Return to Advance CAMP wiki

Advance CAMP Wednesday, Sept. 28, 2016

3:30pm-4:20pm

Star/Palm Room

SP Registration Requirements / eduGAIN

CONVENER: Randy Jones, CAF

MAIN SCRIBE: Eric Goodman

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES:

Harry Lalor, SheerID, Inc.
Nick Roy - InCommon/Internet2
Eric Goodman - University of California

DISCUSSION:

Separate issues noted:

1) What is required to add entities to a federation
2) InCommon's business model is to charge "per registered entity"

Both related to the question of getting SPs into eduGain and needing to register in multiple federations.

There are IdPs in InCommon that block eduGain publishing, and they don't read non-InCommon registered entities, so the SP needs to register in multiple places.

Similarly, some SPs are publishing distinct entityIDs per client, and those make no sense to publish in InCommon (unless they open that instance of the service to other eduGain members).

Australian federation charges vendors, but not education/research institutions. They will allow R&S entities in through eduGain, but not vendors.
Question: what happens if the SP has to pay to join InCommon, pay to join eduGain, pay to be imported into AAF?
Answer: That's a cost of doing business to the vendors.

(Currently eduGain does not charge end points.) If eduGain charged, should that be paid by endpoint or by the participating federation?

Vendor present noted that cost per federation is not much of an issue (as long as not onerous). Even being charged by eduGain, if there's an incremental value, is not an issue.

Discussion of what is being charged for. Some comparisons of the entityID discovery to DNS, IANA, etc. and those behave differently (financially). Don't want we to make these easier?

InCommon got "thrashed" for "censoring" metadata by not importing entity attributes. Could be messy to also start charging. And SPs/IdPs can get the metadata from the direct source...it's extra work and messy, but it is technically feasible.

If no entityIDs can flow (if there's nowhere for an entity of a certain type to go), that's a non-scalable solution.

What is our consistent guidance to SPs that is stable? Regional registration vs. global registration (eduGain) vs. clearinghouse approach (third party that registers you in all regional federations).

Example from Shel: 150 SPs that want to participate in eduGAIN federations at scale. SPs ask: why is NET+ requiring us to join InCommon when I already publish in eduGAIN.

Current advice from Nick is "register in InCommon, check 'export to InCommon', wait a week and look in MET to see where you are listed" to figure out how where your metadata flows.

InCommon CIO focus is frequently more about gaining access to cloud vendors (box, etc) rather than research, which is a different focus.

Sticky "how do we reduce the allure of bilateral agreements".

If you care just about key revocation, then you should want multi-lateral. If it's point to point (and esp where entityID/URLs are unique to the client) and key management isn't the focus, then it's

harder to justify getting people to join. More of an issue for University systems (like Univ of California) where what's needed is really the whole saml2int stack.

Still largely a focus on value statement. What's the value of relying on multilateral federation?

ACTIVITIES GOING FORWARD / NEXT STEPS:

Bring the topic of entity republishing/not republishing from upstream, chargebacks, consistency to eduGAIN steering for consideration. Difficult area, needs more clarity. Likely need to get problem description from Shel. Example of SheerID / Harry Lalor - joining a ton of federations because the entities aren't getting uniformly replicated.