Minutes of Assurance Call of 9-Jul-2014

Assurance Implementers Call of July 9, 2014

Attending

Ann West, Internet2
Steve Devoti, University of Wisconsin, Madison
Jacob Farmer, University of Indiana
Tom Golson, Texas A&M
David Crotts, Virginia Tech
Mary Dunker, Virginia Tech
Karen Harrington, Virginia Tech
Jeff Capehart, Univ. of Florida
Benn Oshrin, Spherical Cow Consulting
David Walker, Internet2
Emily Eisbruch, Internet2, scribe

DISCUSSION

FICAM 2.0

http://info.idmanagement.gov/2013/11/ficam-trust-framework-solutions-tfs.htmlhttp://www.idmanagement.gov/sites/default/files/documents/FICAM_TFS_TFPAP_0.pdf

Background: FICAM informed the Trust Framework Providers of the new FICAM 2.0 spec draft last fall.
InCommon sent a lengthly set of comments.FICAM released their new 2.0 spec early in 2014.

Ann is analyzing the impact of the FICAM 2.0 documents on InCommon Assurance IDPs. The InCommon Bronze and Silver specs may have minor changes, such as new terminology mapping. For instance, FICAM 2.0 refers to Identity Providers as a Credential Service Providers (CSP). A Credential Service Provider handles assurance, can do token management and credential issuance and can assert identity attributes on behalf of the individual.

http://www.idmanagement.gov/approved-identity-services

An issue under negotiation is that FICAM 2.0 requires all Credential Service Provides to release certain attribute bundles which contain legal name and date of birth that the Agencies will use to for identity matching. Since InCommon is focusing on business-to-government services and targeting key agencies most important to our constituency, InCommon is advocating the use of the attribute bundle defined in the Research and Scholarship Category. The next steps are to meet with Agencies of interest to determine if this set of attributes is sufficient for their use.

In addition, InCommon has stressed in discussions with Anil John that the lack of federal services requiring assurance is a major issue.

Assurance Advisory Committee (AAC) Update (Jacob)

The AAC heard from the community that it would be beneficial to have more modular standards in the InCommon assurance program. The background is that the current Bronze and Silver profiles were modeled off a monolithic government document (NIST 800-63). Some Service Providers don't care about every category in the current specs and some IDPs find it very difficult to implement 100% of the spec requirements.

Conversation nationally and within the IDESG focuses on developing modular units, called Trustmarks, for assurance.
The idea is that the current InCommon Assurance Bronze and Silver profiles can be decomposed into smaller chunk standards, making it possible to pick and choose the relevant section, both on the IDP and SP side, providing more flexibility.

The AAC is starting to discuss this more modular approach to assurance, possibly using trustmarks. At the same time the AAC is also working on a community profile. The current InCommon bronze and silver profiles were written explicitly to address requirements for federating with the federal government. The AAC recognizes that the research and higher education community has its own interests concerning identity assurance, such as multi-factor authentication. In response to this, the AAC is working on an overall framework for developing, promulgating and asserting community trust-related profiles.

The AAC will have a Face to Face meeting in mid-August to discuss this topic.

Comments:

- Agree with the trustmark approach conceptually, but will wait for the details

- Using the modular approach is a good idea to keep things moving forward. For an IDP to implement Bronze and Silver, it can happen that 80% of the requirements are not too difficult, but the last 20% is challenging. A mechanism to keep things moving is good.

- Agree, we need to fine a way to make Bronze and Silver assurance more meaningful to people and easier to achieve.
Also, must establish the use cases that this approach will address. Use cases are lacking in the current framework.

Shibboleth Multi-context Broker (MCB) Plugin Update (David)

https://wiki.shibboleth.net/confluence/display/SHIB2/Multi-Context+Brokerhttps://spaces.at.internet2.edu/display/InCAssurance/Multi-Context+Broker

The Multi Context Broker was released in March 2014 and is getting use, moving into production at some institutions. There are two enhancements planned over the next few months:

1. The MCB has not been honoring the default authentication context that can be specified for a relying party if the relying party does not request an authentication context in the protocol. So support for that will be added.
2. University of Chicago raised some concerns around how forced reauthentication occurs, This is related to how we have implemented Duo and Duo-like technologies in the MCB. There will be an option to keep the current behavior of the MCB or change it.

MCB in view of the upcoming release of Shib V3

- Discussion is now underway on how the MCB will work with Shib v3.
- Shib v3 has some of the functionality of the MCB.
- A gap analysis is being conducted. Some issues around configuration files are being looked at.
- In about a month there should be a proposal around MCB and Shib v3
- The team is committed to a good upgrade / conversion path

New Alternative Means for SHA-2

https://spaces.at.internet2.edu/display/InCAssurance/2014/07/01/New+SHA-2+Alternative+Means

Alternative Means is now approved for SHA-2. It states "Identity Provider (IdP) Operators may continue to use SHA-1 to sign assertions through *January 15, 2015* without compromise to their InCommon Assurance certification"

Question regarding eduroam:
At one point, eduroam was not compliant with InCommon assurance because it used a non-compliant algorithm. Is that still an issue? Discussion centered on how one authenticates people for eduroam. The decision on whether there is a problem around assurance for eduroam involves a management assertion and auditor judgement.

Failed Authentication Counter Work (Benn)

https://spaces.at.internet2.edu/display/InCAssurance/Failed+Authentication+Counter+Strawman

https://spaces.at.internet2.edu/display/InCAssurance/Component+Implementation+Guide

Benn reported that he will report on integration work on the Failed Authentication Counter database being done by UC Berkeley and Unicon on an upcoming Assurance Call.

Comment: would be interesting to compare the approaches to the failed authentication counter being used at UC Berkeley and Univ. of Nebraska.