March 05, 2014

Date:

March 5, 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. Metadata and Quilt
3. AOB

Attending:

Warren, Ian, George Laskaris, Mark, Shaun Abshere, Scott, Ann, David Walker, Tom, ?

Recording:

Minutes:

1. Announcements
2. Metadata and Quilt

- Tom would like to have a two-way conversation since he is not very familiar with quilt. Tom has been asked for a metadata registration practice statement, which does not currently exit. It is needed for eduGAIN. Tom will announce on interfed mailing list when it is done.
- Tom assumes the question is how to register a large number of IdPs into InC metadata. He is not aware of IdPs or metadata at this time. The information in the document might help with both metadata and IdP deployment. Assertions that Tom's assumption is correct. More questions about organization - regionals joining InCommon and providing service to it's smaller constituents. One question is what is looked for when metadata is presented for new IdP. Is that what document is about? Not mostly - more about deployment.
- Going through bullets:
    - Refresh metadata daily - not required but strongly recommended. Keep in mind when planning.
    - Sign assertions with SHA-256 digest algorithm - again, not part of presenting metadata but part of process - just in time. Again, important in planning. This will prevent having to change over in the near future. Also approved for federal applications.
    - Use long-lived, self-signed certificates in metadata - this is checked. There can be a problem with certificates that rely on chains. This is not an existing use case for PKI from CAs. Important to handle keys securely, as linked on doc. Shared certs might be tempting if there is a single host with multiple IdPs. But this is an untested scenario - what if you have a compromised IdP, etc. Scott points out that ADFS will not allow the same certificate to show up multiple times. So don't share certs - it will break ADFS IdP. It is possible that this was fixed in the 2012 release?
    - EntityID - this is checked (looks like url). Must reflect owner (IDPO). Host name must be rooted in uri. Difficult to change later - might be impossible in later versions of federation manager. Warren wonders if there is a primary domain for regionals. There are different models being considered. Important to note that it does not need to indicate where IdP is located or hosted. Scott thinks it might be useful to consider what are the most permanent name for a given service (probably the endpoint) and use that.
    - Scope - also permanent, usually primary domain. Should avoid multi-scoped. But multi-scoped is usually used by regionals. This will require conversations with InC ops if it used for metadata.
    - Endpoint Location - also permanent. Require ssl/tls connections.
    - Support recommendations - not part of metadata, but have consequences for maintenance etc. SAML2 required. Not supporting SAML1 is beneficial to others, as is not supporting SAML2 features that are unusual (eg SAML2 artifacts). Ian notes that many of these are supported in default configuration, will be more work to turn them off. Is the suggestion to actively turn them off? Tom notes that what your IdP supports and what your metadata reflect don't need to be the same. Attribute query (required for SAML1), for instance, has caused problems. These are just suggestions for ease of use. Scott notes that there are a number of instances where IdPs claim to handle artifacts but don't - really should be careful with this one. There are discussions of installation packages that turn some of these things off out of the box. Ian notes that it takes only one entity not to support SAML2 to make SAML1 necessary if you want full access to federation. Adjourning at this point due to time - will take it up again later.

1. AOB