September 13, 2013

AD-Assurance Notes from September 13

Michael Brogan, U Washington
Jeff Capehart, UFL
Eric Goodman, UCOP
Mark Rank, UCSF
Ron Thielen, U Chicago
David Walker, Internet2/InCommon

Next Call

September 20 at Noon ET
+1-734-615-7474 PREFERRED
+1-866-411-0013

0195240#

Agenda:

Discussion of AAC feedback on our IAP interpretations. (See David Walker's mail of 9/12/2013.)

Notes

- **Action Item (for everyone):** Review the 2013 Cookbook, our questions for Microsoft, and the parking lot issues (child page to the Cookbook) in light of the reinterpretation of 4.2.5.2 for discussion on 9/20. Add your thoughts to the parking lot issues page.
- Overall, the feedback was good. The AAC accepted all of our interpretations but one (4.2.5.2), and their reinterpretation makes our job easier.
- Regarding SPNEGO, we will describe it as a method for using Windows workstation authentication as the IdP's authentication event. We will also suggest that compliance is less complex if SPNEGO is not used for IdP authentication, as SPNEGO introduces multiple authentication protocols that must be assessed and mitigated.
- We are focused on Silver compliance for AD with minimal modification to the AD environment (so, using passwords). We should state this early on in the cookbook; we can also indicate that other strategies like using MFA, rather than AD authentication methods, may have advantages but is outside the scope of our Cookbook.
- We reviewed and revised IAP Requirements and Gaps for Active Directory Domain Services (AD-DS) in light of the reinterpretation of 4.2.5.2. The changes we made can be seen here.