REFEDS assurance vc 2017-01-09

REFEDS assurance wg vc

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

Pål A
David L
David G
Tom B
Paul C
Mikael L

Notes

1. Key feedback from inCommon assurance call on 4 Jan

- clarify what is supposed to apply to “this account” and what to the whole CSP.
  - Added a sentence to beginning of section 2
- some research collaborations do identity vetting themselves (i.e. record the researchers' identifiers using their own channels). A new fruit with no ID proofing requirements?
  - cross-check that fruits can be multi-valued
  - find out the need in the public consultation
  - not too many fruits or it will get complicated
- what are the implications for federation operators?
  - to be written in the entity attribute profile
  - concerns on workload for fedops for organising the peer reviews

2. REFEDS MFA consultation status

- draft by Nicole: https://docs.google.com/document/d/1j-lb7-maES-Xe95EAVBBwamhQUo1vmgt-WGupEYQHZo/edit?usp=sharing
- please have a look at the e-mail sent by Nicole to the list earlier today

3. Major modifications to the Assurance profile since last vc:

3.1. based on the discussion on the mailing list 8-9 Dec, dropped the attribute assurance section from the profile (except ePSA freshness)

3.2. adopted terms from ITU-T X.1254: credential issuance (was: delivery), credential replacement (was: renewal)

3.3. moved the 5th component (baseline expectations for IdPs) to section 3 (conformance criteria), as Jim and Ian proposed it would clarify the approach.

3.4. on SAML2, dropped the use of AuthenticationContexts. Instead deliver Authentication Assurance using eduPersonAssurance like the other values. Added a footnote that an RP can ask MFA in AuthenticationRequest’s Authentication context as defined in REFEDS MFA profile.

- this modified approach is difficult for IdP configuration -- easier for an IdP admin to get the authncontext right than to mount the value on the fly to ePAssurance.
- Pål to formulate an e-mail on the alternatives and send it to the mailing list for better understanding of the two alternatives and their pros /cons

4. Main comments/proposals from Ian, Jim et al for discussion:

4.5. Banana and Mango. Ian: "hard to take seriously". Nicole's poll: coffees are leading.

- Go for coffees.

4.6. what to do with ePTID? ("ePTID is a legacy thing and therefore probably should not be put into any new specifications.").

- Add an"ePTID is discouraged" footnote

4.7. do we want to expect REFEDS to regularly re-evaluate password entropy requirements: ("their entropy must meet the requirements set by AL2_CM_CRN#040, unless REFEDS has agreed on a higher requirement.").

- drop the requirement to REFEDS re-evaluating password entropy

4.8. ePA freshness requirement imposed just on ePSA or for all ePA, ePSA and ePPA?

- Make ePA requirement to apply to both ePSA and ePA byt not ePPA.

4.9. Jim: "Drop SAML2 metadata entity attributes, too complicated for IdPs and introduces problems for federation operator responsibilities".

- no time to discuss this one.

4.10. Nicole: Rename Level to Profile (to indicate they have no order).

  - no time to discuss this one.

5. Next steps

- Ian volunteered to have another look at the profile

6. next vc: Monday 23th January 2017 at 14:30-15:30 (UTC), 15:30-16:30 (CET), 8:30-9:30 (CST)?