

GN4-3 - T&I - eScience Global Engagement

Maarten Kremers, SURF / SURFnet

EUGridPMA #51 / GN4-3 T&I EnCo / AARC Policy community

Virtual

8th February 2021



GN 4-3 T&I Objectives



Operate T&I services



Develop and Enhance the T&I services



Explore new or disruptive ideas



Engage with the relevant stakeholders

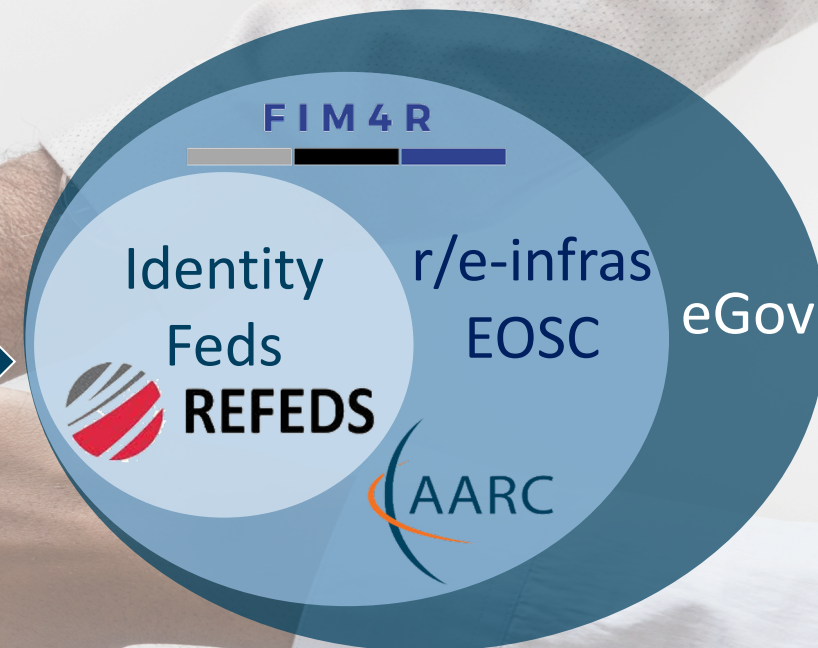
Expand the Reach
of Federated Access

Incubator

T&I Services

Operational Support

Enabling
Communities





Miroslav Milinović
(SRCE)



Davide Vagheti
(GARR)

T&I Services



Christos Kanellopoulos
(GÉANT)



Michelle Williams
(GÉANT)

Trust & Identity

Outreach



T&I Business Development Coordination



Facilitating of the AEGIS group



T&I eScience Global Engagement

Trust & Identity
Outreach

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 e-infrastructures.

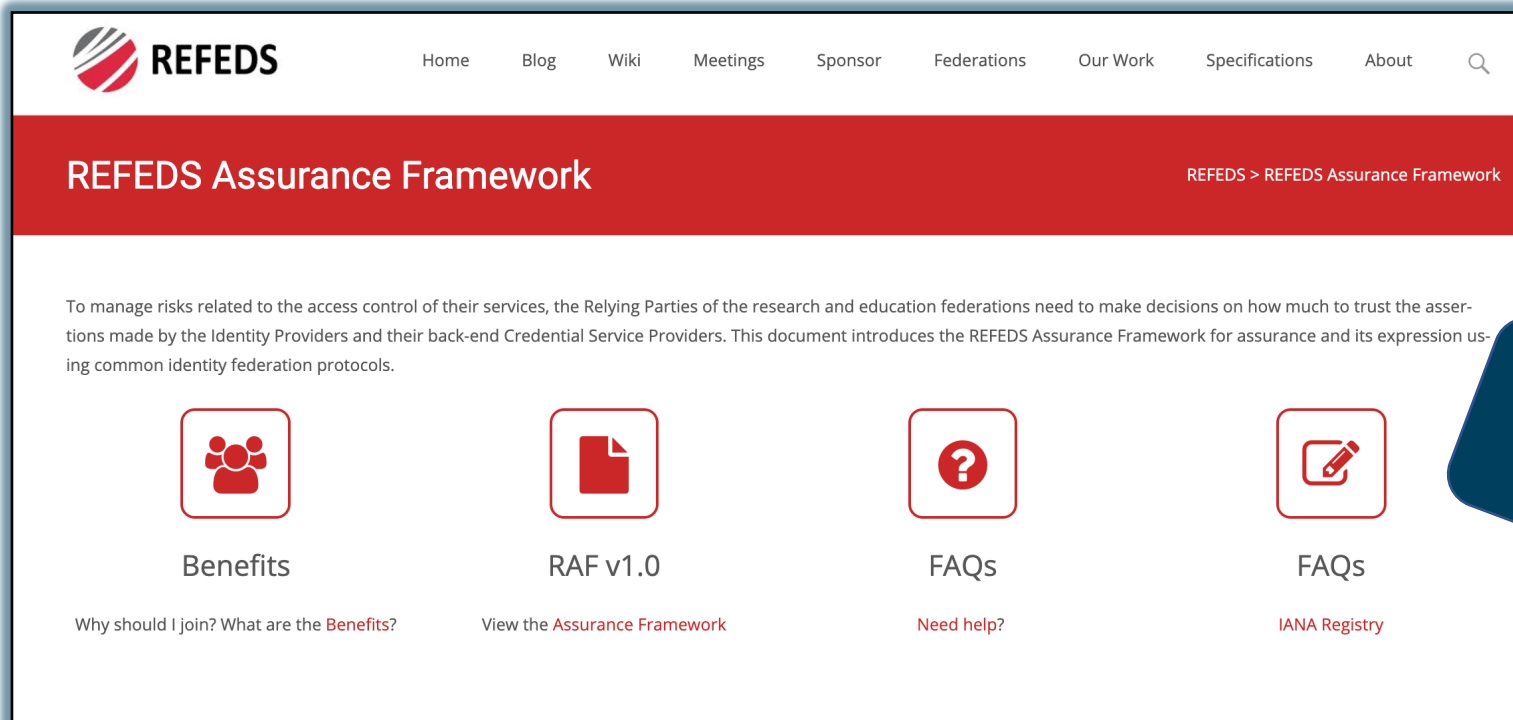


T&I eScience Global Engagement

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 eScience Global Engagement



The screenshot shows the REFEDS Assurance Framework page. The header includes the REFEDS logo and navigation links: 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, a paragraph explains the purpose of the framework. Four icons represent different sections: Benefits (group of people), RAF v1.0 (document), FAQs (question mark), and FAQs (pencil writing). Each icon has a corresponding title and a link below it.

Benefits	RAF v1.0	FAQs	FAQs
Why should I join? What are the Benefits ?	View the Assurance Framework	Need help?	IANA Registry

Paper
Outreach

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](#)

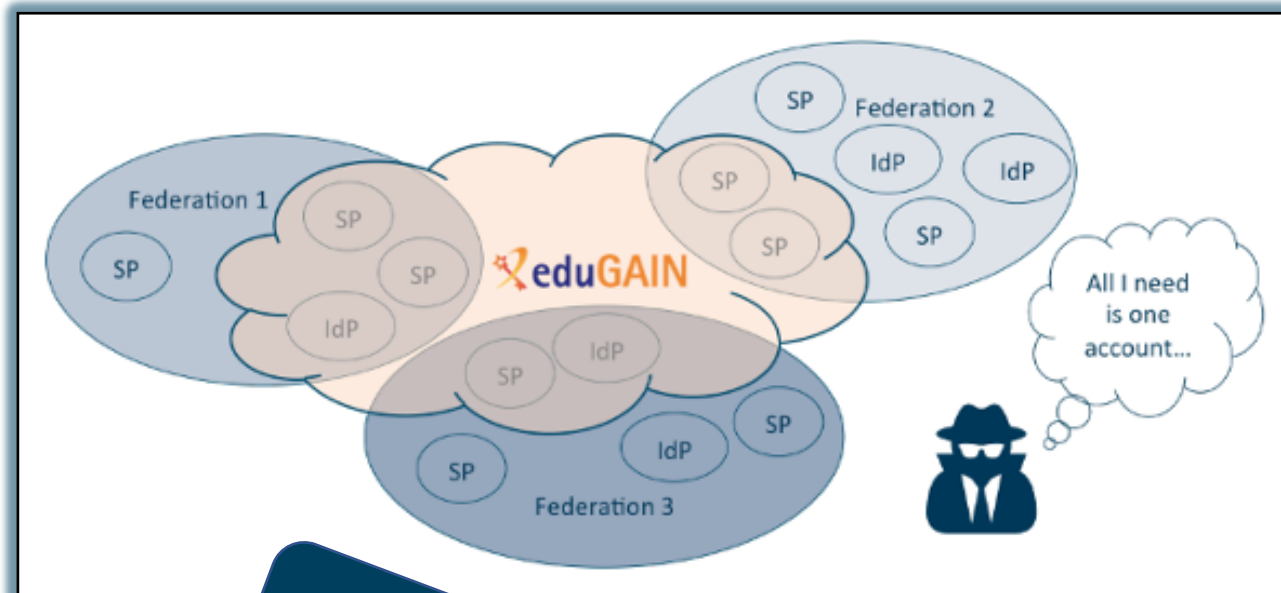
Guidance Doc

Working session

On the agenda



T&I eScience Global Engagement





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.





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

Working session

On the agenda



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

eduGAIN
performed a
communication
challenge

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)
Introducer	August 2019	TI Reaction Test	January 2019	TI Reaction Test	Repeats three times a year

Design information

Challenges can target different constituencies and may overlap. The description of the constituency given here should be sufficient for a human to identify the target. It should 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 used to test if the contact address does not bounce, to testing if the organisation contacted can do system memory forensic analysis and engage effectively. The challenge should be designed to test the following capabilities:

- 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



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:

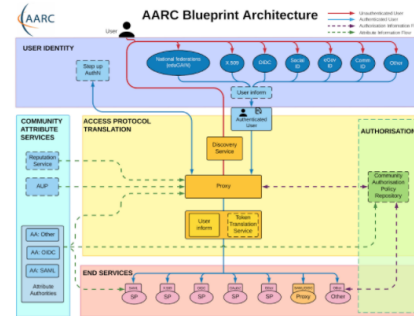
- Which best practices should I follow for my Token Translation Services? [AARC-G004](#)
- How should I translate from Identity Federation information to X.509 certificates? [AARC-G010](#)

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](#).

Near finished

Many thanks to Hannah !

<https://edu.nl/h3dm4>

GN4-3 Project Updates

- STFC/UKRI will officially join the project
 - Welcome DaveK, IanN et al. 😊

Trust & Identity
Outreach

GN4-3 Project Updates

- Halfway the project
- EC Project Review in Oct 2020

Trust & Identity
Outreach

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

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).