Notes-ConferenceCall-March-28-2011

notes, social identity call, 3/28/2011

TOPIC -- Mgmt: Assessing Risk: Matching Technologies to Resource Access Risks

Dedra pointed the group toward OMB 04-04

http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

which is the foundation for the US Federal government's work on risk and Levels of Assurance. Section 2 contains useful suggestions on how to assess risk. It identifies several categories, and provides guidance on mapping low, medium, and high risk in these categories to an appropriate required LoA.

Inconvenience, distress or damage to standing or reputation
Financial loss or agency liability
Harm to agency programs or public interests
Unauthorized release of sensitive information
Personal Safety
Civil or criminal violations

There was a brief summary of how InCommon Silver and Bronze map to NIST Levels 1 and 2, and the business process that results in IC asserting that a campus meets teh Silver criteria (ie campus IT organization writes up why it thinks the campus meets silver criteria; auditor reviews that document and the policy, business practice, and technology the campus uses to meet the criteria; auditor writes letter with opinion as to whether of not the campus is meeting the criteria; if letter is positive then the letter is sent to IC; IC reviews the letter and decides whether or not it i sufficient.)

Discussion followed about current situation. Dedra asserted that SPs would want to differentiate social loa 1 identities form campus asserted loa 1 identities. There was also discussion of account linking -- linking a social identity to a campus-asserted silver account -- would this process have any impact on loa of social account ? CONSENSUS -- NO

Steve Massover asserted that loa is orthogonal to differentiating social vs enterprise identities. He suggested that the key issue is whether the identity provider "in a trust federation" vs not a member (where trust federation currently means a higher ed trust federation, rather than something like OIX). Nate and Keith agreed.

-- Nate suggesting that metrics we're trying to use may not be sufficient to the problem at hand. Socials are on loa 1 today, but equifax and paypal are aiming higher. The conversation might be better framed around metrics that were sufficiently granular to allow differentiating social from enterprise level 1; the group should explore ways to express the difference.

keith -- won't have loa 1.5 available to us anytime soon

mention that google may at some point begin asserting that an authentication event was done with 2-factor; it was noted that this was technology, not LoA.

CONSENSUS -- relying parties will want to know more than just the LOA.

CONSENSUS -- IDPs will probably have to assert LOA, may need to also assert social vs enterprise

What needs to be asserted ?

-- Nate suggested that SPs should NOT care about the protocol; they should only care about something akin to LOA
-- Dedra stated that her SPs want to know that if this is loa 1 and a social identity...
Nate -- GW could say "we don't know whether this authn was done over ssl"
Keith -- likes Chris' approach of asserting NO LOA (just missing)
Steve C -- SPs won't implement complex algorithms, just a couple of differentiators
Steve M -- agree, anything more complicated is probably beyond them at this point.
Steve C, Steve M -- over time, this will change, but now is not the time to provide or use any more finer grained differentiator...

CONSENSUS -- seemed to be "if provider asserts LoA then the GW should pass that value through; the GW should not attempt to develop or compute an LoA based on the information available to it; the GW SHOULD assert whether the identity provider is a social provider or a campus."

TOPIC -- Mgmt: Tradeoffs: How Do I Choose My Approach

Quick notes on protocols used by various social identity providers:
yahoo is an openid provider
google can be an openid provider, and they will accept openid from yahoo;
facebook is oauth; however, they don't force their users to use ssl (use ssl during authn, but not during session, so others can hijack the session cookie)

How can SPs actually use these providers? What PII does each share ?
-- Chris Hubing has doc on what his SP accepts from various providers, and his algorithms
https://wikispaces.psu.edu/display/EmergingTechnologies/OpenID+Implementation+for+WikiSpaces

-- only accepts if email address matches domain name
-- some people are willing to vet people out of band, and accept that, even if they don't match; Chris won't accept that, tho
-- Chris's GW doesn't pass any LOA INFO RIGHT NOW
Dedra stated that the info provided by the social providers dedra needs to be mapped to something that business partners can understand.

-- The role of facebook privacy settings, controlling what gets shared with who, was noted
-- Chris has an app that will ask facebook for everything it can share...

AI -- Dedra will take a first cut at language differentiating social loa 1 from campus loa 1

AI -- group -- the group should explore ways to express the difference between social and enterprise level 1.

AI -- Nate to share url's for other LOA frameworks.