InCommon TAC Meeting 2015-03-05

InCommon Technical Advisory Committee Meeting Minutes

March 5, 2015

Attending: Tom Barton, Scott Cantor, David Walker, Ian Young, Jim Jokl, Nick Roy, Jim Basney,

With: Tom Scavo, Dean Woodbeck, Steve Zoppi, Ann West, IJ Kim, Nate Klingenstein

New TLS Vulnerability

https://freakattack.com/
https://www.smacktls.com/#freak

There was discussion about the new TLS vulnerability “FREAK” that has been commented on this week and whether InCommon operations should probe whether any SPs export ciphers in the TLS handshake. The consensus was that we should inform the community prior to doing such a scan and outline the benefits. This will be considered by the proposed best practice working group.

2015 Projects and Priorities

A small group has been meeting to sort through proposed priorities and develop some programmatic concepts and themes. Ann anticipates presenting a draft to the Steering Program Subcommittee on March 9.

“Using Other Software” wiki page

Tom Scavo reported that the page has been edited after discussion on the participants list concerning the calling out of Active Directory. Tom will follow up with the participants list.
https://spaces.at.internet2.edu/display/InCFederation/Using+Other+Software

REFEDS R&S Migration Strategy

Tom Scavo asked for comments on the wiki page he has developed concerning InCommon’s strategy for migrating to the REFEDS R&S category.
https://spaces.at.internet2.edu/display/inctac/REFEDS+RandS+Migration+Strategy

New Entities recommendations

https://spaces.at.internet2.edu/display/NewEntities/Recommendations

Jim Jokl presented the recommendations developed by the New Entities Working Group. Among the highlights:

1. The anticipated multiple sources of new entity metadata should not change metadata distribution practices
   a. InCommon should continue to provide a single production metadata
   b. It is anticipated that InCommon will continue to operate under one Registration Authority practice
2. InCommon should sufficiently annotate entity metadata so that IdP operators and SP owners can maintain current federation behavior in the short term and subsequently make informed policy decisions as needed
3. InCommon should start to place metadata generated by the Quilt Initiative for K12 entities into the single InCommon aggregate subject to some conditions
   a. There will be several kinds of entities and some may not have signed the InCommon agreement directly
   b. If the legal organization does the equivalent of signing the PA, the registrar will be listed as InCommon
   c. If the organization has not signed the PA, the attribute might be steward.incommon.org or x.regoinal.net, depending ont eh situation
   d. We need an attribute for underage users
4. InCommon should take no special action on proxy metadata entities
   a. Need to make sure no one is proxying around the PA
5. InCommon should provide members with a mechanism to insert additional entity attributes into the metadata to support relationships with other entities and organizations within InCommon and other federations.
   a. Unverified attributes – InCommon takes no action beyond including the attribute in metadata
   b. Verified attribute – InCommon will need a method for documenting who is asserting attribute.
6. InCommon should start importing eduGAIN metadata
   a. Publish a cookbook for how to do Shibboleth configurations to keep current behavior while moving to the new procedure
7. InCommon should allow any authorized Site Administrator to introduce metadata into the InCommon production aggregate”
   a. The entity descriptor will be tagged with the registrar ID of the organization that submitted the metadata
   b. The entityID must be an absolute URL whose host part is rooted in a registered domain owned by the organization that submitted the metadata (as determined by the whois database).
8. Default attribute release
   a. Education and outreach is needed to support new entities and we need to push on releasing an attribute set by default

In summary:

- Metadata distribution is orthogonal to the source of content
- We need to recognize an increasing variety of producers of entities distributed through the metadata
- For different kinds of use cases, we need ways for metadata consumers to distinguish the types of metadata coming through the distribution channel (eduGAIN, Quilt, K-12, a single university, etc)

Next Meeting - March 19, 2015 – 1 pm ET