REFEDS assurance vc 2018-02-12

REFEDS Assurance wg call
Monday 12 February 2018 at 15:30 CET/8:30 CST
CERN's Vidyo portal: https://www.nikhef.nl/grid/video/?m=rawg

Matthew E
David L
Davide V
Alan B
Pål A
Tom B
Mikael L

Notes
- review of SFA document suite
  - SFA: https://docs.google.com/document/d/1HOcM2o4N7Ly9elRd5OQH2dCmftfY83WBv7ZCPgFysNmE/edit
    - document title: keep the name single-factor authentication and don’t replace single with secure. Prepare FAQ to describe how SFA is different from REFEDS MFA
    - section 1: use “Relying Party” and “Identity Provider” and provide explanation in parenthesis
    - section 3: consolidate the separate OIDC and SAML sentences into a single one.
    - section 5: no KBA at all (or set a sunset date for it)?
    - section 5: procedure to bypass authentication factor => procedure to reset authentication factor. Cross-check what NIST 800-63B states for this
    - section 5: many COTS products use 6 digit PINS. Update the section to reflect NIST 800-63B
  - memorized secrets: https://docs.google.com/document/d/1iUp9ls7FLlk1_xGHDLBsa1LuBxqFWTv4PyYr2cefl3A/edit
    - section 4: rename column “compliant use” and add more explanatory descriptions in the column
    - section 4.C1: maximum secret length. There may be products with relatively short maximum password length. Consider removing the minimum requirement on the upper bound for password length
    - section 4.C5: it may be difficult for sites to disable password quality checks. Make password complexity checks optional (i.e. allow them)?
    - section 4.C8: consolidate the three requirements into one
  - cover the remaining comments in the next call

- next call
  - a 90 min call Monday 26 February 2018 at 15:30 CET/8:30 CST