REFEDS assurance vc 2017-11-20

REFEDS Assurance wg call
20 Nov 2017 15:30-16:50 CET

Jule & Michael
Alan
David G
Pål
Tom
Mikael

Notes

- SFA BCP for Active Directory
  
  Draft: https://docs.google.com/document/d/1VRIHWTWvB1CU0yqHzHnwDr_5FQ8oXEW1cENI90Fi8PD0/edit
  
  Is this really a Best Current Practice or rather a minimal requirements specification to meet the requirements of SFA? Many of the requirements are actually less than a best practice? Consider renaming (e.g. SFA baseline requirements)
  
  AD would be used as the verifier (i.e. the component that verifies passwords) so other applications relying on AD are out of scope
  
  Should the document cover also the authentication protocol to connect to the AD (the legacy protocols like NTLM that are these days deemed insecure)?
  
  “Passwords in transit must be protected by TLS” only when plaintext passwords are passed (normal Windows login works differently).
  
  strategy for managing the risk of compromised/blacklisted passwords? (e.g. password filtering)
  
  Remove the second table on guidelines (applications are out of scope for the document).
  
  generally the meeting was OK with the structure
  
  before the next call: update the document based on the feedback and create a similar document OpenLDAP.

- RAF open issues
  
  are SFA and MFA incremental?
    
    REFEDS MFA is mostly an interoperability profile with little qualitative requirements to the MFA but SFA has also qualitative requirements for the tokens (currently passwords)
    
    therefore SFA and MFA are not comparable and cannot be defined to be incremental
    
    this means also that Cappuccino and Espresso are not incremental
  
  floor value for ID vetting
    
    Pål suggests to have a new ID proofing value to indicate self-asserted ID with e-mail handshake and Captcha. The value would be useful for homeless IdPs
    
    the value would be weaker than verified and assumed in the hierarchy and table
    
    Pål will write a draft of the text
  
  extend ePA-1m to cover eduPersonPrimaryAffiliation as well
    
    ePPA added for consistency
  
  section 3 on conformance criteria: Federation metadata is accurate, complete and includes […] MDUI information? What MDUI information exactly?
    
    refined the criteria: at least one of the following contacts: admin, technical, support, security.
    
    No MDUI information requires for RAF as it serves usability whereas RAF focuses on assurance

- goal is still to expose all 4 documents to a public consultation together: RAF, SFA, BCP for AD and BCP for OpenLDAP

- next call: 4 Dec 15:00 CET (to avoid clash with Sirtfi call)