Minutes of Assurance Call of 8-May-2013

Draft Minutes: Assurance Implementers Call of 8-May-2013

Attending

Ann West, Internet2
Michael Hodges, University of Hawaii
Oleg Chaikovsky, Aegis Identity Software
Chris Spadanuda, UW-Milwaukee
Jacob Farmer, Indiana University/AAC
Susan Neitsch, Texas A&M
David Walker, Independent
Benn Oshrin, Internet2
Tom Scavo, Internet2

==========
Assurance Wiki: https://spaces.at.internet2.edu/display/InCAssurance/InCommon+Assurance+Program
==========

DISCUSSION

UPDATES

RFP for Shibboleth IDP enhancements

The RFP for Shibboleth IDP enhancements to provide plug-in to support for assurance and MFA is available at https://spaces.at.internet2.edu/display/InCAssurance/InCommon+Assurance+Program#InCommonAssuranceProgram-RequestforProposal%3AShibbolethIdentityProviderEnhancements

Proposals are due by end of May.

AD Alternative Means Working Group

https://spaces.at.internet2.edu/display/InCAssurance/AD+Alternative+Means+-+2013

The AD Alternative Means Working Group has been meeting regularly and looking closely at the Assurance specs. They have an upcoming call with Microsoft's AD domain service product manager, and have developed a list of questions this call:https://spaces.at.internet2.edu/display/InCAssurance/Questions+for+Microsoft

The AD Alternative Means Working Group hopes to have a report ready this summer.

Password Entropy Tool

Shreya Kumar has continued her work on the Password Entropy Tool, that she showed on the 3-April-2013 call.
Shreya hopes to share the new version with this group the progress on an upcoming call.

Assurance Advisory Committee (AAC)

The AAC had productive discussions during its Face-to-Face meeting in Ann Arbor on May 2, 2013. One of the topics explored is how to fix the IdP POP.

Jacob (member of the AAC) solicited input on this idea of replacing the IdP POP with the Bronze assurance profile. Currently, there is a major challenge in enforcing the expectation that every IdP have an up-to-date POP. The fact that the POP is unstructured and isn't a practice set are seen as disadvantages.

Comments on idea of replacing the IdP POP with the Bronze assurance profile

Michael, Chris and Susan all stated that moving towards Bronze has value to their organizations. It would help with the prioritization of their local projects and increase the trust value across the federation.

Michael and Chris expressed concern about password entropy requirements. Imposing password lifetimes would be a big hurdle. Jacob noted that there are multiple ways to meet the password requirements of Bronze instead of imposing password lifetimes. Jacob said Indiana is looking at phased approach. Some users may not agree to change their password under the new policy, so Indiana University may have the policy that "if you have a password over two years old, we won't assert assurance for you." Benn said that institutions he works with are looking at putting focus on the number of failed authentication events that are allowed, where a high number would trigger a user needing to change the password. There is some infrastructure to be built around this. It was agreed that a further discussion on password entropy would be helpful.

Susan said Texas A&M is looking at getting Shibboleth to assert bronze for certain portion of the population, and also looking at some of the privacy requirements. She also mentioned that they also need to be able to distinguish Bronze users from other users in their IdM system.

Tom Scavo endorsed replacing POP the Bronze, noting the advantages of Bronze being more structured and easier to enforce, and the fact that compliance with Bronze can be verified in real time by incorporating it into a SAML flow.

Q: Is the POP for SP's also being looked at?
A: Only the POP for IDP's is in scope for this discussion. The POP for SP's is another important conversation to have at a later date.

Concerning timing, most on the call thought 18 months was okay but would rather have two years or more to allow for the transition from the IdP POP to Bronze. Jacob proposed that the timeframes be tied to InCommon pricing tiers with less time being given to the L1 schools (or big research institutions) and more time given as one progresses through the tiers.

Short Updates from Those on the Call

Michael: U. of Hawaii is looking at MFA and how to incorporate it into CAS. David: the Scalable Privacy Project may consider funding some CAS modifications to support MFA.https://spaces.at.internet2.edu/display/scalepriv/Scalable+Privacy

Susan: Texas A&M is working towards silver assurance. There is a focus on the delegating identity agents and also on second factor authentication.

Oleg: Aegis has been working with the California Community Colleges on federation. Ann noted that the InCommon affiliates have an important role in paving the way for federation.

Next Assurance implementers Call: Wed. 5-June-2013 at noon ET