SAML and real time attribute queries by Policy Decision Points

Q: Blakley talked about the PDP sending out pull requests for identity info and then plugging in all the variables in the policy statement with facts about the authenticated user and sending back the allow or deny access decision. Can SAML perform these kinds of operations?

Q: Can SAML behave the way a PDP could behave in initiating queries against an IdP? (This is a question to take back to Shib-dev)

Q: What are the issues around SP knowing what the policy is and what attributes the PDP requires?

Q: What about situations where you don't know up front what attributes you need? (such as with the use case Blakley presents for a loan issuer.)

Q: How does an SP make an assertion against an IdP different than the one that initiated the request. I.e. if you have central authorization (e.g. grouper), then the user might sign in from another institution, but the group of people or the privileges they have for a local application might be stored locally and could be accessed by an assertion against the local IdP... is it possible, it is how things should work, etc? (question from Chris Hyzer)

A: (from Scott Cantor) If by "assertion" you mean query, then the Shibboleth SP already includes simple aggregation by means of a query with a common identifier between the original IdP and the additional one(s). It can handle hardcoded references, or can follow dynamic references to authorities within attribute values it gets from the IdP.

That isn't a privacy-appropriate model (it's exactly what I was railing against on the educause list), but it's a simple one, and totally appropriate if the SP and additional sources are co-located anyway (i.e., a VO). SWITCH, among others, has built VO platform functionality on it.

The SP could be extended with plugins to query other sources (LDAP, ODBC) in a similar manner.

The questions about SAML are essentially misdirected. SAML queries are generic, just like LDAP queries are. You can't ask the question about the standard, only specific software.

See:

https://spaces.at.internet2.edu/display/SHIB2/NativeSPAttributeResolver#NativeSPAttributeResolver-SimpleAggregationAttributeResolver%28Version2.2andAbove%29