# REFEDS assurance vc 2018-03-12

REFEDS Assurance wg call
Monday 12 March 2018 at 14:30 CET/8:30 CDT (90 minutes)
CERN’s Vidyo portal: https://www.nikhef.nl/grid/video/?m=rawg
Jule Z
Matthew X
Michael S
Pål A
Tom B
Mikael L
Alan  B
Davide V
David L
Sami S

## Notes

- minor RAF updates for notice

- https://docs.google.com/document/d/15v65wJvRwTSQKViep_gGuEvxLl3UJbaOX5o9eLtsyBI/edit#
- added ePA-1d as an optional value based on a request from BBMRI research infrastructure
- Injected OIDC mounting to section 5.2 and appendix B. Credits to Mischa and Roland. Issues: REFEDS MFA and eduPerson not yet mounted on OIDC

- RAF open issues

- section 2.1: “The user identifier is eduPersonUniqueID or one of the pairwise identifiers recommended by REFEDS”.  Agreed to add “or OpenID Connect sub (type: public)”
- section 2.1: “The person and the credential they are assigned is traceable i.e. the CSP knows who they are and can contact them”.
    - AARC2 JRA1 has found traceability is not orthogonal with IAP component and proposes to drop or reformat traceability meaning "the CSP gathers sufficient logs to trace the transactions associated to a credential"
    - WG sees RAF should remain orthogonal to SIRTFI which covers the traceability/log issues
    - WG decision: ”CSP can contact the person to whom the account is issued”. For instance, the CSP can record the person’s e-mail address.
- section 2.3: RAF pilots propose authentication component ("CSP has capacity to do SFA or MFA for this user") is removed from RAF to avoid misunderstandings/false expectations
    - Agreed on proposed change
    - RAF should be complemented with a best practice that encourages to use e.g. Cappuccino + SFA or Espresso + MFA
- section 2.4&4: Can CSP assert Cappuccino if it does not assert any affiliation?
    - Yes it can (“all statements are true for an empty set”)

- review of SFA document  suite

- SFA: https://docs.google.com/document/d/1HOcM2o4N7Ly9elRd5OQH2dCmfjY83WBv7ZCPgFysNmE/edit
    - The WG decided to request REFEDS to describe the REFEDS consultation process. The description could be for instance the parent of REFEDS consultations page https://wiki.refeds.org/display/CON/Consultations+Home. Mikael will write to Nicole and cc the assurance list.
    - add sending a recovery OTP to the user’s address (of record) using an appropriate life time (e.g. OTP delivery by SMS – 10 min, e-mail – one day , postal mail – one month)
    - provide some content to the “recovery keys” – what does it mean in practice? (e.g. “Currently authenticated users can generate themselves recovery keys…”)
    - explain the last bullet ("replacing authenticator secret...") a bit more for better understanding
- memorized secrets: https://docs.google.com/document/d/1iUp9ls7FLlk1_xGHDLBsa1LuBxqFWTv4PyYr2cefI3A/edit
    - AD doesn’t meet C8 (secret hash functions) and C9 (salt length) and needed to use compensatory controls
    - the meeting discussed if the minimum requirements can impose something which cannot be met with COTS products
    - Some of the R and C references in the document are out of date, cross-check

- next call: exceptionally on Friday 23 March at 14:30 CET/8:30 CDT