InCommon TAC Meeting 2017-01-05

TAC Members Attending: Mark Scheible, Jim Jokl, Albert Wu , Mike Grady, Tom Barton, Eric Goodman, Steve Carmody, Keith Wessel, Tom Mitchell, Kim Milford

Others Attending: Dean Woodbeck, Paul Caskey, David Walker, IJ Kim, Nick Roy, Scott Koranda, Ian Young, Ann West, Tom Scavo, Chris Phillips, Steve Olshansky

Minutes from December 8, 2016, were approved.

Per-Entity Working Group Report - Scott Koranda

Scott Koranda, chair of the Per-Entity Working Group, provided a summary of the working group's final report. Scott reviewed the charter, which assumes that InCommon will move to per-entity metadata distribution, with the working group developing a roadmap for moving from the current aggregate model to an MDQ model. This was deemed necessary because of the growth within InCommon (and thus the growth of the aggregate file size), as well as the importing of eduGAIN metadata, which contributed to a substantially larger aggregate. Note: InCommon metadata now exceeds 40MB.

The working group included participation by SAML deployers, software developers, and several federations, including InCommon, JISC, CANARIE, and SWITCH.

In addition to developing a roadmap, the working group was asked to address issues involved with moving to the new model, including high availability, performance, and site redundancy. THe WG was also asked to identify risks and recommend mitigation strategies. Specifically stated to be out of scope was the "discovery problem." Currently discovery assumes you are using the aggregate. T**he WG recommends that TAC charter a working group to address discovery**. Note: Some SPs will not be able to leverage per-entity metadata until the discovery problem is addressed.

Per-entity MD distribution comes down to an entity querying for the MD that it needs at the moment, a process similar to using DNS.

High availability - An advantage of the aggregate model is that most entities have already downloaded the aggregate, so if InCommon has a service interruption, it will likely have minimal impact on local operations. With MDQ, however, the SSO flow will stop with a service interruption. Section 7 of the report recommends a requirement of 99.99% availability, which translates to 4.3 minutes of downtime per month.

The working group identified two potential architectures for MDQ: 1) a CDN (content delivery network) distribution; or 2) a more traditional server-based distribution. Most CDNs have a 99.9% availability, which translates to 43 minutes per month, which the working group deems unacceptable.

Risk - The working group identified these risk parameters:

For a campus using the InCommon MDQ server, a service interruption would affect both on-campus and off-campus services. This is a change from the aggregate model.

For the MDQ service, the much higher volume of queries (compared to the aggregate structure) means an increased security risk, such as potential vulnerabilities to man-in-the-middle and other types of attacks. The Shibboleth developers have deployed most of the necessary changes in this regard with the release of IdPv3.3. The WG has also made the SimpleSAMLphp (SSP) developers aware of the changes that would be required. **The Working Group recommends that InCommon formally request the required changes of both the Shibboleth and SSP developers.** Some software (such as ADFS) may be more problematic.

Scott also noted that the MDQ protocol includes criteria that should be addressed by the Deployment Profile Working Group.

Because of the nature of MDQ (as opposed to the aggregate model), local caching intervals may need to change. InCommon should be ready to educate participants and document and track this potential issue.

Please see Section 9 of the report for the recommended roadmap.

Nick Roy confirmed that InCommon operations had substantial involvement with the working group and its report, and there are no concerns about the recommendations or timelines.

Chair Mark Scheible asked for any objections to TAC accepting this report and recommending its acceptance by InCommon Steering. Hearing none, the report is accepted by TAC.

(AI) Mark and Ann will collaborate on developing a summary and proposal for InCommon Steering to address at its meeting on January 9. TAC members suggested calling out a few items:

1. A need to ask the SSP and Shibboleth developers to make the required changes
2. Demonstrating that the MDQ plan has budget implications
3. Education about the need for MDQ, the impact on InCommon operations, and the risk involved in doing nothing
4. The planning and communications that will be required

Global Summit 2017

An informal poll shows that there will likely be a critical mass of TAC members at the Global Summit, so a face-to-face will be scheduled. (AI) Dean will submit this to the Global Summit program committee.

Ops Advisory Group Background

Nick provided a summary for the new TAC members. The Ops Advisory Group was created last year as a sounding board for Ops, with a focus on technical changes. Send Nick and Tom Scavo a note if you are interested in being added to the list (or if you know of people who you'd like to see on the list).

Ops Update

Tom Scavo has developed an Ops Update and will provide a summary on the email list. The update is here.

InCommon Staff Planning

InCommon staff met in early December to lay out operational goals for 2017.

Governance Update

Ann provide a summary of the governance and advisory group changes that will happen this year in Trust and Identity. Currently InCommon has the Steering committee and TIER has the TIER Community Investor Council (TCIC), which is roughly analogous to Steering. Since Trust and Identity is now an Internet2 division, there is a requirement to have a PAG (Program Advisory Group) that looks at all things Trust and Identity. The plan is to morph Steering and TCIC into this PAG.

On the technical advisory group side, TAC will continue in its role, but a new group architectural group, CACTI, will form as advisory to the PAG and to replace the current TIER Ad Hoc Committee. The community consultation on the CACTI charter is closed and the charter is expected to be finalized soon, which will be followed by recruiting members.

OIDC Working Group

Albert reported that the survey, sent on Dec 22 - has had 40 responses. A second and broader request to complete the survey was sent today..

Next Meeting - Thursday, January 19 - 1 pm ET