# REFEDS assurance vc 2018-02-26

REFEDS Assurance wg call
Monday 26 February 2018 at 15:30 CET/8:30 CST (90 minutes)
CERN's Vidyo portal: https://www.nikhef.nl/grid/video/?m=rawg

Tom B
David L
Pål A
Alan B
Mikael L, notes
Apologised: Michael S and Jule Z

## Notes

Review of SFA document suite

- SFA: https://docs.google.com/document/d/1HOcM2o4N7Ly9elRd5OQH2dCmfjY83WBv7ZCPgFysNmE/edit
  - Section 4: Discussion on "REFEDS approves or REFEDS publishes" the minimum requirements specs. The latter intends to indicate that there is no formal approval process. Mikael to send to the list a link on the process REFEDS has for approving documents.
  - Section 5: Proposal to add a separate fourth bullet point to cover explicitly the magic links sent by e-mail to the user's verified address of record (potentially after KBA)
- memorized secrets: https://docs.google.com/document/d/1iUp9ls7FLlk1_xGHDLBsa1LuBxqFWTv4PyYr2cefI3A/edit
  - Section 3: all components of the back-end IdM do not need to comply, only "the secrets and verification processes used by an Identity provider…"
  - Section 4: Password rotation and quality checks should not be banned. Either drop C5-C7 (i.e. be silent on them) or use the expression "need not be" (which would be a non-normative statement and make the table inconsistent). In all cases, provide explanation in FAQ.
  - C10: Proposed a less specific requirement: "do any form of mitigation of the risk of online guessing"
  - C11: Current deployments have issues with these requirements (e.g. SHA1 used)
  - C12: Proposed similar to C10: "do any form of mitigation of the risk of off-line cracking. " (downside: we don't give idea what is sufficient)
  - in general, the meeting appeared to think that the minimum requirements should provide several mitigation strategies for the IdPs to choose from
  - the AD recipe was found not to be consistent with the current minimum req (one way hash function, offline cracking).

Next call

- Monday 12 March 2018 at 14:30 CET/8:30 CDT (90 minutes)
- notice: the US has started the summer time; the meeting is one hour earlier for Europe