Minutes of Assurance Call of 5-Nov-2014

Notes: InCommon Assurance Monthly Implementers call for 5-Nov-2014

Slides used for this Assurance Call are here.

Attending:

Ann West, Internet2
Steve Devoti, UW-Madison/AAC Chair
David Walker, Internet2
Mark Jones, UT Houston
Eric Goodman, UCOP
Benn Oshrin, Spherical Cow Consulting
Randy Miotke, Colorado State University
Susn Neitsch, Texas A&M University
Tom Golson, Texas A&M University
Jeff Capehart, University of Florida

Discussion

The October 2014 Assurance Call was an IAM Online featuring University of Nebraska and UMBC presenting on their experience with InCommon Bronze certification and security. The archives are linked from here http://www.incommon.org/iamonline/

Today's call will focus on **InCommon Assurance and US Government Discussions** Slides used for this Assurance Call are here.

Topics:

- Update on the FICAM Program
- Implications on the InCommon Assurance Program
- Next Steps for the Assurance Advisory Committee (AAC)

FICAM

FICAM was based on NIST 800-63.
Currently there are 3 FICAM Approved Trust Framework Providers:

http://www.idmanagement.gov/adopted-trust-framework-providers

- Kantara (large IDP's and international) https://kantarainitiative.org/idassurance/
- Safe BioPharma http://www.safe-biopharma.org/
- InCommon (addressing FICAM requirements with HE flexibility)

FICAM 1.0 spec and related documents focused on identity provider and credential practices.
With the approval of FICAM 2.0, there are changes. FICAM 2.0 also encompasses:

- federation requirements outside identity assurance
- Citizen2Government target
- Componentized Identity Assurance approach

Token Manager + Identity Services Manager = Credential Service Manager

FICAM 2.x includes federation requirements

- Change Management
- Contacts
- Entity Info
- Memorandum of Agreement
- Attributes for ID Matching

Question arose: Can't InCommon handle this for the InCommon IDPs?

Much progress in the discussions with FICAM. See slide 6 for details.

Componentized Services

An important topic is componentized services (see slide 7 and 8 for details)

Discussions with NIH and NSF

See slide 9

InCommon's discussions with NIH and NSF resulted in FICAM accepting our standardized attribute bundle (R&S) rather than the attributes FICAM had been requiring (which has included legal name and DOB)

GSA (home agency for FICAM) has joined InCommon, GSA will likely be the focal point for other agencies.

Community Profiles

See Slide 10

- In addition to the FICAM-based Bronze and Silver profiles, there are community needs, such as for an MFA profile.
- Also need to replace the POP approach of "Post your Practices" and have baseline practices

Next Steps for the Assurance Advisory Committee (AAC)

Steve Devoti, AAC chair, reported

- The AAC is working to revise its charter to do more than manage the assurance process for certification. This does not expand a lot the AACs charge. But it is broader than managing a process.
- The AAC is looking at what needs to be modified to increase trust within the federation. The goal is to get people on the road to higher trust and higher assurance.
- We have received feedback (from our SP partners) on the lack of usefulness of the POP and the lack of compliance. Some InCommon participants are not updating their POPs.
- We have talked about decomposing the assurance profiles into trust marks to drive incremental progress within the federation.
- There is work at GA Tech on Trust Marks https://trustmark.gtri.gatech.edu/the-pilot/

Q&A

EricG asks, there is Vectors of Trust group. The UC system is are is taking a similar approach in standards, for incremental progress short of silver. Is there a sense of what the scope of the trustmarks (being discussed by the AAC) might be? Wants to do things that would map to trustmarks. Are there specific targets that would be useful for us to use?

SteveD: The AAC's work on this is at the beginning. The AAC has not yet taken our InCommon assurance profiles and decomposed them into trust marks.

The GA Tech GTRI group has looked at breaking 800-63 into trustmarks.

See:
https://trustmark.gtri.gatech.edu/concept/#framework-example-ficam

See pages 44-45 here: https://trustmark.gtri.gatech.edu/wp-content/uploads/2014/01/Trustmark-Pilot-Concept-Slides-for-IDESG-Briefing-2014-01-16.pdf

MFA Profile

For a community MFA profile, there are decisions on how granular to be. There are apps that want MFA. Some campuses have MFA and some don't. Under what circumstances would the SP application trust that MFA had been done by the campus, versus the app requiring its own MFA? We don't want to have campus MFA plus ALSO application MFA.

It was noted that with a light/simple definition of MFA trustmark (MFA? Y or N), there are concerns. Example: an SP that remembers the user for 30 days, with no forced re-authentication. There would be a need to disallow that kind of practice.

TIER

Question: How does the TIER work related to Assurance?
Info on TIER:https://drive.google.com/folderview?id=0BzRHp0xie6WFUVRqQXBwd3VSa1U&usp=sharing

Ann: TIER aims to accelerate IDM across HE. We need to help researchers get access to services,including participants in a VO. Also need to accelerate ability for schools that don't have an effective IDM system and need one to access federated services.

Question: Can a campus be in TIER and not do Assurance?

Ann: Don't know yet. TIER is in an early stage. Requirements are not yet set by the community.

Next Assurance Implementers Call: Jan. 2015 (no call in Dec. 2014)