

AARC TREE & EnCo policy coordination call

Monday July 15 2024

Present: Arnout, Casper, Marcus, Nick, Diana, PeterB, DavidG,

Apologies: MaartenK,

- AARC TREE & EnCo policy coordination call Monday July 15 2024
 - Actions from the coordination calls
 - New action items as of July 15th
 - Ongoing items
 - Completed items
 - AARC-G081 Recommendations for Token Lifetimes
 - AARC-G082 Trust in Distributed Proxy Scenarios framing document
 - Evolution of G040
 - AARC Community Survey: input for questions and context
 - AARC Strategy
 - AOB

Actions from the coordination calls

New action items as of July 15th

Ongoing items

- What is missing today in G071? bounce to the AEGIS group for operational input: **Action by DavidG or DaveK**
 - token lifetime joined by Hannah and Tom Dack
- "lifetime of tokens" new guideline document (G081): **Action by MarcusH** (google-doc working area (<https://docs.google.com/document/d/1U9vvJfWuE8oO7u0FcGVGr3KySvBqwjnkzKO8TKzgoX4/edit>))
- Create (and write draft ToC of) the 'framing' document (Informational AARC-I* document) to describe the challenges before starting to write guidelines: **Action by DavidG** to start a shared document on sharemd/gdocs/overleaf – Now available as <https://docs.google.com/document/d/1tduCLBcc8UAqlqfqxjZp4zvAvvzKyFzy> (<https://docs.google.com/document/d/1tduCLBcc8UAqlqfqxjZp4zvAvvzKyFzy>)
- initiate trust and tracability working parties (CT-like append-only logging by proxies: **Action by Jens**
- TTX exercise models: **Action by DavidG & Maarten** (see also https://sharemd.nikhef.nl/s/_pNTbKy9f#Table-top-exercises-TTX-for-proxies-and-federations) (https://sharemd.nikhef.nl/s/_pNTbKy9f#Table-top-exercises-TTX-for-proxies-and-federations); there will be a TTX at EGI in Lecce and at TechEx/Boston)
 - At TechEx: MarcusH (considering...), DavidG, SvenG, MaartenK, PeterB,
- Collect any EOSC SMS onboarding documents for community input: **Action by Baptiste**
- Start with a ToC of the AARC documents: **Action by DavidG**
 - end of June/early July
 - Milestone early september
 - writing completion during the September 23+24 workshop /PMA62
- Actions based on AARC PDK Feedback:
 - capture stories from smaller communities
 - separate the PDK into policies and procedures as ancillary documents
 - look at the top-level policy to see if it recasts into foundational principles
 - split the policies (and procedures) by topic area
 - review and draft something by July (DaveK)
- token lifetime and revocation guidance: **Action by MarcusH**
 - MarcusH to set up a google doc (google-doc working area (<https://docs.google.com/document/d/1U9vvJfWuE8oO7u0FcGVGr3KySvBqwjnkzKO8TKzgoX4/edit>))
 - Document good practices what communities are currently doing. Via the

questionnaire in AARC TREE WP3 or ask that later.

- What do the communities have configured with the AAI providers?
- Do one-on-one interview with policy/security experts from the communities
- there are two more token types to consider: SSH keys and KRB TGTs

Completed items

- WP3 survey: survey is now final and questions being asked by Marina and Janos. Question for the community policy contact is in.

AARC-G081 Recommendations for Token Lifetimes

(MarcusH) – (google-doc working area (<https://docs.google.com/document/d/1U9vvjFWuE8oO7u0FcGVGr3KySvBqwjnkzKO8TKzgoX4/edit>))

- should still go (also) to the Applnt list.
- there are several types of token, some are revocable, some not, other are verifiable or off-line verifiable, &c
- focusses on Impact assessment in case they get stolen/compromised. The risk derives from the EGI Risk Assessment Team, even though these look primarily at software vulnerabilities. This has been translated to access and data risks. Using the low ... critical scale as has been used for software
- the it proceeds to describe the token types, including MyTokens (and VAULT tokens) that are aiming to be more secure than refresh tokens. These are compared to existing other types of keys (ssh keys, ssh certificates, Kerberos TGTs)

The section on 'existing guidance' is still lacking, but this should be about new guidance anyway. Section 6 has a flattened representation of the structure of tokens (based on an underlying spreadsheet). When matched to the impact of the access, this inspired appropriate choices. Things can be related back to X.509 as needed (and kill ssh keys).

The actual work will start now, in both Policy and Architecture. Iteration may start in Applnt, and then iterate to policy (and security) and - if needed - have dedicated joint meetings on an ad-hoc basis.

Request:

- contribute use cases to drive development: LS AAI, CoreAAI platform (Christos)

AARC-G082 Trust in Distributed Proxy Scenarios framing document

See document -

Evolution of G040

Similar framing doc for the T&C presentation?

The attribute profile (from the Arch WG) already has a multi-valued "Agreement to policies" (https://docs.google.com/document/d/1jO1X7GSXWf_R604j5LXinr37ZUf96YVdIXSvjpS_Vyk/edit#heading=h.6gx8etqyba0s) attribute to express acceptance of a policy (examples include T&Cs, privacy notices, and AUPs already accepted). Done in the LSAAI, SURF SRAM, ... and there is the WISE Baseline AUP.

Lead to be assigned ... DaveK? Usecases from Arnout and Peter.

"To more resources with Fewer Clicks"

AARC Community Survey: input for questions and context

Questionnaire (accessible to AARC TREE participants) is available at https://docs.google.com/spreadsheets/d/1NXj0T0u2JkC_-htaDE7_whVcgTcZKL8amB42NuqTYds (https://docs.google.com/spreadsheets/d/1NXj0T0u2JkC_-htaDE7_whVcgTcZKL8amB42NuqTYds)

Participants will be asked to provide a policy/security contact.

AARC Strategy

Submitted! Data Management Plan is next ...

AOB

- planning for FIM4R meetings: how to get the right people from the AARC community in, and what would we like to get out of it? Both for "us" and for the communities.
July 15th at 1600 CEST (and then first and third Monday of each month).
FIM4R at TechEx is on Sunday December 8th!
- Colocation of ~one day AARC with TIIME in Reading, UK (March 31st ... April 4th). Ian Collier organising.
- WP4 will start in August, and in the first month will review WP1 and WP2 to evolve the validators and pilots.
- next meeting should be on Aug 19th at 1500 CEST, chaired by DaveK (DavidG is still away).

Meeting closed at 15.50 CEST.