Social2SAML Issues of Gateways and other Solutions

#	Issue	Comment
1	Social Provider Policy (SPP)	What policy does each of the social providers put on proxies between the IdP and ultimate SP? The gateways are proxies in some sense in all models before us, though Roland Hedberg's model ultimately connects IdP and SP on the basis of the SPs credentials.
2	SPP	Will each social IdP have to be scrutinized by the legal team for the Gateway operator?
3	SPP	SPP policy must be assumed to be susceptible to change
4	Multiple IdPs per user	As insurance agains a social IdP "going away", users should register with more than one
5	Need for account linking	If users have more than one IdP (social or otherwise), they may forget which one they used to access a given resource. Without some form of self-service account linking this problem is hard to solve
6	Instability in provided attributes	Attribute values from an IdP may change at whim of social provider
7	Minimal reliance on social IdP	As a general principle, the less dependent systems are on the social IdP the better. Authentication plus an undecorated identity are the smallest set of useful things a social IdP can provide; Raises the question of the value of the gateway service: Is getting out of credential management a big enough win to support social2SAML gateway services?
8	Lightweight gateway	As a general principle, gateways should be designed to be as lightweight as possible
9	Conflicting principles	Principles 7) and 8) are incompatible in practice
10	Central service or shared code	Either approach would yield valuable commonality of practice
11	Same IdP different Gateway, different results	If our gateways are more than pass-throughs, there is the danger that users and service providers will see different results even with the same SP and IdP if the gateway is different.
12	Gateway with per-SP credentials	Only way this scales; model is similar to Janrain Engage
13	SimpleSAMLphp (SSP) as alternative to gateway	Institutions could run a single SSP service which would scale down the proxy issue to an institutional level vs. central gateway which has to scale to a federation level.
14		
15		