Minutes of Assurance Call of 10-July-2013

Draft Minutes, Assurance Implementers Call, 10-July-2013

Attending
Ann West, InCommon
Mark Rank, UCSF
Dave Langenberg, U. Chicago
Brett Bieber, Univ. of Nebraska, Lincoln
Jeff Capehart, University of Florida
Lee Trant, U of Nebraska Medical Center (UNMC)
David Walker, InCommon
Emily Eisbruch, Internet2, scribe

DISCUSSION

Shib IdP Enhancements

https://spaces.at.internet2.edu/display/InCAssurance/Request+for+Proposal+-+Assurance+and+MFA+Enhancements+to+Shibboleth+Identity+Provider

The Assurance and MFA Enhancements to Shibboleth Identity Provider RFP was awarded to Paul Hethmon. Information on this work will be posted on the the Shibboleth wiki. This URL will be shared with the Assurance list. The goal is to have the work completed by end of 2013. The RPF has acceptance criteria that 3 campuses will test the code, and we hope to identify the 3 testing campuses within a few weeks. Most likely testing will take place in September or October. David will send out a solicitation for testing campuses. Let David know if you are interested in helping with the testing.

Assurance Advisory Committee - Recent Activities

The AAC is working on a proposal (to be sent to InCommon Steering) to make Bronze the baseline for participation in the InCommon Federation.

Process for Re-Certification from 1.1 to 1.2 - Ann reported that the AAC has been working on the re-certification requirements for migration from version 1.1 to version 1.2, including compliance requirements and timeframe for upgrading. The AAC currently has a "Process for Re-Certification" recommendation to InCommon Steering for review. Review is expected at the end of July. When approved, the "Process for Re-Certification" requirements will be posted on the Assurance wiki.

Counting Failed Logins Update

https://spaces.at.internet2.edu/display/InCAssurance/Failed+Authentication+Counter+Strawman

The group looking at counting failed password authentication events (led by Benn Oshrin) had a call on June 20. Due to scheduling issues, the plan is to begin further work in August. Benn will announce the next call on the Assurance list. https://spaces.at.internet2.edu/display/InCAssurance/Discussion+Items+%28Counting+Failed+Logins%29

Brett was on the June 20 call. At U. Nebraska, the goal is to implement a system for counting failed logins by Aug. 1, since Nebraska has a target to achieve bronze by Aug. 1. Brett currently has an implementation counting the LDAP failed authentication attempts. This work is posted on GITHUB and there is information on the wiki at https://spaces.at.internet2.edu/display/InCAssurance/Component+Implementation+Guide However for AD, Nebraska has challenges around identifying the proper event codes. Brett has discussed the AD event codes issues with U. Chicago and would like to confer with other institutions also. Ann suggested writing a note to the assurance list to ask if anyone can help with the AD code. The AD topic came up at the CIC IDM meetings taking place this week in Columbus. Brett will be in touch with Ann to arrange an opportunity to talk about the AD issues with the AD Assurance Group. https://spaces.at.internet2.edu/display/InCAssurance/AD+Alternative+Means+-+2013

Assurance Use Case

Ann reported that the Business School of a large research institution recently approached InCommon with a new use case. At this institution, Central IT has stated that the Business School needs to be Bronze certified to federated internally. The Business School has an IDP, but does not need to be in InCommon metadata, it needs to conform to the bronze profile to achieve security goals.

Ann has encouraged the Business School to talk with Central IT about having the institution (not the Business School) sign the assurance addendum with same signature authority as signed the InCommon POP. Further, if they want InCommon to manage the assurance re-certification every 3 years, they would need to put the Business School IDP in the InCommon metadata. This would mean the institution would need to pay for a second IDP for the Business School.

David suggested that it would make sense for the institution to get the bronze certification instead of just the Business School. The IDPO is the institution. The institution will need to explain to users which IDP to use for which situations.

Ann asked if InCommon Assurance should consider offering a service to enable institutions to get a "stamp of approval" for good practices. David suggested that this makes sense, it would be like an audit report saying "yes we agree with management's assertion that they meet the requirements for the assurance program." It was noted that without a SAML IdP it is not possible to be bronze certified under 4.2.7.

Brett: The University of Nebraska system is creating a federation, and has discussed using the InCommon standards, though this is not yet in place yet

Round Robin

Jeff Capehart stated that at University of Florida, the password policy has been revised adding some new options associated with use of longer passwords. The new policy still complies with entropy requirements.

Lee stated that UNMC is examining the different levels of assurance currently in use.

Brett, stated that the CIC IDM Meetings in Columbus have been interesting, including
- discussion of looking at Bronze as the stepping stone to Silver.
- discussion of which campuses, in addition to U. Nebraska at Lincoln, would be willing to help testing the SHA-256 issues.

Next Call: Wed. Aug 7 at noon ET