Minutes of Assurance Call of 7-Aug-2013

Minutes: Assurance Implementers Call of 7-Aug-2013

Attending:
Ann West, InCommon/Internet2
Dave Langenberg, U. Chicago
Ron Thielen, U. Chicago
David Walker, Independent
Dedre Chamberlin, UCSF
Mark Rank, UCSF
Sharon Welna, University of Nebraska Medical Center
Steve Devoti, University of Wisc.
Jon Miner , University of Wisc.
Michael Hodges, Univ of Hawaii
Eric Goodman, UC Office of the President
Jeff Capehart, University of Florida
Emily Eisbruch, Internet2, scribe

DISCUSSION

Migration of Certified IdPOs from 1.1 to 1.2

https://spaces.at.internet2.edu/display/InCAssurance/Community+Migration+from+Version+1.1+to+1.2

Steve Devoti reported that the AAC has developed an upgrade process that will serve for the current upgrade from 1.1 to 1.2, and will also provide the framework for future upgrades to the assurance spec. The migration process currently only applies to Virginia Tech, but the expectation is that a greater number of IdPs will be impacted by future upgrades. What is required for this upgrade is a written statement attesting to compliance with each criterion that is highlighted yellow in Substantive DIF: IAP v1.1 versus v1.2. No audit is required for this upgrade.
-The approach for future upgrades to the assurance spec will be:
  -AAC identifies the extent of the changes
  -AAC decides on what is appropriate (attestation?, audit? other?) given the extent of the changes

The version 1.2 spec laid out the process for handling alternative means. Virginia Tech will be submitting their alternative means as part of the upgrade.

Shib IdP Enhancements Progress

As reported last month, the Assurance and MFA Enhancements to Shibboleth Identity Provider RFP was awarded to Paul Hethmon. Paul has started work on the design documents, and progress can be reviewed at:https://spaces.at.internet2.edu/display/InCAssurance/Shibboleth+Enhancements+-+Project+Status

Campuses doing acceptance testing for the Shib IdP Enhancements will include U. Chicago, U. Florida and Brown. The project is on schedule to finish by the end of the year (or possibly sooner). Paul Hethmon has been communicating with the Shib developers to align his work with their Shibboleth UI work.

Q: Is SHA-2 going to be part of the Shib Enhancements?
A: There is going to be a plug in for SHA-2. There is a different group looking specifically at SHA-2, led by Tom Barton under the auspices of the InCommon TAC.

Assurance Advisory Committee Update

SteveD reported that the POP has been a focus area for the AAC. Issues include:
-some IdP's never published an initial POP
-other IdP's have an outdated POP

The AAC has heard from InCommon Service Providers that the current system makes it difficult to evaluate risk of working with an IDP. The AAC looked at whether it might be reasonable to require IdP's to assert a bronze level of assurance.
-Dedre: it makes sense to require that campuses maintain an up-to-date POP.
-Michael: Perhaps the POP should have a life span, with a requirement the IdPs do an update at a certain interval.
-Ann: Every six months, InCommon reminds IdPs without a POP that they need to provide one.

It was noted that even if every IdP had a current POP available, this would not address all the concerns that are being raised by the Service Providers. Enforcement of the current POP requirement may be a logical first step, but the problem would still exist that SP 's with high trust requirements would still need a lot of staff to check every POP. Ann suggested a scenario (being brainstormed), where IdP's are required to use an online checklist or series of checklists to describe their practices. There could be bundles of questions around categories such as credentialing, identity management, interoperability, etc. AuthNContext might be expressed in some of the bundles. Numeric values could be assigned to an IdP based on their self-assertions on these checklists. The numerical score could be asserted as an attribute, to allow an SP to decide whether to federate with a given IDP. This would be an informal program, separate from Assurance, but it might somehow feed into Assurance.

Dedra commented that the simplicity of this checklist approach is appealing and could provide important benefits, and it would be especially helpful if there was also more detailed documentation available describing each IdP's practices.

Q: Would this checklist approach be flexible enough to reflect how a campus uses an alternative practice (such as using MFA instead of password reset)?
A: There could be registered, community-defined standards (apart from the FICAM standards) expressed via AuthNContext.

Comments
-It's important to use password protected transport, and to avoid bilateral handshakes.
-We should look at solutions that feed into the assurance program.

Counting Failed Login Attempts

https://spaces.at.internet2.edu/display/InCAssurance/Counting+Failed+Logins

Benn will report on this effort on a future call. Dedra stated that UCSF is interested in working with another campus as partners in looking at Counting Failed Login Attempts.
Ann suggested that Brett Bieber at Nebraska might be a good partner.

AD Alternative Means Update

https://spaces.at.internet2.edu/display/InCAssurance/AD+Alternative+Means+-+2013

The AD Alternative Means group is working with Microsoft and also looking at possible interim approaches. The issues include a couple of the encryption algorithms that are not NIST compliant. One action item for the AD Alternative Means group may be to update the AD Cookbook.

Round Robin

Dedre reported that UC Trust Federation has a goal of moving towards InCommon Silver, but is currently focusing on an interim target to get the UC Trust campuses to comply with the assurance requirements of the local federation by the end of the year. This will move the campuses part of the way towards InCommon bronze or silver.

Michael reported that at U Hawaii they have set up an AD instance, and so the work being done by the AD Alternative Means group has become of great interest.

Cohort Group on Bronze Implementation

Ann Is putting together a plan for a bronze implementation cohort group. This will involve walking through the bronze spec. The group will most likely talk about entropy issues, controlling access to your password store, interpreting the spec, old clients, and other issues.

Next Call: Wed. September 4, 2013