AARC TREE & EnCo policy coordination call Monday April 15 2024

Present: MaartenK, CasperD, ArnoutT, DavidG, JensJ, SlavekL, MarcusH, NicolasL, DianaG, ValeriaA
Apologies: DaveK

Resulting actions

- Finding a better suitable recurring timeslot ?
- Maarten: draft the venn diagram on the EnCo vs AARC TREE main activities
- initiate trust and tracability working parties (CT-like append-only logging by proxies: Jens; TTX exercise models: DavidG & Maarten)

AARC Policy: Introduction to the monthly meetings

Resolve clash with Arch and REFEDS calls.
REFEDS call starting at 1600L, and AARC Arch terminates at 15.30L.
Or start the ARCH call 30 min earlier once a month?
This will be discussed (for the >= June meetings) on Signal, to avoid the overlap with the Architecture call

SKA AAI

EnCo support for the communities, which is available with IanC in GN5 EnCo, and maybe use that for the *generic* aspects of SKA and bring back the lessons learnt to AARC. That would be nice, *as long as no specific SKA work is funded* (that must be in SKA, obviously). This may materialise in conjunction with the Canadians (whose work is slightly orthogonal to other efforts, though they’d have to align as well at some point), and there is the discussion for “SRCNET 0.1”. As we understood from IanC’s trip to China, the initial aim was to have four countries joining SRCNET 0.1, but ended up with seven since everyone wanted to be in and get resources. The UK is the largest of these, and .cn is included, as well as .nl (there is funding from FuSE for that via John Swinbank). Arnout and Raymond from SURF have been asked to provide input for the user stories prioritisation for the SKA AAI.
The aim of the AAI in SRCNET 0.1 is to connect users across countries in a simple way with a single attribute authority for a ‘global profile’. We could help .cn, but maybe start with a more friendly

timezone to make collaboration easier. Maybe NL? But then for the downstream use of the attributes (with Mischa, Marcus, Jens, &c). Sequency diagrams are thus needed for 'how to consume' the attributes.
There will be a SINGLE attribute authority for SRCNET and SKA! Yeah.
Each country will look a bit like a *sub-community in* the common community AAI, and maybe run an infra proxy as well. The SKAO will run a single AA for all these community AAIs (see picture on confluence.skatelescope.org (http://confluence.skatelescope.org)).

From the architecture call ...

Identifier may issued by an authority that issues for multiple communities. That needs to disentangle for which authority the ISS will be used. So there is needs additional scoping of the memberships?
This is coming currently out of the architecture call "community user attributes" (->G056)
There is also a NIST document (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.32.ipd.pdf (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.32.ipd.pdf)) about community attributes. Make it easier to detect if something is amiss.

EnCo and FIM4R coordination and joint meeting

There should be no overlap betwene GN5-1 WP5 EnCo and AARC (both not during GN5-1 and during GN5-2). There is no double funding by construction, but where can we use effort most effectively to complement AARC.
It should be separable between EnCo and AARC TREE. Keep your organisations timesheet model in case of audits (which should prevent double counting anyway).

Any EnCo relevant work not in AARC TREE? Most of it is inside, so we use EnCo to provide further support for OpenID Connect Federation deployment and practical work. And Maarten will create a Venn diagram in topics for the Abingdon meeting.

Questions for the WP3 survey?

Time schedule for a first draft set of questions we would like to get feed-back on, and how to get the input we need?

There are no draft survey questions yet, only a discussion on to which communities WP3 is connected and where the input might be connected. Maarten will poke Marina and Janos.
MarioR set up a survey that included AARC AAI questions. "New AARC Communities Questionnaire" is now a google doc (cuirculated through aarc-use-cases@lists.geant.org (mailto:aarc-use-cases@lists.geant.org)):

- https://wiki.geant.org/display/AARC/WP3+Team+and+RI+represented (https://wiki.geant.org/display/AARC/WP3+Team+and+RI+represented)
- https://docs.google.com/document/d/1spr5QecowvAjklY2MXTpwob1y-R76SYuBPsnt6npWGU (https://docs.google.com/document/d/1spr5QecowvAjklY2MXTpwob1y-R76SYuBPsnt6npWGU)

Update G040 "T&C and privacy notices" based on community requirements

Especially useful for G040 update. Slavek will keep track of the discussion in WP3.

Operational trust and baseline questions

Does G071 give us enough info to trace users through the mesh of proxies, where you have

multiple proxies in the mix, and you might need to trust all the proxies that are somehow connected. You will need to know who issues the statement, but also that it was not altered somewhere inbetween.
You usually follow upstream, but does that work operationally?

- do we need exercises/ Sirtfiv1 exercise showed some may be accidentally left out, like SURF then
- in a perfect world, all data is available and people react fast, but do they?
-

This was also discussed in the architecture meeting... but there is also practice?
This maybe worse in case of capabilities that are not tied to specific communities but you only have the URN namespace. If you want any entity in the chain downstream to use these, the traceacbility to a community is lost. You need group info for that.

In theory you can limit acceptance capabilities from specific communities. But that could go aaginst the concept. If you are a community AAI and have a URN namespace, and you create group entitlements that are unique globally. Do you then accept those from outside? Probably should should (MUST) not. This is a URN namespace check. You can do that for group info, but this does *not* work for capabilities.

While this is recoded in the proxy that translated group->capabilities, but that is lost unless you convey the trail inside the entitlements. This in the arch was for tracerability purposes, not for authoritzation. This *was* mandatory, *now* it is optional (since they were pretty long).
In the new revision of the group entitlemernts specification, this is now optional (!), and adding a component in all those URNs makes it overly redundant in most cases.
If *all* entities in the chair record correctly (and share), the communication will work in case of an incident, but does that work?

- c.f. work in tracability of 3820 that Akos Frohner did
- RFC 6962 CT logging of these translations in an (external) registry. Would proxies want to do that? Encrypted?

See also: https://sharemd.nikhef.nl/jlglUMNQRTqdzVn9W6AasQ#From-the-architecture-call-... (https://sharemd.nikhef.nl/jlglUMNQRTqdzVn9W6AasQ#From-the-architecture-call-%E2%80%A6)

And we need to run some ‘fake’ exercises to check if any proposed policy is possible. This does not need a real proxy or software, just a TTX with a few people thinking they are a proxy ... inspired by the eduGAIN TTX from March '24.
This also implicitly validates (or not) elements of G071 ...

Set up smaller teams that come with (draft) proposals

- look at the use of RFC6962/CT “append-only” idea for this - Jens, DavidG,
- run (tabletop) exercises or a ‘live’ incident and trace an event, and also exercise G071 - scenario planning? Maarten, DavidG, Jens, (optionally Arnout, Marcus)

Outreach and promotion

Upcoming events and opportunities:

- Abingdon, May 29-30 on policy++ (https://www.eugridpma.org/meetings/2024-05/)
- TNC Rennes (https://tnc24.geant.org/) - whole AARC session

FIM4R: will come later (4 meetings can be supported). We need the people on board that are

being targeted (also) by WP3.

Make sure we also get other outreach that only in the T&I slots, so we reach a larger audience and not the usual gang. The issue is getting people interested for whom it is not a primary interest. Illaria/EGI have a great plan for that (which is in the proposal).

Events with AARC Policy presented in March and April 2024:

- International Symposium on Grids and Cloud ISGC 2024, Taipei, March 2024 (https://indico4.twgrid.org/event/33/contributions/1339/)
- GEANT Security Days, Prague, April 2024 (https://events.geant.org/event/1515/contributions/1776/)

Next meeting

- Next meeting on May 20th may not be the best. So push to **Tuesday May 21st at 1500 CEST** as a short coordination meeting.
- The next one will be the longer one in Abingdon the week after - register at https://www.eugridpma.org/meetings/2024-05/ (https://www.eugridpma.org/meetings/2024-05/). There *will* be remote attendance possible via Zoom.
- a permanent new Monday slot for June and beyond will be discussed on Signal