InCommon TAC Meeting 2017-04-13

Minutes

TAC Members Attending: Mark Scheible, Janemarie Duh, Keith Wessel, Albert Wu, Eric Goodman, Kim Milford, Tom Barton, Chris Misra (following online notes only)

With: Ian Young, David Walker, Nick Roy, IJ Kim, Dean Woodbeck, Steve Olshansky, Kevin Morooney, Tom Scavo, Paul Caskey

Uncompleted AIs from past calls

(AI) TAC members are asked to review the document regarding TIER and potential changes to Shibboleth and see if there is anything that should be added.

(AI) TAC members should review the charter and membership process prior to Global Summit

(AI) Kim Milford will promote the technical-discuss list among the REN-ISAC community

(AI) Mark Scheible and Ann West will develop an executive summary of the OIDC Survey WG report and recommendations for the InCommon Steering Committee.

Action Items from this call

(AI) ??? (someone) will send a note to technical-discuss kicking off a discussion about requiring HTTPS endpoints for SPs

(AI) Mark and Ann will draft a charter for an attribute release working group, with Mike Grady and Steve Carmody

(AI) Keith asked that TAC members review the current charter of the Deployment Profile WG (which addresses the Federation Interoperability Work Item), since that charter is now several months old, with an eye toward any changes that have occurred in the interim.

(AI) Janemarie will draft a charter for a proposed Service Provider Onboarding Working Group

(AI) Mark/Nick will start a discussion on the technical-discuss list about the Discovery 2.0 work plan item. Perhaps focus the discussion on use cases with a goal of a REFEDS discussion at TechEx.

Ops Update

Domains in Endpoint Locations - As of Monday, April 10, the InCommon RA is no longer validating domains in endpoint locations in metadata. This includes the domains in the endpoint locations in both SP and IdP metadata. Tom Scavo sent a message to inc-ops-notifications on April 7 and has received no feedback from site admins one way or the other.

Incident Response - This is continuing follow-up on the Incident that occurred March 10 when eduGAIN changed the entity order of their aggregate, which caused problems with the InCommon metadata. Ian has been making changes to the metadata aggregator (which will take control of the entity order). IJ is planning to change the process for creating the DIFF, which will prevent the signing process from going awry.

InCommon MDA v7 - A new version of the metadata aggregator is being deployed. See the InCommon MDA v7 Issue List, which lists the changes.

HTTP Compression - We are supporting HTTP compression on md.incommon.org and sent a message to that effect on April 5. This has been deployed on the preview aggregate and the IdP-only aggregate so far, and will be deployed on the main and export aggregates on April 18. Deployment to the fallback aggregate TBD.

Trust and Identity updates

Nick shared the InCommon Software Development/DevOps roadmap for next 6 months. The first set of changes will face the RA staff, then move to the community-facing pages

Shibboleth Consortium (Kevin) - Justin Knight and Kevin presented a webinar about the state of the consortium. 55-60 total attendees over the two webinars. This is a first step in raising awareness of the status of a process of a consistent cadence of communications from the consortium board. HEAnet has indicated that if their managed IdM service takes off, they intend to become a principal member in 2018. Will turn what was a closed meeting for the Shib board at the Global Summit into a public meeting.

Attribute Release Roadmap - DRAFT - Ann presented this to Steering and is looking for comments/review from TAC. This will likely be fodder for an Attribute Release working group, as well.

HTTPS endpoint discussion

The current policy is that endpoints in IdP metadata shall be HTTPS-protected. This includes metadata imported from eduGAIN. The proposal is that all SP endpoints also be HTTPS-protected. Almost all SPs imported from eduGAIN are already protected. Tom has talked to a few site admins who say they would be willing to make this change.

It would be good to develop a summary of why it is reasonable to require this of SPs. While TLS may not be sufficient, it does eliminate risk.

One idea as a starter - require HTTPS of new SPs.

Next step - Let people consider this and bring it up again at the next TAC meeting. We need to have a good story (accurate and with desired end results) before taking this to the community for feedback. Also in the next two weeks start a discussion on the technical-discuss email list.

2017 TAC Work Plan

OIDC/OAuth - Steve Carmody has drafted a proposed charter for an OIDC/Oauth Working Group. He will be sending it to the TAC for review shortly.

Attribute Release - Will spin up a working group. (AI) Mark and Ann will draft a charter. Mike Grady and Steve Carmody have volunteered to help.

Federation Interoperability - Extend the Deployment Profile WG charter to continue with that work. (AI) Keith asked that TAC members review the charter , since it is now several months old, with an eye toward any changes that have occurred in the interim and could affect or add deliverables.

SP Onboarding - Will develop a working group. (AI) Janemarie will draft a charter.

Discovery 2.0 - Nicole Harris has indicated that REFEDS will be doing some work in this area and plans to set something up soon. Tom Scavo noted that InCommon has the largest MD file in the world and so has incentive to move to per-entity metadata to solve this problem. Other federations may not have the same incentive to do this. Nick noted that one of the first priorities for the new DevOps person will be a production per-entity MD server. (AI) Mark/Nick will start a discussion on the technical-discuss list. Perhaps focus the discussion on use cases with a goal of a REFEDS discussion at TechEx.

Once charters are approved, send a message to both participants and technical-discuss lists, partially as a way to drive more subscribers to technical-discuss.

Question - how will we determine the sequencing of the working groups? How many WGs can be simultaneous (also keeping in mind that a lot of people are working on TIER WGs right now)? It is likely that the WG requests will target different groups of people.

Next Meeting - Monday, April 24 - 8 am (F2F at Global Summit)