REFEDS assurance vc 2018-06-25

REFEDS Assurance WG call to check the consultation comments
Monday 25th June at 15:30 CEST/8:30 CDT
CERN’s Vidyo: https://www.nikhef.nl/grid/video/?m=rawg

Pál
Sami
Tom
Alan
Michael
Jule
Mikael

Notes

1. REFEDS Assurance Framework

   • 10 comments received: https://wiki.refeds.org/x/qwHoAQ
   • comments added to the Google doc: https://docs.google.com/document/d/15v65wJvRwTSQKViep_gGuEvxLi3UJbaOX5o9eLtsyBl/edit
   • major comments
     ◦ #4: clarify “pairwise IDs recommended by REFEDS”
       ▪ decided to be forwards-leaning and adopt ePUID, subject-ID and pairwise ID for SAML and public/pairwise for OIDC
     ◦ #1: clarify “ePPN reassign” w.r.t. other properties of ID/unique
       ▪ to speed up adoption, keep the door open for eppn being the (only) unique id an IdP can provide
     ◦ #2, #8, #9: protests on references to external closed specs (like Kantara SAC)
       ▪ let’s find out if we can cite the relevant specs in the RAF appendix.
     ◦ #2, #8, #9: protests on references to external closed specs (like Kantara SAC)
       ▪ Tom to suggest a logic table that clarifies the CSP behaviour
     ◦ #2, #8, #9: protests on references to external closed specs (like Kantara SAC)
       ▪ Tom to check if Kantara allows us to cite SAC directly
     ◦ #2, #8, #9: protests on references to external closed specs (like Kantara SAC)
       ▪ Kantara SAC now known as Kantara Classic
   • minor comments
     ◦ #10: the commentator appears to have misunderstood the ePA-1m and ePA-1d concepts.
       ▪ Mikael to find out a wording that would be more clear on the difference on the business and IT decision
     ◦ #10: should we replace 30 days by 31 days so “one month” will qualify also for months with 31 days?
       ▪ Adopted
     ◦ #3: Sirtfi proposed for conformance criteria (in the 2017 consultation the WG already rejected this)
       ▪ Stick to the previous decision. Respect the orthogonality of RAF and Sirtfi
     ◦ #5: espresso missing from the example in Appendix B
       ▪ Adopted proposal
     ◦ #6: Appendix C has become irrelevant after dropping authN from RAF
       ▪ Adopted proposal
   • thanks to Ian Young for style/grammar corrections

2. SFA profile

   • received 4 comments: https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+SFA+Profile
   • https://docs.google.com/document/d/1ZjpzyYWZhqbiTclzxX9Vug9Whq99YeKk29e1FbJL5VM/edit#
   • #1: rephrase the introduction section to be more explicit on the intention w.r.t. NIST 800-63.
   • #4: changed bullet lists to numbered lists
   • #3: make the definitions more clear (including memorized secrets are supposed to be user selected)
   • #2: provide examplar

Next steps: Monday 2 July at 15:30 CEST/8:30 CDT