2017-01-09

Attending: Dee Childs, Michael Gettes, Marty Ringle, Ted Hanss, Michele Norin, Ann West, Sean Reynolds, Dave Vernon, Dennis Cromwell, Celeste Schwartz, Melissa Woo

With: Kevin Morooney, Steve Zoppi, Mark Scheible, Von Welch

Items approved via the wiki since the December meeting

1. December 5, 2016, minutes approved
2. Baseline Expectations for Trust in Federation resolution approved

Welcome

Kevin Morooney welcomed Marty Ringle and Dee Childs as the new Steering members and expressed appreciation for their agreeing to serve. All of the Steering members introduced themselves.

Officer Nominations

The deadline for officer nominations is 2 pm (ET) Weds, Jan. 11. Once nominations close, Kevin will contact the nominees to see if they are willing to be nominated, then we will set up an online voting process.

Per-Entity Working Group Report

TAC has approved the report of the Per-Entity Working Group (WG) and is bringing it to Steering for information. The working group was formed to provide recommendations on a different way of maintaining the trust registry and delivering the metadata. InCommon currently delivers an XML file aggregate of all of the items in the trust registry. With the growth of InCommon and our participation in eduGAIN, the aggregate file has grown large and it now takes a significant amount of memory to verify the signature of the file.

The WG and TAC recommend that InCommon move to a per-entity delivery (also called Metadata Delivery Query, or MDQ) of the metadata, meaning that an Identity Provider or a Service Provider requests and receives only the metadata they need, rather than the entire aggregate. The summary and recommendations of the WG are here: https://spaces.at.internet2.edu/x/JAdhBg

The full WG report is here:
https://spaces.at.internet2.edu/download/attachments/98992975/FinalReportofthePer-EntityMetadataWorkingGroup.pdf?version=1&modificationDate=1481896602337&api=v2

The Working Group recommendations also include:

- Availability/Uptime of the MDQ service should be at least 99.99%.
- Utilization of InCommon's MDQ service will require reconfiguration of participants' Identity Providers (IdPs) and Service Providers (SPs). InCommon should provide communication and education to facilitate that work.
- SAML implementations other than Shibboleth and SimpleSAMLphp (e.g., Microsoft ADFS, Ping Identity, Ellucian/WSO2) will likely require community pressure to support federation-distributed metadata and per-entity distribution functionality.
- The per-entity metadata support in Shibboleth and SimpleSAMLphp should be enhanced to mitigate the effect of network and service outages and slowdowns affecting InCommon's MDQ service. InCommon should advocate resources and community support for those efforts.

Keys for Steering:

1. Note that Shibboleth is used by more than 90% of InCommon Identity Providers and the software supports MDQ, but not quite in the way we would like (for instance, there are some caching recommendations that Shib does not support). The Shibboleth Project is aware of this.
2. The other open source Identity Provider software is SimpleSAML.php. These developers are also aware of the WG report.
3. There are commercial providers (as noted above) that do not support MDQ. InCommon and the community will need to come up with a plan to deal with these instances.
4. InCommon intends to run the aggregate and the MDQ in parallel for some time to come. MDQ will increase InCommon's costs substantially because of the uptime requirements, which are much different than publishing an XML file once a day.

Question: Will the MDQ service be used and/or integrated with the other federations around the world. Answer: the UK federation is already in production with MDQ. The UK and InCommon have the largest scaling problems, because we are much larger than the other federations. We will use the same protocol as the UK but host and deliver the service in a different way. We plan to rely on each other for back-up, helping achieve the required uptime.

To achieve the 99.99% uptime, InCommon also intends to ask for an update to Shib to support caching and the other requirements, and is looking at a content delivery system (CDS) with multiple points on the network to help prevent outages.

The WG also recommended a follow-on working group to look at the problems with discovery. That would likely be a TAC-sponsored working group, but the international REFEDS organization is also considering such a project.

Attribute Release Policy

Steering passed a policy on April 6, 2015, encouraging the release of a minimal set of attributes (those specified in the Research and Scholarship Category), to make things easier on research and science collaborations. We intend to return to this issue during 2017. Von mentioned that there is a large amount of inertia to get campuses to release the necessary attributes and it is time for InCommon to require the release of such attributes.

Steward Program

Ann and Mark reported that the Steward Program is now in the proof-of-concept phase with MCNC, following a two-day kick-off meeting at the MCNC offices in Research Triangle Park, NC. The Steward Program allows a regional (like MCNC) to perform the organizational and individual vetting for K-12 and community colleges in their service area.

Next Meeting - February 6, 2017 - 4 pm ET