REFEDS assurance vc 2017-09-25

REFEDS assurance working group call
Monday 25 Sep at 15:30-17:00 CEST/8:30-10:00 CDT
CERN's Vidyo portal: https://www.nikhef.nl/grid/video/?m=rawg

Michal S and Juli Z
Nicolas L
Chris W
Pål A
Tom B
Dave L
Mikael L

Notes

- link to the Assurance Framework consultation comments: 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
- Michael has analysed NIST 800-63B section 5: all SHALL requirements are OK and necessary
- no reference implementation profile to satisfy the SFA profile developed yet
- alternatively, there is now an alternative proposal 2: "do what you think is appropriate and document it" (or use 63b)
- to avoid further references to other federal standards, the profile now describes the approved encryption methods explicitly
- Pål: Make sure Windows AD can satisfy the profile
- Tom: SFA needs to be widely applicable to be adopted. What is good enough for Home Organisations should should be good enough for RPs.
- It is difficult to demonstrate that there is no alternative less secure way to bypass the authentication
- Can we roll out a process that HOs would use to demonstrate SFA compliance? The process needed to be managed by federation operators
- What would be state of the art? It would change over time.
- At least the ordering of the bullets in the list needs to be changed so that 63b is the first. The first item in the list is an important hint of expected level
- Are the three proposed alternative bullets now balanced?
- How much does the profile span to the policy side of thigs. For instance, is the way password reset is done in or out of the SFA scope?
- it would be good to make an exercise to configure LDAP+Shibboleth IdP to qualify to the alternative 2
- Make the local security culture part of the profile? "Secure enough" may mean different things in different countries
- In the RAF the baseline expectations for IdPs covers already "good enough for local use", would that be enough? That appears to be too weak approach and wouldn't meet the expectations of the SFA
- As the conclusion, it was decided to revert back to Proposal 1 which uses 800-63b section 5 as the definition of SFA, supplemented by good practices for deploying compliant LDAP/AD authentication backends.

- discussion on the relation of RAF and Authentication profiles

- 3 alternatives described in: https://lists.refeds.org/sympa/arc/assurance/2017-09/msg00008.html
- adopt approach 2 where the coffee drink in ePAssurance indicates the capability of a given user to be authenticated according to a given authentication profile (e.g. MFA) and Authentication context indicates the actual authentication profile used.
- the reasoning for the choice is that certain IdP products cannot populate ePAssurance attribute on-the-fly based on the authentication context

- comments from e-infrastructures

- EGI (28 Aug): "local-enterprise" vague/difficult for e-infrastructures (who have typically no "HR/financial" SPs). Decided to keep local-enterprise value in the ID proofing component but drop it from the hierarchy of ID proofing

- address comments in the P category

- Is NISO ESPRESSO report a reason to change the coffee drink name? https://discovery.refeds.org/guide/
- No, let's call it REFEDS Espresso to avoit confusion.

- next steps

- send the resolutions to the people who provided the comments and to the REFEDS full list
- pilot: looking for volunteer IdPs and SPs (potential volunteers at least UChicago, EGI, EUDAT, ELIXIR)

- next meeting: 9 Oct at 15:30-17:00 CEST/8:30-10:00 CDT