UMA telecon 2013-04-25

UMA telecon 2013-04-25

Date and Time

- **All-hands** meeting on Thursday, Apr 25, at 9am PT (time chart) - Eve regrets - Maciej will chair
  - Skype: +99051000000481

Agenda

- (Get on join.me)
- Roll call
- Approve minutes of UMA telecon 2013-02-28 and UMA telecon 2013-03-28, and read into today's minutes the notes from UMA telecon 2013-03-21, UMA telecon 2013-03-14, and UMA telecon 2013-03-07
- Action item review
- Review new spec rev 07c (out shortly) and its thread model/security considerations
- Plan for an implementor's draft release effort
- AOB

Minutes

Logistics

Quorum was reached.

APPROVED by unanimous consent: Approve minutes of UMA telecon 2013-02-28 and UMA telecon 2013-03-28, and read into today's minutes the notes from UMA telecon 2013-03-21, UMA telecon 2013-03-14, and UMA telecon 2013-03-07.

Action item review

Done. See that page for details.

IIW planning

We should assume that IIW is effectively only two days long: Tue and Wed. The IDESG meeting Thu and Fri overlaps the final IIW day.

UMAnitarians attending: In addition to Thomas and Andrew, George and Keith will be attending. Keith will convene a GPII session that includes UMA intro slides (fodder provided by Eve). Eve's proposal for sessions:

- Day 1: Convene an UMA 101 session and an Accessibility Attribute Sharing with UMA session.
- Day 2: Convene an Optimizing OpenID Connect and UMA Flows session.

Implementor's draft release effort

There's value in doing this type of process to gather implementors. We've got at least three independent implementations but we'd like to attract more (Thomas is working on getting resources to do a new one). Do we feel the spec is basically stable? Interop would be a subgoal of such an effort. The test wiki isn't really ready for prime time.

We think we're not quite ready yet for this stage because there's too much work to do around the OpenID Connect optimization. This is our main technical priority. Let's drive that conversation at IIW and convey our state of readiness around "enterprise" use cases.

The RS = C optimization opportunity (e.g., Alice and Bob are both users of the Flicker app, and it mediates person-to-person sharing through UMA somehow) seems to be very high priority. The recent Twitter AP account breach occasioned a Twitter and blog conversation about how Twitter business tools would handle constrained delegated access.

Rev 07c threat model

We're looking at the new security considerations section. George notes that the JOSE specs add an audience field, and an authorized party (AzP) field. If you combine this with client authentication when presenting the token, the recipient can verify the client and compare it to the AzP in the token. This isn't identical to HoK, but similar. Thomas notes that the SAML Kerberos browser SSO profile published last year takes a very similar approach, but it just has identifier matching.

The IETF preferred language around HOK is "proof of possession" (POP), so we should probably stick to that.

The "intended audience" approach has been proven valuable in the SAML era, even in its weakest form, because it demonstrates intent — a friendly concept for our Binding Obligations. To prevent a malicious attack, you do need to have some way to verify the client, but this doesn't need to reach HOK/POP levels. In JOSE, you could have a signed bearer token. Would signing the RPT help? The goal is to prevent replay by unauthorized parties, so it sounds like not, without validating the client that presents the token.

At: All to weigh in on the "minimum viable action" the UMA core spec itself should take to solve the bearer token problem on a technical level (could be zero action).
AI: Thomas to check the OAuth Threat Model doc for whatever it might say about the bearer token vulnerability.

**Attendees**

As of 28 Mar 2013 (pre-meeting), quorum is 6 of 10.

1. Eve
2. George
3. Keith
4. Thomas
5. Maciej
6. Sal

Non-voting participants:

- Susan
- Andrew

Regrets:

- Domenico
- Adrian
- Lukasz

**Next Meetings**

- **Focus** meeting on Thursday, May 2, at 9am PT (time chart)
- **No** meeting on Thursday, May 9 due to IIW/IDESG
- **Focus** meeting on Thursday, May 16, at 9am PT (time chart)
- **Focus** meeting on Thursday, May 22, at 9am PT (time chart)
- **All-hands** meeting on Thursday, May 30, at 9am PT (time chart)