Minutes from Quilt / InCommon Pilot Tech Call

2:00 PM Eastern Time Friday March 22, 2013

Notes taken by Steve Thorpe, thorpe@mcnc.org

Recording of the call is available at https://edial.internet2.edu/call/0199118

Reminder on Group Logistics:

Email list is inc-quilt-pilottech@incommon.org

Box folder is https://www.box.com/files/0/f/680471824/InC-Quilt_Pilot_Tech

Standing meeting is Fridays at 2:00 PM Eastern

Dial-in numbers for our standing meeting are:
+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)
Access code: 0110688#

Attendees:

Bernie A'cs, NCSA
Chris Giordano, MOREnet
Steve Olshansky, Internet2
Tom Scavo, InCommon/Internet2
Mark Scheible, MCNC (chair)
Steve Thorpe, MCNC
Ann West, InCommon/Internet2

Action Items From Last Week's Meeting:

[AI] **Steve T**: Publish these minutes around to the various lists / box folder. **DONE**: See "**20130315.InCommon.Quilt.Pilot.Tech.Call.Notes.docx**" in the "Minutes of Pilot Tech Calls" box folder.

[AI] **All**: Put yourselves into the shoes of the person trying to answer the questions. If you were asked to answer them, could you do it? **Basically DONE though any further comments are welcome**

[AI] **Mark**: Put a glossary together [**DONE** – see Quilt_Federation_Pilot_Questions_v02_mas.docx]

[AI] **Mark**: Provide feedback to the pilot definition working group, that having some supplemental material to the questions would be helpful – e.g. diagrams, motivation, etc. To put things into context. **DONE**

[AI] **Chris G**: (If can identify spare cycles) Explore MDA and provide any feedback to this group. **TBD**

Action Items From Today's Meeting:

[AI] **Steve T**: Publish these minutes around to the various lists / box folder. **DONE**: See "**20130322.InCommon.Quilt.Pilot.Tech.Call.Notes.docx**" in the "Minutes of Pilot Tech Calls" box folder.

[AI] **TBD**: Review the documents, notes, questions, glossary.

[AI] **TBD**: Send additional thoughts to list.

[AI] **TBD**: At next call: Discuss future schedule

Discussion:

1. Updates from Admin & Pilot WG meetings

Steve O: Admin WG is closing in on the home stretch. Hoping to get this out soon (sooner rather than later is best). Working toward a CFP date, trying to make the process as open as possible.

Ann W: On yesterday's Pilot WG call, Jack suggested that we not be so formal about it. If we make it too formal, perhaps it seems like there are actual resources at stake – and there aren't.

Mark S: George had put together a cover letter that looks good. Ann has a process document that is also good. I think we **need to think through the process from the technical side, to make sure from this group we have enough supporting information so it will help the reviewers in deciding whether the proposed pilots will be useful**.

To Ann's point about transparency, we need the process / criteria that will be used to review the proposals. With the key points that we want to do it relatively quickly, so something could be in use before school starts in the fall. Hence **simpler is better, sooner is better** – those would be advantages in proposals.

Also important is to establish cohorts of regionals that are planning to use the same model / tools – have them work together.

Steve O: There is in fact **no money from I2 flowing from this**. Shel is presuming that we'll be able to negotiate some attractive Net+ pricing for this. Also the idea is some enhanced support capabilities; e.g. mailing lists etc.

Mark S: **Could we offer free IdP services from Fischer**? Supposedly they're offering a service through regional networks such as OARnet for either free or reduced cost. Doesn't include the InCommon membership fee however.

2. Discussion around models - clarification

a. MDA benefits
b. Proxy IdP benefits
c. Why one over the other?
d. Hybrid – when appropriate

3. Pilot Decisions

a. Short-term Model

b. Long-term Model (same?)

4. Review documents for usefulness

From the InC-Quilt Pilot Tech Folder:

- InC-Quilt Technical Options DRAFT.docx
    - This one gets into some of what Mark was thinking the options / services regionals could look at providing. **It's really the 2nd page that applies here**, where you actually get into running a federation, or working with the metadata. Items on the 2nd page include:
        - Run/Support Local Federation
        - Run Metadata Aggregator (MDA)
        - Run Proxy IdP (Authentication Gateway?)
            - Bernie A: expects this is a likely option that will be presented.
        - Run Social2SAML Gateway
    - Mark S. says it would be helpful to list out the pros / cons of Proxy IdP vs. MDA
        - Proxy IdP is "easier" with respect to InCommon (only need a little bit added to InC metadata)
        - However Proxy IdP still has lots of local metadata issues
    - Bernie A: Metadata management component is critical regardless of the model actually.
    - Mark S: For testing / piloting it would probably be beneficial to have a small number of participant institutions. Once the bugs are worked out then you start expanding to cover more organizations.
    - Chris G: Question with regard to the pilots: If we have three technical models, is the outcome of the pilots to choose one exclusively over the others? Answer: Not required to have any one exclusively be picked.
    - Mark S: Proxy IdP at least gives you the option to tie in a back-end account. So for example you wouldn't have to run all back-end IdPs – could just tie into a directory. There is however two points where the DS choice would have to be made. Would want to have cookies to remember your DS choices so don't have to repeat every time.
- MDA Scenarios.pdf
- Regional Federation Models.pptx
- Proxy IdP-SP Slides.pdf

Update from Steve on his simpleSAMLphp experimentation:

- Setup includes
    - **SP1** protected via Shibboleth
    - **Discovery Service1**
    - IdP Proxy in the middle (implemented using simpleSAMLphp)
        - has the IdP side (**IdP-proxy**)
        - Its own **Discovery Service-proxy** (realized using a pull down menu)
        - the SP-side (**SP-proxy**)
    - (test version of) **IdP1** (Also Shibboleth)
- Metadata for SP1 and IDP 1 happens to be in InCommon
- None of the metadata for the proxy is in InCommon

- In this context my goal is simply to learn how to connect all the pieces. All of these elements could be configured to grab their Metadata only from InCommon, but in this case I manually set up the bi-lateral relationships involving the IdP Proxy
- I believe the **basic flow should be:**
    1. User seeks to log into SP1
    2. Redirected to Discovery Service1
    3. Choose IdP Proxy as desired IdP (choice is remembered by a cookie if desired by user)
    4. Redirected to IdP-proxy
    5. IdP-proxy seeks to have the user logged in to the SP-proxy by redirecting user to Discovery Service-proxy (pull-down menu choice is remembered by a cookie if desired by user)
    6. Redirected to IdP1
    7. User logs in at IdP1
    8. User gets redirected back to the Proxy
    9. Proxy consumes attributes from IdP1, populates its own assertion for SP1
    10. User gets redirected back to SP1 and is granted access
- **I can successfully do Steps 5…10** to get the user logged on to SP-proxy, where I can observe the attributes from IdP1 that are consumed by the SP-proxy
- **Steps 1….”5.5” are working fine right now** but in that flow, I’m still having some issue locking on the Proxy-SP to IdP1. IdP1 is throwing an exception I still need to resolve.
- **So I’m still having troubles with the “bridging” of the above two scenarios.**
- When all is said and done, I also hope to write up a short doc to help others who might choose to stand up a proxy

Tom S:

- The model we’re talking about for this pilot is:
    - SP part points outside InC
    - IdP part points inside InC
- So your explorations are not exactly the model we were talking about (that your Proxy is not on the boundary of InC metadata).
- Steve T: correct – right now simply learning how to connect the pieces

Mark S: Proxy allows TX federation entities to access SPs in InCommon that are appropriate, but not have all the entities in the InCommon metadata

Tom S:

- Despite the desire to keep all those entities out of the InCommon metadata, there are some that want to put them in. Duke has 800 that are totally local. CMU has ~150 SPs that are totally local, however they still use InCommon as the metadata source. That actually should be a third model / approach – to use InC as a service to maintain its metadata.
- When you talked about Alaska you mentioned two very different use cases. Recall with the Proxy we discussed SP-in / IdP-out; OR IdP-in / SP-out. If you have attributes flowing OUT of the federation it is more onerous. Terena is that case – but by policy we have Terena’s word for it, if you will, that the services on the other side are in their security domain. So we view it from our point of view as simply one SP. Its when the attributes

are flowing outside into another security domain – leaving your control – that we're in a different ball game all together.
- R&S is a game-changer because it enables multi-lateral configuration in one fell-swoop.
- Imagine my goal is to propagate R&S throughout the federation. In that case I would like IdPs to start using R&S entity attributes rather than bi-lateral entity Ids. In other words it is a harder sell for R&S and R&S-like categories, without being very careful / transparent about these proxies at the boarder.

Mark S:

- Is there a way for the SP that is using an IdP proxy, to be able to know what the original org was where the attributes came from? (A: It depends on what the proxy releases, and what the SP consumes)

Tom S:

- Check the SAML2 core spec, they address this exact question on how the end IdP can be carried along and presented, so the end-SP would know exactly where it came from. Does anybody implement it and use it today? No. Could it be helpful? Yes.

Steve T:

- Could IdP proxies have a special static tag denoting that in the metadata? A from Tom S: could be done – very interesting.

5. Anything still needed (RA diagram?)

Bernie A:

- Do we need to do something with Registration Authorities? There hasn't been a whole lot of definition about how that might work and how it would apply to the other pieces.
- Are the existing SPs that are ready to participate in this process? Perhaps "Elastic SSO"? (which seems to be carrying all the right badges for their services)

Mark S: I'd asked John K. about the RA function. Essentially its an administrative function as opposed to a technical one – it's the Id proofing of the key executive of any organization that is joining InCommon. And the vetting that the person is who they say they are.

The RA function is certainly something that should be put down into a business plan, certainly as part of the larger effort.

6. Action Items

Review the documents, notes, questions, glossary.

Send additional thoughts to list.

At next call: Discuss future schedule

7. Next Steps

Next Meeting: Friday March 29, 2:00 PM EDT

8. Adjourn