InCommon TAC Meeting 2016-05-26

Minutes

Attending: Walter Hoehn, Mark Scheible, Kim Milford, Tom Barton, Jim Jokl, Steve Carmody, Ian Young, Janemarie Duh, Scott Cantor, Chris Misra

With: Dean Woodbeck, David Walker, Mike LaHaye, Tom Scavo, IJ Kim, Paul Caskey, Steve Zoppi, Ann West, Kevin Morooney

Minutes from May 17

Approved

Ops Update

Tom Scavo presented the Ops Update and shared a link to the issues that are unresolved or recently resolved.

An incident “Metadata signing process failed (2016-03-21)” has been resolved with a new metadata import and signing process. This process will avoid this problem, which resulted in the process of retrieving metadata from eduGAIN. Coincidentally, the process was put into use on May 20 and it worked.

The ops advisory group has identified four interfederation technical policy rules. These are ready but waiting on deployment:

1. Implement a whitelist of entityID prefixes: “http://”, “https://”, “urn:mace”
2. Filter all imported IdP entities with an endpoint location that is not HTTPS-protected
3. Filter all imported <mdui:Logo> elements (not entities) with a URL that is not HTTPS-protected
4. Filter all imported IdP entities with a faulty <shibmd:Scope> element

Update on Discussion with Microsoft

Nick Roy, Walter Hoehn, and Steve Carmody met with representatives from Microsoft during the Global Summit to follow-up on the interoperability spec and the lack of comment from Microsoft to date. The meeting included three Microsoft reps (education rep, program manager for Azure, and program manager for ADFS). None were familiar with the spec, so the session focused on ADFS and Azure and the mismatch between those products and the multifederation model. The meeting seemed productive as an educational session.

Security Vulnerabilities

There was discussion as a follow-on to the Global Summit discussion about the potential for an InCommon incident response process and the potential removal of entity descriptors or compromised key material from the InCommon metadata. This wa prompted by the approaching end-of-life of Shibboleth IdPv2. Nick drafted a document with the problem statement, the current lack of basis for any such action by InCommon, and a proposed solution.

The TAC proposes this sequence of events:

1. Kim Milford will ask the REN-ISAC technical advisory committee to review the document and make comments and recommendations. Chris Misra and Tom Barton volunteered as resources for questions or other information from the REN-ISAC TAC.
    1. A key question to ask is what actions they believe would trigger this policy
2. TAC will then review the REN-ISAC recommendations
3. TAC will likely propose to Steering a change to the FOPP, either incorporating this document or referring to it.
4. When this policy proposal is sent to Steering, it will include information about which people/groups have reviewed and had input.

At what point would this be vetted with the community (before or after going to Steering)?

TAC also needs to consider how InCommon would recognize the potential security issue and what the incident response looks like - what is the procedure?

TAC 2016 Priorities

At the Global Summit, the TAC asked a subgroup to make a recommendation on to move forward on prioritization (Steve Carmody, Jim Jokl, and Mark Scheible volunteered for the subgroup). The subgroup has met twice and has these recommendations:

1. TAC needs a comprehensive list of what InC intends to do in 2016, not just the TAC work list.
2. TAC should look at the list of priorities developed by InCommon/Internet2 staff and comment the prioritization, whether additional information is needed, and whether any items should be added/subtracted

The goal is to give the community a single InCommon work list that includes the priorities developed by the staff and the TAC work list (and, presumably, any AAC list).

(AI) The subgroup will develop a method for soliciting TAC feedback on the InC priorities list, as well as on the TAC work list.

The suggestion is to look at three topics from the TAC work list in detail: 1) the “gold star program” - which recommended practices are a must?; 2) Support for non-SAML protocols (like OIDC); 3) Per-entity metadata - what is needed to go to production?

Given that TAC has a draft charter for a per-entity metadata working group, and all agree that this should be on the short list of things to accomplish, it was decided to constitute that working group. (AI) TAC will find a chair and constitute the WG.

Next Meeting - Thurs., June 9, 2016

1:00pm ET | 12:00pm CT | 11:00am MT | 10:00am PT