EnCo – science engagement

aarc-community.org

David Groep

Nikhef, PDP group

EnCo monthly update

Feb 28, 2020

EnCo – policy and best practice update

From our last (Prague) update meeting:

- SCI Security for Collaboration v2 and AARC Policy Development Kit > ‘Smplyfi’
- SCCC Communications Challenges Joint Working Group
- Assurance Profiles > ISGC paper
- Sirtfi
- Attribute Authority Operations (AARC-G048)
- FIM4R - Federated Identity Management for Research
- OpenID Federation for Research
- Outreach for policy work

Policy Development Kit / SCIv2 evolution

- New work is needed on the top-level policy (on which more later), since the version in the current Policy Development Kit (PDK) - when applied to a new infrastructure - depends too much on adopting the PDK as a whole.

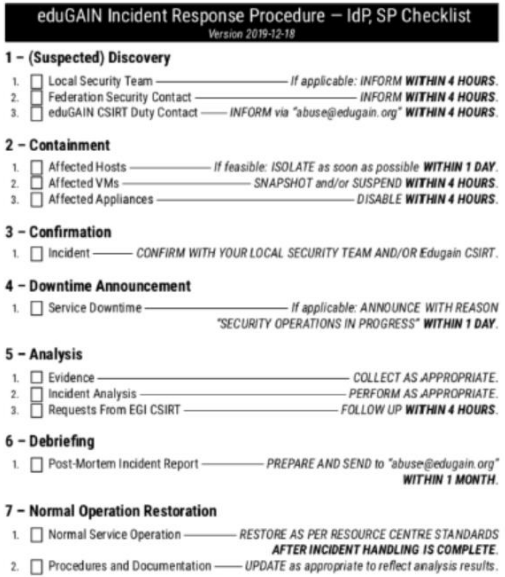
- Work on a new top-level policy that will contain directly applicable high level concepts, which is then supported by more specific implementation measures for specific target groups

Assurance Profiles - and RAF, SFA, and MFA

- “Signalling the capability for RAF profiles as well as SFA and MFA for (a non-negligable number of) entities in an IdP, or the need for having this for SPs, is an open question”
- introducing new entity categories is a challenge – and the REFEDS survey is for now inclonclusive
- it was also proposed at the TIIME meeting as a topic – similarly inconclusive …
- Jim Basney has also developed an assessment spreadsheet for REFEDS RAF, MFA and SFA, and both XSEDE as well as FNAL (Fermilab) have been assessed against this. It makes TAGPMA/IGTF in the US a good place to perform these peer-reviewed self-assessments
- assurance paper structure discussion next week

Sirtfi – towards concrete guidance for eduGAIN entities

- eduGAIN Security Team is now also involved in the Sirtfi working group
- aligning guidance from Sirtfi WG and the eduGAIN sec team (now good participation in Sirtfi from this side as well)
- communications remains a challenge – and what is the overlap in case of crisis exercises?
  There are several frameworks now available for probing
- Sirtfi is not the solution to everything – what about incidents on e.g. CMS platform that has a federated admin login for site management?
  Sirtfi gets you only those entities that are not affected anyway …



eduGAIN Incident Response Procedure – IdP, SP Checklist
Version 2019-12-18

1 – (Suspected) Discovery

1. ☐ Local Security Team — *If applicable: INFORM* ***WITHIN 4 HOURS.***
2. ☐ Federation Security Contact — *INFORM* ***WITHIN 4 HOURS.***
3. ☐ eduGAIN CSIRT Duty Contact — *INFORM via "abuse@edugain.org"* ***WITHIN 4 HOURS.***

2 – Containment

1. ☐ Affected Hosts — *If feasible: ISOLATE as soon as possible* ***WITHIN 1 DAY.***
2. ☐ Affected VMs — *SNAPSHOT and/or SUSPEND* ***WITHIN 4 HOURS.***
3. ☐ Affected Appliances — *DISABLE* ***WITHIN 4 HOURS.***

3 – Confirmation

1. ☐ Incident — *CONFIRM WITH YOUR LOCAL SECURITY TEAM AND/OR Edugain CSIRT.*

4 – Downtime Announcement

1. ☐ Service Downtime — *If applicable: ANNOUNCE WITH REASON "SECURITY OPERATIONS IN PROGRESS"* ***WITHIN 1 DAY.***

5 – Analysis

1. ☐ Evidence — *COLLECT AS APPROPRIATE.*
2. ☐ Incident Analysis — *PERFORM AS APPROPRIATE.*
3. ☐ Requests From EGI CSIRT — *FOLLOW UP* ***WITHIN 4 HOURS.***

6 – Debriefing

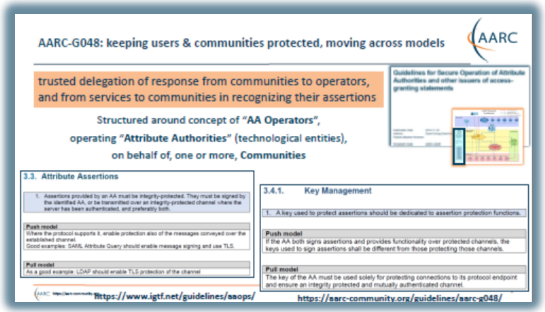
1. ☐ Post-Mortem Incident Report — *PREPARE AND SEND to "abuse@edugain.org"* ***WITHIN 1 MONTH.***

7 – Normal Operation Restoration

1. ☐ Normal Service Operation — *RESTORE AS PER RESOURCE CENTRE STANDARDS* ***AFTER INCIDENT HANDLING IS COMPLETE.***
2. ☐ Procedures and Documentation — *UPDATE as appropriate to reflect analysis results.*

Attribute Authority Operations (AARC-G048)

- presented to AEGIS as a means to get exposure and feedback on the guidelines
- https://www.nikhef.nl/~davidg/presentations/AARC-G048-AEGIS-202002010.pdf
- emphasise that is can be used in virtualised environments – and that one can rent HSMs in AWS …
- AEGIS members promised to come back to see if they can evaluate and if needed help improve guidance
- The final version will come later for endorsement



FIM4R – see the 15th FIM4R blog

- https://indico.cern.ch/event/871628/
- with EnCo and AEGIS overviews
- review/reflection paper planned involving all communities
- on a short (few weeks) time scale

OIDC fed for research RP collections

- There is now an IGTF prototype OIDC federation service (formally: the meta-data signing service or MDSS), which for the time is a signed blob (signing by file-based key or HSM) but without entities in it.
- The application of this is discussed in the session on OAuth2 federation for WLCG and others.

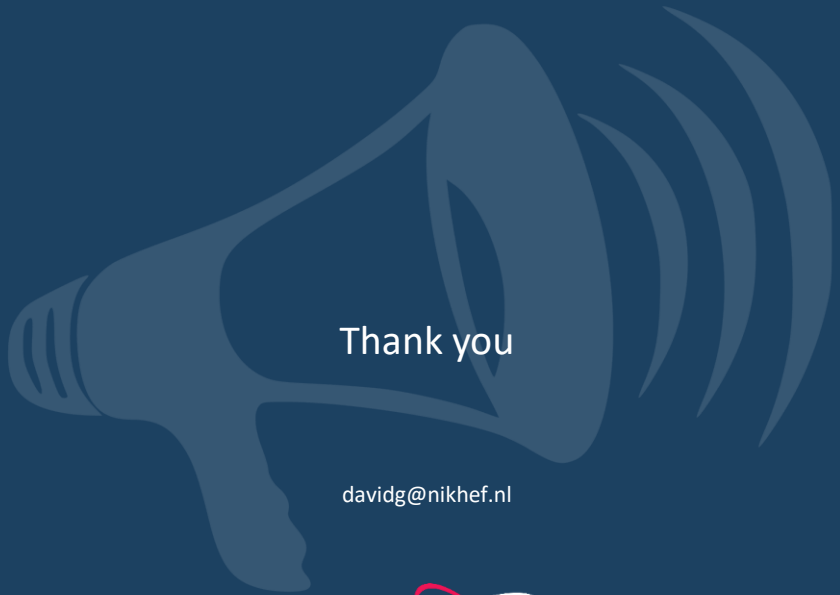
- https://oidcfed.igtf.net/.well-known/openid-federation
- https://github.com/rohe/oidcfederation
- https://www.axini.com/files/2019_jouke_roorda.pdf

Other activities that are ticking along fine

- SCCC JWG – prepare for an update at the SIGISM/WISE workshop in April 21-23 (JISC, London)

Planning for the next months!

…



Thank you

davidg@nikhef.nl

GÉANT

Networks · Services · People

www.geant.org

This work is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).