March 8, 2013

AD-Assurance Notes from March 8

Eric Goodman, UCOP

Mark Rank, UCSF

David Walker, InCommon/Internet2

Etan Weintraub, Johns Hopkins

Michael Brogan, UWash

Jeff Capehart, UFL

Ron Thielen, UChicago

Lee Amenya, UCSD

James Oulman, UFL

Brian Arkills, UWash

Ann West, InCommon/Internet2

Next Call

March 15 at Noon ET

+1-734-615-7474 PREFERRED

+1-866-411-0013

0195240#

Action Items

Ann will invite Chris Irwin from MS to join the group

Ann will work with Debbie Bucci (NIH) to set up calls with Federal Agencies that have certified IdPs.

Michael will add a scope statement to the Charter Page.

Etan will pursue developing approach for Office365 and Bronze/Silver compliance.

Michael and Eric will develop a draft table in the wiki that summarizes the profile requirements, relevant AD behaviors and gaps.

Ron will send a draft of log checking as compensating control.

Ann will set up a standing weekly call.

Notes

Notes from 3/8 were approved

Action item Update

- Ann to contact Brian re: MS AD Expert – DONE - Ann and Brian requested expert involvement from MS to help with the specifics of what AD does and doesn't do. Result is that [AI] Ann will invite Chris Irwin, MS HE Identity contact, to join us and he will bring in Dean Wells, AD PM, (or his designee) once we have scoped questions.
- Brian to send out background resources - DONE
- David to send out information on FIPS and NIST-approved algorithms - DONE
- Brian to send out AD components and thoughts about how they map to what's in scope for the profiles. - DONE

Federal Agencies that have Certified IdPs

Debbie Bucci from NIH has identified a team at NASA that has a certified IdPs. She has offered to set up a call with them. Jeff C mentioned that they may be using two-factor which is not in scope for us. The group would still like to interview the team and gather information.. Instead of including them on a group call, [AI] Ann will set up a side call with Brian, David, Eric, Lee and any agency team we identify. We'll then produce a summary for the larger group to review.

Scoping

[AI] - Michael will add a scope draft to the Charter wiki page.

The Cookbook was developed to address 1.1 and minimally has to be brought up to comply with 1.2.

What AD products should we consider in scope under the Framework:

- AD-DS is in scope
- AD-FS possibly in scope. Must support the Federal SAML2 Profile for ADFS. Touches passwords too.
- Office365 – Out of scope for the group since it's an application, but [AI] Etan will pursue developing recommendations for general use that could be added to the Cookbook recommendations.
- Azure AD (or cloud-based AD) would be considered part of your IdM, but you have the option of storing passwords there or not. One can also host AD in an Azure VM, and it would be the same as hosting your IdM systems in the cloud elsewhere. There are many ways to host your authn, attribute, and directory services and the Azure use cases seem to be more edge than germane cases. Probably out of scope.

Work Plan Moving Forward

[AI] Michael and Eric will draft a wiki table including the relevant profile sections and intent, AD behavior/configuration one could use to clear the bar, and gaps. The goal is to highlight what we do and don't know and develop questions for MS to ensure accuracy of the final product. Once the gaps are verified, we'll then determine if there Alternative Means (AM) that can be used to satisfy the criteria. For instance, one could set up an audit process to ensure credentials are still valid: checking the log could be a compensating control. [AI] Ron will send an example of this approach. We also may identify more than one AM; more than one could be proposed.

Call Schedule

[AI] Ann will set up a standing weekly call. The group would like to meet weekly to keep momentum going and hit the end of April deadline.