November 6, 2013

Date:

October 30, 2013

Time:

12 Noon Eastern, 9AM Pacific, 5PM UK

Dial-in Info:

+1-734-615-7474 (English I2, Please use if you do not pay for Long Distance),

+1-866-411-0013 (English I2, toll free US/Canada Only)

PIN: 0195401 #

Agenda:

1. IdP extensions from to incorporate a service provider's registrationAuthority value into attribute release policies (email from Ian).
2. Discussion of Code of Conduct service category and technical implications (email from Tom).
3. REFEDs meeting next week.
4. AOB

Attending:

Warren Anderson, Steve Olshansky, Ian Young, Scott Cantor, Tom Scavo, I.J. Kim, Steven Carmodie, John Kreinke

Recording:

https://edial.internet2.edu/call/0104276

Minutes:

1. IdP extensions from to incorporate a service provider's registrationAuthority value into attribute release policies (email from Ian).** Straightforward for Shib 2.x#* Allows keying attribute release and registration authority
    - Primarily aimed at enabling dropping edugain metadata into UK Federation
    - LIGO might be able to make use of it fairly quickly
2. Discussion of Code of Conduct service category#* Lawyers have been asked to comment on whether they can sign off on meeting registration page can say it complies with CoC
    - Steven gives brief history of where policy comes from#** implementation of EU privacy law and directive
        - differs slightly from country to country to comply with local laws
        - attempt to reduce risk of privacy
        - rules out optional attributes
        - recognizes EU and countries with comparable privacy laws (Canada) or assurances from other countries that are sufficient (US Safe Harbor)
        - Goal is to automate release of PII based on information provided by relying parties
    - Tom dives into technical details#** complicated so this is based on best understanding
        - Tom most recently dove into it to help TAC review proposal
        - REFEDs is proposing R&S and CoC specs (and now others)#*** R&S spec is one pager
            - CoC is multi-doc and complicated, needs to be simplified
        - Notable operational differences between R&S and COC:#*** CoC requires privacy policy to be published
            - CoC has reliance on RequestedAttributes in metadata (so does R&S but in other ways)
            - RequestedAttributes are supposed to be FYI - few IdPs in InCommon supply them unlike in other federations.
            - This is partly an implementation issue (simpleSAMLphp vs Shibboleth) - simpleSAMLphp relies on RequestedAttributes.
            - One other difference is an xml attribute of isRequired for RequestedAttributes, which is not a supported attribute for inCommon (because inC uses ReqAttr as FYI)
        - Tom will be asking for one page summary of CoC (like R&S) and may have suggestions for
        - Scott thinks RequestedAttributes could be considered useful, but the issue is more that it is not used because we use back-channel
        - Also thinks that it doesn't support our use case because the way we use attribute information is too rich
        - Also no SPs are willing to take it
        - Tom points out RequestedAttribute is insufficient for R&S attribute bundle
        - Steven thinks we need to start defining best practices to simplify the way we use attributes#*** For instance, IdP asking user "we are releasing your name to this SP, is that OK"?
        - Tom points out that in R&S the policy for names is not expressible #*** Scott disagrees, is possible but just not with isRequired
        - Scott thinks we ether need to get everyone to start over with new "best practices" or get to a small set of RequesteAttribute metadata.
        - Tom thinks it's obvious that the Attribute Bundle idea from R&S is a better way to go
        - Warren asks if this is just throwing it back over the fence - is it just as difficult to implement Attribute Bundles in simpleSAMLphp as it is to do RequestedAttributes in Shibboleth?#*** Scott and Tom suspect this must be possible based on principal and prior experience.
        - Steven thinks that attribute bundles will contain attributes that are not required by SP, which is a violation of CoC.

-
    - Tom points out that bundles can be reduced based on relying party metadata (work done by Scott) but is largely unleveraged.
    - Scott thinks that this doesn't really work for required attributes - it works for signaling when you won't use it, but that's not the same as only passing required activity.
    - In fact, Scott thinks that the implementation that are being suggested are incompatible with the directive.
    - Scott wonders if this is even where interfederation should start? Seems ambitious to try to bring so many IdPs under the tent initially. Seems like an intractable problem.
-