Minutes of Assurance call of 13-Feb-2013

Draft Minutes: Assurance Implementers Call of 13-Feb-2013

Attending

Ann West, InCommon/Internet2
Mary Dunker, Virginia Tech
Jim Green, Michigan State University
Susan Neitsch, Texas A&M
David Walker, Independent
David Bantz, University of Alaska
Benn Oshrin, Internet2
Lee Trant, University of Nebraska Medical Center
Brian Arkills, University of Washington
Michael Brogan, University of Washington
Arlene Allen, UCSB
Michael Hodges, University of Hawaii
James Oulman, University of Florida
Joe St Sauver, University of Oregon, Internet2
Shreya Kumar, Michigan Tech University
David Langenberg, University of Chicago
Ron Thielen, University of Chicago
Eric Goodman, University of California
Bry-Ann Yates, University at Albany, SUNY
Colorado State University

DISCUSSION

Assurance Requirements for the IDP

David Walker reported that a small group has met several times to discuss assurance requirements for the Shib IdP. The objective is for the IdP to recognize and facilitate communication with the SPs based on the InCommon assurance profiles. Shreya Kumar at Michigan Tech is documenting the specifications for the group. Completion target is March. 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.

Q: In the SP metadata, is there an indication of what assurance level the SP requires?
A: No. The metadata contains an entity tag for the IdP if certified, but not the SP. The SP specifies its required assurance at the start of each session.

Approval of 1.2

Version 1.2 was approved by Incommon Steering on Feb. 11, 2013, and it is now the production spec. The Assurance website will be updated soon with the new information. Simplifed bronze is now in effect; an audit is no longer needed for bronze and certification is free. Longer term, it's possible that bronze assurance will replace the InCommon IdP Participant Operational Practices (POP).

FICAM has a list of IdPs that have been approved by a trust framework provider. Virginia Tech is on that list, and it would be good to get additional institutions listed to make it clear that higher ed is ready to play with the Agencies:http://www.idmanagement.gov/pages.cfm/page/ICAM-TrustFramework-IDP

Alternative Means

There is now an approved process for submitting alternative means. http://www.incommon.org/assurance/alternativemeans.html
This was added to the spec in 1.1, but was not approved by FICAM until the FICAM review of 1.2. The process allows submission of alternative means:
-along with an application for assurance
-prior to an application for certification
-by a community group (such as the AD Silver group)

Approved alternative means will be added to the website and will be considered normative.

The AD Silver Issue and 1.2

The issue with 1.2 and Active Directory is around the technologies (MD5 hash) that AD uses for storage of password secrets. There are doubts that AD could pass the "approved algorithm" bar set in version 1.2, although the alternative means option must be explored to determine this. While AD makes it possible to enable two-factor authentication, it is not possible to turn off authentication via password. Microsoft has not indicated that they plan to change the way passwords are stored in AD.

The AAC has determined that a first step is to convene a group to look at AD under alternative means and develop a risk assessment and mitigation strategies using the AD Cookbook as a basis. Brian, Michael, Eric and Ron expressed interest in participating in the group.

Password Entropy Tool

Shreya presented her work on a new UI-driven password entropy tool. This is being built on many of the capabilities in the existing Entropenator tool developed by University of Wisconsin-Madison. The user will enter information on their password security policies (password length, lockout duration, allowed guesses, etc.), and the tool will calculate the password level, based on the NIST specification. The tool will calculate the current LOA eligibility and will specify what more is needed to increase LOA. There will be a "View Report" feature and it will be possible to generate a PDF report. There will be an "About Us" tab that will present FAQs, explain the the tool is based on the NIST specifications and will present information on the InCommon Assurance program.

Re-Registration for Bronze

Benn Oshrin notes that version 1.2 could lead to some confusion around what is needed for password reset under bronze assurance. The issue is that v1.2 makes section §4.2.4.3 part of bronze, and this section says:

"After expiration of the current Credential, if none of these methods are successful then the Subject must re-establish her or his identity with the IdPO per Section 4.2.2 before the Credential may be renewed or re-issued."

However, almost none of §4.2.2 applies to Bronze, since Bronze has no registration record requirements. So what does this imply for a Subject with an expired credential, a no longer valid Address of Record, and no (or forgotten) pre-registered questions?

Ann explained that the AAC felt this was a logic bug in the spec when the issue was raised a few weeks ago. The spec is not incorrect. The AAC did not want to go back to FICAM to address this and risk delaying release. This issue will be corrected in the next iteration of the spec. The intended solution is for the institution to protect PII gathered in the registration and re-registration process. It was agreed that it would make sense to clarify this in an FAQ.

Next Call: TBA