EUGridPMA
Status and Current Trends
and some IGTF topics

August 2018
APGridPMA Auckland Meeting

David Groep, Nikhef & EUGridPMA

Recent EUGridPMA topics

- PMA membership and reviews

- Infrastructure Policy Alignment & AARC
  - assurance frameworks – evolution and components
  - Joint Infrastructure policies
  - Acceptable Use and Conditions of Use
  - Policy Development Kit
  - Attribute Authority Operations
  - Incident response and communications challenges

See also the EUGridPMA43 summary:
https://www.eugridpma.org/meetings/2018-05/

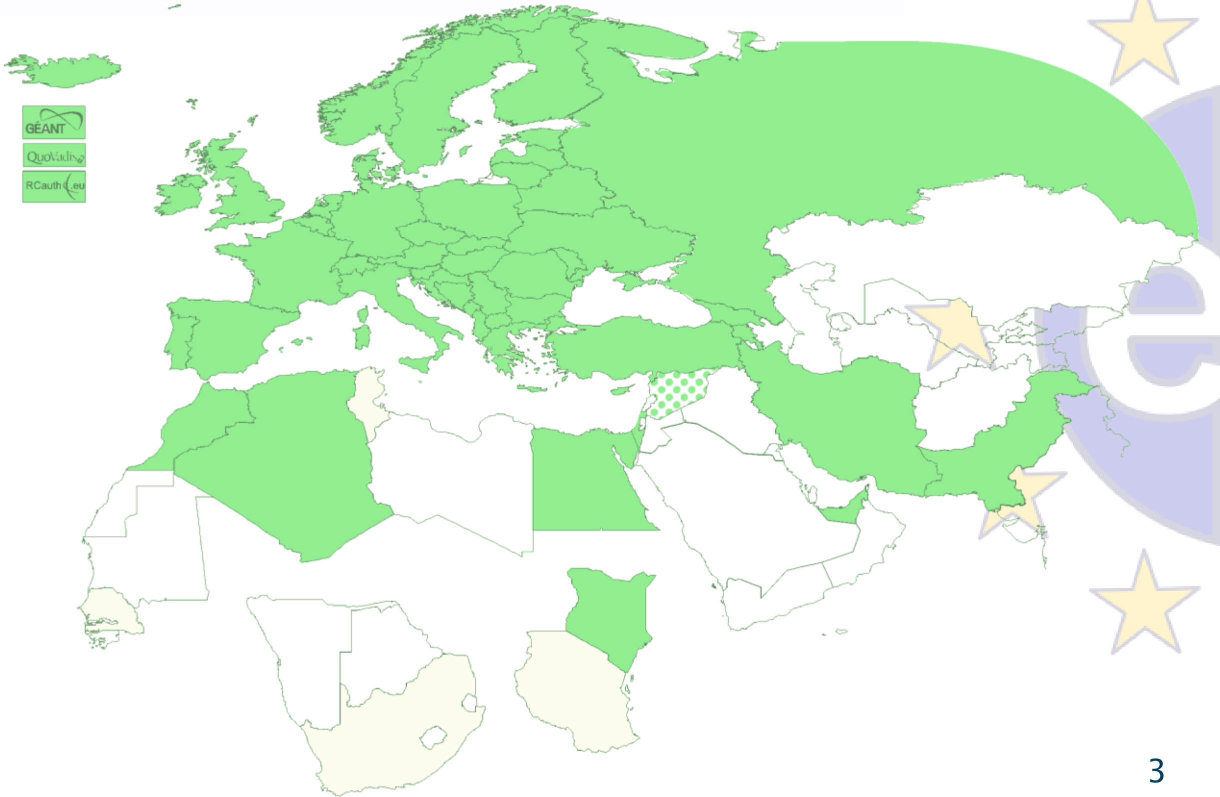
Authority coverage in EMEA

- Europe: AT, CY, CZ, DE, DK, ES, FI, FR, GR, HR, HU, IT, NL, PL, PT, RO, SE, SI, SK, UK; AM, GE, IS, MD, ME, MK, NO, RS, RU, TR, UA and the GEANT TCS and EGI *catch-all*

- Middle East: AE, IR, PK

- Africa: DZ, EG, MA, KE

- Multinational: CERN, RCauth.eu, QuoVadis (BM)



47+4

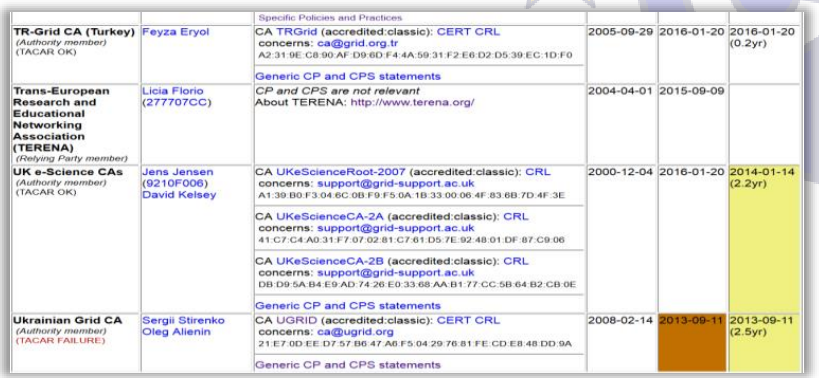
Membership and other changes

- Responsiveness challenges for some members

  PLEASE take care to renew your trust anchors in time, as well as your CRLs

- Identity providers: both reduction and growth
  - RCauth.eu distributed operations (GRNET, STFC, Nikhef)

- Self-audit review
  - Cosmin Nistor as review coordinator
  - Self-audits progressing on schedule for most CAs



		Specific Policies and Practices			
TR-Grid CA (Turkey) *(Authority member)* (TACAR OK)	Feyza Eryol	CA TRGrid (accredited:classic): CERT CRL concerns: ca@grid.org.tr A2:31:9E:C8:90:AF:D9:6D:F4:4A:59:31:F2:E6:D2:D5:39:EC:1D:F0 Generic CP and CPS statements	2005-09-29	2016-01-20	2016-01-20 (0.2yr)
Trans-European Research and Educational Networking Association (TERENA) *(Relying Party member)*	Licia Florio (277707CC)	*CP and CPS are not relevant* About TERENA: http://www.terena.org/	2004-04-01	2015-09-09	
UK e-Science CAs *(Authority member)* (TACAR OK)	Jens Jensen (9210F006) David Kelsey	CA UKeScienceRoot-2007 (accredited:classic): CRL concerns: support@grid-support.ac.uk A1:39:B0:F3:04:6C:0B:F9:F5:0A:1B:33:00:06:4F:83:6B:7D:4F:3E CA UKeScienceCA-2A (accredited:classic): CRL concerns: support@grid-support.ac.uk 41:C7:C4:A0:31:F7:07:02:81:C7:61:D5:7E:92:48:01:DF:87:C9:06 CA UKeScienceCA-2B (accredited:classic): CRL concerns: support@grid-support.ac.uk DB:D9:5A:B4:E9:AD:74:26:E0:33:68:AA:B1:77:CC:5B:64:B2:CB:0E Generic CP and CPS statements	2000-12-04	2016-01-20	2014-01-14 (2.2yr)
Ukrainian Grid CA *(Authority member)* (TACAR FAILURE)	Sergii Stirenko Oleg Alienin	CA UGRID (accredited:classic): CERT CRL concerns: ca@ugrid.org 21:E7:0D:EE:D7:57:B6:47:A6:F5:04:29:76:81:FE:CD:E8:48:DD:9A Generic CP and CPS statements	2008-02-14	2013-09-11	2013-09-11 (2.5yr)

AAI in a wider context

IGTF traditionally well-linked to research and e-Infrastructures

- *support for research use cases*
- *user-centric authentication based on a ‘bottom-up’ approach*

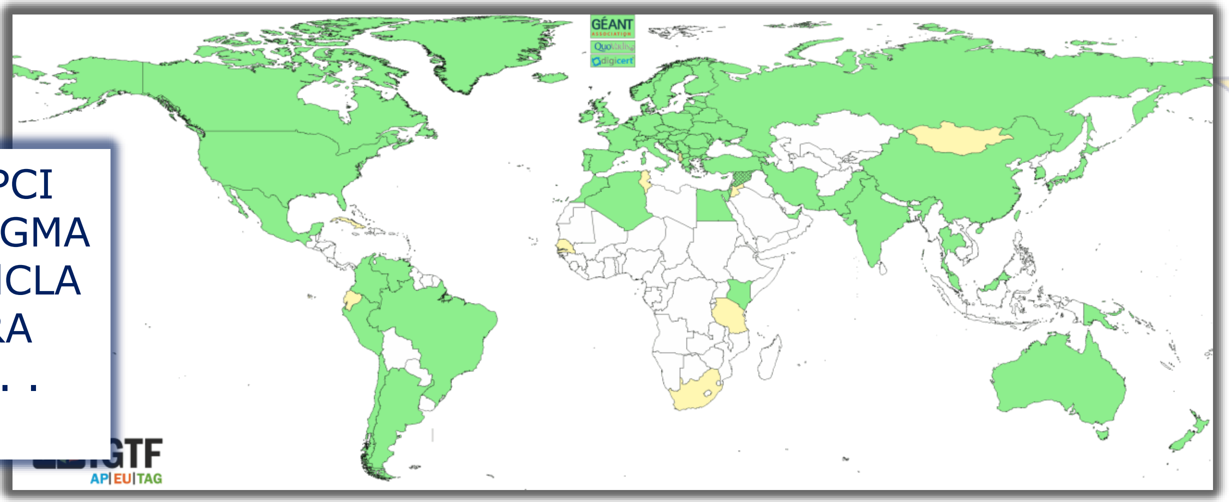
In Europe, the AARC project supports evolution of ‘traditional’ R&E federations towards this research and collaboration use

- *common Blueprint Architecture promoting **SP-IdP Proxies***
- *harmonised **policy supporting production use** of federations (Sirtfi and “R&S”, non-reassigned identifiers and assurance)*
- *help communities express ‘common’ qualities through **Snctfi***
- *allow newer technologies (**OIDC**) on the Infrastructure side*

Trust for global e-Science infrastructures

“establish common policies and guidelines that enable interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers,
and relying parties”

EGI
PRACE
GEANT
WLCG
XSEDE
OSG
HPCI
PRAGMA
RedCLA
RA
. . .



Selected topics from EUGridPMA & AARC

- Assurance frameworks – evolution and components

- Joint Infrastructure policies
- Acceptable Use and Conditions of Use
- Policy Development Kit

- Attribute Authority Operations

- Incident response and communications challenges

Assurance and trust frameworks

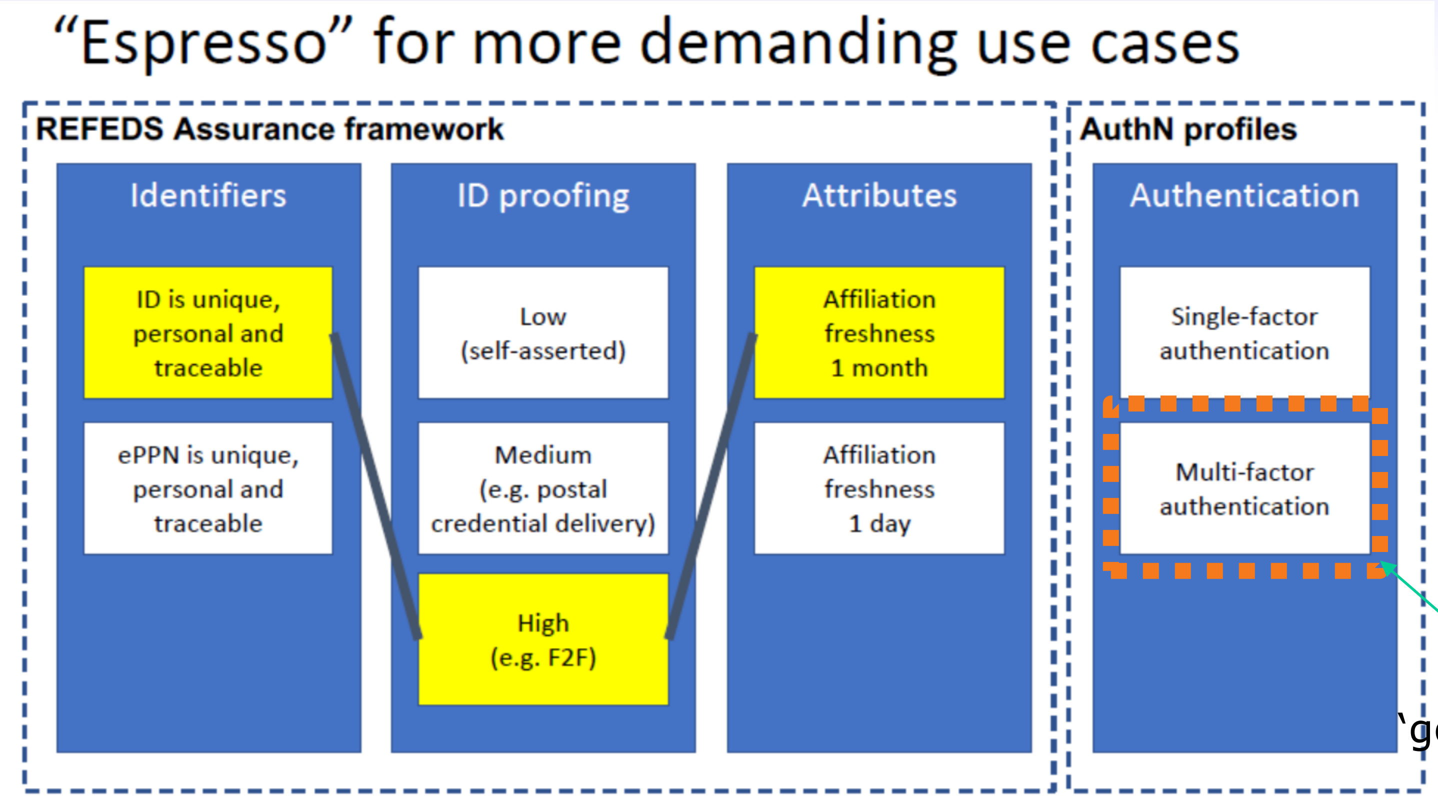
Identity Assurance Profiles for Infrastructure risk scenarios
https://igtf.net/ap/loa/

- BIRCH - good quality (federated) identity,
  DOGWOOD - identifier-only with traceability (*R&S+Sirtfi+a few bits)*
- RFC 6711 Registry: https://iana.org/assignments/loa-profiles
- technology-specific 'trust anchor' distribution services

Assurance landscape is becoming more complex again

- 'components of trust' in SP800-63v3, IETF VoT, and in REFEDS RAF
- for Research and collaboration use case use *profiles*,
  for home organization IdPs use *components* and REFEDS RAF + [MS]FA

Example: “Espresso” profile for demanding use cases



“Espresso” for more demanding use cases

REFEDS Assurance framework

Identifiers	ID proofing	Attributes
ID is unique, personal and traceable	Low (self-asserted)	Affiliation freshness 1 month
ePPN is unique, personal and traceable	Medium (e.g. postal credential delivery)	Affiliation freshness 1 day
	High (e.g. F2F)	

AuthN profiles

Authentication
Single-factor authentication
Multi-factor authentication

‘goes well with’

alignment with REFEDS SFA/MFA WG is part of the work programme of AARC2

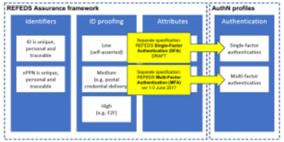
Using the REFEDS Assurance Framework in practice: the RAF Pilot ☺

Goal: gain practical experience with Assurance framework *and* REFEDS Single-factor authentication (SFA) profile, both on specification and in deploying existing SAML products

XSEDE
Extreme Science and Engineering
Discovery Environment

CSC
CSC-TIETEEN TIETOTEKNIIKAN KESKUS

Aalto University


REFEDS Assurance framework
Identifiers
ID is unique, personal and traceable
ePPN is unique, personal and traceable
ID proofing
Low (self-asserted)
Medium (e.g. postal credential delivery
High (e.g. F2F)
Attributes
Separate specification: REFEDS Single-Factor Authentication (SFA) DRAFT
Separate specification: REFEDS Multi-Factor Authentication (MFA) ver 1.0 June 2017
AuthN profiles
Authentication
Single-factor authentication
Multi-factor authentication

elixir

egi

BBMRI-ERIC
Biobanking and
BioMolecular resources
Research Infrastructure

Today: both IdP software (now mostly Shibboleth) can express components and profiles, and use cases can leverage REFEDS assurance profiles (Cappuccino, Espresso) directly

https://wiki.refeds.org/display/GROUPS/Pilot+on+RAF+and+SFA
https://wiki.refeds.org/display/GROUPS/Pilot+resources

Snctfi: aiding Infrastructures achieve policy coherency

- ✓ allow SP-IdP-Proxies to assert ‘qualities’, based on assessable trust
- ✓ Develop **recommendations for an Infrastructure’s coherent policy set**

Snctfi v1.0 AARC

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi)

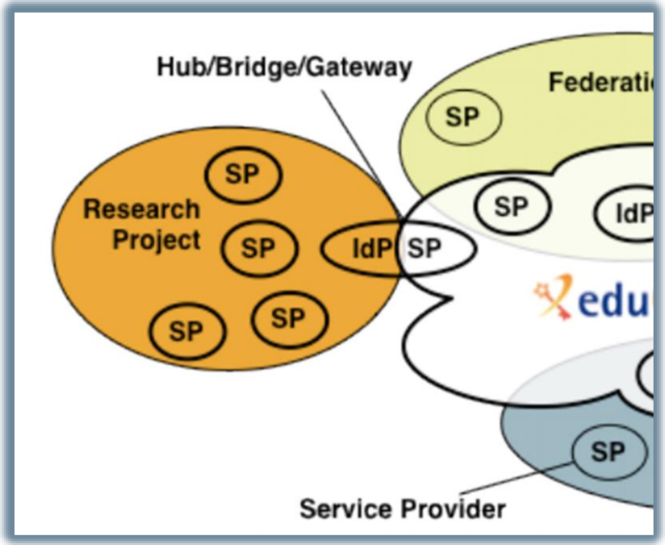
Licia Florio (GÉANT), David Groep (Nikhef), Christos Kanellopoulos (GÉANT), David Kelsey (STFC), Mikael Linden (CSC), Ian Neilson (STFC), Stefan Paetow (Jisc), Wolfgang Pempe (DFN), Vincent Ribaillier (IDRIS-CNRS), Mischa Salle (Nikhef), Hannah Short (CERN), Uros Stevanovic (KIT) and Gerben Venekamp (SURFsara)

AARC - Version 1.0 - 26 Apr 2017

e-mail: david.kelsey@stfc.ac.uk

Abstract: This paper identifies operational and policy requirements to help establish trust between an Infrastructure and identity providers either in an R&E Federation or in another Infrastructure, in each case joined via a Service Provider to Identity Provider proxy.

Audience: 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.



Graphics inset: Ann Harding and Lukas Hammerle, GEANT and SWITCH

Snctfi

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures

- Complements Sirtfi with requirements on internal consistent policy sets for Infrastructures
- Aids Infrastructures assert *existing* categories R&S, Sirtfi, CoCo
- Support communities and infrastructures with a *policy kit* and *Acceptable Use Policy* alignment

https://igtf.net/snctfi

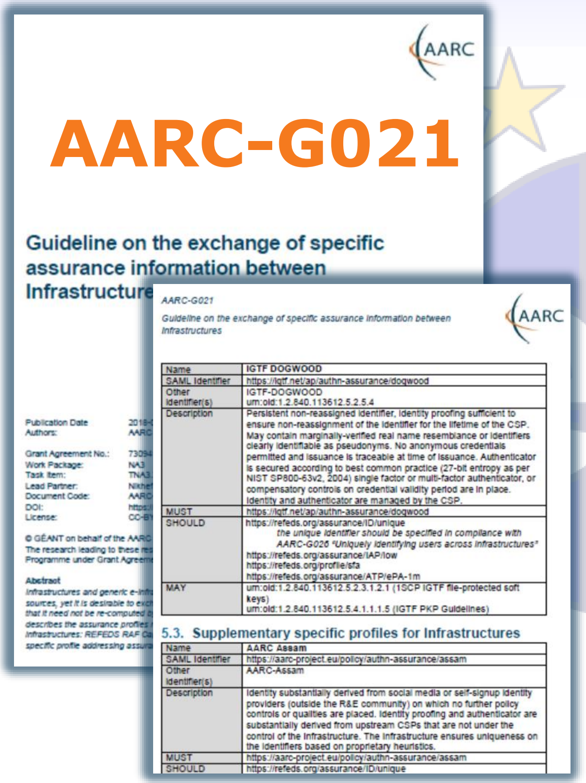
Re-usable Assurance between Infrastructures

- BPA (community) proxy constructs identity based on multiple sources: home organisation, attributes, linked identities, authenticators
  – and process these with (community-specific) heuristics
- resulting assurance level may be different from one in home organization – and may depend on intelligence (components) that are not 'passable' to the next (infrastructure) proxy
- luckily: number of proxies in an exchange limited, and there's explicit trust

each BPA IdP-SP **proxy should convey its 'established assurance'**

use a **limited number of *profiles*** targeted
at Infrastructure and Services risk levels (not in IdP capabilities)

re-use existing profiles as much as reasonable



AARC

AARC-G021

Guideline on the exchange of specific assurance information between Infrastructure

Publication Date 2018-0
Authors: AARC

Grant Agreement No.: 73094
Work Package: NA3
Task Item: TNA3.
Lead Partner: Nikhef
Document Code: AARC
DOI: https:/
License: CC-BY

© GÉANT on behalf of the AARC
The research leading to these res
Programme under Grant Agreeme

Abstract

Infrastructures and generic e-infra
sources, yet it is desirable to exch
that it need not be re-computed b
describes the assurance profiles
Infrastructures: REFEDS RAF Ca
specific profile addressing assura

AARC-G021

Guideline on the exchange of specific assurance information between Infrastructures

AARC

Name	**IGTF DOGWOOD**
SAML Identifier	https://igtf.net/ap/authn-assurance/dogwood
Other Identifier(s)	IGTF-DOGWOOD urn:oid:1.2.840.113612.5.2.5.4
Description	Persistent non-reassigned identifier, identity proofing sufficient to ensure non-reassignment of the identifier for the lifetime of the CSP. May contain marginally-verified real name resemblance or identifiers clearly identifiable as pseudonyms. No anonymous credentials permitted and issuance is traceable at time of issuance. Authenticator is secured according to best common practice (27-bit entropy as per NIST SP800-63v2, 2004) single factor or multi-factor authenticator, or compensatory controls on credential validity period are in place. Identity and authenticator are managed by the CSP.
MUST	https://igtf.net/ap/authn-assurance/dogwood
SHOULD	https://refeds.org/assurance/ID/unique *the unique identifier should be specified in compliance with AARC-G026 "Uniquely identifying users across infrastructures"* https://refeds.org/assurance/IAP/low https://refeds.org/profile/sfa https://refeds.org/assurance/ATP/ePA-1m
MAY	urn:oid:1.2.840.113612.5.2.3.1.2.1 (1SCP IGTF file-protected soft keys) urn:oid:1.2.840.113612.5.4.1.1.1.5 (IGTF PKP Guidelines)

5.3. Supplementary specific profiles for Infrastructures

Name	**AARC Assam**
SAML Identifier	https://aarc-project.eu/policy/authn-assurance/assam
Other Identifier(s)	AARC-Assam
Description	Identity substantially derived from social media or self-signup identity providers (outside the R&E community) on which no further policy controls or qualities are placed. Identity proofing and authenticator are substantially derived from upstream CSPs that are not under the control of the infrastructure. The infrastructure ensures uniqueness on the identifiers based on proprietary heuristics.
MUST	https://aarc-project.eu/policy/authn-assurance/assam
SHOULD	https://refeds.org/assurance/ID/unique

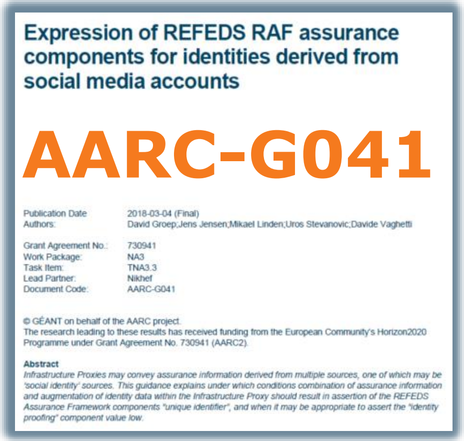
AARC-G021: https://doi.org/10.5281/zenodo.1173558

Specific assurance information BETWEEN Infrastructures

- from REFEDS Assurance Framework: Cappuccino, Espresso
- from IGTF Assurance Profiles: BIRCH, DOGWOOD (https://iana.org/assignments/loa-profiles)
- from the AARC JRA1 use case analysis: Assam – derived from a user-held social identity

Can be extended to social ID
between the e-Infrastructures

from assessment:
this level is below DOGWOOD
unless specifically augmented by
an Infrastructure proxy and registry



Expression of REFEDS RAF assurance components for identities derived from social media accounts

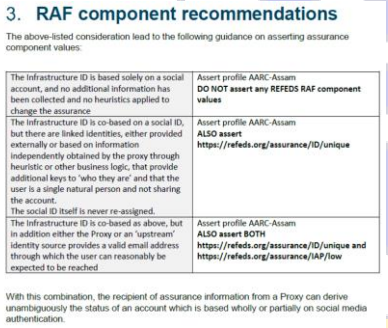
AARC-G041

Publication Date	2018-03-04 (Final)
Authors:	David Groep;Jens Jensen;Mikael Linden;Uros Stevanovic;Davide Vaghetti
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	TNA3.3
Lead Partner:	Nikhef
Document Code:	AARC-G041

© GÉANT on behalf of the AARC project.
The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract

Infrastructure Proxies may convey assurance information derived from multiple sources, one of which may be 'social identity' sources. This guidance explains under which conditions combination of assurance information and augmentation of identity data within the Infrastructure Proxy should result in assertion of the REFEDS Assurance Framework components "unique identifier", and when it may be appropriate to assert the "identity proofing" component value low.



3. RAF component recommendations

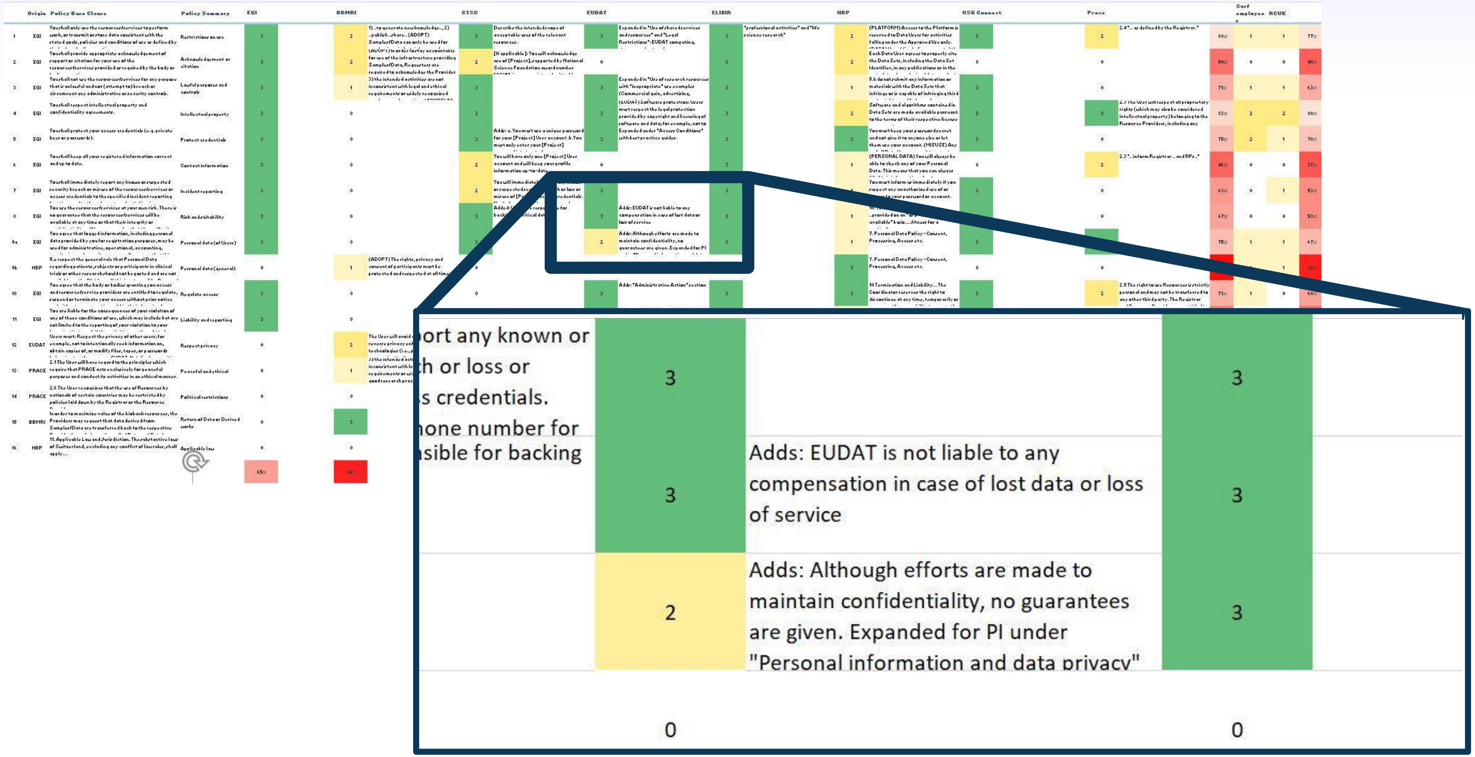
The above-listed consideration lead to the following guidance on asserting assurance component values:

The Infrastructure ID is based solely on a social account, and no additional information has been collected and no heuristics applied to change the assurance	Assert profile AARC-Assam **DO NOT assert any REFEDS RAF component values**
The Infrastructure ID is co-based on a social ID, but there are linked identities, either provided externally or based on information independently obtained by the proxy through heuristic or other business logic, that provide additional keys to 'who they are' and that the user is a single natural person and not sharing the account. The social ID itself is never re-assigned.	Assert profile AARC-Assam **ALSO assert** **https://refeds.org/assurance/ID/unique**
The Infrastructure ID is co-based as above, but in addition either the Proxy or an 'upstream' identity source provides a valid email address through which the user can reasonably be expected to be reached	Assert profile AARC-Assam **ALSO assert BOTH** **https://refeds.org/assurance/ID/unique and** **https://refeds.org/assurance/IAP/low**

With this combination, the recipient of assurance information from a Proxy can derive unambiguously the status of an account which is based wholly or partially on social media authentication.

https://aarc-project.eu/guidelines/aarc-g041/

Divergence and convergence – the AUP Alignment Study



	Origin	Policy Base Clause	Policy Summary	EGI	BBMRI		CTSC		EUDAT		ELIXIR		HBP		OSG Connect		Prace			Surf employees	RCUK	
1	EGI	You shall only use the resources/services to perform work, or transmit or store data consistent with the stated goals, policies and conditions of use as defined by	Restrictions on use	3	2	1) ..to generate new knowledge..., 2) ..publish ..share.. (ADOPT) Samples/Data can only be used for	3	Describe the intended scope of acceptable uses of the relevant resources.	3	Expanded in "Use of shared services and resources" and "Legal Restrictions": EUDAT computing,	3	"professional activities" and "life science research"	2	(PLATFORM) Access to the Platform is reserved to Data Users for activities falling under the Approved Use only.	3		2	2.4 "... as defined by the Registrar."	88%	1	1	77%
2	EGI	You shall provide appropriate acknowledgement of support or citation for your use of the resources/services provided as required by the body or	Acknowledgement or citation	3	2	(ADOPT) In order to stay accountable for use of the infrastructure providing Samples/Data, Requesters are required to acknowledge the Provider	2	[If applicable]: You will acknowledge use of [Project], supported by National Science Foundation award number	0		3		2	Each Data User agrees to properly cite the Data Sets, including the Data Set Identifier, in any publications or in the	0		0		50%	0	0	40%
3	EGI	You shall not use the resources/services for any purpose that is unlawful and not (attempt to) breach or circumvent any administrative or security controls.	Lawful purposes and controls	3	1	3) the intended activities are not inconsistent with legal and ethical requirements or widely recognized	3		3	Expanded in "Use of research resources with "inappropriate" use examples (Commercial gain, advertising,	3		1	5.h do not submit any information or materials with the Data Sets that infringe or is capable of infringing third	3		0		71%	1	1	63%
4	EGI	You shall respect intellectual property and confidentiality agreements.	Intellectual property	3	0		3		3	(EUDAT) Software protection: Users must respect the legal protection provided by copyright and licensing of software and data; for example, not to	3		2	Software and algorithms contained in Data Sets are made available pursuant to the terms of their respective license	3		3	2.7 The User will respect all proprietary rights (which may also be considered intellectual property) belonging to the Resource Providers, including any	83%	2	2	80%
5	EGI	You shall protect your access credentials (e.g. private keys or passwords).	Protect credentials	3	0		3	Adds: a. You must use a unique password for your [Project] User account. b. You must only enter your [Project]	3	Expanded under "Access Conditions" with best practice guides.	3		3	You must keep your password secret and not give it to anyone else or let them use your account. (MISUSE) Any	3		0		75%	2	1	70%
6	EGI	You shall keep all your registered information correct and up to date.	Contact information	3	0		2	You will have only one [Project] User account and will keep your profile information up-to-date.	0		3		1	(PERSONAL DATA) You will always be able to check any of your Personal Data. This means that you can always	0		2	2.3 "...inform Registrar .. and RPs.."	46%	0	0	37%
7	EGI	You shall immediately report any known or suspected security breach or misuse of the resources/services or access credentials to the specified incident reporting	Incident reporting	3	0		2	You will immediately ... or suspected se... ch or loss or misuse of [P... credentials.	3		3		1	You must inform us immediately if you suspect any unauthorized use of or access to your password or account.	3		0		63%	0	1	53%
8	EGI	You use the resources/services at your own risk. There is no guarantee that the resources/services will be available at any time or that their integrity or	Risk and suitability	3	0		3	Added: U... responsible for backi... critical dat...	3	Adds: EUDAT is not liable to any compensation in case of lost data or loss of service	3		1	10. ... ..provided on an "as ... available" basis.....fitness for a	[illegible]		0		67%	0	0	53%
9a	EGI	You agree that logged information, including personal data provided by you for registration purposes, may be used for administrative, operational, accounting,	Personal data (of Users)	3	0		3		2	Adds: Although efforts are made to maintain confidentiality, no guarantees are given. Expanded for PI	3		1	7. Personal Data Policy - Consent, Processing, Access etc.	3		[illegible]		75%	1	1	67%
9b	HBP	5.e respect the general rule that Personal Data regarding patients, subjects or participants in clinical trials or other research should not be posted and are not	Personal data (general)	0	1	(ADOPT) The rights, privacy and consent of participants must be protected and respected at all time	0						3	7. Personal Data Policy - Consent, Processing, Access etc.	0		0		[illegible]	[illegible]	1	20%
10	EGI	You agree that the body or bodies granting you access and resource/service providers are entitled to regulate, suspend or terminate your access without prior notice	Regulate access	3	0		0		3	Adds: "Administrative Action" section	3		3	10 Termination and Liability... The Coordinator reserves the right to discontinue at any time, temporarily or	3		2	2.5 The right to use Resources is strictly personal and may not be transferred to any other third party. The Registrar	71%	1	0	60%
11	EGI	You are liable for the consequences of your violation of any of these conditions of use, which may include but are not limited to the reporting of your violation to your	Liability and reporting	3	0																	
12	EUDAT	Users must: Respect the privacy of other users; for example, not to intentionally seek information on, obtain copies of, or modify files, tapes, or passwords	Respect privacy	0	2	The User will avoid ... reverse privacy enh... technologies (i.e., p...																
13	PRACE	2.1 The User will have regard to the principles which require that PRACE acts exclusively for peaceful purposes and conduct its activities in an ethical manner.	Peaceful and ethical	0	1	3) the intended act... inconsistent with le... requirements or wi... good research prac...																
14	PRACE	2.6 The User recognises that the use of Resources by nationals of certain countries may be restricted by policies laid down by the Registrar or the Resource	Political restrictions	0	0																	
15	BBMRI	In order to maximize value of the biobank resources, the Providers may request that data derived from Samples/Data are transferred back to the respective	Return of Data or Derived works	0	3																	
16	HBP	11. Applicable Law and Jurisdiction. The substantive laws of Switzerland, excluding any conflict of law rules, shall apply....	Applicable law	0	0																	
				65%	24%																	

ort any known or ch or loss or s credentials. hone number for	3		3
sible for backing	3	Adds: EUDAT is not liable to any compensation in case of lost data or loss of service	3
	2	Adds: Although efforts are made to maintain confidentiality, no guarantees are given. Expanded for PI under "Personal information and data privacy"	3
	0		0

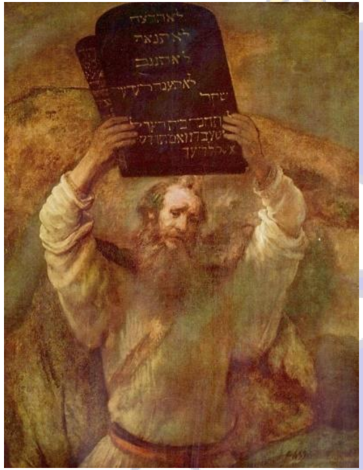
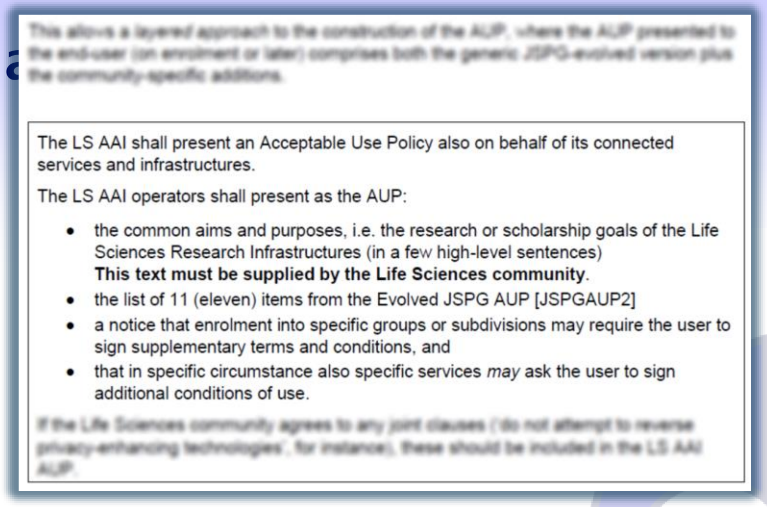


Image: Mozes en de tafelen der Wet, Rembrandt van Rijn, 1659

Scaling Acceptable Use Policy and da



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.

impractical to present user 'click-through' screens on each individual service

Community conditions

Community specific terms & conditions

Community specific terms & conditions

RI Cluster-specific terms & conditions

Modular approach: applicable to Snctfi proxies (also) on behalf of a community

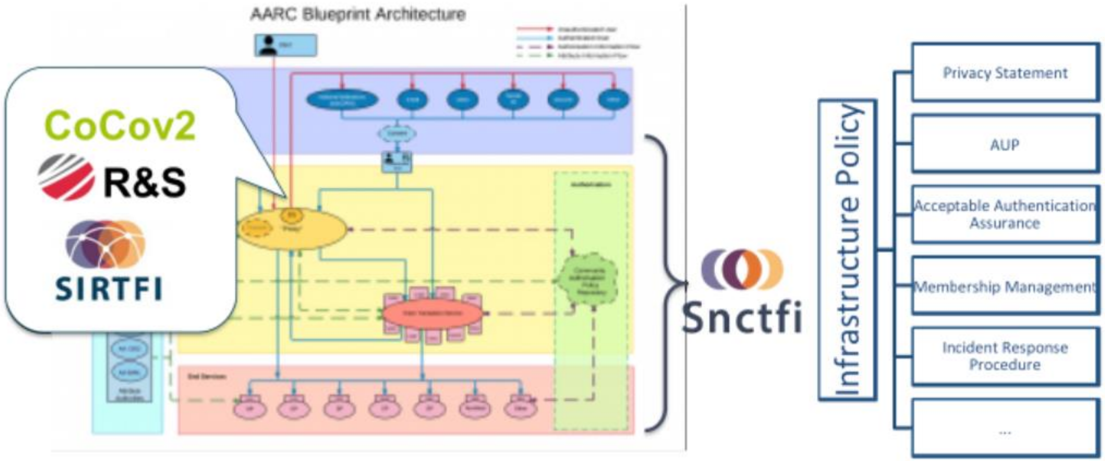
Common baseline AUP for e-Infrastructures and Research Communities

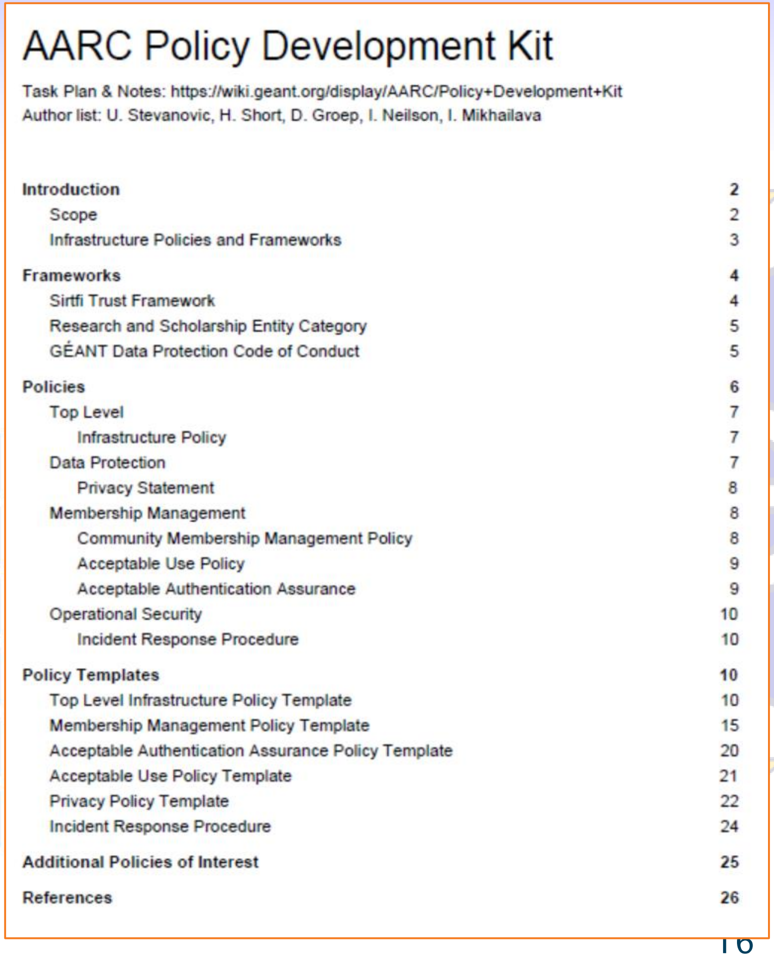
(current draft: JSPG Evolved AUP – leveraging comparison study and joint e-Infrastructure work)

https://wiki.geant.org/x/P4bWBQ

Policy Development Kit

- Bring together a consistent suite
- based on e-Infrastructure best practices in particular EGI, WLCG, and the JSPG


AARC Blueprint Architecture
CoCov2
R&S
SIRTFI
Snctfi
Infrastructure Policy
Privacy Statement
AUP
Acceptable Authentication Assurance
Membership Management
Incident Response Procedure
...



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
References 26

Attribute Authority Operations

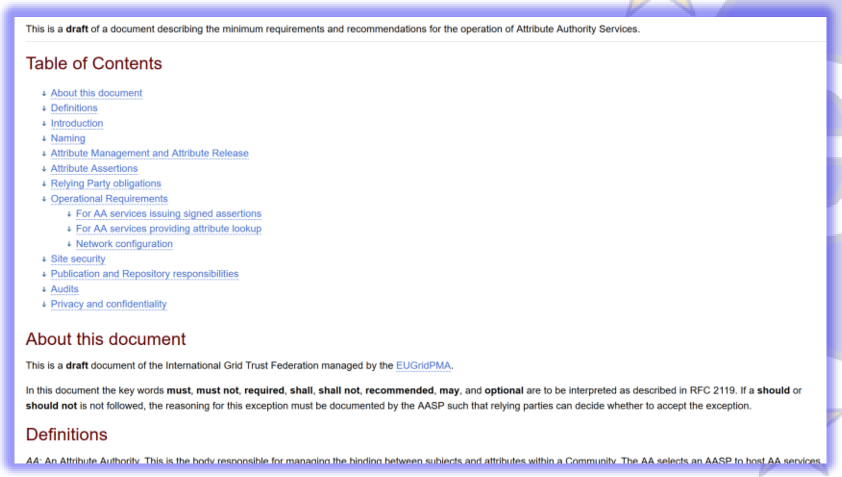
- Extending OpSec and trust capability in the authorization space
- Based on initial IGTF work in 2012, which can now be put on a *Snctfi* basis

https://www.igtf.net/guidelines/aaops/

AAOPS as basis for Infrastructure Proxies

Extend scope of 'proper secure authorities' to the community membership services at the *Snctfi* Proxy

Bring best practice of *Sirtfi* operational security for infrastructure proxies to same level as for identity authorities



This is a **draft** of a document describing the minimum requirements and recommendations for the operation of Attribute Authority Services.

Table of Contents

- About this document
- Definitions
- Introduction
- Naming
- Attribute Management and Attribute Release
- Attribute Assertions
- Relying Party obligations
- Operational Requirements
  - For AA services issuing signed assertions
  - For AA services providing attribute lookup
  - Network configuration
- Site security
- Publication and Repository responsibilities
- Audits
- Privacy and confidentiality

About this document

This is a **draft** document of the International Grid Trust Federation managed by the EUGridPMA.

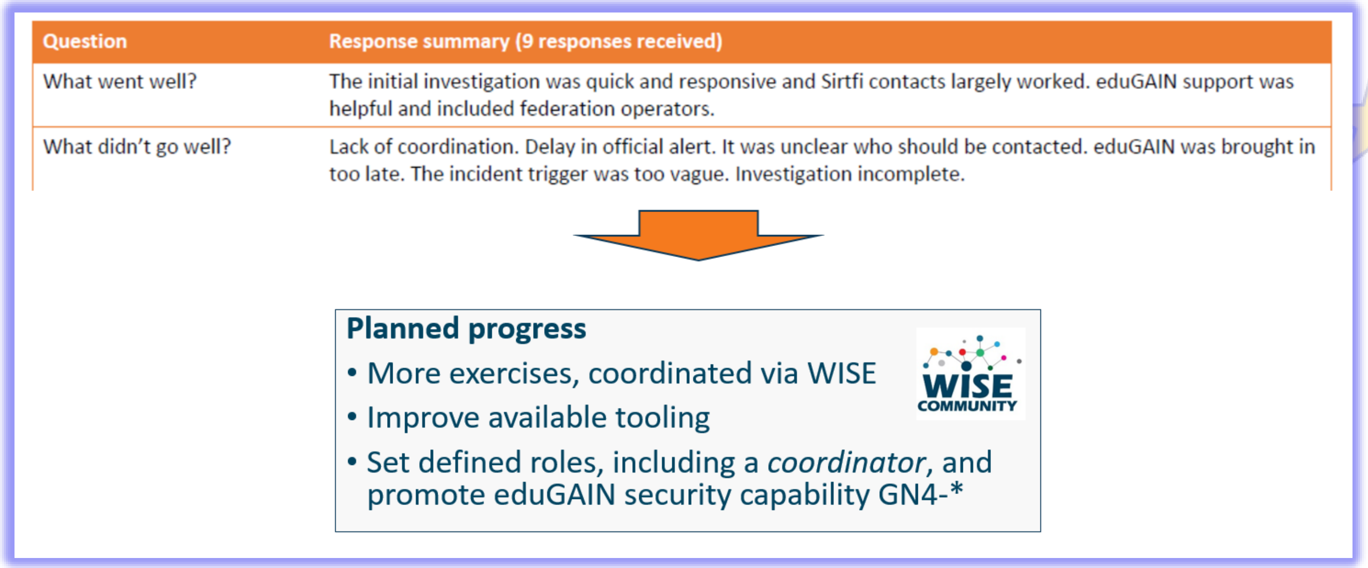
In this document the key words **must**, **must not**, **required**, **shall**, **shall not**, **recommended**, **may**, and **optional** are to be interpreted as described in RFC 2119. If a **should** or **should not** is not followed, the reasoning for this exception must be documented by the AASP such that relying parties can decide whether to accept the exception.

Definitions

AA: An Attribute Authority. This is the body responsible for managing the binding between subjects and attributes within a Community. The AA selects an AASP to host AA services

Communications Challenges

Based on *Sirtfi* incident role play of AARC in eduGAIN:
testing communications channels identified as high-prio target
Initial model might be along the IGTF RAT CC challenges – can be extended later



Question	Response summary (9 responses received)
What went well?	The initial investigation was quick and responsive and Sirtfi contacts largely worked. eduGAIN support was helpful and included federation operators.
What didn't go well?	Lack of coordination. Delay in official alert. It was unclear who should be contacted. eduGAIN was brought in too late. The incident trigger was too vague. Investigation incomplete.

Planned progress

- More exercises, coordinated via WISE
- Improve available tooling
- Set defined roles, including a *coordinator*, and promote eduGAIN security capability GN4-*

Proper OpSec needs to be exercized!

Like the IGTF RAT Communications Challenges, and TF-CSIRT processes, opsec really needs to be exercised often and in-depth to ensure readiness

Logical candidates that could all run the test against IdPs, CAs, SPs, RPs … … and 'legitimately' claim an interest in their results

- eduGAIN
- IGTF
- GEANT.org
- EOSC-HUB ops, or EGI CSIRT
- each of the e-Infrastructures XSEDE, EGI, EUDAT, PRACE, HPCI, …
- every research infra with an interest: WLCG, LSAAI, BBMRI, ELIXIR, …
- any institution (or person) with access to https://mds.edugain.org/

so soon: all the email in the world will be about Sirtfi Incident Response tests??

Frequency of challenges and tests - examples

Trusted Introducer and TF-CSIRT

- 2-3 Reaction Tests per year
- supported by web click infrastructure, but requires (team) authentication

SURFcert challenges

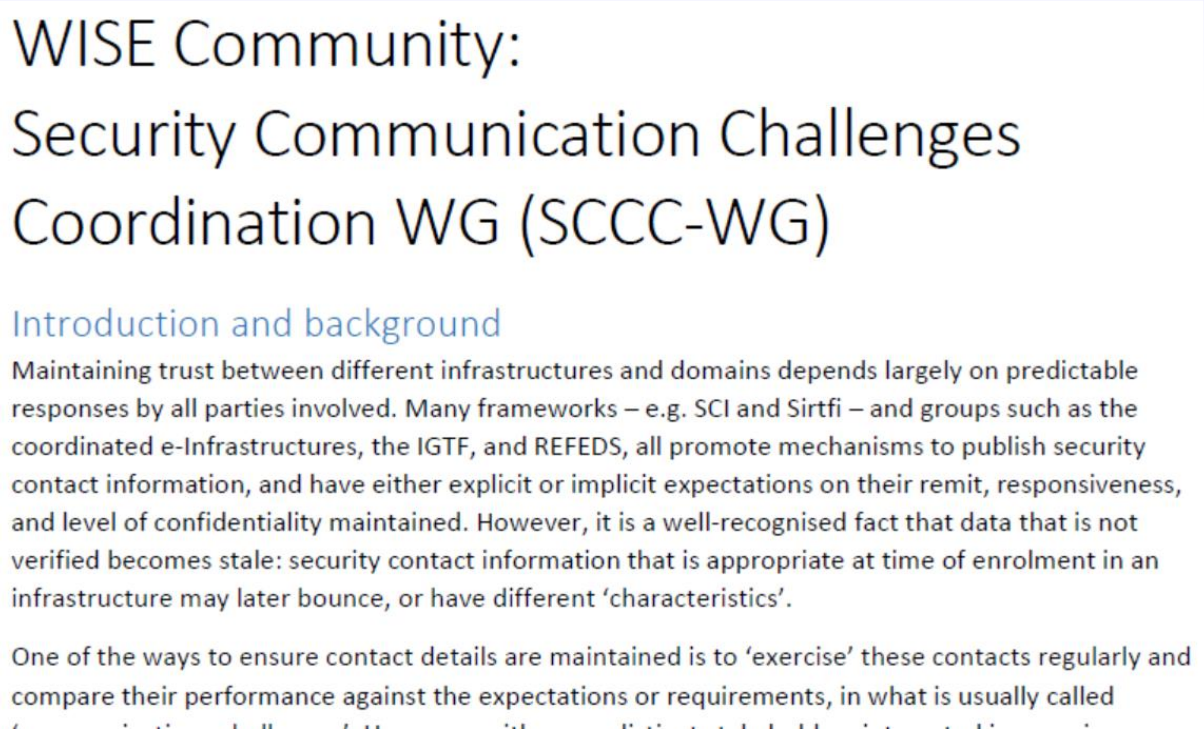
- annual response challenges, just reply to email to a (traceable) ticket

IGTF RAT Communications Challenges

- every 1-2 years
- in parallel with continuous operational monitoring

yet we already listed 14 entities that have a real interest in running tests, 5000+ entities can claim the same

WISE SCCC-WG proposal – participate!



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 verified becomes stale: security contact information that is appropriate at time of enrolment in an infrastructure may later bounce, or have different 'characteristics'.

One of the ways to ensure contact details are maintained is to 'exercise' these contacts regularly and compare their performance against the expectations or requirements, in what is usually called

Proposed working group to WISE SC – see wise-community.org and join!

Upcoming PMA events

EUGridPMA 44, Toulouse	**September 24 – 26, 2018**
TechEx	Oct 15-18, Orlando, FL, USA
TNC19	June 16-20 2019, Tallinn, EE