UMA telecon 2017-01-26

UMA telecon 2017-01-26

Date and Time

- Thursdays, special meeting times through Feb 9: 8:30-10am PT
  - Skype: +9905100000481 / US +1-805-309-2350 / international lines / web calling interface / code 1782540
  - Screen sharing: http://join.me/findthomas - NOTE: do not use the join.me dial-in line
  - UMA calendar: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Approve minutes of UMA telecon 2017-01-19
- Logistics:
  - Idea: Vote on WG draft on Feb 9 and open it up to a "last call" period for about four weeks? We need burn-in/beta time, it seems
  - No meeting Feb 16 because of RSAC
- 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 13 (updated) and RReg is up to 05 (updated)
    - Core: mostly authorization assessment and editorial changes; "claim token" also now defined (closing #256)
    - RReg: #276 trial text for the scope property
  - 266: Set math
    - Critique new wording and spec structure (Sec 1.4.2 / Sec 3.6.5)
    - What should be done about previous RPTs on requests – if they're allowed, why, what does the AS do in return, and what does the client do with its various RPTs?
    - How (and where in the spec) should the RS document its permission request practices so the client has an idea what's in its RPTs?
    - Are our "notes" for default-deny and everything else as they should be?
    - Can we close the issue after this?
  - Discuss and clear the RReg issues
    - 269, 270, 271, 272, 273, 276, 277
  - 260: Cascading authorization servers
    - Discuss Mohammed's input
    - Decide next steps
  - Claim token profiling: 263: Claim token profiling / 119: Create an IANA registry for URIs that stand for claim token formats
  - "Easy issues":
    - 264: Authentication-related error details (will close with only editorial/example text)
    - Shoebox: Will remove V2.0 label from 246, 245, 224, 63, 24 and make them a parallel activity
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

Approve minutes of UMA telecon 2017-01-19: APPROVED.

Logistics

- Idea: Vote on WG draft on Feb 9 and open it up to a "last call" period for about four weeks? We need burn-in/beta time, it seems
- No meeting Feb 16 because of RSAC

We like the idea of a Last Call period to shake out things. Several of us are doing some incremental implementation work. We can never make people look, but we can do our best to draw attention. So our new plan of record is to publish a WG draft by Feb 9.

UMA V2.0 work

266: Set math:

Typo: "RequestedScopes contains view, print, and print" should obviously be "RequestedScopes contains view, print, and download".

The list discussion, netted out, is:
- Should the AS be able to issue fewer scopes than the RS put into the permission ticket, or not? And if so, should it be able to do so on a per-resource basis?
- Since OAuth happily tells the client what scopes were issued, why can't we do the same? Can we do this and not share the resource IDs? We have seen the resource IDs as privacy-sensitive personal information. It's unfortunate that the OAuth architecture overall hasn't yet had a way to identify specific resources.
Eve had put this language in rev 13: "The client attempts what the resource server interprets as view access to rsid_1. The resource server chooses to request view and print scopes on its behalf". (Should be "...to request view and print scopes for rsid_1...") This is hinting at what the RS is authoritative for: interpretation of the API call and choices about the extent of the permission request. This needs to be discussed in a proper place in the spec. All this probably belongs in Sec 1.3 somewhere. The client should be discussed here too!

George proposes, and James supports, that PermissionTicket scopes MUST be met per resource, which ties the AS's hands in terms of what it rejects and incentivizes the RS in terms of requesting "too much". Park this for a moment. This would change the Venn diagram, and the decision on the issue below would change the outcome of this discussion.

---

James proposes having the AS report rejected scopes in the token introspection object so that the RS can decide if it wants to keep trying (that is, requesting permissions on behalf of the client again and again). But what if the RS is tired of dealing with looping? We do have a clause that says "The recipient of each request message SHOULD respond unless it detects a security concern, such as a suspected denial of service attack that can be mitigated by rate limiting."

Cigdem says: "I agree with the second option. If RS records what permissions it asked for the client, and then checks it against received RPT, it can diff what is denied. (And the missing permissions in the RPT was a result of RS being permissive and AS granting only resources that fully match RS's permission, RS can try again)."

A more informative token introspection object allows the RS to craft a permission request that is responsive to what the requesting party/client is actually seeking access to, while adhering to minimum disclosure principles if it wants to. Could we still have the concept of the client including a previous RPT on its request? It appears so, because all the scopes in such an RPT are associated with resources.

Because the client doesn't know how its tokens relate to its successful accesses, its only choice is to try and send all of its previous RPTs. But it would only have one because it would have had to invalidate each last one.

The idea is that the AS would provide the last-issued ticket, broken out with the state it had kept associated with it.

At: James: Send concrete example of how to solve this problem.

Other:

The "easy issues" will be resolved as noted:

- 264: Authentication-related error details (will close with only editorial/example text)
- Shoebox: Will remove V2.0 label from 246, 245, 224, 63, 24 and make them a parallel activity

Spec instructions:

- Fix typo shown above
- Fix permission request language shown above
- "Easy issues"

Attendees

As of 19 Jan 2017 (post-meeting), quorum is 5 of 8. (Domenico, Sal, Andi, Maciej, Eve, Mike, Cigdem, Sarah)

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

Non-voting participants:

- James
- George
- Justin
- Ishan
- Kathleen
- Jin

Regrets:

- JohnW
- Andi