Minutes of Assurance Call of 12-Feb-2014

Notes: Assurance Call of Feb. 12, 2014

Attending

Ann West, Internet2
Karen Harrington, VA Tech
Scott Koranda, Spherical Cow Group
Benn Oshrin, Spherical Cow Group
David Walker, Internet2

DISCUSSION

FICAM 2.0 and the InCommon Assurance Program

FICAM has released a 2.0 version of the spec.

http://info.idmanagement.gov/2013/11/ficam-trust-framework-solutions-tfs.html

Trust framework providers, such as InCommon, have 6 months to comply with the new FICAM spec. There are discussions underway to determine the impact of FICAM 2.0 to the InCommon Assurance program and the community. An important question is: what are the service providers FICAM will be working with first? The Veterans Admin is a big one. InCommon is aware that many campuses don't want their faculty and staff to leverage their campus credentials to interact with consumer based services like the VA. Campuses want the campus credentials to be used for grant submissions and teaching resources or for interactions with the Dept of Ed. InCommon is hoping to find out from FICAM, what is the ETA for FICAM to bring on board the services that are more relevant to higher ed? The answers to these questions will help the AAC determine how to support FICAM 2.0.

There is interest in our community in exploring/pursuing assurance for research and in developing a community profile to address research needs. There has also been a request for a community profile that is more multifactor oriented. The hope is to address the needs of those SPs that are of interest to the InCommon community and the needs of the IDPs for good practices. The AAC seeks to grow the trust level of the InCommon federation in a logical way.

Q: Scott: has the AAC had input from Steering or TAC on the amount of effort to continue to put into FICAM?

A: Ann: InCommon TAC has been working on priorities and has passed along its recommendations to Steering. TAC wants to make assurance relevant to the community as a whole. One approach is to set a baseline set of practices for the community, to bring up the trust level. This can potentially address the fact that the current POP (Participant Operational Practices) document does not provide sufficient transparency to help SPs and IdPs fully understand the identity practices in effect.

Q: Scott: If new profiles are developed for HE and Research will there be a chance to help influence Federated Incident Response in the profiles from the beginning?

A: The first step is requirements gathering. Eventually yes, there will be the chance to provide input

AD Assurance Update

https://spaces.at.internet2.edu/display/InCAssurance/AD+Silver+Cookbook

The comment period for the AD Assurance work closed at the end of January. The comments that were received have resulted in some tweaks to the document. Soon there should be an announcement of publication of the 2014 version of the AD Assurance Cookbook.

Multi Context Broker

https://spaces.at.internet2.edu/display/InCAssurance/Multi-Context+Broker

David reported that the Multi Context Broker (MCB) code (version 1.0) is ready and a community announcement will be coming soon.

https://wiki.shibboleth.net/confluence/display/SHIB2/Multi-Context+Broker

David has developed documentation introducing the key concepts for the MCB. The Shibboleth users list will be used for questions and comments on the MCB. Community input is welcome. The code is stored on GitHub and an issue tracker will be used for tracking bugs. A roadmap will be developed for next steps, such as if additional authentication modules may be needed. It will also be important to understand what will be required to integrate into Shib V3 when it comes out.

Failed Authentication Counter

Benn reported that UC Berkeley has been interested in counting failed authentication attempts as a way of looking at password entropy and reset policies for the bronze and/or silver profiles. A strawman proposal is seen at https://spaces.at.internet2.edu/display/InCAssurance/Failed+Authentication+Counter+Strawman

Berkeley has contracted with Unicon to build out the Failed Authentication monitor. The work is moving along and development is about to start. This will be an open source project. Code will be in GitHub.

The scope of the work involves an aggregator that writes failed authentication events to a database that logs the subject, the time, and IP address and a service. The monitor periodically queries this. Actions will be triggered at a given threshold. So for example, the system might be configured so that after 10K events, email a particular address. The email might go to the subject, or to an another email address such as the security team. Another action that could be triggered might be to generate a ticket to an issue tracking system. End goal is ability to stop asserting an IAQ for someone. There may be the ability to add or remove somebody from a group (such as Grouper group), where removing somebody from the group would effectively remove them from LDAP. There would be an API into this system for user level and admin operations, such as obtaining current counts for a user. That could be tied into the user identity portal, so it would be possible to show a notification when a user logs in. Thresholds will be configurable. Benn will keep the Assurance informed as portions of the work are released publicly.