AARC Athens AHM meeting – NA3 session

David Groep

5th AHM Athens meeting
20-22 March 2017
Athens
Introduction and outline of NA3 in AARC and AARC2 (15’)

Hauling in the final AARC1 results
• DNA3.3: presentation of final document (15’)
• DNA3.4: scalable policy presentation and feedback (input to M24 document) (15’)

The highlights of 24 months of AARC (30’)
What do you think should be highlighted as a success for NA3?
• For NA3 people: which elements are you proud of having achieved?
• For non NA3 people: which elements did you find most useful in the NA3 output?

Towards AARC2 (15’)
• Structure and community engagement
• what elements should be prioritized from May this year?
Solving the Policy Puzzle

Pushing forward best practices and like policies across many participants

- “Levels of Assurance” – baseline and differentiated profiles, capabilities and grouping
- “Incident Response” – beyond Sirtfi: a common understanding on operational security
- “Sustainability, Guest IdPs, use models” – how can a service be offered in the long run?
- “Scalable policy negotiation” – helping SPs move beyond bilateral discussion
- “Protection of (accounting) data privacy” – necessary aggregation without breaking the law too much

Strategy

support and extend established and emergent groups (REFEDS, FIM4R, WISE, IGTF, …)
leverage their support base - and ‘multiply’ the effect of policy work from AARC
Specific definitive guidance to IdPs and federations

- **Uniqueness** at least ePUID or ePTID/NameID extra: ePPN non-reassigned or 1-year-hiatus
- **ID proofing**: ‘local enterprise’, ‘assumed’ (Kantara LoA2, IGTF BIRCH, eIDAS low), or ‘verified’ (LoA3, eIDAS substantial)
- **Authenticator**: follow REFEDS MFA ‘good-entropy’ or ‘multi-factor’
- **Freshness**: ePA/ePSA reflect departure within 30 days

All: organisational-level authority, also used locally for ‘real work’, good security practices

Logical grouping and profiles for the Infrastructures

<table>
<thead>
<tr>
<th>Value</th>
<th>Cappuccino</th>
<th>Espresso</th>
</tr>
</thead>
<tbody>
<tr>
<td>$PREFIX$/ID/unique</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>$PREFIX$/ID/no-eppn-reassign</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$PREFIX$/ID/eppn-reassign-1yr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$PREFIX$/IAP/local-enterprise</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>$PREFIX$/IAP/assumed</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>$PREFIX$/IAP/verified</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>$PREFIX$/AAP/good-entropy</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>$PREFIX$/AAP/multi-factor</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>$PREFIX$/ATP/ePA-1m</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

... and simplicity for all

https://docs.google.com/document/d/1HHbXG48WippMEAVnPybZngEyTyl6l0Hh84Arr-l2MW8/pub
Security Operational Procedures

‘A Very Timely Activity’

Incident response capabilities at IdPs and SPs: Sirtfi v1 brings these to light

Beyond v1: establish proper channels, expectations, and the operational capability

Establish ‘homogeneous’ Incident Response Procedure

• with central operational capability
• and information sharing

Mar 17th 137 IdPs (+23) that support Sirtfi

Recommendations for research and e-infrastructures to build sustainable services

Sustainability model template
• With concrete examples from SA1 pilots

Recommendations to
• Infrastructures to adopt standard practices
• Federation ops to align approaches – keeping in mind the FIM4R requirements

We got ourselves +2 months (now just 1 week left ...)
David Hübner and Peter Gietz will present it 😊
Developing scalable policy models in light of the Blueprint: Snctfi!

- Allow proxy operators to assert ‘trust marks’ based on known SP properties
- Develop framework recommendations for RIs for **coherent policy sets**

Evaluate with the SP-IdP-Proxies in pilots, based on the Blueprint (DNA3.4)

Many SPs are alike

*Policy frameworks for collective service providers
Shared use of and collaboration on reputation services, together in FIM4R*

David Kelsey will talk about Snctfi and DNA3.4 shortly!
• InfoShare on March 2\textsuperscript{nd}

• Guidance continues to evolve as the GDPR date comes closer

• \textbf{BCP-like} (\textit{not} BCP!) for communities that fit that model – ‘say what you do and do as you say’ – and keep the users always informed

• \textbf{New-style code of conduct} can also address the similar set of challenges, but depends strongly on the new GDPR (it cannot take effect before March 2018), may require some new hoops (and maybe even a body to take on liability!)

• and would benefit from minor tweaks to wording to explicitly put attribute authorities in scope
Work items with some dedicated time (once I stop talking ...)

• DNA3.3
  Recommendations for research and e-infrastructures to build sustainable services
  now at M23

• DNA3.4 & Snctfi
  Recommendations on the grouping of entities
  and their deployment mechanisms in scalable policy negotiation
  at M24
Review Highlights Survey

Survey https://goo.gl/5hYwP4

• 3 responses already beforehand
• this is an interactive session, so you will have to contribute 😊

Contribute Live at https://goo.gl/32OFRP
Some early input for the review

• Proud that we have generated discussion within a broad community of requirements for a interfederation incident response procedure. The AARC work can probably take some credit for inspiring the eduGAIN support platform. Proud of the work done trying to decrypt GDPR and make it understandable for our community, in the form of an adoptable policy. Proud of the efforts made to quantify LoA in line with existing research community practices. This way it should be useful straight out of the box.

• Data protection primarily. Snctfi and LoA are also very useful to see how we should work together.

• I really like Sirtfi for it's simplicity but still great usefulness. As a good second, I like the sustainability model for e.g. RCauth.eu, since sustainability is often missed in finite-time project-based development work, resulting in the loss of good products. The other work is very important too, but perhaps more difficult to show-case.

Contribute Live at https://goo.gl/32OFRP
Towards AARC2 ...

- Recommendations for the infrastructures
- How to ensure that AARC results are deployed
- What to push, highlight, or prioritize in AARC2 starting in May?
AARC2 Structure Refresher

NA1 – Project Management & Sustainability

NA2 – Training and Outreach
NA3 – Policy & Best Practice Harmonisation
JRA1 – Integrated AAI development
JSA1 – Use Cases, Pilots & AAI Integration Support

Research Communities Use Cases

Integration Use-cases

Delivery Platforms

Community Engagement
Competence Centre

Research Communities
Research/e-Infrastructures
objective 3 Deliver an integrated identity management infrastructure that responds to cybersecurity and community assurance requirements

Collaboration with Infrastructures

• Training and outreach
• Incident Response
• Levels of Assurance (LoAs) – read Assurance Profiles
• Deployment of results

International Liaisons (again, many on policy)

• REFEDS
• FIM4R (RDA)
• IGTF
• WISE
Policies in support of collaboration

Reflected in updated AARC2 structure

- Operational security capabilities and Incident response in federations – beyond Sirtfi v1
- **Service-centric policies**: traceability & accounting, privacy, gateway operations & proxies
- **e-Researcher-centric policies**: alignment of AUPs and templates, authentication assurance, community attribute management models and provisioning
- Policy Engagement and Coordination: contributes to Community Engagement, provision of policy expertise to the Competence Centre, promotion of best practices globally (WISE, FIM4R, IGTF, REFEDS), easing *end-to-end coordination* across the chain
- Structuring the *exchange of information* amongst SP groups
In AARC, NA3 has fewer explicit partners – yet we need all of you!

In work programme only: BBMRI-ERIC (CSC), CERN, EMBL, FZJ (PRACE), Nikhef, RAL

• Define a reference framework to enable different parties to compare policies and assess compatibility as needed. [SCI-V3, convergence of Snctfi & Sirtfi - RAL]

• Create (baseline) policy requirements, driven by research to engage with a large number of compliant stakeholders without the need for mapping. [...] Permits scalability in negotiating agreements [through] the Competence Centre. ['researcher-centric’ policies, baseline AUP, Assurance Profile for BMS, frameworks for attribute management and provisioning - RAL]

• Identify all necessary policy elements and develop guidelines and assessment models to support communities in establishing, adopting, or evolving their own policies – covered by the topic-based work on operational security, service-centric policies, and community-centric policies. [ensemble of ‘service-centric’ policies, think Accounting, GDPR, Attribute authority mngt, evolution of Snctfi, IdP-SP-Proxies - KIT]

• Operational Security and Incident Response [move beyond re-active communications - RAL] 

http://aarc-project.eu
After the last month of AARC …

**Recommendations and policy** templates & guidance

- Which recommendations do we push most urgently?
- To which infrastructures beyond the ‘usual’ ones (ELIXIR, EGI, EUDAT, EOSC-HUB, PRACE)?
- How do we reach those in AARC2 not yet involved in AARC1?

**The ‘90% we miss’** (from AARC2 and in FIM4R as well)

- should we recommend policy alongside the federation training?
- or get them ‘hooked’ first?

What are the **most urgent items** we should start working on in May?

Contribute Live at https://goo.gl/32OFRP
Thanks to all P&B collaborators from CSC, CERN, DAASI, RAL/STFC, KIT, GRNET, DFN, Renater, SURFsara, LIBER, and Nikhef, and to Jim Basney of NCSA, CTSC and CIlogon

Thank you
Any Questions?

davidg@nikhef.nl