REFEDS assurance vc 2017-09-11

REFEDS Assurance wg call

11 Sep 2017 at 15:30-17:00 CEST/8:30-10:00 CDT
Adobe Connect: http://connect.sunet.se/eduGAIN
Jule Z
Michael S
Mikael L
Nicolas L
Pål A
Tom B
Chris W

Notes

- link to the Assurance Framework consultation comments doc: https://docs.google.com/document/d/1_30AeM1zUySTcRmfva66y2WVfKDkroEzPQg1k-vDpMY/edit

- status of Good-entropy single-factor profile (Michael, Jule):

- draft: https://docs.google.com/document/d/1HOcM2o4N7Ly9elRd5OQH2dCmfjY83WBv7ZCPgFysNmE/edit?usp=sharing
- RAF comment #22: Will Good-entropy profile cover non-password authentication?
- RAF comment #15: will MFA satisfy good single factor, making Espresso>Cappuccino?
- Current draft proposes to rely on 800-63b because it is more concrete and specific than Kantara SAC
- Q: Will 800-63b section 4 be used to identify those items in section 5 that are applied. A: No, instead every SHALL requirement in section 5 would be applied
- Q: Does this profile now match our expectations on what the good-single-factor means?
- Q: Are the requirements on passwords clear enough? In Sweden the federation operator has gone even further and defined template policies/Best Current Practices for CSPs
- Q: What is "approved encryption" (section 5)? When you follow the references you may learn it e.g. refers to US federal government criteria/FIPS. We need to understand/clarify "a reasonable interpretation". E.g. can a normal AD serve as an authentication backend (AD is a good expectation level)
- Summary: 63b is a good idea to use as a reference, but requires some BCP/reference implementations to document/demonstrate how to match the criteria.
- next steps: clarify SHALL/SHOULD items. Next draft in the next call

- follow-up on other comments in the C category

- #3 “email-consonance”: will we include this to RAF?

    - No, we'll just add explanatory text like don't mix the identifiers that are there for different purpose

- #9 baseline expectations: "trusted enough to access organizational systems" Add "financial or student administration systems"?
    - not all CSPs are universities.
    - Clarify the section that triggered Lalla's comment that the CSP does not actually need to be used. perhaps add extra sentence below e.g. can=>could

- #7-8 federation operators role and SAML2 entity attributes. (Tom/24 Aug: central registry for RAF compliance, c.f. Sirtfi)
    - Let's not put RAF on hold until the central registry for RAF compliance materialises
    - Instead, in ver 1.0 don't introduce SAML2 metadata elements at all. Instead do all signaling runtime in the SAML assertions. This means we need to accept that we cannot instrument the adoption rate
    - In ver 2.0 introduce the saml2 metadata elements and an alternative central registry for them

- other comments

- Pål (3 Sep): drop Authentication component completely from RAF
    - Nicolas: can be done for SimpleSAMLphp with an extra module.
    - Can be problematic for Shibboleth IdP
    - Keep authenticaton part of RAF but don't expect runtime calculation of coffee drinks and their population as an attribute assertion/claim in an IdP?
    - Pål: to write e-mail to list to explain the alternatives on the table and their limitations

- next meeting: 25 Sep at the same time, then start a bi-weekly call cycle

---

The remaining issues were postponed to the next call:

- EGI (28 Aug): "local-enterprise" vague/difficult for e-infrastructures (who have typically no "HR /financial" SPs)

- address comments in the P category

- I have preliminarily gone through them and proposed text
- Is NISO ESPRESSO report a reason to change the coffee drink name? https://discovery.refeds.org /guide/