REFEDS assurance vc 2017-12-04

REFEDS Assurance wg call

Monday 4 December 2017 at 15:00 CET/8:00 CST (30 min earlier than usual due to an adjacent Sirtfi call)
CERN's Vidyo portal: https://www.nikhef.nl/grid/video/?m=rawg

David G
Jule
Michael
Nicole
Pål
Tom
Maarten
Mikael

Notes

- Single-factor authentication (SFA) profile and the related documents, Jule&Michael
  - There were concerns if the current approach is clear enough for the IdP admins – what documents needs to be read? Do OpenLDAP/AD deployers need to follow NIST 63b as well?
  - It was proposed to clarify the order of the docs:
    - If you have an AD/OpenLDAP deployment you need to follow the associated minimal requirements only
    - If you have some other product you'll have some harder work ahead to read 63b but you can help us to develop a minimal requirements for your product
  - 63b section 8 on security threats has criteria that are not and cannot be done in the minimal practice docs (e.g. educating users against phishing) so the CSPs need to have other controls
  - what if someone uses a product whose configuration is similar to OpenLDAP but is not openLDAP. Find a wording that allows the minimal requirements to be applied to products with similar configuration ("or equivalent").
  - how the rate limiting is addressed when there is actually a pool of LDAP servers? Clarify in the document (the pool is per server)

- discussions on the mailing list
  - introduce a new "good-entropy MFA"?
    - ACAMP discussion demonstrated that many CSPs in the US say they can hardly even meet the REFEDS MFA. Better to take small step first and defer "good-entropy MFA" to the future.
  - drop authentication component from Cappuccino and Espresso?
    - no conclusion on this

- next steps
  - public consultation for RAF, SFA, AD and OpenLDAP?
  - pilot?

- next call: 18th Dec at 15:30 CET/8:30 CST