Email string regarding SAML readiness

———

All,

Mary McKee sent me email outlining some significant challenges at Duke regarding their support of “federated” access. Her thoughts below are way more interesting than my replies so I’m hoping to engage you all in this existential thread that Mary has started.

See comments in line.

From: Mary McKee <mary.mckee@duke.edu>
Date: Thursday, February 13, 2020 at 8:59 AM
To: Ann West <awest@internet2.edu>
Cc: Albert Wu <awu@internet2.edu>
Subject: Re: SAML readiness

Hi Ann,

In a nutshell, here are the issues we're seeing with Microsoft:

· A proliferation of usage and marketing around federated services, where "federation" is defined as a network of Microsoft's own products and customers. This is paired with promises to our stakeholders (which they are increasingly finding compelling) of seamless integration with peer institutions for the purposes of research and academic collaboration that sidesteps InCommon completely.

If we wanted to do an education campaign, how would we reach your stakeholders and who are they? What might the message be? Does the “seamless integration” with peer institutions working for them?

- Academic community representatives with Microsoft who have never heard of InCommon (among the last dozen I've talked to, 0 were familiar - I would like to ask Microsoft to not send us another higher ed rep who is not conversant on InCommon and eduGAIN, but that is contingent on whether it's going to be worth it to have a larger conversation at all).

MS has a huge turnover and our space is small compared to their global markets. In our experience, we’ve had to educate and re-educate every time we get a new rep. MS is not alone in this and given your preceding point, one can see why they don’t really care. They want to own our space on their own terms. How do we make a case to them that they should care?

· An uptick in SSO requests by the Duke community for vendor solutions that support plug-and-play integration with Microsoft services. Our OAuth-to-SAML investment (intended to make SAML as viable as possible in as many cases as possible) has not paid off the way we'd hoped, because what vendors are supporting is "OAuth through Azure" or "OAuth through Google".

To me, this is simply another side of the "make SAML integrations more straightforward with vendors" problem - the competition is getting ridiculous, because plugging into Microsoft is extremely objective and straightforward and plugging into SAML means a lot of different things to different schools (including, admittedly, Duke). The conversation is now to a point where I feel that being a good federation participant means telling my stakeholders that they are not allowed to use a free, instant integration with infrastructure that Duke does possess because we're committed to a process that will cost them more money and take us more time to turn around.

The no-limit poker player in me is feeling that my chip stack is dwindling to the point where I have to go all in on my next good hand or I won't have any meaningful influence over the table at all. Microsoft is willing to hear our case on needs to engage with their services in a way that does not undercut our commitment to InCommon, but so far I have failed to drum up any level of feedback from the community on how to go about this that would make such a conversation productive.

The vendors want to own identity of their customers and because they are providing “valuable” services, users are willing to let their privacy go for ease of use, access, etc. It’s not in MS’s interest to integrate with us in the way we would like.

How do we make our stuff “extremely objective and straightforward “? Given that is the competition, what steps should InCommon take to make integration as easy as possible? That IS a TAC discussion that could be done with CACTI too. Regarding your communications point, do we start educating stakeholders about corporate control of identity? Do they care?

Microsoft services are currently in use at Duke for mail and some collaborative tools. We do not use them as an enterprise authentication solution, and we are using Shibboleth for O365 login via ECP. This approach is currently under fire due to its limiting effect on integrations with other desired Microsoft products, and if we can't prevail in those conversations, I don't see us holding off requests to use Microsoft for SSO on other enterprise products for long. I've approved two such exceptions this week (under duress), and am hoping that the community chooses to rally on this one before the choice is made for us.

Is your point more that we are slowly outsourcing key pieces of our IAM infrastructure to vendors, whether we like it or not? That becomes a business risk issue for Duke. Can we stop or slow it? Do you believe you have options?

As an intellectual exercise, if we decide that we can’t influence the vendor market, what are we left with? What are our options now? What do we need to protect and focus on as a community?

Hope that helps,

Yes it does. Thanks for sharing your ideas and taking the time to do so.

Ann

Mary

From: Ann West <awest@internet2.edu>
Sent: Wednesday, February 12, 2020 5:30 PM
To: Mary McKee <mary.mckee@duke.edu>
Cc: Albert Wu <awu@internet2.edu>
Subject: Re: SAML readiness

Hi Mary,

Thanks for your thoughts and suggestions about the vendor risk assessment profile. I could see this being used/added to the IdP portion of the InCommon wiki when we cover working with service providers. I've cc'd Albert to get his thoughts on whether I'm nuts or it makes sense.

Regarding Microsoft, what were your specific issues that you raised in the hallway at CSG? My apologies but I can't remember the detail now. Does advocating for common values mean an outreach and comm campaign to the campuses about how they should talk to MS? And then an action that MS can take? What are the specific things you'd like to see?

Thanks also for your patience!

Ann

From: Mary McKee <mary.mckee@duke.edu>
Date: Thursday, January 23, 2020 at 9:44 AM
To: Ann West <awest@internet2.edu>
Subject: SAML readiness

Hi Ann,

Sharing the form we've introduced into the vendor risk assessment process at Duke:

https://duke.app.box.com/v/shibbolethReadinessProfile

Prior to introducing this form, our biggest pain point in IAM operations was dealing with departments who entered into a contract with a vendor who claimed to support SAML2, but with a number of nasty surprises (security concerns, custom attribute needs that would create overhead and complexity in our environment, etc) that made the implementation dangerous and/or labor intensive.

Simply introducing this form into the vendor assessment process has solved this problem for us. Duke departments are able to sidestep vendors with poor SAML implementations and we have better positioned Identity Management as a facilitator of business rather than a barrier to business. We can now better protect our architecture and security posture by not inviting political situations that will likely end with compromises we don't want to make.

Although our operational issues are now resolved, so many other schools have asked us for this form that I can't help but feel that it's a real missed opportunity that we aren't pushing for (optional) adoption of a shared one. I wish that the takeaway when a vendor doesn't pass Duke's risk assessment is not that the product didn't meet a Duke requirement, but that it didn't meet a common R&E best practice that will very obviously affect marketability to a range of customers rather than just one.

The lukewarm reception from TAC has me inclined to give up on this, but before I do, I wanted to put it out there in case there is a good place for this to get picked up. This may seem distinct from my Microsoft small-f federation problems, but to me, both are examples of places where InCommon could support institutions in supporting InCommon by helping us use common language to express common needs to advocate for common values. Microsoft is willing to listen to us, but what should we be saying?

While I can appreciate that many IAM teams may feel limited in their ability to influence business at their institution, I have to think that I'm not the only University IT person who feels very empowered to influence change, and a little more guidance/support about how to amplify InCommon's messaging would go a long way in helping us be good federation participants.

Thanks for listening!
Mary