January 29, 2014

Date:

January 29, 2014

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. Announcements
2. Review of EduGain Metadata Profile
3. Any other business

Attending:

Warren, Ian, Steve, John, IJ, Tom, Chris, Paul,

Recording:

Minutes:

1. Announcements
    a. John is still hoping to meet with Counsel this week. He had a chance to meet with one of the attorneys and scope the review.
2. eduGAIN Metadata Profile
    a. Introduction - John clarifies that v3 is the correct version since there is versioning information. Ian confirms.
    b. Section 2 - standard stuff.
    c. Section 3
        i. Tom comments that the first bullet is met already by inCommon
        ii. Second element is not currently in inCommon metadata. The interpretation is that if the element exists, then the following MUST and SHOULD clauses apply. Tom comments that that the mdrpi schema is on the horizon for inCommon and that this element will be included at that point. Ian says this is recommended for debugging purposes.
        iii. Tom says inCommon does not include cacheDuration flag and has no plans to do it, but recommend to consumer to refresh every hour. Tom asks about MDS Aggregation Practice Statement. Ian says it does not exist yet. Original documentation in Polish and writer is no longer in eduGAIN. Ian says that most people stick with validUntil. John asks if it would not be useful for each Federation to have something like an Aggregation Practice Statement. Ian agrees that it would be useful, though it doesn't exist as a separate document. Chris agrees that having a description of how the metadata stream is created is important and it is a work in progress in the Canadian Federation. Chris says the CAF points members who want to participate in eduGAIN to compare their metadata with the specs on the eduGAIN website.
        iv. Notes on validUntil - Tom needs to get more information, but asks what to do if you are aggregating several metadata streams with different validUntil values and how that is refactored into a validUntil for the root element. Ian says that there are two schools of thought: the first is to set the validUntil to encompass all the validUntil values it represents, but he thinks this is a mistake. If this view is adopted, having a very short validUntil value for one stream creates an effective DOS. He believes validUntil should be viewed as a point-to-point value. He has a document that is a proposal for a formal specification for the next generation of specifications for eduGAIN. Tom finds this very helpful. SAML metadata spec does not cover this because it doesn't address aggregation at all. Ian volunteers to circulate his document. John plays devil's advocate, and points out that if he has tied his validUntil value to a certificate lifetime that the preservation of validUntil values from individual metadata streams means that the aggregator is preserving this binding. Chris points out that individual values are only part of the whole security package and it can be misleading to focus on just one.
        v. 51-65 - Tom notes that mdrpi is not currently in the inCommon metadata, as described earlier. He does note that the RegistrationPolicy is an optional element, which means inCommon does not have to have such a document before joining. Ian points out that the tag is optional but that the document is required to join eduGAIN. Tom also comments about 57-65, which inCommon has and are SHOULDs. He wonders about the wisdom of having them since there is no semantic for them currently and so it's unclear how it can be used. Ian agrees. Chris points out that native languages bring with them an education piece. They had a Quebec institution that wanted to be known only by their French name.
        vi. 67-74 - Tom points out that there is a bug here - there needs to be a name for every IdP. These appear to be optional here. Ian points out that this is not really an issue in practice.
        vii. 76-79 - Tom points out that inCommon does not use MD:requestAttribute in the same way as other federations. Chris asks how inCommon uses it. Tom thinks that attribute bundles are more appropriate to use for these sorts of things, and they have a better chance of success in inCommon. Chris sees it as a positive thing to do - if they exist they are semantically meaningful. Tom simply points out that this is just not how SPs in inCommon interact. There is work in REFEDs to try to define how to express how to do this more clearly. Chris asks if there are attribute bundles exist it would be stripped out? Ian sees eduGAIN only as a conduit, and should never remove anything. The current practice is that any valid XML is passed through, and category assertions will make it through unharmed and uninterpreted. So eduGAIN does not check if entity attributes are correct, that has to be checked with the registering entity. This is what Chris expected. Ian says that eduGAIN is supposed to be transparent - that means that it won't remove or validate attributes. John thinks that there is an exception in that if an SP is

represented in two federations metadata aggregate then only the attributes that exist in the first aggregate are passed on, so for instance entity category R&S could be dropped. Ian points out that which aggregate is the source of the entity metadata is in the metadata, so while that can happen you should be able to detect that it has.

3. Other Business
   a. None,