# Minutes of Assurance Call of 3-April-2013

## Minutes: Assurance Implementers Call 3-April-2013

**Attending**
Ann West, InCommon/Internet2
Brett Bieber, Univ. of Nebraska, Lincoln
Michael Brogan, University of Washington
Jeff Capehart, University of Florida
Steven Carmody, Brown
Oleg Chaikovsky, Aegis Identity Software, Inc
Mary Dunker, Virginia Tech
Jeff Globe, University of Nebraska Medical Center
Jim Green, Michigan State University
Michael Hodges, University of Hawaii
Wes Hubert, University of Kansas
Shreya Kumar, Michigan Tech University
David Langenberg, University of Chicago
David Walker, InCommon/Internet2
Bry-Ann Yates, University at Albany, SUNY
Emily Eisbruch, Internet2, scribe

### DISCUSSION

**Internet2 Annual Meeting**

Deborah Gallagher and Anil John, from FICAM, will be presenting at the Internet2 CIO Forum on Monday afternoon, April 21, 2013 at the Internet2 Annual Meeting. If your executives will be at the meeting in Arlington, please encourage them to attend that session, and participate.http://events.internet2.edu/2013/annual-meeting/gensched.html

**Active Directory Assurance Work**

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

A group has been conducting weekly calls to look at issues around AD and the assurance profiles. Michael Brogan and Jeff Capehart stated that the work is moving along well. A matrix is being filled out to track the issues, and the group is looking at alternative ways within the windows environment to provide protection. The group has identified some questions for Microsoft and has identified the right person within Microsoft to answer those questions.

Q: If a campus is using MIT Kerberos 5, would they also have to go through the process of developing alternative means?
A: Yes, some investigation and workarounds would likely be needed. Where Kerberos is used, but NOT used for authentication, there is likely less of an issue.

Jim Green noted that Michigan State uses Kerberos and AFS and there are some issues to be looked at around single DES keys.

**CIC Assurance Documentation**
+ http://bit.ly/Yu2erK

Jim Green reported:
-The CIC Assurance Documentation Group call (open to all) is on the 4th Thurs. of the month at 4pm ET
-Jim posts minutes to the assurance listserve and the CIC group and in the Assurance wiki at https://spaces.at.internet2.edu/display/InCAssurance/InCommon+Silver+with+Active+Directory+Meeting+Notes

**Value Proposition for Assurance**

Ann has started working on the value propositions for Assurance. Collaborators and comments are welcome:https://spaces.at.internet2.edu/display/InCAssurance/Bronze

**Shib IdP Enhancements for Assurance Progress**

The draft of the Shib IdP Enhancements is ready for review. This is intended as about a 2 year stop-gap until the release of Shibboleth v3.https://spaces.at.internet2.edu/download/attachments/9185/AssuranceReqShibIdPv17.pdf

Please provide suggestions by April 10, per David's email to the list. Appreciation to David and Shreya for their work on this.

**Assurance Advisory Committee**

The AAC is having a F2F meeting in Ann Arbor in early May. If you have something for the AAC to address, please send your question to Ann or Mary Dunker (dunker@vt.edu).

Recently the AAC has been looking at how an IDP will upgrade from 1.1 to 1.2. Also, the AAC has received an Alternative Means proposal and is evaluating that. This is from an institution submitting the Alternative Means proposal prior to submitting their assurance application.

**Communicating with Users about Assurance**

Ann noted that there is a need to define the best ways to communicate assurance issues. For example, if a user is downgraded from Silver to Bronze because they are using an insecure machine, how does that get communicated at authentication time?

Ron Thielen has shared an interesting approach U. Chicago is considering of using a personal credential page --- a checklist of what needs to be in place for silver status and what they must do to re-up their credential if it has been downgraded.

Michael Brogan said the University of Washington has a U-W Net ID "manage page" for each user that could be leveraged to provide assurance information. There are also other mechanisms being considered to communicate to the users. Eventually UW may involve user experience experts to help recommend the best language to use, for example whether to use the word "assurance." One issue is that if a user loses their assurance, an application could appear to be "broken." Want to avoid the appearance of brokenness.

It was agreed that it makes sense to formulate recommendations, points of communication, language to use (analogies would be helpful), etc.

[AI] (Jim) will explore if this is a good topic for one of the CIC Assurance Documentation calls

**Password Entropy Tool**

Shreya provided a demo (via AdobeConnect ) to the Entropy Tool she has been working on.

The tool does calculations:
1. For a user-selected password
2. For a randomly selected password
3. For a numeric-only password

There are tooltips for each field.
Based on the inputs, the tool calculates if a password is valid for LOA 1 or 2.

Mary commented that it looks great, Would be good to include the calculations. Nice, easy to use interface.

Q: Does the tool provide a calculation for Multi Factor approaches?
A: Not yet, this feature could be added in the future, possibly using a tab for the different types of multi-factor. Would take work to develop the probabilities.

Suggestions
-Add lockout in minutes in addition to hours, as an input.
-Use check boxes and sliders for the gains and losses
-Provide the result at the bottom.

Shreya stated that these are all doable and good suggestions.

Q: What about terminate versus account lockout?
A: Will will look at that.

Shreya will share the next iteration of the Password Entropy Tool with the list.