UMA telecon 2015-08-06

UMA telecon 2015-08-06

Date and Time

- Thu Aug 06 8:30-10am PT (we start 30 minutes earlier and meet for 90 minutes in August)
- Voice: Skype: +9905100000481 or US +1-805-309-2350 (international dial-in lines), room code 178-2540#
- Screen sharing: http://join.me/findthomas - NOTE: IGNORE the join.me dial-in line shown here in favor of the dial-in info above (Kantara
  "line C" and the Skype line)
- UMA calendar: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Minutes approval
  - Sample motion: Approve the minutes of UMA telecon 2015-07-30.
- Quick hits:
  - APAC-friendly sync update
  - Spec versioning process update
- Issue resolution work
  - Goal is to discuss and resolve issues 165/153 (ranked #1) and issue 154 (ranked #2) -- please review!
  - Issues on GitHub
  - UMA V1.0.1 issue nominations spreadsheet
- AOB

Minutes

Roll call

Quorum was reached.

Minutes approval

MOTION: Approve the amended minutes of UMA telecon 2015-07-30. APPROVED by unanimous consent.

APAC-friendly sync update

This sync schedule is working really well.

Spec versioning process update

No update. Eve hasn't moved the repo over.

Issue resolution work

- Goal is to discuss and resolve issues 165/153/154 (all ranked #1) – please review!
- Issues on GitHub
- UMA V1.0.1 issue nominations spreadsheet

Issues 153 and 154

Not meaning to guess Justin's exact thought process in any way...

Observation #1: AS has a special "RPT endpoint", making up the entirety of the special "UMA authorization API", at which the UMA client asks for a special UMA "RPT" with authorization data on Bob's behalf, that acts suspiciously just like an ordinary OAuth token endpoint. If it were more like an OAuth token endpoint, greater UMA-OAuth alignment could be achieved.

Observation #2: The UMA "authorization API token" (AAT) is an extra layer and hindrance to the entire OAuth-friendly cycle in this case, particularly because it appears to require that Bob have a login at the AS.

Discussion: Isn't the last bit, about the login, just an implementation decision? He has to either be SSO'd into the AS, or have a local login at the AS, or be offered a federated ("NASCAR-like" or whatever) login option at the AS. More accurately stated, he has to be able to establish an authenticated relationship with Alice's AS.

Observation #3: If the AAT flow were entirely removed and the RPT endpoint were turned into a ordinary token endpoint, then Bob's client would approach it to ask for "an access token" (perhaps of some UMA-flavored type?).

Discussion: Eve contends that, since we are trying to keep everything as much the same as possible, then this new "UMA-flavored grant flow" would still (so far) have the the client approach the RS, fail, get a ticket, go to the AS's (now) token endpoint, ask for a token, and engage in the trust elevation flow we have already designed.
Observation #4: Instead of using an AAT in the header of the token request, it would use its client credentials to identify itself, basically using its own recognizance.

Discussion: Where else is the AAT required in headers? Is it required in the redirect of Bob for claims-gathering? No, there are other security measures imposed. What about in the case of an autonomous web service client? We think that this could use pushed claims to the token endpoint as well.

More discussion: The AAT isn't very high-value! So a kind of "merge" to elevate what was the AAT flow up into what was the RPT flow to become an analog of a typical OAuth flow looks attractive. That means the claims flow would be the very first thing Bob does – no AAT step before. That seems kind of clean as a UX, if we're not missing anything like Bob's consent. And we don't think we're missing that, because that's what the OAuth flow is designed to do. The RPT represents everything the AAT did, but more. Why didn't we consider this before? In fact, we did.

More discussion: In both the authorization API circumstances and the newly imagined grant flow circumstances, how does Bob know exactly what claims the client is pushing?

Observation #5: UMA is still OAuth++ or value-add or something, in that the protection API that makes the AS and RS loosely coupled and makes possible trust establishment between them (using OAuth) is added on top, and in that Bob is a completely autonomous actor wrt Alice (which is why the grant flow we're considering has trust elevation as a key part of it), and in that the grant flow we're considering has asynchronicity as a key part of it. All the value-add still seems to adhere even if the AAT isn't part of the picture.

Discussion: Regarding the Privacy concerns: if the Client does a POST on the RPT to get the AuthzData added to it, the AS can still decide to return a new RPT to the Client (if the presented RPT had AuthzData for another RS attached to it). So that could be a AS-privacy setting? According to the APAC discussion yesterday, the answer appears to be yes. We can use a MUST to force the AS to mint a new token per RS. (Justin also noted in email that if the client tries to present a token from RS1 for upgrading with authorization data for RS2, the AS should not allow that.)

Discussion: Is UMA all pseudonymity-based? The AS knows Alice by AliceID(AS). The AS knows Bob through some set of claims, potentially. Each RS knows Alice by AliceID(RSn). Each PAT is a kind of pseudonymous federated ID by which both the AS and that RS know Alice. Each client has a set of access tokens (in the putative new solution) with a set of permissions, but not identifiers.

Discussion: How would the client manage multiple access tokens? All it knows is that it's trying to access a resource. How would it know that the token it has been given is new for this RS? What if the spec said this (bold is new)?

"If the client did not present a token in the request for authorization data, the authorization server creates and returns a new token. If the client did present a token in the request, the authorization server returns the token with which it associated the requested authorization data, which MAY be either the token that was in the request or a new one. In any case, the authorization server MUST return a new token when the client presents a token that is associated with a different resource server."

Summarizing our sense: Generally positive about most aspects, but there is a concern about how clients handle the token situation, and some uncertainty about ensuring that the requesting party really has a chance to authorize the interaction.

Next steps:

- AI: Eve: Develop swimlanes (web sequence diagrams) of the putative new flows, along with pros and cons, and share with the group by Monday.
- Let's TRY and have an active discussion, drawing in Nat, about the client concerns, before next Thursday.
- Let's TRY and conclude issues 153 and 154 in the early part of next Thursday's meeting. If we have a specific proposal in front of us for issue 165, we'll consider it, otherwise not. We'll also take up 160, 161, 162, and 168 next time.

Regrets for next time: Andi, Robert, François, Ishan, James, Domenico. Ooh, next week is going to be tough for quorum, so everyone else please try and attend if they can!

AI status

- AI: Thomas: Review the charter for potential revisions in this annual cycle.
- AI: Sal: Investigate IP implications of formal liaison activities with other Kantara groups with the LC, and ultimately draft an LC Note as warranted.
- AI: Gil: Edit the UIG to add Ishan's content and excerpt it for Eve to add to the FAQ, pointing everyone to the UIG.
- AI: Sal: Fill out IDESG form to have UMA adopted as a recommended standard for use in the IDESG framework.
- AI: Mike: Write SCIM protection case study to highlight client claims-based use case.
- AI: Maciej: Write as many sections for the UIG as he can.
- AI: Justin: Write a UIG section on default-deny and race conditions.

Attendees

As of 30 Jul 2015 (pre-meeting), quorum is 7 of 12. (François, Domenico, Sal, Thomas, Andi, Phani, Robert, Maciej, Eve, Arlene, Irwin, Mike)

1. Eve
2. Andi
3. Irwin
4. Domenico
5. Maciej
6. Robert
7. Mike
8. Arlene
9. François

Non-voting participants:

- Adrian
• James
• Rene
• Mark
• Ishan
• Allan
• Jin

Regrets:
• Thomas