
experience



T&I Enabling Communities

WISE Community: Security Communication Challenges Coordination WG (SCCC-WG)

Introduction and background

Maintaining trust between different infrastructures and domains depends largely on predictable responses by all parties involved. Many frameworks – e.g. SCI and Sirtfi – and groups such as the coordinated e-Infrastructure for the IGTF, and REFEDS, all promote mechanisms to publish security contact information, and set explicit or implicit expectations on their remit, responsiveness, and level of confidentiality. It is a well recognised fact that data that is not

Contributions
by EnCo



Dashboard / ... / SCCC-JWG

Communications Challenge planning

Created by David Groep, last modified by Maarten Kremers on Jan 22, 2020

| Body | Last challenge | Campaign name | Next challenge | Campaign name | Status |
|--------------------|----------------|------------------|----------------|------------------|----------------------------|
| IGTF | October 2019 | | | IGTF-RATCC4-2019 | Completed |
| EGI | March 2019 | SSC 19.03 (8) | | | (Completed) |
| Trusted Introducer | August 2019 | TI Reaction Test | January 2019 | TI Reaction Test | Repeats three times a year |

Campaign information

Campaigns can target different constituencies and may overlap. The description of the constituency given here should be sufficient for a human. It need not be a detailed description or a list of addresses (which would be a privacy concern since this page is public). Challenges can also be performed on a contact address does not bounce, to testing if the organisation contacted can do system memory forensic analysis and engage effectively.

- ability to receive – mail does not bounce or phone rings
- automated answering – ticket system receipt or answering machine
- human responding – a human (helpdesk operative) answers trivially (e.g. name)
- human familiar with subject-matter responding – responsible person responds
- service analysis capability - a responsible person or team can investigate and resolve common incidents reported to the contact address

See also <https://www.eugridpma.org/agenda/47/contribution/6/material/slides/0.pptx> for some background.

Please **do not post sensitive data** to this Wiki - it is publicly viewable for now.

FIM4R



FIM4R (Federated Identity Management for Research) is a collection of research communities and infrastructures with a shared interest in enabling Federated Identity Management for their research cyber infrastructures. In order to achieve this, FIM4R develops requirements bearing on technical architecture, federated identity management, and operational policies needed to achieve a harmonious integration between research cyber infrastructures and R&E Federations.

T&I Enabling Communities

FIM4R



Support by EnCo



T&I Enabling Communities



Workshop #16 @ Denver,
Dec 2022

Workshop #17 @ CERN,
Feb 2023



FIM4R



Engage!

- <https://fim4r.org>
- <https://refeds.org>
- <https://wise-community.org>
- <https://www.igt.net>
- <https://aarc-community.org>

- Contact us: policy@aarc-community.org



FIM 4 R

A horizontal bar composed of three segments: a grey segment on the left, a black segment in the middle, and a blue segment on the right.

Thank you

Any questions?

maarten.kremers@surf.nl



As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).