UMA telecon 2013-06-06

UMA telecon 2013-06-06

Date and Time

- **Focus** meeting on Thursday, June 6, at 9am PT *(time chart)*
  - Skype: +9905100000481

Agenda

- *(Get on join.me)*
- Action item review
- Spec issues review and resolution
- RS=C optimization opportunities
- AOB

Minutes

Action item review

Done. See that page for details.

Spec issues review and resolution

Issue 79: no comments right now.

Issue 81:

- The 2xx codes are explained here. OAuth Bearer mentions 2XX in passing, but just seems to assume that this all rides on HTTP, so naturally 2xx is appropriate for success. UMA only mentions 200 OK “in passing” (though it’s probably technically normative) in the introduction to its Section 3. It’s a simple fix to change to 2xx Success. Since success is defined wholly by the API you’re calling, we can keep this very light. Should we say instead that “... the resource server responds with whatever its application-specific interface defines as a success response”? (George notes that something like this came up in the Token Revocation conversation.) Thomas should make that change.
- as_uri: We think there was some history here around lopping off the http: scheme, but we can’t think why. You could use a URN or a proprietary scheme too. If we were going to require RSs and clients to verify that they’re getting config data over https, it could be argued to leave off the scheme. But if we want to be friendly to, e.g., testing with localhost:, then having a whole string makes sense. Eve argues to keep the string whole, including the protocol, so as not to overspecify. **Agreed.**
- Requested permissions: Can we add non-normative text explaining that the resource owner (subject) associated with this resource set ID (object) and scope or scopes (verbs) comes implicitly from the PAT? Eve suggests “The resource server MUST provide its valid PAT in order to get access to this endpoint; this PAT implicitly identifies the resource owner (“subject”) to which the permission applies.” **Agreed.**

**AI:** Thomas: Implement issue 81. (Part of his standing AIs.)

Issue 82: George muses: If the AAT is just a standard OAuth 2 token (which is true), it can be revoked, it can be invalidated, etc. We believe that this proposal constitutes an interesting OpenID Connect-, LOA-, and authn context-friendly profile that inserts itself at the AAT juncture (which, as the "head" of the requesting party and client authentication chain, seems appropriate). Gluu’s use case is related to enterprise needs – thus the "initial AAT issuance through web services", i.e., silently since the human resource owner agent doesn't have the right to withhold consent to claims-sharing, as this is simply part of their employment contract.

OpenID Connect has some global optional parameters to represent some light authentication context, e.g., to handle LOA. Gluu’s proposed solution is finer-grained. The UMA AS and the requesting party’s IdP/AP would need to establish trust at the AAT level in order to start to gather authentication context (outside of the claims system) as well as any claims. Domenico’s older banking use-case work did have an element of LOA in it. Eve likes that the AAT’s tuple doesn’t correlate with the RS, and the RS is kept properly out of the policy-assessing equation.

**AI:** Domenico will share the links to his most recent UX exploration that include LOA types of considerations.

**AI:** Eve: Ask Mike Schwartz to consider turning the Dynamic Re-Auth of RP proposal into a true UMA profile, referencing the advice in our spec, so that we can begin to catalogue it with others on our wiki (with no favoritism of profiles implied).

RS=C optimization opportunities

Attendees

- Andrew
- Eve
- Maciej
- Domenico
- Sal
- George
- Thomas
• Keith

Next Meetings

• **Focus** meeting on Thursday, June 13, at 9am PT *(time chart)*
• **Focus** meeting on Thursday, June 20, at 9am PT *(time chart)*
• **All-hands** meeting on Thursday, June 27, at 9am PT *(time chart)* - George regrets
• *(No meeting Thursday, July 4 because of the US holiday)*
• *(No meeting – vs. potential F2F/summit during CIS – on Thursday, July 11?)*