LInk to 2020 ACAMP wiki

Title: SPOG Should we try to do anything specific (service provider operating group)

Advance CAMP Friday Nov20,2020

10:05--10:55 am ET

Room - Arts & Crafts

CONVENER: Laura Paglione

MAIN SCRIBE: Jim Basney

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 8

DISCUSSION:

- Laura experienced challenges with the ORCID SP. Other SPs have similar experiences, particularly the smaller ones. Needed a group for SP-specific discussions among SP operators, so SPOG (Service Provider Operators Group) was born. Inspired by FOG (Federation Operators Group). About 65 people on the SPOG mailing list (https://lists.refeds.org/sympa/info/spog). Mailing list is relatively quiet.
- Could we do more outreach about the SPOG list? Some promotion on general mailing lists, but a lot of those SPs are not on those lists. Asked federations to promote to their SPs, but not sure how much this is being done.
- How about sending email to the SP technical contacts from metadata to invite them to join the SPOG list?
- Laura talked to the SPs at TNC in Estonia. Interested, but they weren't the ones involved in day-to-day SP operations. How do we reach the technical SP operators?

- The error-url is a good technical topic to discuss on the SPOG list. We need the software integrators to support error-url. Communication can go through the SP operators.
- Is there an IdPOG? No that we're aware of. The IdPs seem better represented in general federation channels.
- "The federation is the IdPs… and then there are some services…"
- IdP operators have more wide range purposes. SPs are clustered into local groups.
- Many SPs might have to deal with only 1 or few IdPs.
- MFA is a good topic for the SPOG list. What do SPs do when MFA fails? Fail open?
- SP directives include FIM4R, FIM4L. What are similarities/differences? Universal truths? General requirements for SPs?
- There are so many SPs. The weight of the broader group could facilitate change faster.
- When SPs are forming (initial implementation), they have problems. Invite new SPs to the SPOG list?
- Some federations have an announce list.
- Even if you're R&S, there are still problems. Update from IdPv3 to IdPv4.
- Usually once it's up and running, it's OK.
- Test suites that SPOG might advocate for? Some federations have a non-production feed that entities go into before being tested. InCommon doesn't do this, though. Session earlier this week about a test federation / sandbox. The SP is scanned before being added.
- Chris: Building the NIH test page for MFA and assurance was difficult. Not many good examples. CILogon helped. Having a testbed would help, that includes ADFS, Okta, etc., would help SPs test before they deploy.
- How about https://samltest.id/? Doesn't help with ADFS testing. Lack of tooling in the MFA environment.
- OpenID Connect test suite (https://openid.net/certification/) is nice. Need something like that on the SAML side.
- This requires funding. Global issue. Could NSF or EU subsidize? AARC (https://aarc-project.eu/) was an EU funded project that included testbed activities.
- Plenty of test services in InCommon right now. To meet new Baseline Expectations, it will be interesting if they're upgraded to meet the baseline or if they get pulled out. What makes the cut.
- SP operators may have a lot of questions related to Baseline Expectations. SPOG could help.
- Interest in pursuing one of these items?
- Huge demand in pursuing federated identity. Test infrastructure is needed.
- SWAMID has some federation test tools for IdPs but not SPs? Testing R&S and COCO is for the SPs - so they get the attributes they need. The purpose of the federation is so users can log in to SPs. -Fredrik :)
- Will SPs trust a "test" IdP? NIH has a dev/QA/prod environment.
- ORCID experience: In beginning expect to troubleshoot, but then later, trouble happens when an IdP changes something and it impacts the SP. The IdP may know what ORCID needs, but there's no good way for the IdP to test that their change continues to give

ORCID the attribute it needs. Issue with unique IDs from IdPs caused an ORCID security issue (see InCommon security incident write-up).

- There is still no way for the IdP to know if they have made a mistake in config of an upgrade or change, no place to test the response of the SPs to mistakes in the identifiers
- This occurs during upgrades and other times. For example, adding ePTID to comply with R&S. Does this get announced? Without an alert, the SP is surprised.
- SPs tell each other when they detect something - I saw an issue, heads up - you may see it too.
- Challenge: so many SPs, so many areas of federations
- IdP doesn't know which SPs use which identifiers. IdPs need to release identifiers properly. When ORCID detected the IdP problem, that impacted other SPs.
- Need to help IdP check for issues when they change configuration / upgrade.
- Federations could charge for the testbed service. Big IdP/SP might be willing to pay for that service to defray the costs of offering it.
- InCommon is teaching us that IdPs won't do the right thing until it is required. Baseline Expectations is the lever. No carrot, only stick? BE is the stick. NIH is a carrot? Define "Ready-for-Research" Expectations?
- How can we put R&S in Baseline when it requires deprecated ePTID?
- Example: https://release-check.swamid.se/ and https://ladok.release-check.swamid.se/
-
-

POTENTIAL ACTIONS

- ❏ Increase SPOG participation: Mail the technical contacts from SPs to invite them to participate on the list.
- ❏ When there is a new registration as an SP - send out an announcement then to invite participation in SPOG
- ❏ Define a set of criteria/guidelines that would need to be included in testbeds that include items important to SPs
- ❏ MFA - are there any universal “truths” about the needs of SPs?
    - ❏ Setting up a full IdP/SP test environment can be a barrier to to entry - get an external funder to support this work? Who would be interested? What would need to be presented? To be tested:
- ❏ Send a notification to SPs when there is an IdP configuration change
- ❏ There are some specific identifiers that are identified as appropriate for account linking. If IdPs are not using them properly and not testing for consistency and correct use during EVERY change, they should not be releasing them at all. Advocate for this.
- ❏ Suggested use - see a problem, use the list to alert others.

REFERENCES:

- ORCID's Attribute requirements statement: https://members.orcid.org/api/integrate/institution-sign-in - would be great to supplement this with an IdP