Comments from Allan Kim - 2016-04-25

From: UC Identity Management Discussion Group List [mailto:UCIDMGMT-L@LISTSERV.UCOP.EDU] **On Behalf Of** Kim, Allan
Sent: Monday, April 25, 2016 10:25 AM
To: UCIDMGMT-L@LISTSERV.UCOP.EDU
Subject: Re: UC Trust Agenda for 2016-04-21 2-3PM

Comment on the MFA interop profile draft: I like the concept but I think implementation is awkward with the default Shib 3 config and flows. The standard recipe seems to be MCB with initial authentication flow. This means setting idp.authn.flows.initial, which is a global setting that effectively clobbers any SP-requested authentication methods. The recipe probably works for most use cases but you lose potential flexibility.

Also note that when configuring an SP to require a specific auth method it's not enough to configure a requested authnContextClassRef as this can be overriden with the right parameters to the login initiator. This should be combined with a matching AccessControl rule or equivalent.

From: Eric Goodman [mailto:Eric.Goodman@ucop.edu]
Sent: Monday, April 25, 2016 12:00 PM
To: Kim, Allan <jak009@ucsd.edu>
Subject: RE: UC Trust Agenda for 2016-04-21 2-3PM

I assume you're fine with me forwarding the comments along to the MFA interop group?

Good point about the AccessControl rule guidance.

On the other point; I agree some of it is awkward; part of that is lack of knowledge of what the other side "wants". The solution doesn't require MCB, the reference intends to call out that if an IdP separately supports MFA and PasswordProtectedTransport responses, that MCB like functionality can be used to allow MFA to also meet PPT rather than requiring a separate authentication event (presuming the MFA solution is "PPT plus a second factor" of course).

--- Eric