REFEDS assurance vc 2017-10-23

REFEDS Assurance WG Notes:

23 Oct 2017

- SFA Profile was reviewed by the group.
    - Public comment period intended to open in 2 weeks
    - Best practice document to be created that enables common LDAP and Active Directory configurations to be used with the profile since the NSIT reqs are ahead of currently deployed software. First document will focus on Active Directory settings.
        - Acknowledging that there's a huge gap between NSIT & common AD deployment configs
        - Request that the document identify the areas that AD falls short of the NIST requirements, which requirements, and why / how / "how far you're allowed to bend the rules" the NIST req is being "loosened". This will enable folks to use the Best Practice doc to justify compensation controls.
        - Before we bring this document to public comment, we need the Best Practice document to accompany it. – BP documents will be added over time to address various types of single factors (Certs, Bio, etc)
        - Maybe include line of thinking commentary to enable adopters to glean the spirit of the requirement as the author intended
    - Questions about retry limits in 800-63 – They were removed in latest 800-63, so not a concern. Tom: institutions coming to realization that retry limits are not really considered a good mitigation strategy for risk
    - Do we need OIDC/OAuth Bindings? Not right now – OIDC specifications are not yet complete. Eventually we will need it when OIDC is ready.
    - Defining "Acceptable Risk Level": Acceptability is a local concept. It's not something intended to be reviewed by 3rd parties. The problem with the vagueness is that technical people tend to have trouble implementing vague. AI: Wording will be adjusted to make it clear that this is something left to the org
    - Precluding weak KBA: The group agrees with the goal, but how do we compare apples to orange. Is there any set of questions good enough? How do we compare reset process to regular process? AI: reformulate the requirement in a more prescriptive way to enable some kind of KBA reset process and how that should work to be "secure enough".
        - We should try to achieve something between "don't do easy Q/As" and "must be as secure as the first factor"
    - Elimination of Active Directory: Handled by Best Practice Doc
    - BSI Recommendations: Intended to be used non-normatively. AI: Document needs to be updated to remove the non-normative statements and place them in an accompanying document providing implementation guidance.

- Other things related to assurance
    - GEANT assurance call raised a question: Talking about how to implement MFA Profile. Question regarding criteria for mitigating reassignment. What if SP wants to do 2FA as a service? IdP -> 3rd party MFA -> IdP -> SP. That's now 2 single-factors and not MFA. Clarification: the 3rd bullet does not say you must run everything on-prem. Does this process defend against a user's account getting phished? If yes, then you meet the standard. So yes, "step-up" is allowed. If the service (SP) does the 2nd factor, then the service (SP) cannot assert MFA as the additional factor was done just for the service. Bottom line: keep your eyes on the risk-mitigation

- Remaining comments on assurance framework
    - "Generally accepted security policies" statement is vague & hard to measure – 3rd paragraph on normative assertions in SIRTFI document has good language addressing this.

- Next Steps
    - Should we publish a new draft of RAF & SFA together? RAF references SFA and so they should go together. If we're expecting a lot of comments on SFA then we should do consult now, else we should wait. If we write some sentences about what SFA covers, then we can do RAF Consult now.
    - Planning a pilot on RAF and SFA – There are plans in GEANT to do it, but nothing firm. Chicago is also interested once things are nailed down.