EUGridPMA
Status and Current Trends
and some IGTF & AARC topics

April 2019
APGridPMA Taipei
David Groep, Nikhef & EUGridPMA

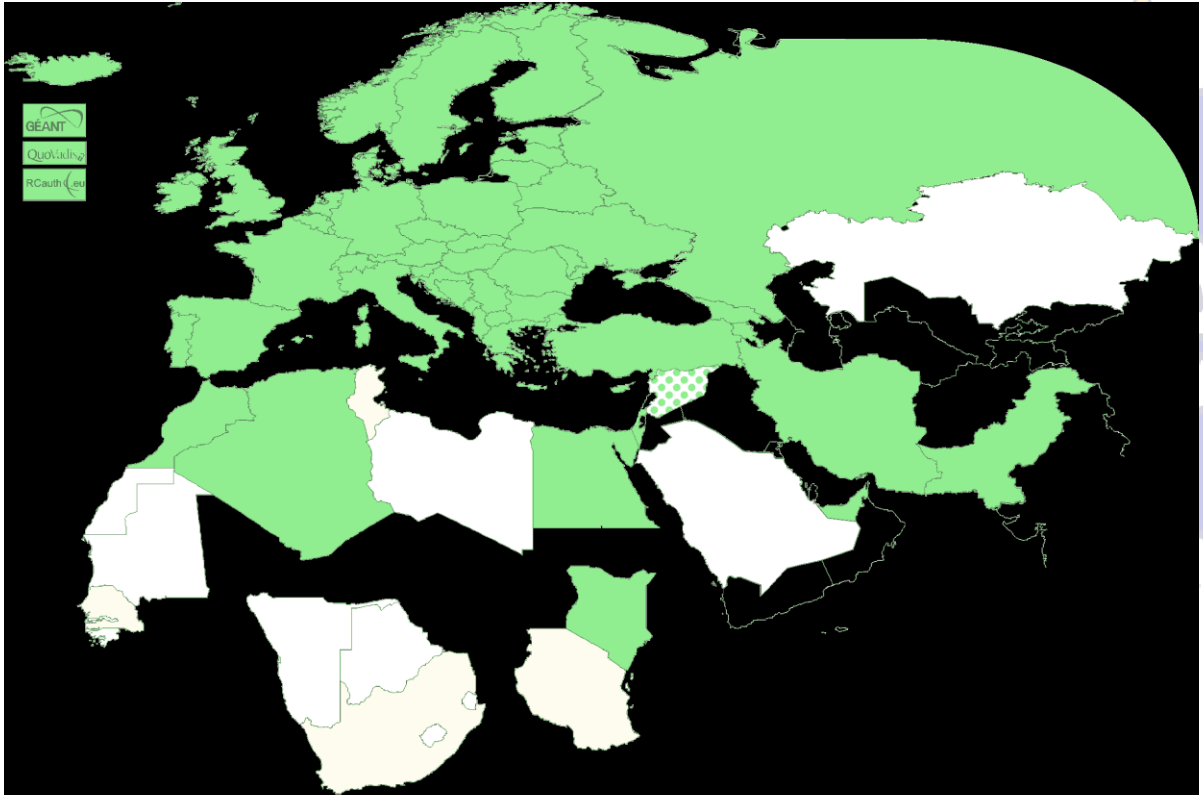
Recent EUGridPMA topics

- PMA membership and evolution of authorities
- Towards TCS G4
- Infrastructure Policy Alignment & AARC
- post- AARC activities and the role of the IGTF and PMAs

See also the EUGridPMA45 summary:
https://www.eugridpma.org/meetings/2019-01/

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

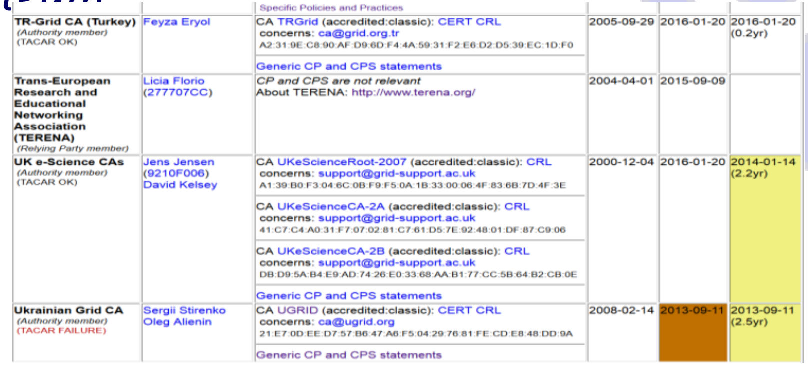
- Responsiveness challenges for some members

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

  EG-EUN now temporarily withdrawn for availability reasons

- Identity providers: both reduction and growth
  - RCauth.eu distributed operations (GRNET, STFC, Nikhef)
    using a shared key (and some smart border-guard-proof distribution)
    governance board + PMA + technical team

- 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)

TGC G4 R/E-Infrastructure requirements

Current ‘grid’ products actually use more widely

- it’s the proper profile for unique user authentication (as opposed to email/document signing)
- robots deserve more exposure (automated emails from CSIRT teams, mailing lists, etc) – like their original role envisioned
- *Naming of the products should probably not be ‘Grid’* ☺

Some thing will change (for better or for worse)

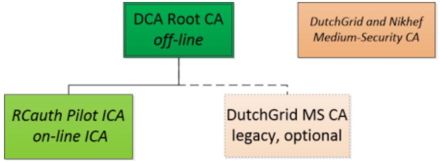
- Hard to keep the propaganda people from changing /DC=org/DC=terena
- Requests for new products: QC for Europe maybe?, better ECC promotion
- push for more standard automation (can we evolve ACME to OV? Standard suggests so!)
- CABForum keeps doing strange things (and is getting biased …)
- MS Outlook also does weird things (mandatory encryption/signing separation)

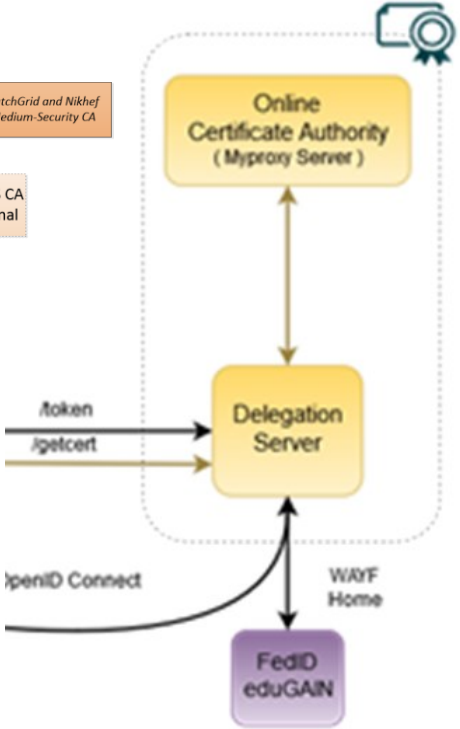
Some things must stay the same

- no GÉANT in the issuer or subject name (stay with 7-bit ASCII)
- Namespace and subject DN construction
- No cyclic issuer graphs, no third-party public trusted root mesh

RCauth.eu – a white-label IOTA CA in Europe

- Cover as much as R&E Federated Europe as possible
- Scoped to research and collaborative use cases
- In a scalable and sustainable deployment model





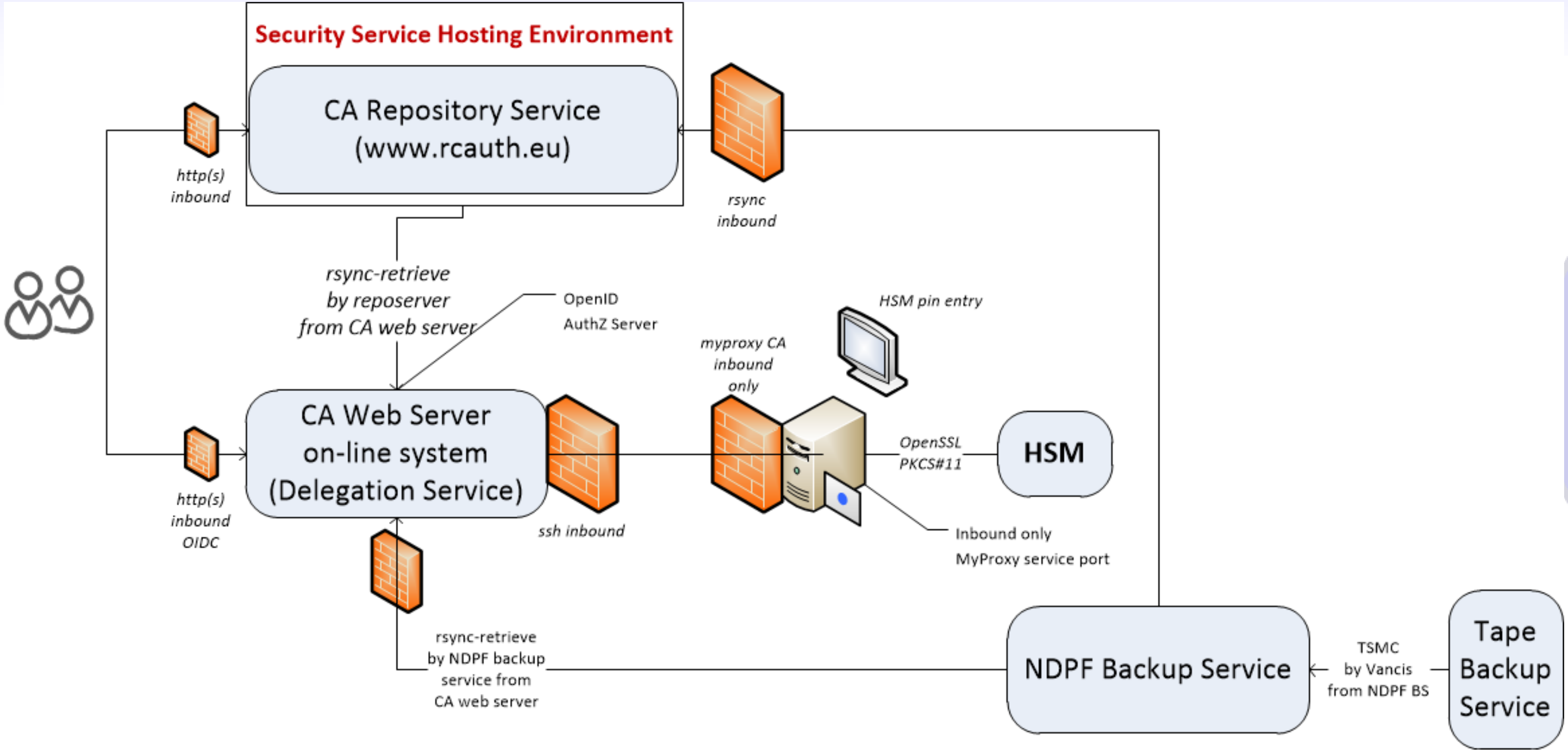
Following the AARC pilot

- operates as a ‘production-compatible’ pilot service
- which will operate for as long as necessary and useful
- is supported by the Dutch National e-Infrastructure & Nikhef

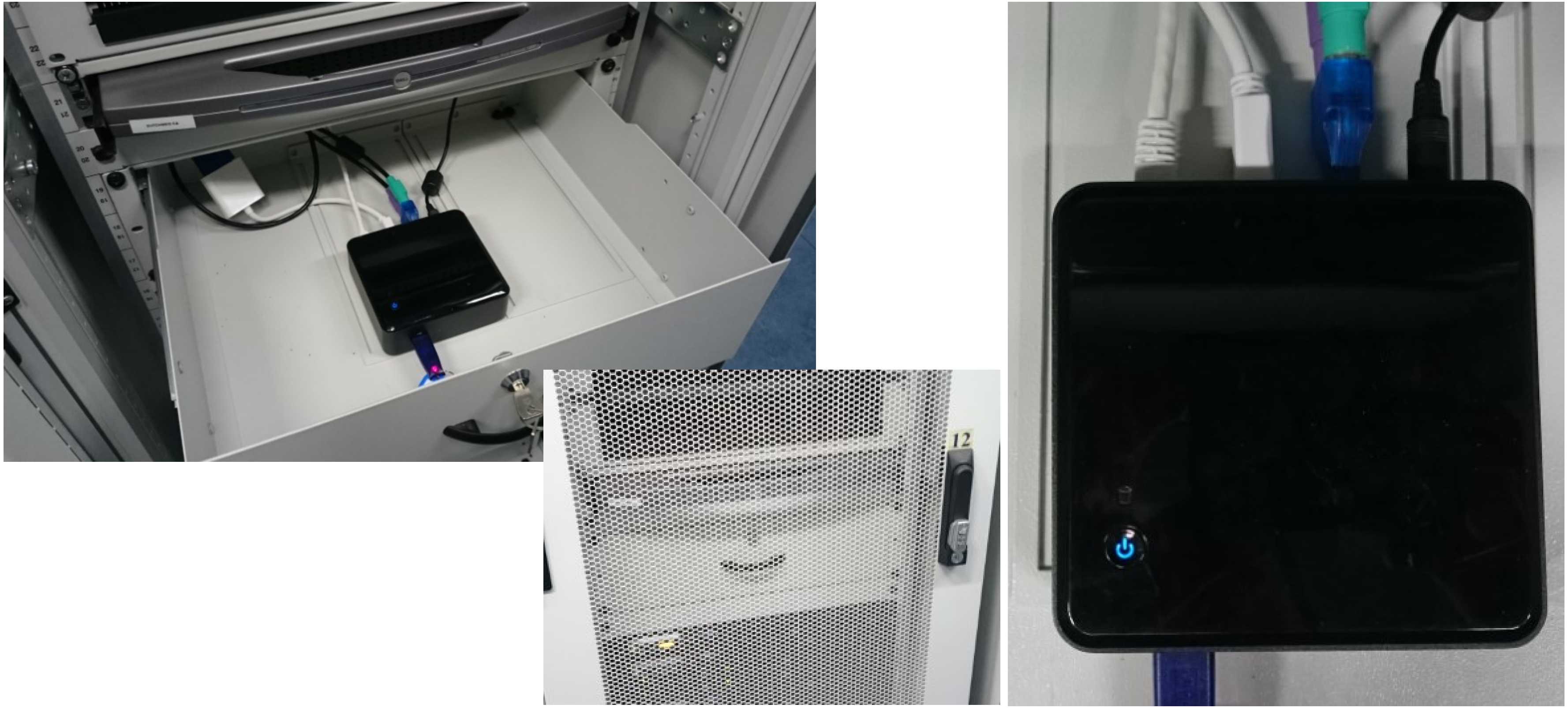
… to support multiple applications and communities:

- EGI CheckIn, B2ACCESS, and WaTTS instances
- Project MinE
- ELIXIR, and the Life Sciences AAI

RCauth.eu: Logical set-up

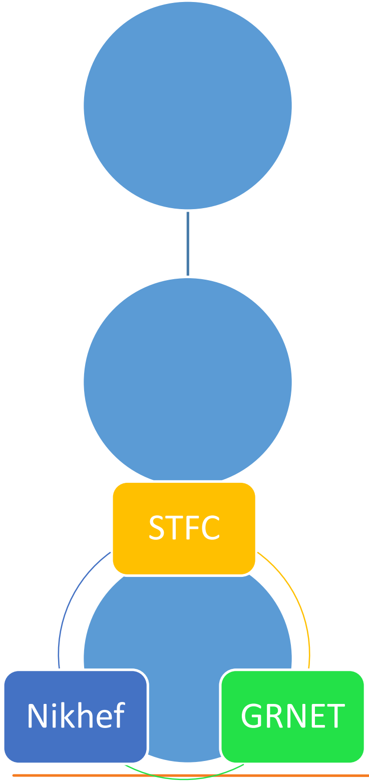

Security Service Hosting Environment
CA Repository Service (www.rcauth.eu)
http(s) inbound
rsync inbound
rsync-retrieve by reposerver from CA web server
OpenID AuthZ Server
HSM pin entry
myproxy CA inbound only
CA Web Server on-line system (Delegation Service)
OpenSSL PKCS#11
HSM
http(s) inbound OIDC
ssh inbound
Inbound only MyProxy service port
rsync-retrieve by NDPF backup service from CA web server
NDPF Backup Service
TSMC by Vancis from NDPF BS
Tape Backup Service

More pretty pictures



Slightly more ugly pictures …

RCauth.eu Governance



Governance Board

Representatives (and one alternate) from each Materially Contributing Stakeholder
EGI.eu, EUDAT (ETFC), GÉANT, Nikhef (SURF)

RCauth PMA

Individuals drawn from the wide community […]
experts in the field of identity management
for research and collaboration,
PKI technology and identity bridging

Ops Coordination Team

Operations people from each of the **hosting partners** with a (copy of) the RCauth.eu signing key,
and those partners otherwise involved in OPS

What do they manage? Two options!

1. Most consistent external view – closest internal coordination and trust
   - Single RCauth.eu signing key
   - Securely distributed to each operational partner
   - Fully owned and managed by the PMA
   - Requires partners to accept stringent controls by the PMA to ensure trust
   - Fully transparent to users and external RPs

2. Most distributed and resilient view – with global user and RP impact on usability
   - Each partner gets a different RCauth.eu signing key
   - These will show up as independent ICAs in the IGTF distribution
   - Same Subject DN namespace, but different issuer names in parallel and simultaneously
   - Partners can join and leave, validity of ICA controlled through the CRL of upstream root
   - Allows PMA to control a leaving party without such party's co-operation and without special measures
   - Floods IGTF distribution with multiple ICAs, and persistently exposes CA internal to VOMS and RPs

Assurance and trust frameworks

REFEDS RAF is there: Cappucino and Espresso

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

- Includes also
  BIRCH - good quality (federated) identity,
  DOGWOOD - identifier-only with traceability (*R&S+Sirtfi+a few bits)*

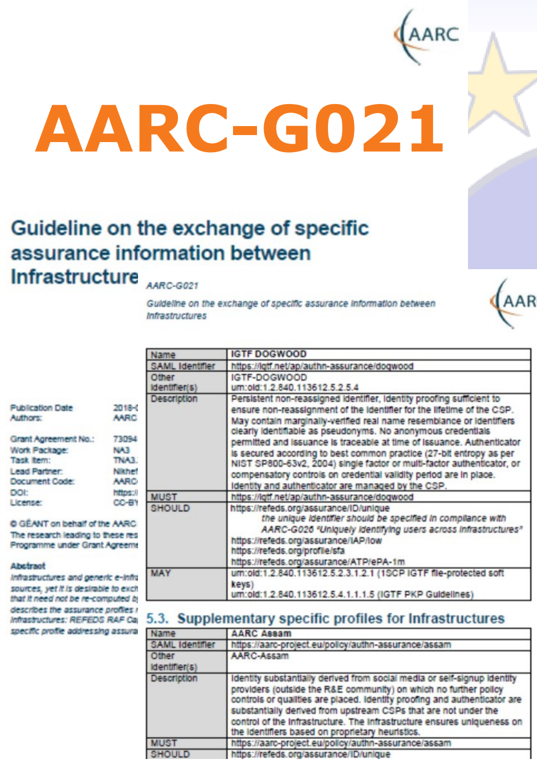
Re-usable Assurance between Infrastructures

- 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-
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

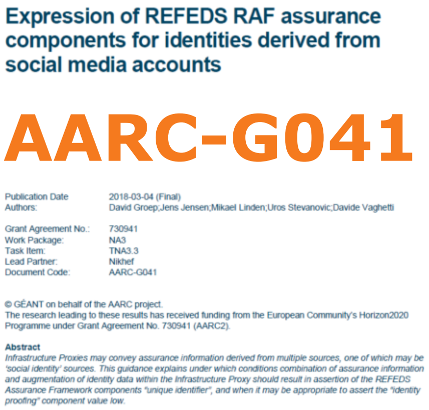
AARC-G021: https://doi.org/10.5281/zenodo.1173558

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

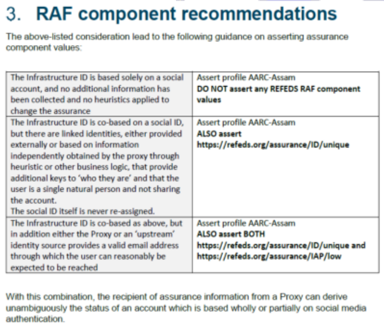
AARC-G041

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:

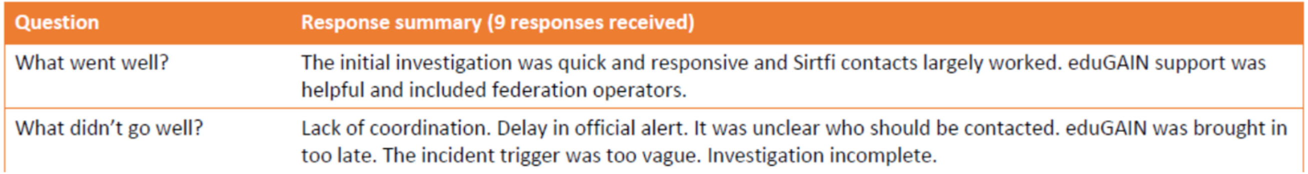
The Infrastructure ID is based solely on a social account, and no additional information has been collected and no heuristics applied to change the assurance	Assert profile AARC-Assam **DO NOT assert any REFEDS RAF component values**
The Infrastructure ID is co-based on a social ID, but there are linked 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.

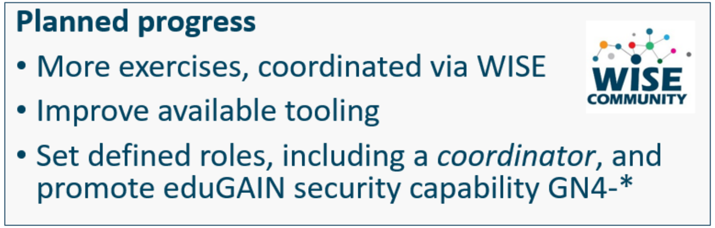
https://aarc-project.eu/guidelines/aarc-g041/

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

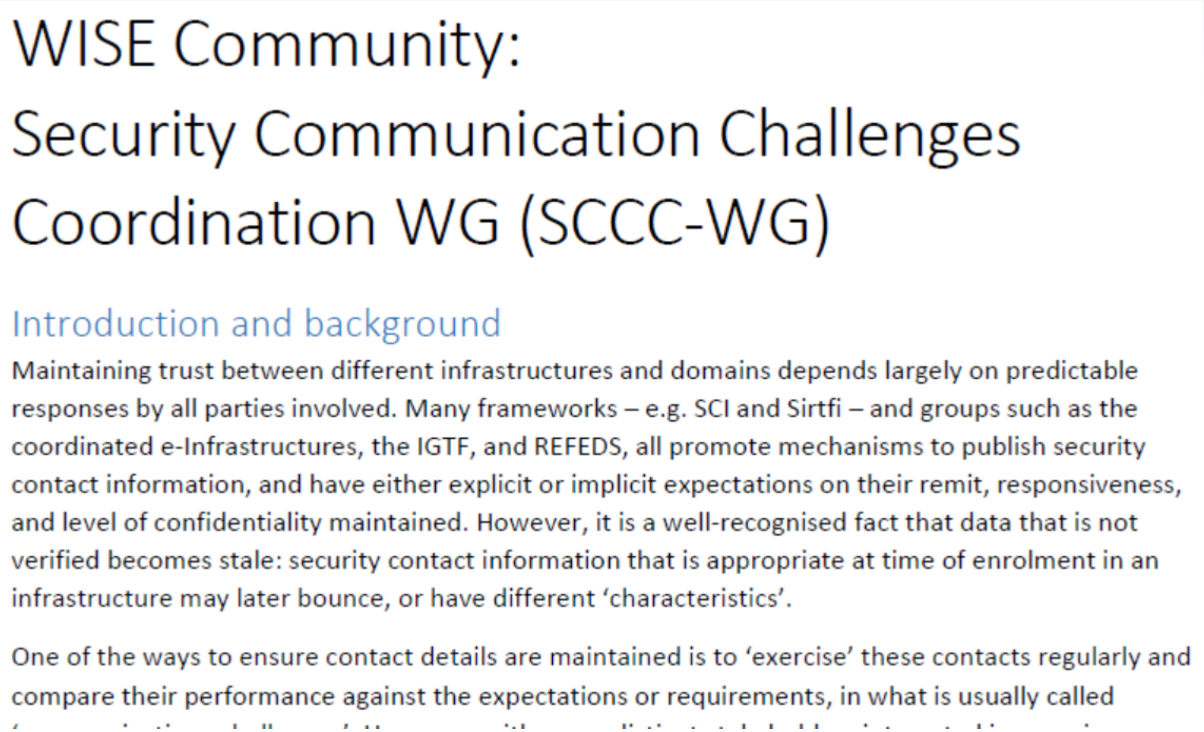
- annual response challenges, just reply to email to a (traceable) ticket

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!

EUGRIDPMA/IGTF AND THE AARC

Beyond AARC – how can the good work continue and thrive?

- EOSC-HUB: mainly WP4.4 “ISM”, WP5.1 “AAI”, and WP13 “Virtual Access” for RCauth
- GN4-3: T5.1.4 – eduGAIN security operations and readiness
- GN4-3: T5.4 – enabling communities

Without specific funding but *endorsed by funded infrastructures & projects*:

- IGTF
- Collaboration Agreement GN4-* and EOSC-HUB
- WISE
- AEGIS
- REFEDS
- FIM4R

Complementary sources: national e-Infrastructures, domain funding, ESFRIs and EOSC projects

Finding a home – some proposals

Sirtfi

- already in a REFEDS WG (Sirtfi+)
- 'response model' to the extent it involves federations can go here as well
- actual incident response plus readiness challenges *on federated ID side* go with new eduGAIN security capability

Communications challenges for security that involve also the Infrastructures

- WISE, specifically the new SCCC WG
- needs some love and care from all Infrastructures

Infrastructure-specific challenges remain infrastructure, but coordinated through SCCC

- like the IGTF RAT CC

Finding a home – some proposals

SCI Assessment

- WISE SCI WG, with assessment in the IGTF
- support through EOSC-HUB WP4.4 and GN4-3T5.4
- but obviously also from PRACE, XSEDE, GridPP, SURF, &c

Assurance Profiles – from federations to Infrastructures, and between R/E infrastructures

- the 'feasible' assurance and alignment with IdPs and federations belongs in REFEDS RAF
- assurance requirements of, and exchange of assurance between, infrastructures: in IGTF

AUP and Terms of Use

- the home is WISE SCI, but it needs care and nourishment from EOSCHUB and GN4-3
- extends beyond just WP4.4/T5.4 and involves e.g. also eduTEAMS, CheckIn, B2ACCESS

Finding a home – some proposals

Data Protection and GDPR – service centric policy support

- we should lean heavily on AndrewC and the TF-DPR, but more is needed
- risk-assessment methodology for infrastructures and communities
- consultancy role for new communities to enable use of the infrastructures -> mailing list?
- joint GN4-3 + EOSC-HUB + WLCG effort, homed (for lack of anything else) in AEGIS?

Tuning the policy development kit

- the WISE SCI WG can coordinate, but the effort should come from somewhere
- again GN4-3 + EOSC-HUB (EGI, EUDAT) seem the natural choice, with input from PRACE
- other sources have been very successful as well: HDF, GridPP, SURF

For the rest and new things needed, leverage GN-EOSCH collaboration agreement & AEGIS?

- one-on-one consulting with communities highly appreciated also beyond AEGIS, but must be and be seen as neutral (maybe a FIM4R or WISE WG? or RDA?)

From now on …

- Coherency of vision and an umbrella for Collaborative policy work will be more challenging
- Exploit personal overlap in the various groups (and cross-membership of lists)
- Provide a forum for cross-fertilization through continued joint workshops

EUGridPMA increasingly hosts such joint meetings

Upcoming PMA events

EUGridPMA 46, in conjunction with EOSChub-WP4.4 and GN4’s *EnCo Policy*
Utrecht, NL May 20-22, 2019

TNC19 & REFEDS	June 16-20 2019, Tallinn, EE
EUGridPMA 47	end of September (23-25?), location *tbd*