UMA telecon 2016-11-10

UMA telecon 2016-11-10

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 2016-10-13, 2016-11-03
- Logistics for upcoming meetings (calendar) and 2016 roadmap check-in
  - Next week: **WG meeting on Fri Nov 18** at 9am PT after legal call instead of Thu Nov 17
  - Week after: **no WG or legal meeting** due to US holiday
- Work on UMA.next issues – Core is up to 07 – please review changes ahead of time if possible
  - The following changes affect syntax:
    - Removed config data to declare pat and rpt profiles supported (as agreed last time)
    - Requesting party claims endpoint --> claims interaction endpoint (language that affects syntax in endpoint config data)
    - Resource set --> resource (language that affects syntax in endpoint config data and token introspection returned object format)
    - New AS-to-client invalid_scope error (because a client can now ask for scopes)
    - RPT token profiling has been properly removed now (means token introspection, if used, requires using the permissions structure)
      - "Authorization data" flexibility can only be added, not substituted – is this OK?
      - Do we need to reconsider the last bullet in Security Considerations Sec 7.1.1 re PoP/HoK?
  - To discuss specifically this time:
    - Set math: See 9-29 and 10-6, and the email thread – including...
      - What scopes should the client ask for, and why? (E.g., least-privilege rationale.) What should the mechanism be for asking for scopes for specific protected resources?
      - What permissions should the RS request on behalf of the client, and why?
    - pat_grant_types_supported: My proposal was to remove it. Any further discussion?
    - claim_token_profiles_supported: My proposal was to keep this profiling mechanism, but clean it up and provide two actual profiles or at least credible examples, say, for OIDC ID tokens and SAML assertions. Discussion?
    - uma_profiles_supported: My proposal was to keep this profiling mechanism, but figure out seriously if the extensibility profiles are doing the right job, and include credible examples of extensions and not just extensibility profiles. Discussion?
    - Is step-up auth the way it was conceived in UMA1 hunky dory according to the claims collection mechanism in UMA2?
    - Is the (client) registration endpoint’s name correct according to the naming pattern used in UMA, and also OAuth and OIDC?
- **See the latest swimlane**
- **AOB**

Minutes

**Roll call**

Quorum was reached.

**Approve minutes**

Approve minutes of UMA telecon 2016-10-13, 2016-11-03: APPROVED by unanimous consent.

**Logistics**

We **ARE** meeting next week, but Friday at 9am PT, not Thursday. That's right after the Legal call.

**Work on UMA.next issues**

Syntax changes as listed above are confirmed OK. The new invalid_scope error is OK. We don't have to say "protected resource" all the time, particularly in syntax.

Eve is concerned that not being able to fully replace the permissions structure in the token introspection response is a bridge too far in having removed the token profile scaffolding. OAuth has token profiling. There is a use case for just conveying RqP identity claims for achieving fine-grained authorization at the edge (along with a use case for conveying RqP identity claims on top of permissions). UMA permissions on their own only convey "scope-grained" permissions. Can we reuse the UMA profiling capability to allow third parties to replace the permissions structure if they need to? It's already possible to create these (so Gluu could consider doing this).

We have some outstanding questions around the token profiling question and the permissions structure. Eve will send an email outlining these with all the options she can think of and possibly making some proposals so we can decide by next week. (She'll include the Sec Consid point from 7.1.1.)

**AI:** Eve: Email about token profiling, as above.
Instructions for Core rev 08:

- Sec 3.4: The RS has the option of using cached RPT status results, so include this in the options (has swimlane implications?). This is also an AS TTL strategy thing (including revocation and disconnected RS scenarios, e.g. IoT scenarios), which we should comment on if we haven't already.
  - Add companion security considerations around TTL for RPTs and permissions, since you need to measure risk and risk appetite based on the RS, the resource itself, and even the nature of the policy conditions etc. Without active revocation infrastructure, the risks are higher.
- `pat_grant_types_supported`: Goes away.

Attendees

As of 3 Oct 2016, quorum is 6 of 11. (Domenico, Sal, Nagesh, Andi, Robert, Maciej, Eve, Jeffrey, Mike, Cigdem, Sarah)

1. Domenico
2. Sal
3. Nagesh
4. Robert
5. Eve
6. Mike
7. Cigdem
8. Sarah

Non-voting participants:

- Francois
- James
- Scott F
- Kathleen
- Arlene
- Jin
- Colin
- John W

Regrets:

- Andi