Social Identity - A Path Forward

Social Identity: A Path Forward

Social Identity was a hot topic at Identity Week in San Francisco last November. Some of the participants questioned the wisdom of Social Identity in the first place: Do we really want to give the keys to the kingdom to Google? Wouldn't it be in the Federation's best interest to continue to encourage campuses to deploy their own IdPs?

I think we can have our cake and eat it too if we properly limit the scope of a centralized Social Gateway for all InCommon participants.

First, what problem are we trying to solve? The primary motivation for a centralized Social Gateway is to attract Federation-wide SPs to join InCommon. Jim Basney says it best: Given the current penetration of InCommon within US higher education (approximately 20% of US HE institutions operate InCommon IdPs), a "catch-all" IdP is essential to provide a complete federation solution. A Social Gateway would go a long way towards filling this gap.

Second, what problems are we trying to avoid? Most importantly, we want campuses to continue their orderly transition to a federated environment, and so a centralized gateway should not be seen as an alternative to deploying a local IdP.

Not surprisingly, there is also a privacy concern. Like most other Social IdPs in this post-Snowden era, Google is seen by many as a privacy risk. To minimize this risk, we can (and should) limit the attributes that transit the gateway regardless of the attributes Google actually asserts. Moreover, note that a social gateway is inherently privacy-preserving in the sense that it masks (from Google) the end SPs the user visits.

With that background, consider the following proposed centralized Google Gateway for all InCommon participants:

- lightweight deployment
- reassert email and person name *and that's all*; any other attributes asserted by Google are routinely dropped on the Gateway floor
- manufacture and assert ePPN at the Gateway
- no extra attributes, no trust elevation, no invitation service

Such a gateway can not be used in lieu of a campus IdP. If a campus wants to go that route, presumably it can deploy a campus-based gateway on its own.