UMA telecon 2014-03-06

UMA telecon 2014-03-06

Date and Time

- **All-hands** meeting Thu Mar 6 8:30-10am PT (time chart)
  - Voice: Skype: +9905100000481 or US +1-805-309-2350 (international dial-in lines), room code 178-2540#
  - Screen sharing: [http://join.me/findthomas](http://join.me/findthomas)

Agenda

- Roll call
- Approval of past minutes
  - No WG meeting next week
  - "Summertime skew" ahead...
  - MIT-KIT workshop on private health data
- Webinar planning and outreach
- Core 09g and claim profiles review
- Interop planning
- AOB

Minutes

Roll call

Quorum was reached.

Minutes approval

Thomas moves: Approve minutes of Nov 2013 and Dec 2013 and read into today's minutes all of the intervening focus group notes. APPROVED by unanimous consent.

Upcoming meetings and webinar planning

We're not meeting next week, and the following week, not only will the US clocks have changed (vs. most of the rest of the world – our canonical time is US Pacific), but we'll do the webinar, starting even 30 minutes earlier than our usual 8:30am Pacific time.

Thomas described the upcoming MIT-KIT workshop. The theme is patient data sharing, and Blue Button+ and UMA types of technologies will be discussed.

CA has offered to sponsor the webinar, and we've accepted! Please be sure to advertise the EventBrite link, and if you have press and PR contacts, leverage those.

Core 09g

Is this draft ready enough for interop? That's the key question. Are we willing to "not touch this spec" for a while while we conduct the first round of interop tests? Eve is. Anyone else?

Thomas moves: Accept Core rev 09g as the next I-D revision, and an "implementor's target" draft that we intend to remain stable during initial interop testing. APPROVED by unanimous consent.

Do we want to report this out to the LC/Kantara board to undergo a Kantara All Member Ballot? The usual assumption is that such specs are considered "final", but we don't necessarily think this is the case; we do have the option of doing this as an All Member Ballot for a DRAFT recommendation. Sal approves of an All Member Ballot in general, eventually, but it seems we're not ready to signal finality of that sort quite yet: Being on the other side of interop is good.

At: Eve: Update the LC on our vote.

Claim profiling

In lay language, we've got two options: a "smart" client that's "claims-aware", and a really "dumb" client that's "claims-unaware", and is only capable – at maximum – of redirecting an end-user requesting party to the AS. This puts it outside the loop of claims-gathering.

Regarding the redirect model, we know there has to be an "out" for homebrew solutions. So it seems to make sense to make the redirect framework essentially synonymous with the sample redirect profile. So our ISSUE in the Section 1 intro can be resolved.

We don't need to mention alternate claim formats, such as X.509. People will do what they want.
What about the difference between an OpenID Connect ID token and a set of user claims? If the client was smart enough to be an OIDC RP (or even an OIDC IdP), then it is in possession of an ID token and it also has access to the claims available at the user_info endpoint. So what makes sense for it to deliver to the AS? Mark is concerned about having the client package up claims data in a novel format vs. some original, standardized format. Sal asks: Can we keep the signed blob and just pass that? The client is sort of acting as a "proxy", so what's the best way to keep the integrity of what's passed along? Ideally, the client should pass along as much context as possible to ensure integrity.

What's the OIDC equivalent of passing a SAML assertion blob (where the assertion might also contain attribute statements etc.)? The Cloud Identity implementation offers the redirect flow, and also is working on the delivery flow. What would be passed by the claims-aware client is claims without the external protections (Eve calls these "naked claims"). Since the client is already trusted, their thinking is that these unwrapped claims are okay to transmit.

Mark notes: The ID token potentially contains audience and issuer information, and other context. So why unwrap the claims from that context? At the least, we should make the name of the profile accurate, either mentioning ID token or user claims, or whatever.

Domenico comments: If the AS acts as a "claim receiver", it's expected to understand the claim format being used. But if it's a "claim connector" (essentially an RP, in loosely or tightly coupled fashion), it might want the token as a whole. Our question: Does the ID token serve as the access token for getting to a user_info claims endpoint? If so, and we believe it's so, then it's exactly what we said in the case of the client delivering "information about how to get claims" and the AS being a "claims connector".

At: Maciej: Investigate the delivery of ID tokens vs. claims themselves wrt our 2014-03-06 conversation.

Attendees

As of 5 March 2014, quorum is 6 of 11.

1. Eve
2. George
3. Mark
4. Jin
5. Keith
6. Domenico
7. Thomas
8. Sal
9. Maciej

Regrets:

• Roland

Next Meetings

• No meeting Thu Mar 13 8:30-10am PT (time chart) - Eve regrets
• Webinar Thu Mar 20 8-9am PT (time chart) followed by focus meeting 9-10am PT (time chart) - N.B.: US has changed clocks by now - "summertime skew"