Authentication and Authorisation for Research and Collaboration

Policy break-out session

AARC All Hands meeting Geneva
2016-11-30

Today's topic proposals …

Evolving Sirtfi – developing needed capabilities and associated processes

- Towards an effective response to a federated or inter-federated security incident
- Initial (strawmen) process recommendations for 3 participants classes
- How to evolve the process and get global adoption?
  (and what shall we put in the deliverable as definite, and which elements as a starting point)
- *Open space for comments …*

Assurance profile adoption – IdP capability and SP grouping alignment

- REFEDS Assurance Wireframe document evolution

Data Protection recommendations: how to spread the word?

- Reaching out to RIs that may save effort by reviewing the Recommendation: FIM4R, WISE?

DNA3.2 --

- How to deal with non-sirtfi entities and federations?
- We cannot base a procedure on participants with different frameworks, so it might be limited to sirtfi or those communities that have document and responsible processes.
- Response is an organisational capability – also for the services
- At what pace will the service provider conglomerates join Sirtfi?
- From the point of view of the RIs/eIs they need all their IdPs and federations to be in scope in order to be useful.
- A single global authority will not happen that can ‘enforce’ sirtfi – beyond close-knit communities
- A level of trust should go into the process in order to protect it from outside parties – there has to be a role of connecting or disconnecting participants to the process to retain integrity.
  Sirtfi could be an indicator of this connection.
- The roles and responsibilities are about agreements, not the specific technical metadata tags
- What is being developed now is the specification of what we expect in terms of capabilities – the document should make that clear that these are requirements and not a fixed normative template.
- This might be a case of rewording in case of the current doc, to clarify requirements – in the spirit of FIM4R (yet for the RIs guidelines might be useful as well as a template)

- With a companion template for those that don’t want to develop their own (akin to DNA3.5 appendix?)
- Do that in the SIrtfi working group in REFEDS to get wider participation

- This is the next step in the SIrtfi process, and the procedure here should be a strawman example, so that the Sirtfi WG can be the place to expose that and kickstart the discussion
- AARC bases the strawman on existing federations
- Express in terms “strawman” (best-practice is overused as a word, we need an equivalent en_UK word for a strawman)

- We can put stronger requirements on RIs services in the way they do incident response

- Federation ops are rther allergic to examples and templates – but can deal with requirements that leave space for them to do their own thing for implementing

- Add the roadmap process on how the document can be realised – mentioning the Sirtfi REFEDS WG process

- Take examples from the fedops space working with Heartbleed and shellshock – which did work fine, but just remained undocumented
  Add those as examples to the doc?
- There are also existing procedures in some federations – and these will remain.

- The structure has to be OK before publication, and we can defer a bit to get the wording right here. But otherwise that will be a snapshot.
- And it will be a input to the workplan for the eScience support desk in GN4

- Research services procedures for incident response should go to FIM4R together with AARC
- This will be a starting point also for Snctfi
- Some federations today got pushback from SPs who think even Sirtfi v1 is too complex

- Management of assessment information and tags can also be outside the federation-ops provided information
- The RIs together can do their own tagging afterwards also on the entities, and o rpeputation based services
- The SP/RI have their own independent requirements and the exchange of intel within that group will happen, including filtering, but this is not in scope for this doc.
  Yet is will just happen anyway, and likeminded SPs can and will share that intel.

- Procedures here should be complementary to existing operational security practices within federations. They complement and augment current procedures.

Assurance WG Wireframe

- The wireframe doc draft is there now – comments open by suggestion https://docs.google.com/document/d/15v65wJvRwTSQKViep_gGuEvxLl3UJbaOX5o9eLtsyBI/edit
- The component element goes to REFEDS consultation early 2017

- Collapsed component groups into a few profiles
- Naming should be opaque and non-sequential (e.g. names of fruits, like the IGTF model) since this is not a 'level' but a profile
- Initially based on self-assessment and using the self-assessment tool
- For the higher levels use peer-reviews

- OIDC mapping needs to be done …

- In attribute quality most are attributes of the IdP as a whole
- But e.g. email-verified can also be by-assertion or per-attribute? Per-attribute assurance does not fit the (SAML) conveyance model. The ePSA freshness quality is the first exception to this. EUDAT uses both ePSA and email that have been verified (and the rest not?)

- Additional assertions can be added to the set, and that can be done later – need not all be in this document just now. It then adds more rows to the component mapping for SAML as well.

- The mapping to the assurance profile scalar representations: if you add one component, will that add a specific new profile that is different from the current ones (minimal, higher, …)
- Every time you add a component value, the profile mapping needs to be reevaluated
- Yet the more detailed this becomes, the more pushback you get from IdPs
  (for EUDAT it's just the proxy, for distributed IdPs its more complex)

- Email may be 'free' in OIDC, but then it is also easily verified by the service

Accounting data protection dissemination (DNA3.5)

- Document ready, that is reflecting also GDPR. And the case appears pretty strong, not only for accounting but also anything in which there is a legitimate interest.
- Legitimate interest is open, as long as data is minimally used
- CoCo and BCR-inspired models are both an option, and exposing EGI as an example
- Legitimate interest is seen at the proper way also by AndrewC
  yet SURFnet lawyers are not reading the WP29 opinions, who also say Legitimate Interests are NOT a last resort
- And also David Foster (with a law degree) endorsed this model ;-)
- When asking an opinion, ask the right question to balance risk and business decisions
- There are AARC resources to including some real experts? And ‘our’ lawyer should give the good answer we want … so they should give the answer to the question “what is a diligent process to follow, given that we need to do what we need to do”.
- Then get the operators together to have them hear the opinion

06/2014

The WP29 recognises the significance and usefulness of the Article 7(f) criterion, which in the right circumstances and subject to adequate safeguards may help prevent over - reliance on other legal grounds. Article 7(f) should not be treated as ‘a last resort’ for rare or unexpected situations where other grounds for legitimate processing are deemed not to apply. However, it should not be automatically chosen, or its use unduly extended on the basis of a perception that it is less constraining than the other grounds.

A proper Article 7(f) assessment is not a straightforward balancing test consisting merely of weighing two easily quantifiable and comparable 'weights' against each other. Rather, the test requires full consideration of a number of factors, so as to ensure that the interests and fundamental rights of data subjects are duly taken into account. At the same time it is scalable which can vary from simple to complex and need not be unduly burdensome. Factors to consider when carrying out the balancing test …

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Thank you

Any Questions?

davidg@nikhef.nl

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).