GN4-3 T&I Enabling Communities

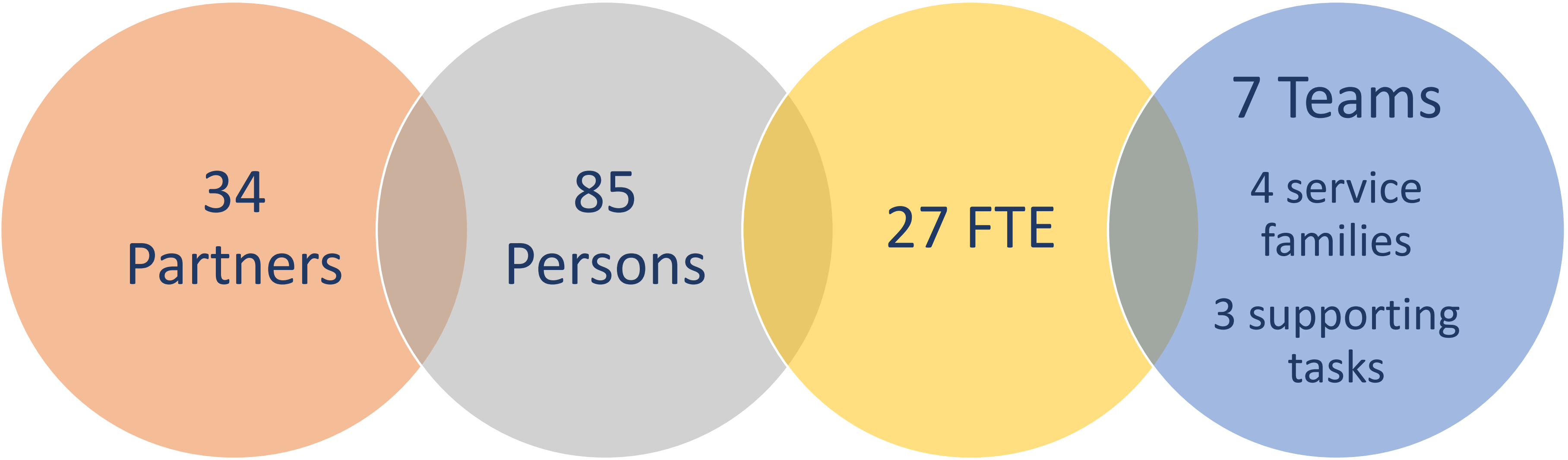
Maarten Kremers SURF

SIG-ISM / WISE joint workshop

Virtual

29th October 2020

GN4-3 T&I TEAM (2019 – 2022)



34 Partners

85 Persons

27 FTE

7 Teams

4 service families

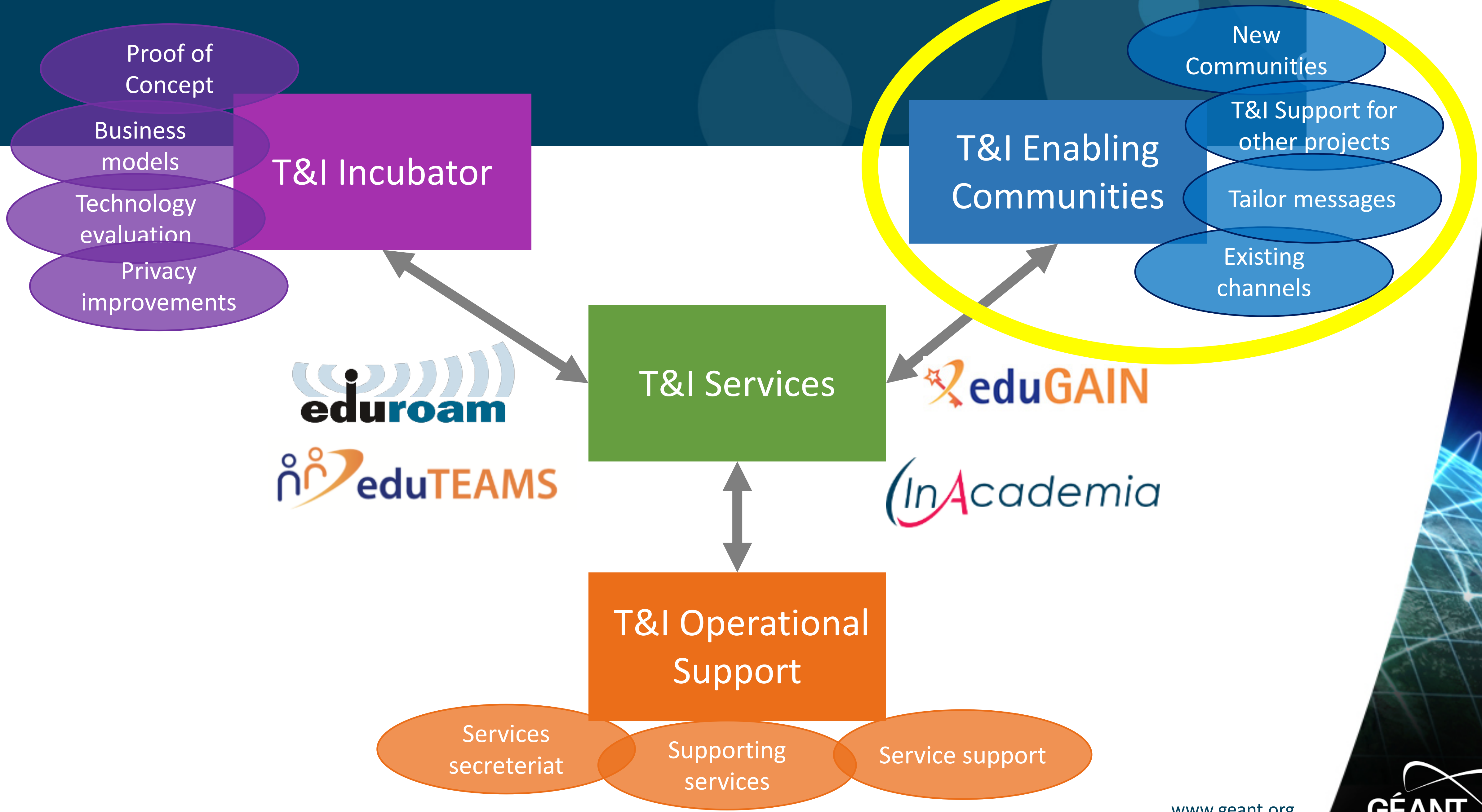
3 supporting tasks

Partners

GÉANT CARNet RedIRIS SURFNET AMRES CESNET NORDUnet Consortium GARR

Asnet AM DFN KIFÜ MARNET RENATER grnet PSNC RASH

CSC LITNET RENAM SWITCH Jisc DeiC RESTENA UNINETT SUNET



T&I Incubator

Proof of Concept

Business models

Technology evaluation

Privacy improvements

T&I Enabling Communities

New Communities

T&I Support for other projects

Tailor messages

Existing channels

T&I Services

eduroam

eduTEAMS

eduGAIN

InAcademia

T&I Operational Support

Services secreteriat

Supporting services

Service support

Operate T&I services

In secure, effective, agile and optimised manner following DevOps principles

Develop and enhance the T&I services

Introducing new features and improving performance, functionality and usability

Explore new or disruptive ideas

Their applicability to T&I services, and feed the results to development and operations teams

Engage with the relevant stakeholders

To understand their requirements and use them to drive the evolution of T&I services

- T&I Business Development Coordination
- Facilitating of the AEGIS group
- T&I eScience Global Engagement

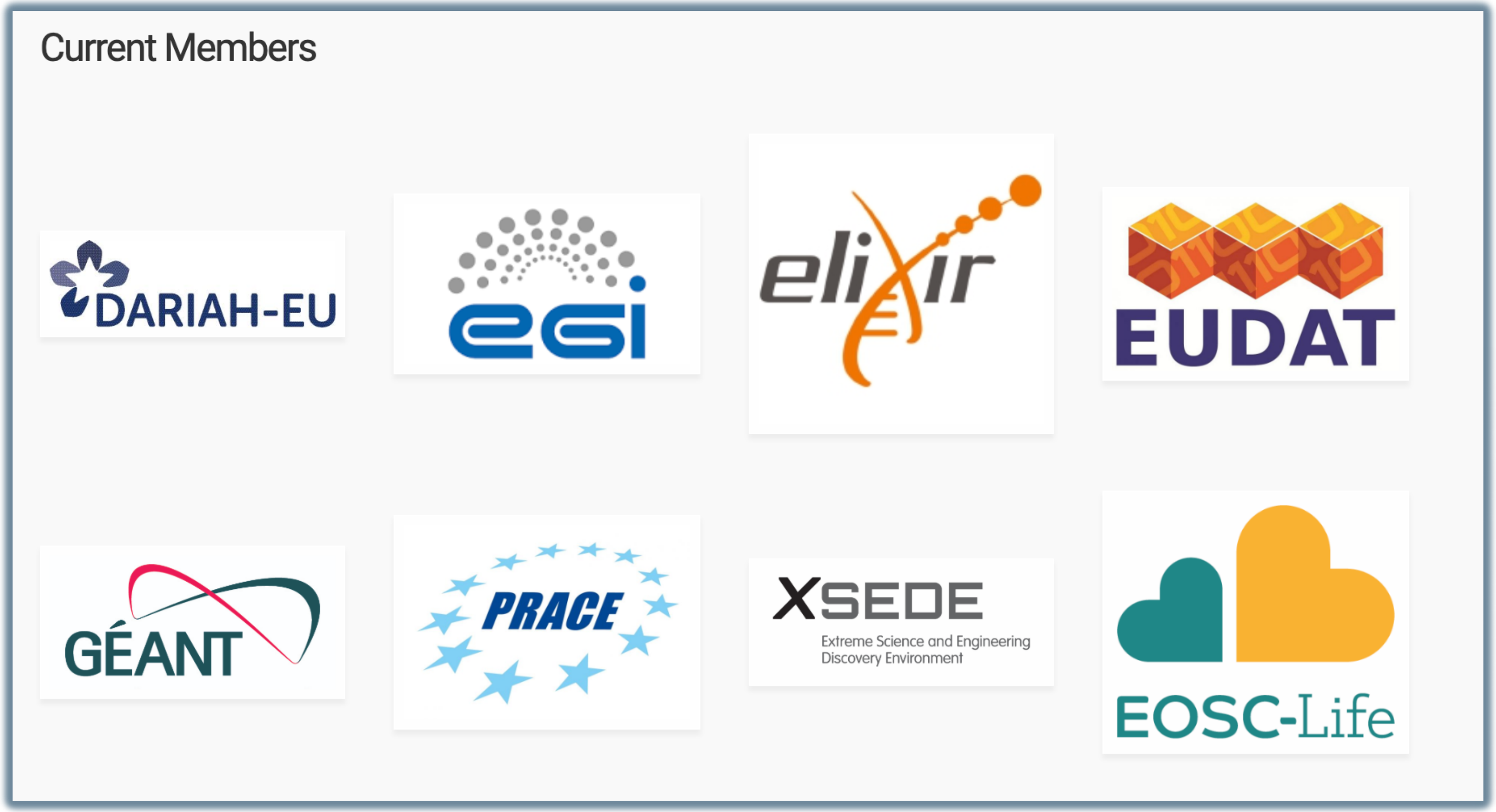
Trust & Identity
Outreach

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.

AEGIS

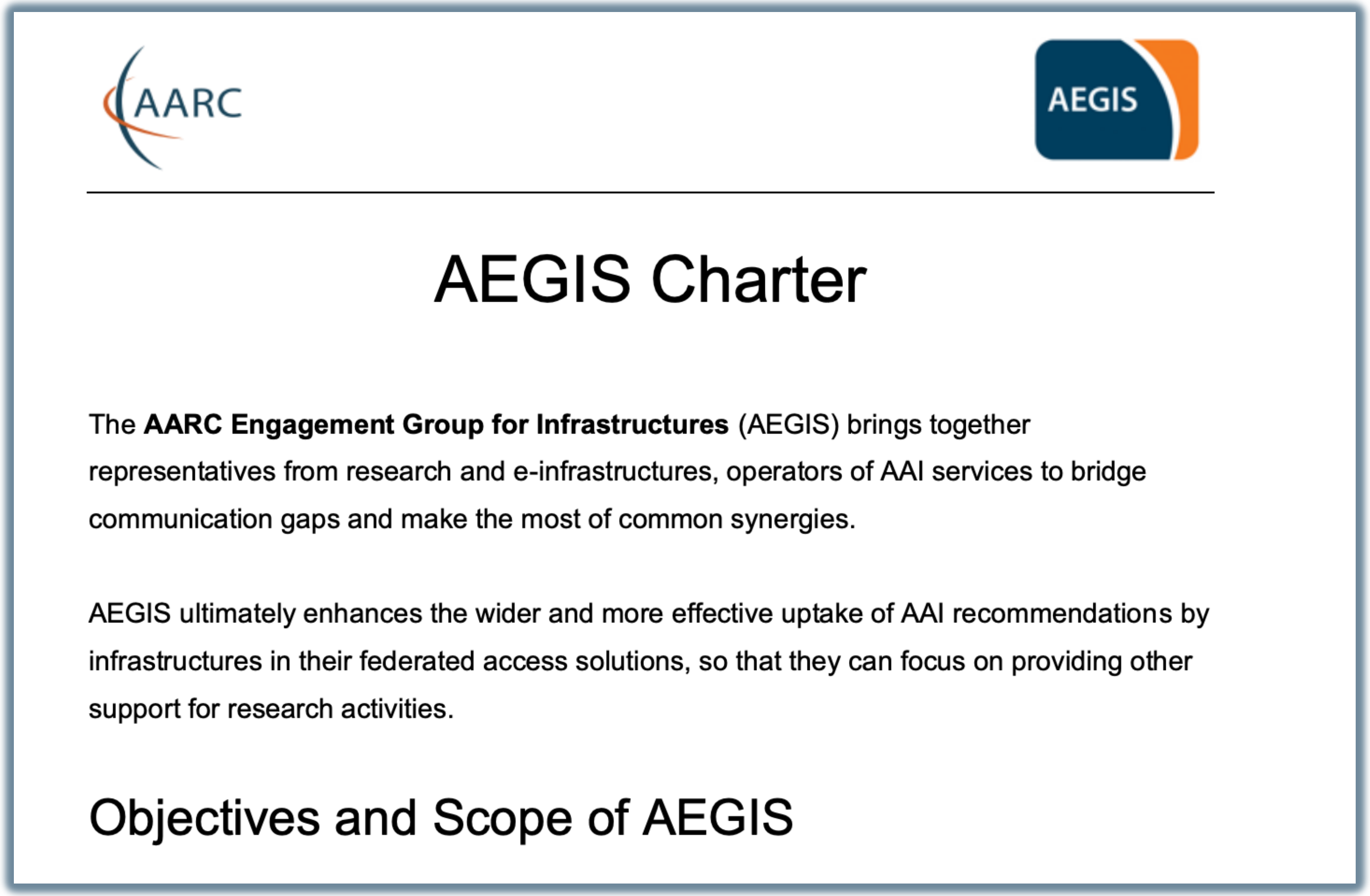
AEGIS



Current Members

AEGIS

AEGIS



AARC

AEGIS

AEGIS Charter

The **AARC Engagement Group for Infrastructures** (AEGIS) brings together representatives from research and e-infrastructures, operators of AAI services to bridge communication gaps and make the most of common synergies.

AEGIS ultimately enhances the wider and more effective uptake of AAI recommendations by infrastructures in their federated access solutions, so that they can focus on providing other support for research activities.

Objectives and Scope of AEGIS

https://aarc-community.org/about/aegis/

AEGIS

GÉANT

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 eScience Global Engagement

AARC

REFEDS

WISE COMMUNITY

FIM4R

IGTF
AP | EU | TAG

AARC

T&I eScience Global Engagement

Nikhef

KIT
Karlsruher Institut für Technologie

CERN

SURF

UKRI
Science and Technology Facilities Council

lrz

CSC

REFEDS

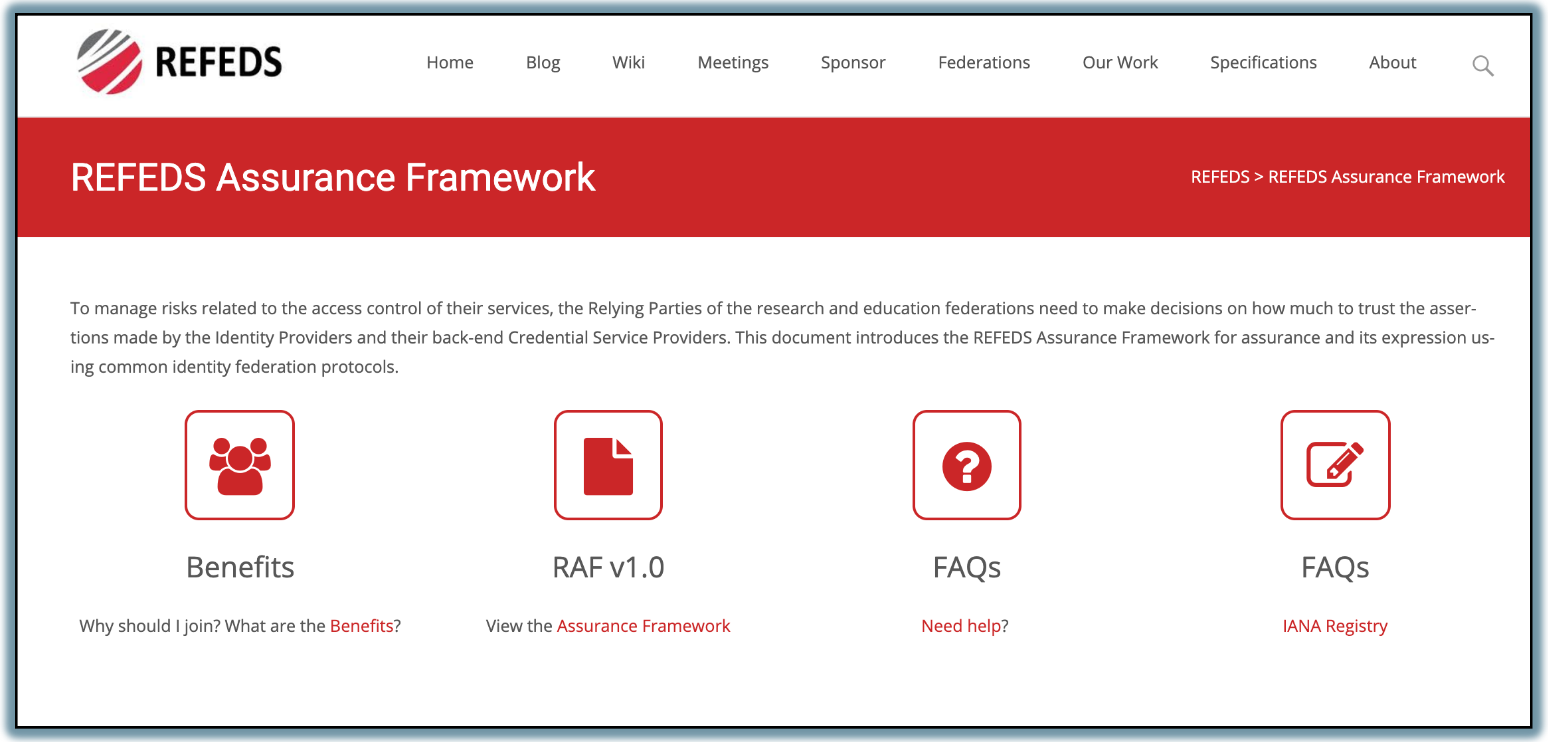
WISE COMMUNITY

FIM4R

IGTF
AP|EU|TAG

AARC

T&I eScience Global Engagement



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?

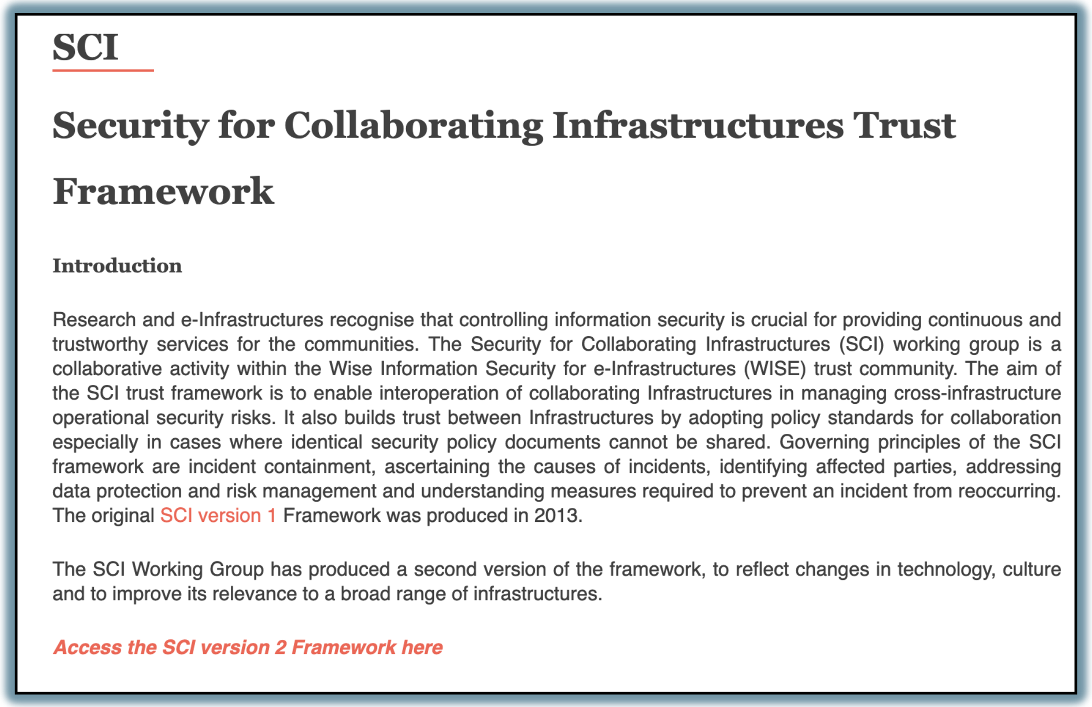
FAQs

IANA Registry

REFEDS

AARC

T&I eScience Global Engagement



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.

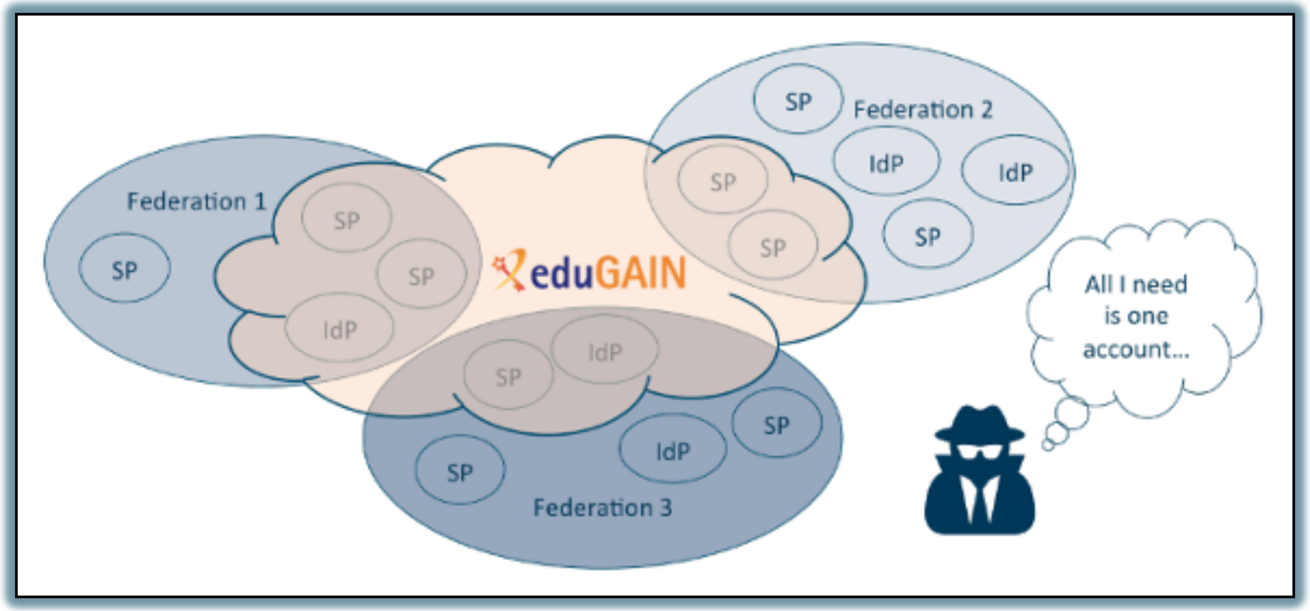
The SCI Working Group has produced a second version of the framework, to reflect changes in technology, culture and to improve its relevance to a broad range of infrastructures.

Access the SCI version 2 Framework here

T&I eScience Global Engagement

SIRTFI

Security Incident Response Trust Framework for Federated Identity



REFEDS

AARC

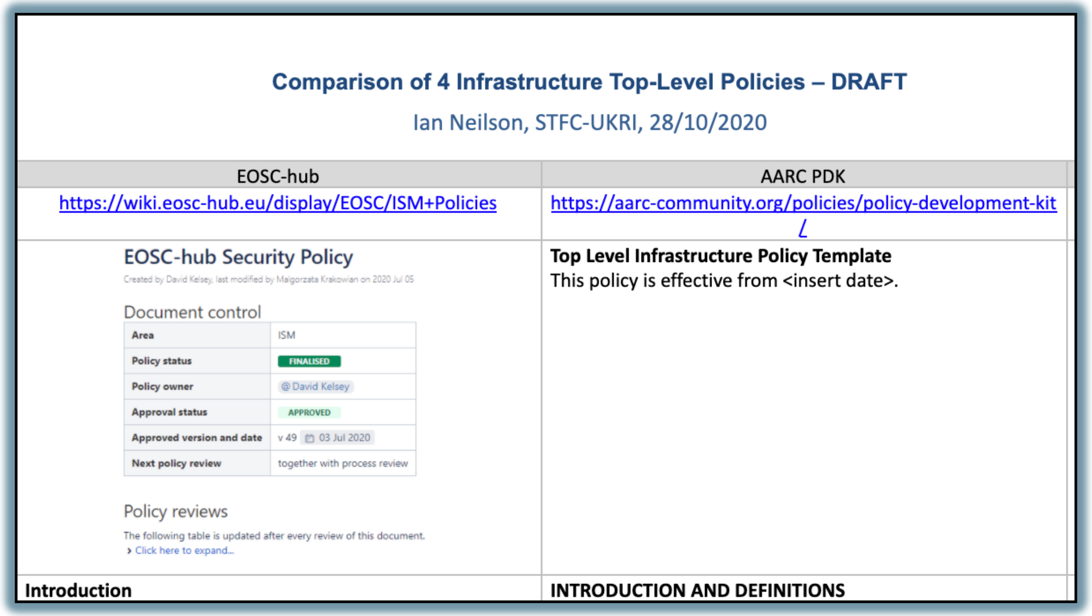
T&I eScience Global Engagement

IGTF
Interoperable Global Trust Federation
AP| EU|TAG

AARC

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

T&I eScience Global Engagement

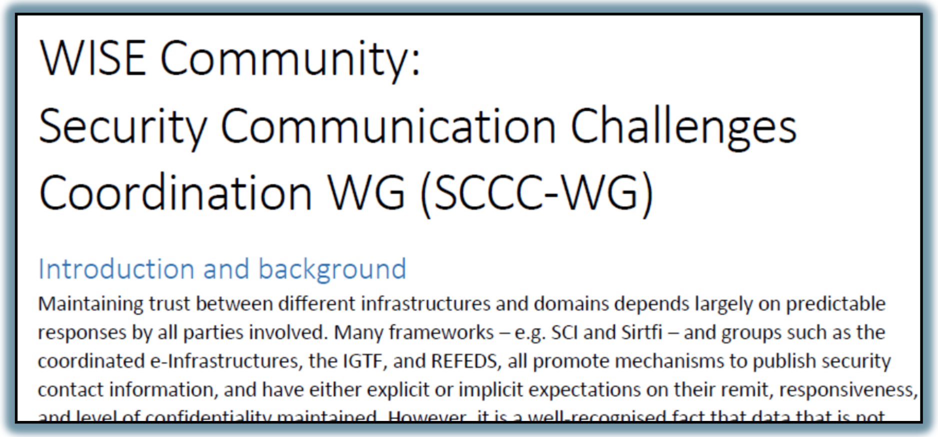


Comparison of 4 Infrastructure Top-Level Policies – DRAFT

Ian Neilson, STFC-UKRI, 28/10/2020

<table>
<tr><th>EOSC-hub</th><th>AARC PDK</th></tr>
<tr><td>https://wiki.eosc-hub.eu/display/EOSC/ISM+Policies</td><td>https://aarc-community.org/policies/policy-development-kit/</td></tr>
<tr><td>EOSC-hub Security Policy
Created by David Kelsey, last modified by Malgorzata Krakowian on 2020 Jul 05
Document control<table>
<tr><td><b>Area</b></td><td>ISM</td></tr>
<tr><td><b>Policy status</b></td><td>FINALISED</td></tr>
<tr><td><b>Policy owner</b></td><td>@ David Kelsey</td></tr>
<tr><td><b>Approval status</b></td><td>APPROVED</td></tr>
<tr><td><b>Approved version and date</b></td><td>v 49 03 Jul 2020</td></tr>
<tr><td><b>Next policy review</b></td><td>together with process review</td></tr>
</table>Policy reviews
The following table is updated after every review of this document.
› Click here to expand...</td><td><b>Top Level Infrastructure Policy Template</b>
This policy is effective from &lt;insert date&gt;.</td></tr>
<tr><td><b>Introduction</b></td><td><b>INTRODUCTION AND DEFINITIONS</b></td></tr>
</table>

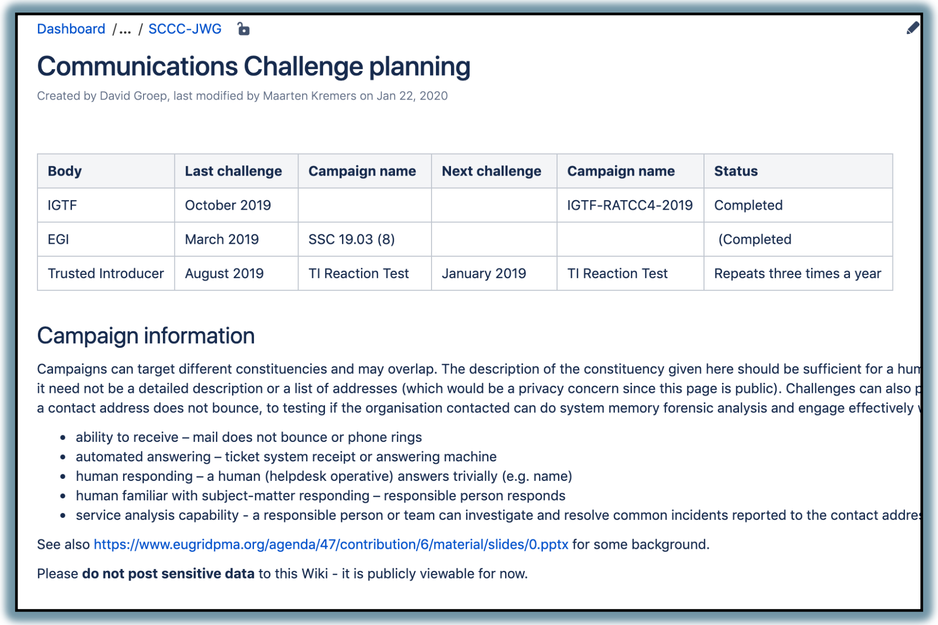
T&I eScience Global Engagement



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 have either explicit or implicit expectations on their remit, responsiveness, and level of confidentiality maintained. However, it is a well-recognised fact that data that is not



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 v

- 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.

Please **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 eScience Global Engagement

GÉANT

FIM4R

REFEDS

WISE COMMUNITY

FIM4R

IGTF

AP | EU | TAG

AARC

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).