



Authentication and Authorisation for Research and Collaboration

Beyond the AARC horizon

Consolidating policy and best practice activities from NA3

David Groep

NA3 coordinator

Nikhef

EUGridPMA54 and AARC NA3 meeting Geneva

January 2019

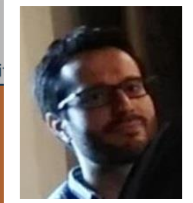
How can policy help you ease collaboration? A holistic view

Operational Security for FIM Communities



GDPR-style Code of Conduct – a new way?

- Global sharing in controlled communities appears attractive
- Uncertainty about requirements (governing body) and timing (> Mar 2018) are not helpful for adoption today ... just yet
- Ongoing work: text needs to allow for (community) attribute authority



supporting policies for Infrastructures

- Note that this is not formally BCR, so requires acceptance
- Collaborations (e.g. based around *Snctfi*) with content
- "Say what you do, and do as you say" – transparency is our real benefit towards the person whose data

AARC-G014 Security Incident Response Trust Framework for Federated Identity
SIRTFI provides a mechanism to identify trusted, operationally secure eduGAIN participants and facilitate effective incident response collaboration.

AARC-G015 Scalable Negotiator for a Community Trust Framework in Federated Infrastructures
The Snctfi Framework identifies operational and policy requirements to help establish trust between an Infrastructure and identity providers either in an RAE Federation or in another Infrastructure, in each case joined via a Service Provider to Identity Provider proxy.

AARC-G021 Exchange of specific assurance information between Infrastructures
Infrastructures and generic Infrastructures compose an 'effective' assurance profile derived from several sources, yet it is desirable to exchange the resulting assurance assertion obtained between Infrastructures so that it need not be re-computed by a recipient Infrastructure or Infrastructure service provider. This document describes the assurance profiles recommended to be used by the Infrastructure AAI Proxies between infrastructures.



3 Community Operations Security Policy

engagement and coordination



1 ACCEPTABLE USE POLICY AND CONDITIONS OF USE

support for Researchers & Community



Baseline Assurance

Value	Cappuccino	Espresso
\$P\$R\$E\$T\$X\$/ID/unique	X	X
\$P\$R\$E\$T\$X\$/ID/no-epgn-reassign		
\$P\$R\$E\$T\$X\$/ID/epgn-reassign-1yr		
\$P\$R\$E\$T\$X\$/IAD/local-enterprise	X	X
\$P\$R\$E\$T\$X\$/IAD/assumed	X	X
\$P\$R\$E\$T\$X\$/IAD/verified		X
\$P\$R\$E\$T\$X\$/AAD/good-entropy	X	
\$P\$R\$E\$T\$X\$/AAD/multi-factor		X
\$P\$R\$E\$T\$X\$/ATP/ePA-1m	X	X

Conditions of Use:

- Known and persistent identifiers
- Documented vetting
- Password verification
- Known and persistent identifiers

Conditions of Use:

- Good entropy passwords. Affiliation freshness better than 1 month
- Multi-factor authenticator

Things to do in AARC's last 6 mo and beyond when you're still alive by now ...

OpSec

Attribute authority operations practice ... also for Infra proxies

Trust groups and the exchange of (account) compromise information: *beyond Sirtfi*

Infra-centric

traceability and accounting data-collection policy framework based on **SCI**, **providing a self-assessment methodology** and comparison matrix for infrastructure services

Evolution of **data protection guidance** for services

Research-centric

Baseline AUP with major Infrastructures (EGI, EUDAT, PRACE, XSEDE) and communities

Deployment of **assurance guidelines** and assess high-assurance use cases (BBMRI)

Engagement

Evolve **Policy Development Kit** and a simpler top-level security policy with a community 'assessment method' or 'guide' to the adoption of appropriate policy

Support communities and use cases in policy interpretation through Guidelines

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

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
- 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 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
- joint GN4-3 + EOSC-HUB + WLCG effort, homed (for lack of anything else) in AEGIS?

Risk Assessment and tuning the policy development kit

- the WISE RAW 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

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

-
- **What AARC policy work have we forgotten?**
 - **Which additional activities could help enable communities?**

Thank you Any Questions?

davidg@nikhef.nl



<https://aarc-project.eu>



© GÉANT on behalf of the AARC project.

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).