Exploring trust for Communities

Trust & Identity Enabling Communities

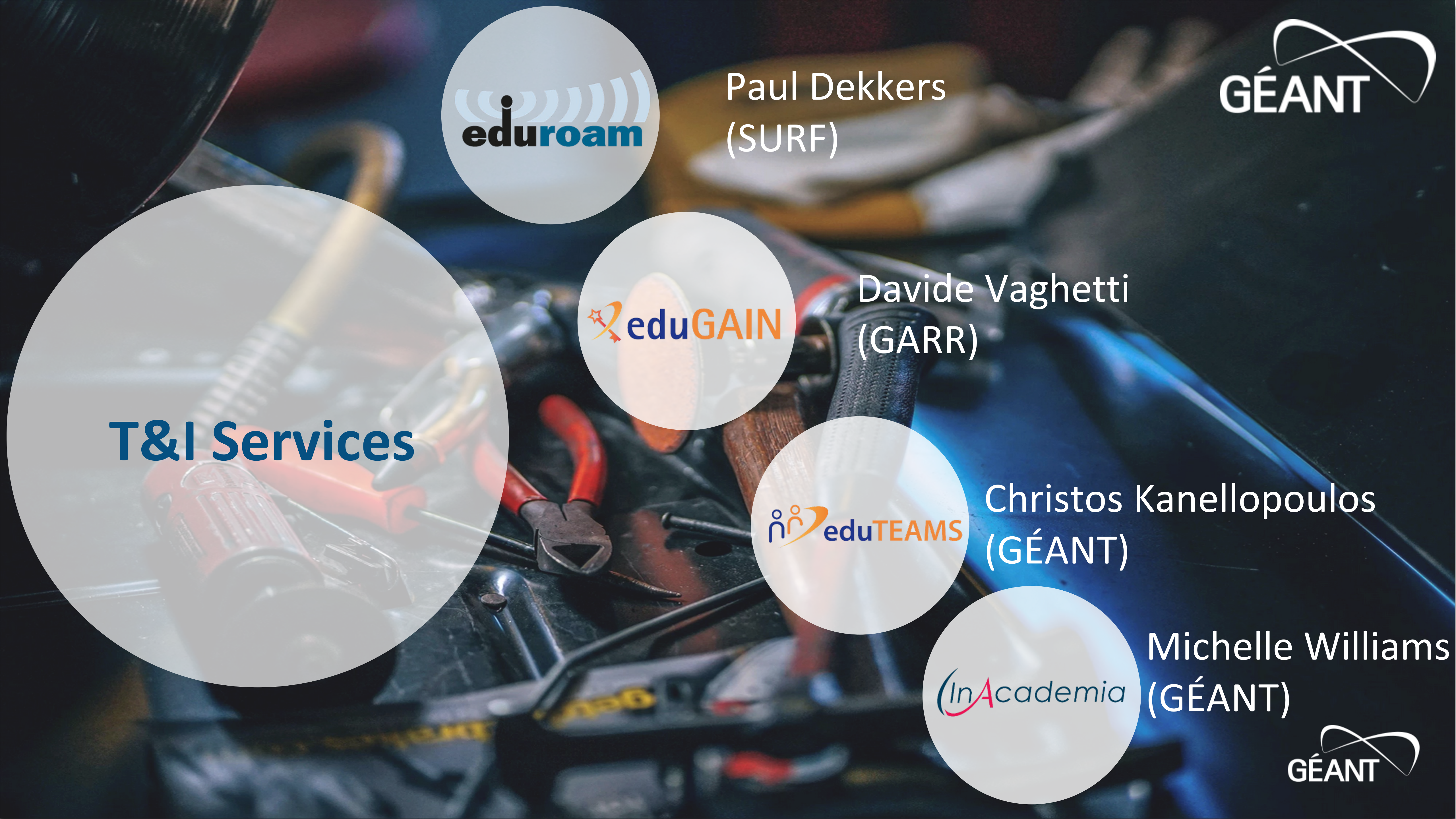
Maarten Kremers, SURF

EUgridPMA #55
24th May 2022
LRZ, Garching bei München

GN 4-3 T&I

Expand the Reach of Federated Access

- Operate T&I services
- Develop and Enhance the T&I services
- Explore new or disruptive ideas
- Engage with the relevant stakeholders



GÉANT

T&I Services

eduroam

Paul Dekkers
(SURF)

eduGAIN

Davide Vaghetti
(GARR)

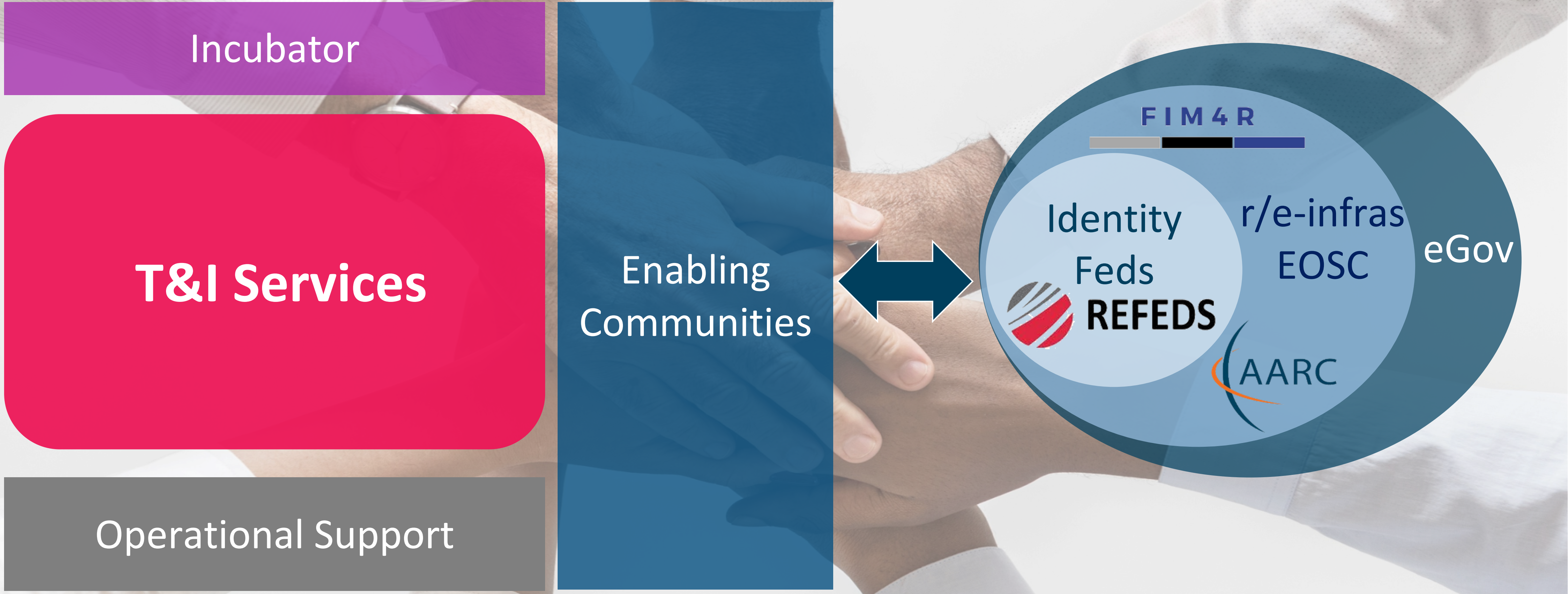
eduTEAMS

Christos Kanellopoulos
(GÉANT)

InAcademia

Michelle Williams
(GÉANT)

GÉANT



Incubator

T&I Services

Operational Support

Enabling Communities

FIM4R

Identity Feds

REFEDS

r/e-infras EOSC

AARC

eGov

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

REFEDS

WISE COMMUNITY

FIM4R

IGTF AP|EU|TAG

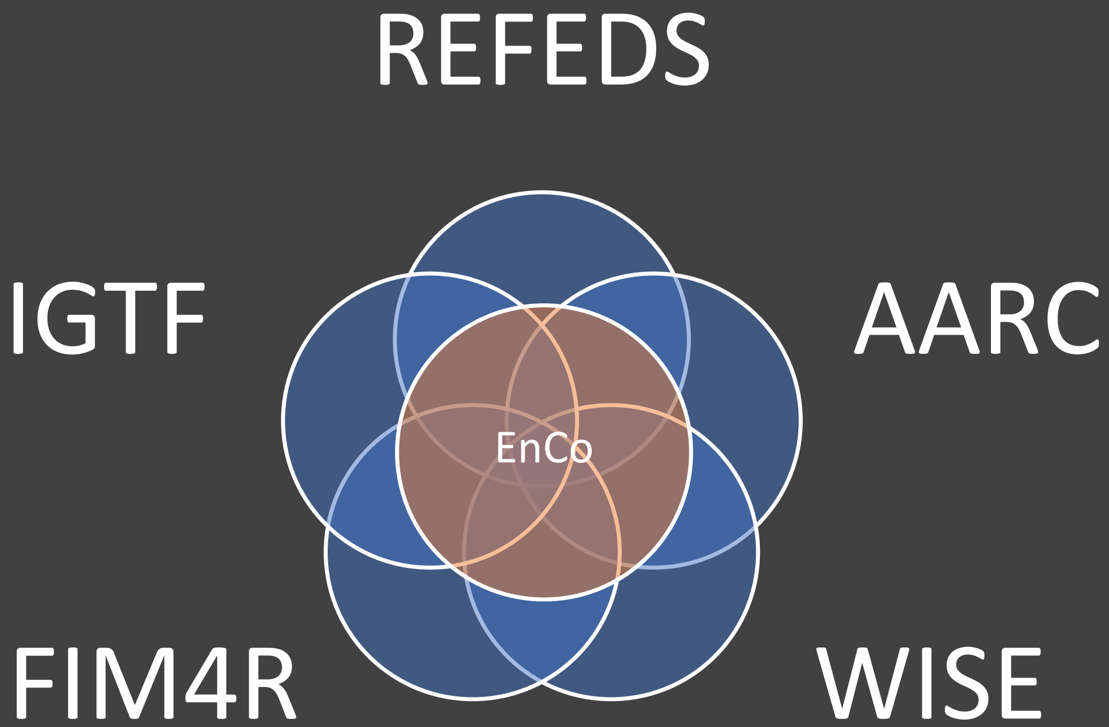
AARC

T&I Enabling Communities

INTEROPERABILITY

TRUST

SECURITY



AARC

REFEDS

WISE COMMUNITY

FIM4R

IGTF
AP|EU|TAG

AEGIS

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 ands e-infrastructures.

Facilitated by EnCo

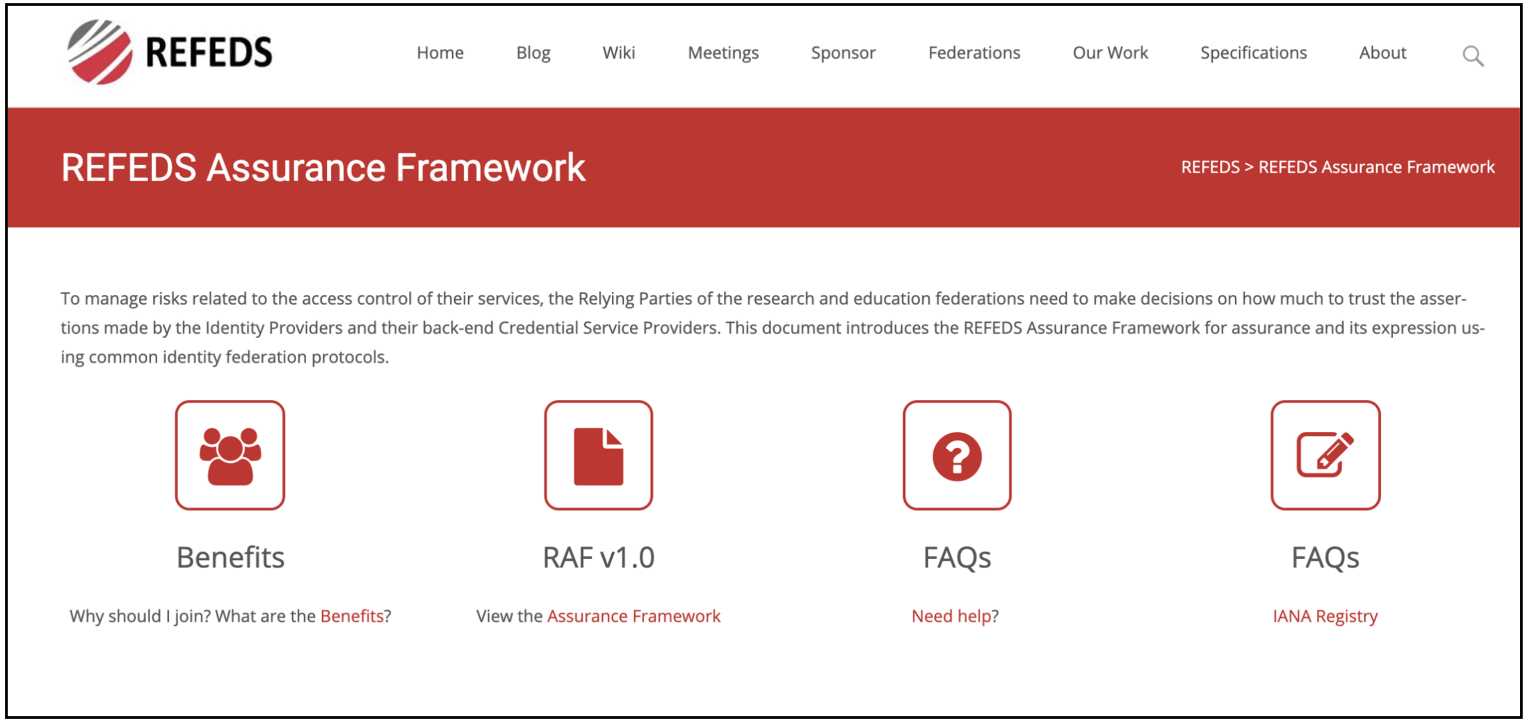
AEGIS

T&I Enabling Communities

REFEDS

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



REFEDS Assurance Framework

REFEDS > REFEDS Assurance 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.

Benefits

Why should I join? What are the Benefits?

RAF v1.0

View the Assurance Framework

FAQs

Need help?

FAQs

IANA Registry

T&I Enabling Communities

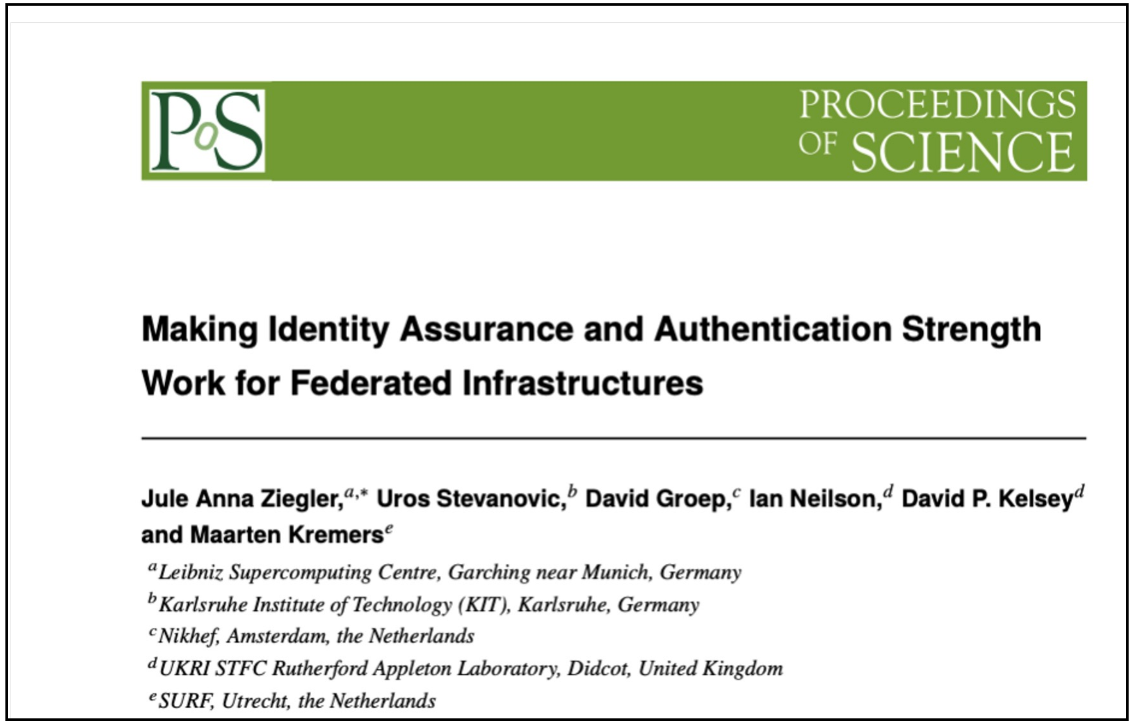
REFEDS Assurance Profile (v1.0)

- 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

Assurance is on the agenda

T&I Enabling Communities



PoS 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]

[a] *Leibniz Supercomputing Centre, Garching near Munich, Germany*
[b] *Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany*
[c] *Nikhef, Amsterdam, the Netherlands*
[d] *UKRI STFC Rutherford Appleton Laboratory, Didcot, United Kingdom*
[e] *SURF, Utrecht, the Netherlands*

Full paper published

https://doi.org/10.22323/1.378.0029

REFEDS

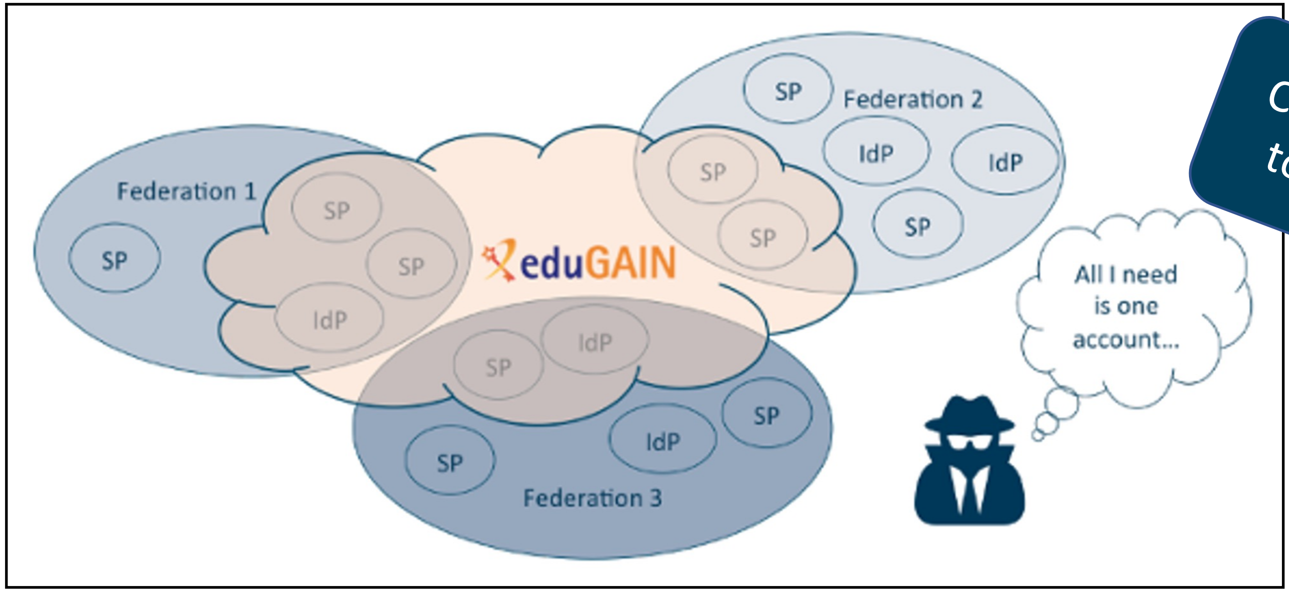
AARC

T&I Enabling Communities

GÉANT

SIRTFI

Security Incident Response Trust Framework for Federated Identity



Contributions to SIRTFI v2

REFEDS

Inviting new vector of attack + Uncertainty in security capability of participants = Lack of trust

AARC

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

T&I Enabling Communities

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

T&I Enabling Communities

GÉANT

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.

Self Assessment Tool

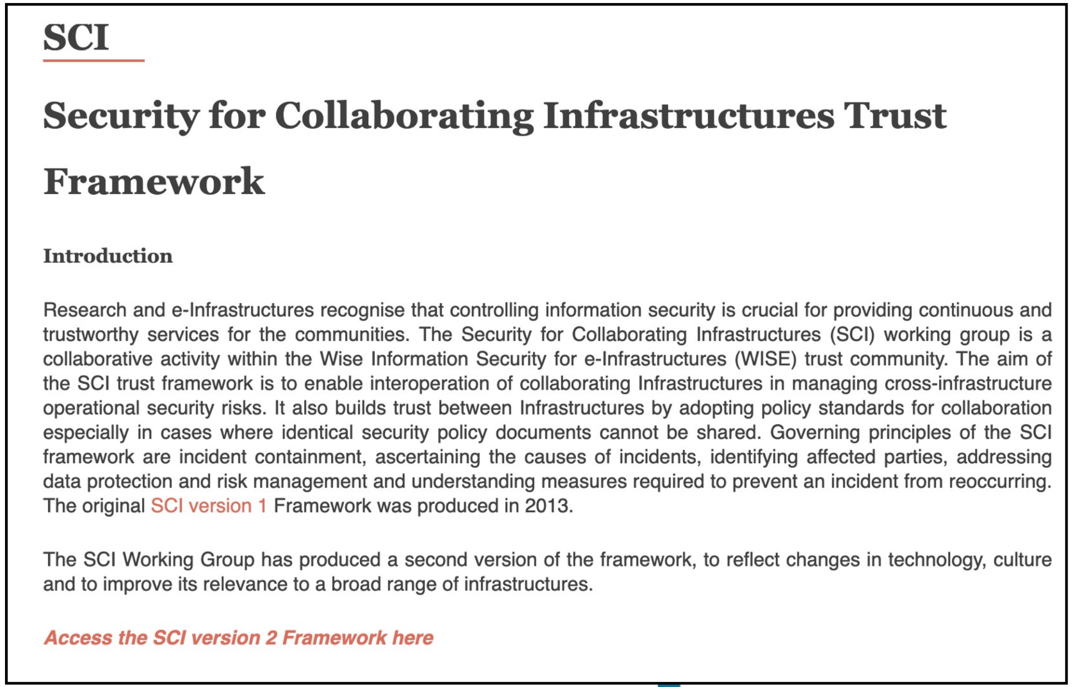
Guidance Doc

On the agenda

WISE COMMUNITY

AARC

T&I Enabling Communities



SCI

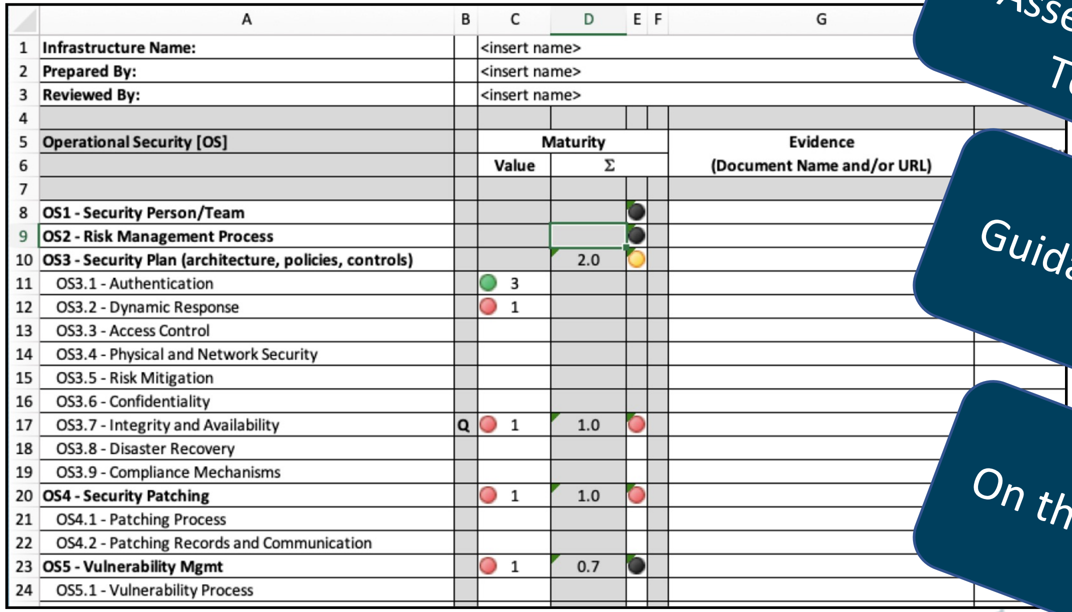
Security for Collaborating Infrastructures Trust Framework

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	OS5.1 - Vulnerability Process						

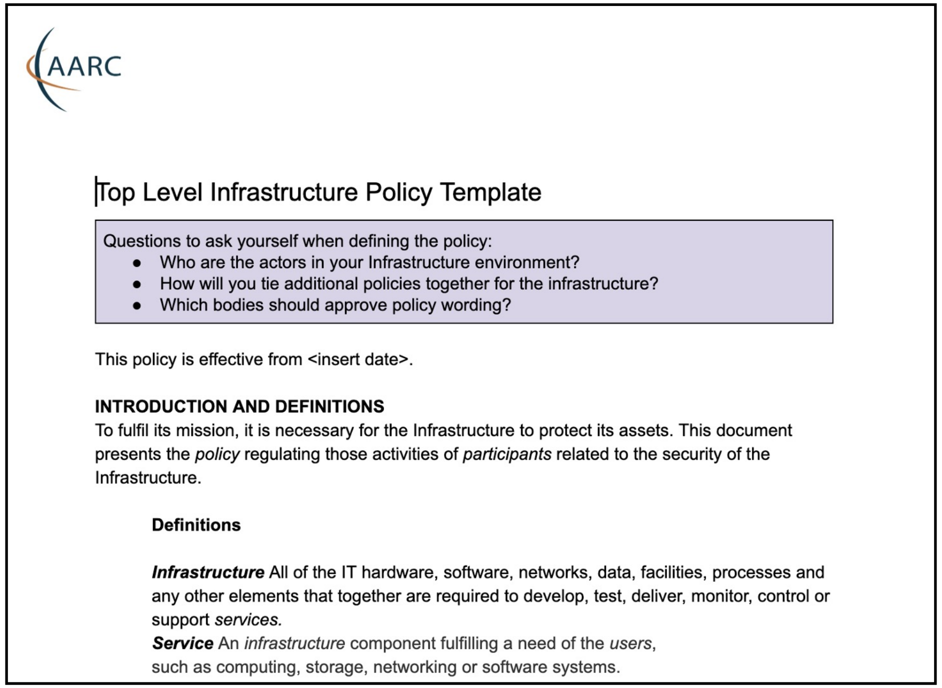
Self Assessment Tool

Guidance Doc

On the agenda

T&I Enabling Communities

On the agenda



AARC

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

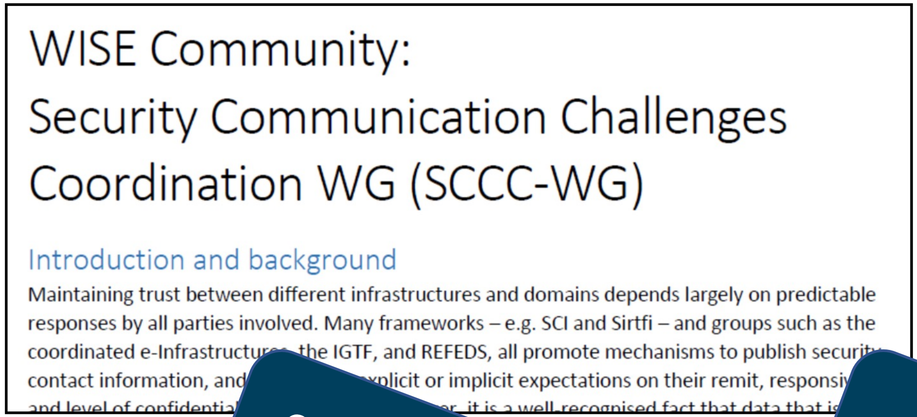
Infrastructure All of the IT hardware, software, networks, data, facilities, processes and any other elements that together are required to develop, test, deliver, monitor, control or support *services.*
Service An *infrastructure* component fulfilling a need of the *users*, such as computing, storage, networking or software systems.

Revision PDK in progress based on feedback and experience

Service Operations Security

Data Protection / Privacy

T&I Enabling Communities



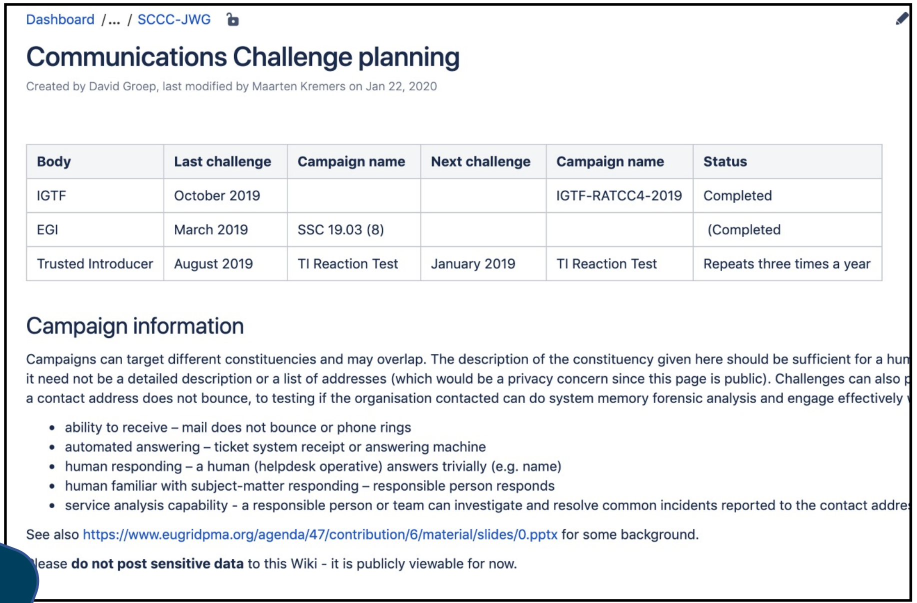
WISE Community: Security Communication Challenges Coordination WG (SCCC-WG)

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-Infrastructures, the IGTF, and REFEDS, all promote mechanisms to publish security contact information, and explicit or implicit expectations on their remit, responsiv and level of confidentia er, it is a well-recognised fact that data that is

Contributions by EnCo

On the agenda



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 hum 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 p 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 addre

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

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

REFEDS

WISE COMMUNITY

FIM4R

IGTF AP|EU|TAG

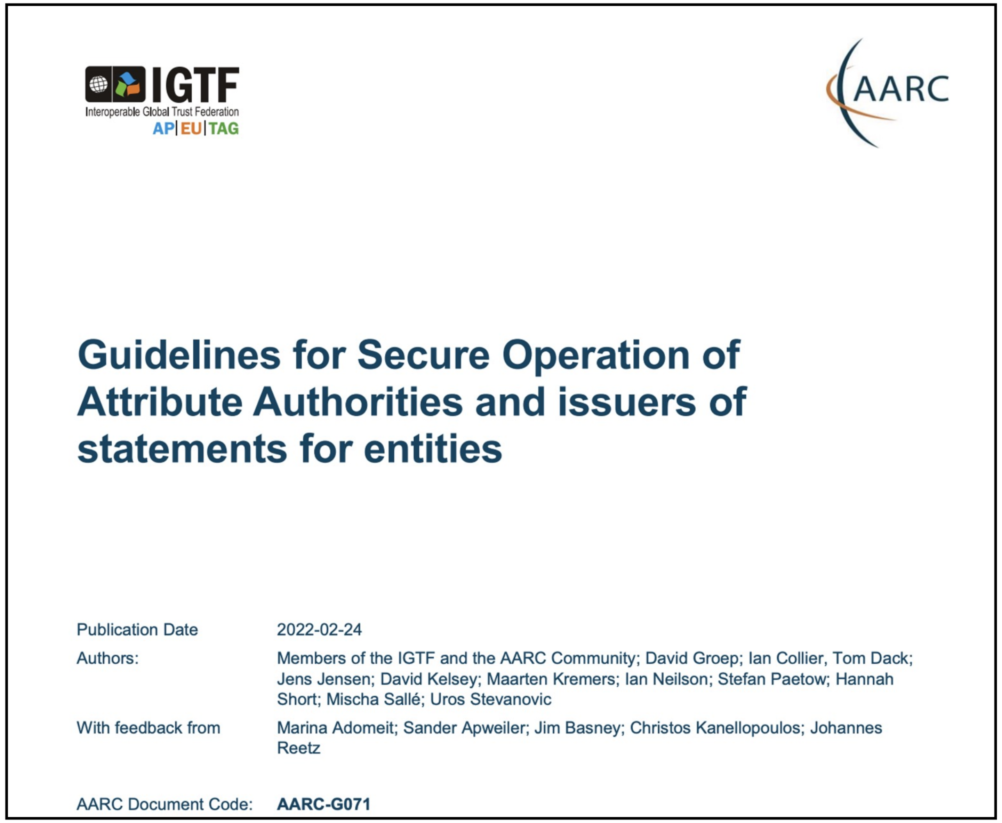
AARC

T&I Enabling Communities

IGTF
AP| EU| TAG

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.

T&I Enabling Communities



IGTF
Interoperable Global Trust Federation
AP|EU|TAG

AARC

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)

AEGIS endorsed

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

T&I Enabling Communities

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

Work in progress: Assurance

REFEDS

WISE COMMUNITY

FIM4R

IGTF

AP|EU|TAG

AARC

T&I eScience Global Engagement

GN4-3 Project Updates

- EnCo Policy presentation at ISGC2022
- Accepted presentation for TNC22 !

Trust & Identity
Outreach

T&I eScience Global Engagement

GN5-1 preparations

- 1st Jan 2023 – 31st Dec 2024 (2y)
- Proposal submitted

Trust & Identity Outreach

T&I eScience Global Engagement

GN5-1 preparations & EnCo

Possible new topics

- Policy for token based interopable trust frameworks
- SNCTFI revisited

Trust & Identity Outreach

T&I eScience Global Engagement

Relevant meetings

- TNC22

14th – 16th June (Trieste, Italy)

- REFEDS

13th June (Trieste, Italy)

- Security day

- 17th June (Trieste, Italy)

Trust & Identity Outreach

T&I eScience Global Engagement

GÉANT

GN4-3 Project Updates

- Review our own workplan
- Activities that need or more less attention
- New Activities
- Activities to dropped

https://edu.nl/ctxxg

Trust & Identity Outreach

Engage!

- https://fim4r.org
- https://refeds.org
- https://wise-community.org
- https://www.igtf.net
- https://aarc-community.org

- Contact us: policy@aarc-community.org

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).