REFEDS assurance vc 2017-01-23

REFEDS assurance wg vc

Monday 23th January 2017 at 14:30-15:30 (UTC), 15:30-16:30 (CET), 8:30-9:30 (CST)
connect.sunet.se/eduGAIN

Pål
David L
Tom
Maarten
David G
Mikael

Notes

Worked on the remaining open issues in the assurance profile:

1. Authentication assurance, concluding the discussion on the mailing list:
   
   1.1. Confirmed the consensus: use AuthenticationContext (not ePAssurance) for authentication assurance
   
   1.2. What are the possible request-response pairs?

   Confirmed that according to SAML2 core and SAML2int:
   
   - SP requests MFA, single, local or base-level (one or several in a preferred order)?
   - IdP responds MFA/single/local/base-level (SAML core permits exactly one in response)?
   - comparison="exact" (SAML2int: "SHOULD" and Eric has found supporting anything else is not realistic) i.e. the response MUST match one requested

   Other considerations
   
   - The SP indicates it supports this profile by requesting an Authentication context defined in this profile. There can also be other Authentication Context class references in the list presented by the SP.
   - Don't specify the IdP behaviour if the SP doesn't request anything (the default Shibboleth SP configuration) – it is out of scope for this profile
   - An IdP can downgrade the authentication i.e. carry out MFA but signal "single" in the response if "single" was requested. It is a responsibility of the IdP to make sure MFA is more reliable than single.

   1.3. Do we need "local-enterprise" or can we drop it and only have "Single" (Pål: AL2 is not that hard)

   Decided to drop "local-enterprise" to simplify the profile and to encourage IdPs to support the password entropy requirements defined in AL2.
   
   To make it explicit that the profile does not require full conformance to AL2 (including audits), use wording "materially equivalent to Kantara AL2".

   1.4. Do we need "base-level" to indicate "nothing"?

   - It would be good to have "base-level" Authentication Context that the SP can add to the end of its list if the SP is happy with "anything".
   - However, the "base-level" authentication context should be defined outside this profile so it can be applied universally.

   1.5. What are the names for "local-enterprise" and "single" (Tom: single->good-entropy)

   Mikael to integrate his proposal to the draft

2. Jim: " Drop the metadata entity attribute. I think REFEDS recommends against SP-side metadata filtering. Better to list all IdPs and handle errors. Also, metadata entity attributes introduce problematic federation operator responsibilities that will delay adoption."

   - The working group thinks having metadata entity attributes is useful to enable SP-side filtering.
   - The intention is that the entity attributes are assigned based on self-assessment (or peer-review) so no major impact assumed for federation operators' responsibilities

3. Nicole: Rename "4. Assurance Levels" to "4. Assurance Profiles" (to indicate they have no order)

   - adopted the proposal

4. Naming the levels

   - Foodle poll (https://foodl.org/foodle/Refeds-assurance-profile-name-58716) results:
     - Espresso (11 votes)
     - Cappuchino and Mocha (7 votes)
   - Mikael will integrate his proposal to the next draft

5. Developing the SAML2 Entity attribute profiles
deferred for now

6. Next steps

- Mikael to update the assurance profile draft in the next few days. Then expose it to the assurance working group for final review before the public consultation.
- next vc Monday 6th Feb 2017 at 14:30-15:30 (UTC), 15:30-16:30 (CET), 8:30-9:30 (CST), with the intention to trigger the public review.