Clarify options for sites not using Shibboleth or SimpleSAMLphp

Subject:	Fwd: [InC] The InCommon Per-Entity Metadata Working Group's final report is now open for community review
Date:	Tue, 22 Nov 2016 09:19:29 -0600
From:	Tom Barton <tbarton@uchicago.edu>
To:	Scott Koranda <skoranda@gmail.com>, David Walker <dwalker@internet2.edu>, Ann West <awest@internet2.edu>, Steven Carmody <steven_carmody@brown.edu>

Hi guys,

I really like this report: detailed, thorough, and clear. Thinking about the roadmap and lack of capability of some vended SAML products, either to perform MDQ, to consume an aggregate, or to consume an aggregate large enough to work in current interfederation, I wondered what should be our message to sites relying on anything but shib or ssp. Change your software? Change your software and TIER will have made that a much easier task than previously? Leave the federation? Hire yourself a consultant like Scott to build a work-around for your site? Don't worry, this time the vendors will all listen to us and do exactly what we say? :-)

We should probably have thought this through a bit before releasing the report or risk some substantial stakeholders believing that we will leave them out of our future.

If you agree, my question is whether the WG should think about this or some other group should focus on it.

Thanks,
Tom

Subject:	Re: Fwd: [InC] The InCommon Per-Entity Metadata Working Group's final report is now open for community review
Date:	Tue, 29 Nov 2016 00:26:42 -0600
From:	Tom Barton <tbarton@uchicago.edu>
To:	David Walker <dwalker@internet2.edu>, Scott Koranda <scott.koranda@ligo.org>
CC:	Ann West <awest@internet2.edu>, Steven Carmody <steven_carmody@brown.edu>

Hi David and Scott,

Yes, adding the paragraph Scott suggested would address the question I raised for the purpose of the WG's report.

Thanks,
Tom

On 11/28/2016 11:11 AM, David Walker wrote:

> *Catching up after the long weekend...*
>
>> 1. *Tom, do you mind if I add this thread to the wiki page that was set up for community review?*
>> 2. *Regarding software support for MDQ, the group did have a little discussion of software that might be closer to supporting MDQ than the aggregates (ADFS?), but in general, the software that isn't expected to support MDQ doesn't support any kind of federation-distributed metadata, anyway. MDQ as a new option for retrieving metadata doesn't change that.*
>
> *David*
>
> *On 11/23/2016 10:11 AM, Scott Koranda wrote:*
>
>> ```
>> Hi Tom (and all),
>> ```

> > I wondered what should be our message to sites
> > relying on anything but shib or ssp.

Are you suggesting that we include in the report a paragraph
(or so) that specifically gives some guidance to those sites?

I think that would be fine.

> > Change your software? Change your software
> > and TIER will have made that a much easier task than
> > previously? Leave the
> > federation?

I think any text we add can detail that the working group
reached out specifically to Ping Identity and Microsoft and
that representatives from both projects are aware of the
working group's and InCommon's efforts and plans around MDQ.

Neither reported that at this time their organizations have
specific plans to support MDQ.

I think the text should then go on to specifically recommend
that sites get in touch with their vendors and direct them to
the working group report and ask their vendors for guidance.

I could imagine a last sentence in that paragraph that says something like

"We remind sites that operate SAML software stacks other than Shibboleth
or SimpleSAMLphp that only those projects have historically
and consistently supported in a timely way functionality
highly desired for the best interoperability in the higher
education and research federations."

> > Hire yourself a consultant like Scott to build a work-around for
> > your site?

To be clear, my participation in the working group has been
directly sponsored by and funded by LIGO. I prefer to keep my
participation in that context. Thanks.

> > Don't worry, this time the vendors will all listen to us and do
> > exactly what we say? :-)

I don't think the working group report is the right place to
rehash the history or vendor support (or lack thereof).

That could be, however, an interesting output for another
working group devoted to that singular issue--provide clear
and detailed documentation of what products supported what
functionality at what time.

I expect campuses might find that a useful tool.

> > We should probably have thought this through a bit before
> > releasing the report or risk some substantial stakeholders
> > believing that we will leave them out of our future.

The report calls out in the executive summary that community pressure will be necessary to cause Ping and others to support MDQ.

Later in the roadmap, specifically in the "Longer Term" section the report suggests InCommon develop a plan to retire aggregate distribution "in the 36-48 month time frame, depending on how vast that majority is". Here the "majority" are those IdPs and SPs that have migrated already to MDQ.

Taken together I think that signals clearly to sites operating other stacks that there will not be any immediate or even short term risk that they will be "left out".

I would be surprised if you receive any feedback from substantial stakeholders that they feel they are at risk due to the timeline in the report.

> *If you agree, my question is whether the WG should think about this or some*
> *other group should focus on it.*

I agree that we could add a paragraph specifically addressing sites that run other stacks, as I indicated above.

Other then that, I would like to see this working group complete its task, deliver the report to TAC, and then end.

If the TAC (or some other group) wants a more detailed roadmap developed for such sites I suggest it be done by another working group.

Thanks much for your feedback.

Cheers,

Scott K for LIGO