InCommon TAC Meeting 2016-03-31

Minutes

Attending: Michael Gettes, Tom Barton, Steve Carmody, Janemarie Duh, Jim Jokl, Mark Scheible, Scott Cantor, Chris Misra, Keith Hazelton, Tom Mitchell

With: Dean Woodbeck, David Walker, Nick Roy, Mike LaHaye, IJ Kim, Steve Olshansky, Ann West, Paul Caskey, Tom Scavo

Minutes of March 17, 2016 approved

Ops Update

Discussion of the failed metadata signing process on March 21

1. Monday, March 21: Metadata signing process failed
2. Tuesday, March 22: Difficult to handle '' characters in metadata. This caused the metadata signing process failure (caused an invalid signature, which caused the process to fail when attempting to publish metadata on March 21). The process worked Tuesday, March 22, but including these characters exposed a bug in the Shibboleth SP software (which won't be fixed anytime soon).
3. Tuesday, March 22: Delayed notification of published metadata. This unrelated issue was caused by change in spam filter by Office365 (Internet2's cloud email provider)

Ian is building a tool that will allow publishing of a cache version of metadata if the signing process fails. Also, eduGAIN operations has started to verify what they publish with a separate XML security stack. But this does not solve this specific problem.

Moving to per-entity metadata would eliminate this problem. However, that is a long-term fix. There was discussion of reducing the risk of this happening again.

(AI) Nick will talk with eduGAIN steering group, letting them know the InCommon TAC believes this is a critical problem for the trust platform. Are there things eduGAIN can do to alleviate this risk? Depending on the answer, we may then look at what InCommon can do to protect itself.

Ops Advisory Group

A core group has agreed to participate. Nick is still looking for an SP operator to participate. Nick is setting up a poll to agree on a regular call time.

Potential TAC F2F at Chicago I2 Global Summit (Tuesday, May 17, 9-11 am)

(AI) TAC members should develop agenda items that would benefit from a F2F.

Per-entity metadata - question of scope

(AI) Nick to review/revise the charge based on the discussion on the TAC email list. The WG will not produce a production MDQ. It will propose a plan for rollout - a blueprint - which will be fed into an InCommon plan for creating a production service. There is agreement within TAC that moving to per-entity metadata is the end goal, but there there also needs to be a parallel discussion about a shorter-term solution.

TAC 2016 Work Plan

(AI) TAC review this document and identify what want/can do in 2016.

Comments/ideas on priorities for 2016:

- MDQ
- A number of items support the first item - growing the number of IdPs in InCommon
- Suggestion - add something about packaging/distributing software configured specifically for supporting InCommon (e.g. InCommon defaults). For instance:
    - Attribute release policies
    - Automatically point at an MDQ server
- Keith, Mark, Albert all support a working group regarding LTI. Keith proposes drafting a WG charter with the goal of seeing if we can get them out of the WebSSO business by providing an alternative path. Consider this as part of the bigger authNZ for web APIs problem.
- SirTiFi - there are things that InCommon (and other federations) will be asked to do (security contact info will be one of the main things)
- POP replacement = baseline practices - AAC has started to work on this. There will be a need for feedback at some point. There will be a BoF at Global Summit on this.

(AI) Steve will review the TAC work plan document and resolve comments, then construct a voting spreadsheet and distribute to TAC (target Apr 6 for distribution to TAC).

(AI) TAC - by Global Summit have draft charters for a number of the 2016 work plan efforts.

Next Meeting - Thursday, April 14, 2016 - 1 pm ET