UMA telecon 2017-01-05

UMA telecon 2017-01-05

Date and Time

- Thursdays, 9-10am PT
- Skype: +99051000000481 / US +1-805-309-2350 / international lines / web calling interface / code 1782540
- Screen sharing: [http://join.me/findthomas](http://join.me/findthomas) - NOTE: do not use the join.me dial-in line
- UMA calendar: [http://kantarainitiative.org/confluence/display/uma/Calendar](http://kantarainitiative.org/confluence/display/uma/Calendar)

Agenda

- Roll call
- Approve minutes of UMA telecon 2016-12-01
- Logistics
  - Hold WG votes on specs this month (as often as we like?), and add publicity
  - WG vote on proceeding to Public Review no later than Feb 9 (Feb 16 is RSAC; no meeting)
  - Refer to telecon 2016-12-01 minutes to see how voting/balloting process goes
- UMA V2.0 work
  - 2016 roadmap / GitHub issues for V2.0 (all issues to be kept here for the duration!) / dynamic swimlane
  - Core is up to 10 and RReg is up to 03
  - Issues to discuss in the telecon:
    - 266: Set math
    - 264: Authentication-related error details
    - 254: Hashed claims discovery
    - 263: Claim token profiling / 119: Create an IANA registry for URIs that stand for claim token formats
    - Shoebox (stretch goal; let's make assignments for proposals for next week):
      - 246: Endpoint for collection of "receipts" and notifications of RS action in case of extraordinary behavior / 245: Location Constraints / 224: RS Notifies AS or RO of Access / 63: Audit logs to support legal enforceability / 24: Possible e to audit host's compliance in giving access based on a legitimate active permission from the AM?
      - 260: Cascading authorization servers (stretch goal; let's plan to study this and decide whether it's in the WG's scope by next week)
    - Issues that will close with no action or take the action recommended if no one brings them up for discussion by next week:
      - 261: Caching token inspection results (take the action recommended)
      - 249: Is there a way to elevate trust in Client Operators further, with a claims-like mechanism? (take no action)
      - 108: Protection and authorization scopes implicit/recommended vs. MUST? (take no action)
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

Approve minutes of UMA telecon 2016-12-01: APPROVED by unanimous consent.

Logistics

- Hold WG votes on specs this month (as often as we like?), and add publicity
- WG vote on proceeding to Public Review no later than Feb 9 (Feb 16 is RSAC; no meeting)
- Refer to telecon 2016-12-01 minutes to see how voting/balloting process goes

Eve, Andi, Sarah, and likely Sal among those who are attending today are going to RSA. Eve and Sarah are speaking. Eve's talk touches on UMA and consent receipts.

Andi reminds everyone that the CIS CIP closes tomorrow. Justin has submitted a bunch of talks, including one about UMA2 changes and a wider view of "V2 standards".

UMA V2.0 work

266: Set math:

The whole notion of a client registering at an AS for scopes is weird because it's not bound to resources. It's only later that the scopes get bound. **Option 1** is to completely ignore pre-registered scopes. **Option 2** is to add the pre-registered scopes to the requested scopes at the token endpoint and the scopes in the permission ticket carried there. **Option 3** is to limit the client to only the scopes pre-registered for, and not any additional scopes.
Option 3 seems impractical because of the lack of resource context for scopes at that "OAuth-only" stage in the proceedings as well as limiting Bob's abilities to express his wants. George is looking to help make clients simpler through pre-registration, so that they don't have to "repeat themselves" asking for scopes dynamically every time and just assume it will be taken as read that scopes will be requested by virtue of pre-registration – so, option 2. Mike likes option 2 as well. At the time of doing matching, the AS needs to determine what the scopes are that match against resources. The AS unions the pre-registered and dynamically requested scopes (if any), and does a matching process of some kind (either "generous" for any resource ID in the ticket as possible or "stingy" somehow?), and issues an invalid_scope error if there's no matches at all. Our invalid_scope error probably needs to be revised to account for not just any (dynamically) requested scopes but also statically or dynamically pre-registered scopes.

**AI:** Justin: Propose a concrete example for the AS scope-matching and resolution spec text by Jan 12.

There's consensus that the RS can request permissions that cover less than what the client was trying to do, on "Adrian clause" thinking.

Do we need to issue a warning or error somehow if the AS avails itself of the clause (that's always been in there) about "granting a subset of requested permissions" vs. "treating the result as an authorization failure"? George suggests an alternative: The AS is required to fail the client if it can't fulfill the entire permission ticket's worth of permissions with their scopes, but it can treat any additional request scopes with discretion.

Let's decide this latter issue next week.

**AI:** Eve: Spec out all the set math text that can be spec'd out modulo the remaining issues in rev 11.

### 264: Authentication-related error details:

It would be desirable in a lot of cases to specify hints about things like a certain kind of hard token etc. Whereas before we had an error_details hint authentication_context, now the client would redirect the user to the AS, which would "communicate with itself" about all the needed context. But if the client were sending along an ID token previously, wouldn't hints about what to send be helpful? This is where Eve was suggesting in the issue text that an error_details extension might be necessary to think about.

**AI:** Eve: Send email about issue 264 and the next few issues for discussion prior to next week.

### Attendees

As of 22 Dec 2016 (post-meeting), quorum is 5 of 9. (Domenico, Sal, Nagesh, Andi, Maciej, Eve, Mike, Cigdem, Sarah)

1. Domenico
2. Sal
3. Andi
4. Eve
5. Mike
6. Cigdem
7. Sarah

Non-voting participants:

- Justin
- George
- Adrian
- James

Regrets:

- JohnW
- Maciej