Minutes of Assurance Call of 4-Dec-2013

Draft Minutes: Assurance Call 4-Dec-2013

Attending:
Ann West, InCommon/Internet2
Arnie Miles, Georgetown
Benn Oshrin, NYU/UC Berkeley/SCG
David Walker, InCommon
Mary Dunker, Virginia Tech
Jeff Capehart, Univ. of Florida
Lee Trant, U Nebraska Medical Center
Eric Goodman, UCOP

DISCUSSION

Assurance Program Update (Ann)

Identity Week – If you attended Identity Week in November, you know that multifactor authentication (MFA) and addressing phishing for both on and off campus services was a big topic. Building on that, there was interest from the national LIGO research project in developing a community (not US Government) assurance profile that coupled MFA with federated incident notification.

SHA -1 – If you're working on applying for Bronze or Silver certification, you probably know that you have to support SHA-2 signed assertions by January 1, 2014. The InCommon is developing a plan to ease this transition for assurance-certified organizations and those planning to apply for certification. Stay tuned.

Reading Bronze – Looking for some light reading? Join the community every other Thursday for a discussion of the Bronze Identity Assurance Profile. First call is December 5 at 3:00 pm. Next call scheduled for Thurs. Dec. 19 at 3pm ET. See the Assurance wiki for more info.

FCCX and Virginia Tech-- The Federal Cloud Credential Exchange (FCCX pronounced F-6), slated to be released in January, is new gateway (think credential aggregator) for the purpose of easing the load on US Government agencies offering federated services. The services behind FCCX will only be available to certified IdPs. First agencies to get connected will be the VA, USDA, and Commerce (NIST). Virginia Tech is in discussion with them on testing with InCommon. Thanks Virginia Tech.

Bronze as POP replacement – A while back, we discussed using Bronze as a Participants Operating Practices (POP) replacement for IdPs which requires IdPs and SPs to post their practices on a website. It turns out that Bronze is really a subset of the POP and doesn't address things like interoperability, attribute integrity, and so on. However, the POP is still an issue for the Federation---maybe 2014 will be the year of the new POP.

AD Assurance Cookbook

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

The AD Assurance group is making some edits to the updated "InCommon Silver with AD Domain Services Cookbook" based on the suggestions received during the comment period of Oct. 2-Nov. 8, 2013.

Assurance Advisory Committee (AAC) Update

Mary reported on AAC activities:

-The AAC is developing a recommendation to Steering on new AAC members to replace those who complete their term at the end of 2013.

-The AAC is helping the Net+ Security Initiative move forward with recommendations about IDM. The Cloud Security Alliance is developing a cloud control matrix, primarily focusing on controls for SP's. The AAC is working to add content to the matrix about federated authentication and IDM. https://cloudsecurityalliance.org/research/ccm/

-Virginia Tech has been involved with the Federal Cloud Credential Exchange (FCCX pronounced F-6) effort. Virginia Tech has submitted some questions and are waiting for the response. One of the issues: if there is no existing agreement with a trust federation like InCommon, then Virginia Tech would want some kind of contract in order to release attributes. The hope is that the FCCX gateway will have a relationship with InCommon so it will be possible to leverage the trust framework already in place.

More about FCCX

Ann said that she and others recently had a call with Anil John, who is program manager for FICAM and chair of the FCCX technical committee. Anil supports the FCCX joining InCommon. The FCCX is looking at an attribute bundle that would be released by IDP's accessing federal applications through FCCX. There are some issues to work through. For example, one of the attributes mentioned was "legal name" which is not an attribute in eduPerson.

Assurance Enhancements for the Shib IDP / Multi-context Broker Plugin

https://spaces.at.internet2.edu/display/InCAssurance/Shibboleth+Enhancements+-+Project+Status

David reported that the Shib Enhancements work (known as Multi-context Broker) is in the acceptance testing phase. All issues that were identified by the acceptance testers have been fixed by the developer. The acceptance testers are now reviewing these fixes to determine if they give their stamp of approval.

David presented on the Multi-context Broker project a few times during ID Week and there was positive response. The initial purpose of the Shib enhancements was to address adding an indication of bronze or silver as part of authentication. Campuses are now thinking about using the Multi-context Broker to improve integration with AD and for other purposes, as seen in these notes from Advance CAMP: https://spaces.at.internet2.edu/display/ACAMPScribe2013/Multi-Context+Broker+and+Bootstrapping+AuthN+Requirements

David reported that there is interest in a Duo authentication module for the Multi-context broker.
There is also interest in a module to be used with X509.

Failed Authentication Attempts Effort

Benn reported there is no update at this time on the Failed-auth-attempts-counter work. However, there was discussion of this topic at Advance CAMP: https://spaces.at.internet2.edu/display/ACAMPScribe2013/Tues+4.15pm+Monterey

Round Robin

Mary reported that Virginia Tech was certified under v 1.1 and is required to move to v 1.2 per the earlier announcement to the community.
Several issues around approved algorithms have required review as part of the 1.2 certification.
Concerning the SHA-1 issue, the hope is that the SP 's with which the Virginia Tech users interact will support SHA -2.
There is an effort to identify the relevant SP's for the VA Tech users and be sure those SP's can support SHA-2
Then VA Tech will implement the plug-in for SHA-2.

====
Jeff Capehart reported that University of Florida has done a gap analysis and an overall audit on IDM. There will be meetings upcoming with the CIO to present the report. Some areas that must be addressed in order to meet InCommon Silver. The SHA-1 and SHA-2 issues are of particular interest after today's discussion.

Use of eduroam is of interest at U. Florida. It was noted that eduroam does not ask for an AuthnContext, rather eduroam authentication is done via RADIUS servers.

Mary commented that Virginia Tech does not use eduroam (they use another wireless server), and the use of RADIUS servers was considered a roadblock to use of eduroam. Ann mentioned that a some schools have separate passwords for their wireless service. Va Tech does this too.

====

Lee Trant reported that U. of Nebraska Medical Center has recently submitted documentation for Bronze certification.
The issues with SHA-1 and SHA-2 are of interest and it will be useful to discuss those on the "Reading Bronze" calls.

Ann noted the U. of Nebraska bronze application has been received by InCommon and a response will be forthcoming.

===

Eric Goodman stated that the UC System in considering doing a self-audit.
A decision must be made on whether to refer to the assurance profiles that were developed along with UCTrust (before the Incommon Silver was developed) or to refer to the InCommon Silver profile for the purposes of the proposed audit. There is discussion with the UC System CIOs to formalize and clarify the audit process.