

Minutes of Assurance Call of 6-March-2013

Draft Minutes: Assurance Implementers Call of 6-March-2013

Attending

Ann West, InCommon/Internet2
Mary Dunker, Virginia Tech
Karen Harrington, Virginia Tech
Jim Green, Michigan State University
Mark Rank, UCSF
Marlena Erdos, Harvard
David Walker, Independent
Benn Oshrin, Internet2
Wes Hubert, University of Kansas
David Langenberg, University of Chicago
Oleg Chaikovsky, Aegis Identity Software, Inc
Jeff Capehart, University of Florida
Ron Thielen, University of Chicago
Tom Scavo, Internet2
Emily Eisbruch, Internet2, scribe

DISCUSSION

Active Directory Assurance Work

The new group looking at Active Directory in view of the version 1.2 assurance profiles had their first call on March 1, 2013. The group discussed their charge, which is to review AD in light of Bronze and Silver and determine if an Alternative Means can be developed. The group will also look at whether the AD cookbook needs to be tweaked. One of their first tasks will be to map the various products of AD to the framework of the profiles.

Ann is reaching out to make contact with AD experts within Microsoft to discuss issues around assurance.

Also, Ann is working to identify federal government agencies that have implemented Active Directory and have been certified with a FIPS 140-2 level or with a NIST level roughly equivalent to Silver. Based on early discussions, it seems that NASA is in this category. Debbie Bucci, who is on the AAC, is helping Ann connection with the right individuals within NASA.

CIC Assurance Documentation

Jim Green leads a group known as the "CIC and Friends Assurance Documentation workgroup." The group has conference calls once per month and is collecting and sharing documentation from various institutions related to certification in the InCommon assurance program. This group is now open to any institution that is a member of InCommon. All are invited to participate. There is a link in the Assurance wiki <https://spaces.at.internet2.edu/display/cicincsilver/CIC+and+InCommon+Silver>

Defining the Assurance Value Propositions

Ann is defining the assurance value proposition. Ideas for points to emphasize in the value proposition:

-For research use cases, discuss the synergy with the work of both CI Logon and the NIH Electronic Vendor Invoicing Processing (eVIP) System. (By the way, let Ann know if you are interested in testing the eVIP system.)

-Assurance can be useful even if a campus is not SAML-enabled. For example, even without a technical control to enforce silver, a report on the silver status of the service's users might be required. This would be a local, not federated, control.

Value proposition for Bronze

-Highlight the fact the bronze is now self attested, that no audit is needed for bronze under v. 1/2

-Mention the National Student Clearinghouse use of bronze for student interactions where it's not necessary to confirm a specific identity, but rather just to have the campus vouch for the student,

-If a campus is interested in silver, bronze is a good way to get started, provides a stepping stone to silver

-There are collaboration services for which bronze is sufficient, where ID can be based on reputations, rather than government ID

-Could use the bronze profile as a baseline for a generally accepted practice for passwords.

Shib IdP Assurance Enhancements Progress

As mentioned on February call, a small Shib IdP Assurance Enhancements Group has been tasked with exploring ways for the Shib IdP to recognize and facilitate run-time assurance interactions. David reported that the group is close to having a spec. When completed, the spec. will be distributed as an RFP for a short-term development project to enhance Shibboleth 2 to better support assurance. The specs will also be given to the Shib Consortium for long term incorporation in their roadmap.

Assurance Advisory Committee work

Mary reported on behalf of the AAC:

-the AAC is working on processes for handling Alternative Means submissions.

- the Virginia tech case study is now complete and available at <https://spaces.at.internet2.edu/display/InCAssurance/Assurance+Implementation+Example+-+Virginia+Tech>

-There is a timeframe for which all certified IDPs must comply with a new version spec. Virginia Tech is looking at compliance with 1.2 spec, and this will involve writing up a description of the Virginia Tech alternative means

Updates from Campuses

-University of Chicago is doing a high-level walk through with their auditors, going over each of the exceptions of the IAP and the management assertions. They are finding gaps in their documentation and working to fill those gaps

-Harvard is conducting gap analysis related to assurance. They plan to review docs on the assurance wiki to learn from the experiences of other campuses.

-UC Berkeley is launching their silver assurance effort. There is work to do on registration & credential reset for VIPs

-UCSF is looking at their AD environment and staying tuned to the work being done around AD

-Virginia Tech has some applications that require higher levels of assurance, including multi factor authentication. They are looking at mapping these to silver assurance and considering requiring the silver versus bronze indicator.

Next Assurance Implementers Call: TBA