UMA telecon 2015-02-23

UMA telecon 2015-02-23

Date and Time

- Mon Feb 23 9:30-11am PT
- Voice: Skype: +9905100000481 or US +1-805-309-2350 (international dial-in lines), room code 178-2540#
- Screen sharing: http://join.me/findthomas
- UMA calendar: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Minutes approval
  - Sample motion: Approve the minutes of UMA telecon 2015-02-19.
- Consider asking LC to approve specs as Kantara Initiative Draft Recommendations and asking LC to request All-Member Ballot for Recommendation status
- Other outstanding AIs
- AOB

Minutes

Roll call
Quorum was reached.

Minutes approval

MOTION: Andi moves: Approve the minutes of UMA telecon 2015-02-19. APPROVED by unanimous consent.

Specs status

Reviewing RSR:

The slash on the ends of the POST and GET calls should go away.

Does ETag have any reason for existence now? It appears not.

Justin notes that OAuth dynamic client registration uses the name policy_uri to mean something else! There, it means a user-facing policy description page for an end-user to be presented during the authorization flow. What would be a better name for our version? policy_setting_uri? policy_ui_uri? resource_policy_uri? uma_policy_uri? access_policy_uri? as_policy_uri? policy_config_uri? end_user_policy_management_uri? user_policy_setting_uri?

user_access_policy_uri? This seems to be the winner. Do we accept applying this to all five methods? Mark wonders what it means for a deleted resource. Andi's thinking on this was that the overhead of having the option there as an option was minimal compared to the missed opportunity in case someone thinks of a reason to want it. Maciej thinks having the property apply to Delete is fine, but it's maybe a good idea to explain that the value would be different in this case, obviously not applying to the just-deleted resource. The AS needs to give meaning to the portion of the interface pointed to.

Core security considerations:

George painted a picture of an OAuth/OIDC implicit client, to see if its usage in UMA created a new attack surface. If the attacker can get Bob to visit a malicious website, and the client ID isn't protected, can it get hold of Bob's AAT and then do damage? Even if Alice's policy requires Bob to log in to prove he controls that email address, without forcing Bob to re-log in fresh, there's a risk.

What's neat is that a mitigation is for Alice (and/or the AS, through system-default policy and an access federation trust framework – Binding Obs) to set policy about the nature of the client and its credentials. Implicit clients have an inherent security issue in that you can't verify the client identity. Lots of threats come directly out of this. When a client requests an RPT, the AS could embed in the RPT some external metadata about the client (IP address, User-Agent fingerprint, etc.), and then on introspection it could doublecheck the context of the requester. Thomas asks: Could the embedded metadata be a URL to the X.509 cert of the client? Yes, sure – this could legally bind the Client Operator (in Binding Obligations terms) to the transaction.

Security considerations: State that implicit OAuth clients add risk, and there are several opportunities for mitigation: RO/AS policy that limit implicit client usage, RPT/UMA profiling, other TTL strategy, Binding Obligations at a trust framework level.

MOTION: Thomas moves and Ishan seconds: Ask LC to approve Core rev 12 (as amended) and RSR rev 05 (as amended) as Kantara Initiative Draft Recommendations and request Kantara All-Member Ballot for Recommendation status. APPROVED by unanimous consent.

MOTION: Mike moves: Promote the latest drafts to IETF I-Ds. APPROVED by unanimous consent.

Logistics
Eve is arranging for editing of the specs to "look like Kantara" vs. IETF specs for All-Member Ballot purposes.

The Kantara board is meeting on Thursday.

Other outstanding AIs

- AI: Eve: Edit UIG (Mike's input, Zhanna/Andi's input)
- AI: Maciej: Write as many sections for the UIG as he can. (smile)
- AI: Pending.
- AI: Eve: Send suggested updates to Will at Gluu for English page updating, and to Domenico for Italian page updating, and to Rainer for hoped-for German page updating, and to Riccardo Abeti for the Spanish page, and to Mark for a Dutch translation.
  - AI: Pending.
  - Suggestions sent – review together?
- AI: Robert: Noodle on the kitten metaphor.
  - Pending.

Attendees

As of 13 Feb 2015, quorum is 7 of 13. (Dom, Sal, Mark, Thomas, Andrew, Robert, Maciej, Eve, Mike, Jin, Ishan, Ravi, John)

1. Eve
2. Andi
3. Thomas
4. Mark
5. Mike
6. John Mathon - WSO2 - founder of TIBCO - inventor of the TIB - interested in privacy and IoT aspects
7. Domenico
8. Ishan
9. Sal
10. Maciej

Non-voting participants:

- George
- Adrian
- Justin
- Marcelo