UMA telecon 2018-06-07

Date and Time

- Thursdays 9am PT
  - Screenshare and dial-in: https://global.gotomeeting.com/join/857787301
  - See UMA calendar for additional details: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Approve minutes: Approve minutes of UMA telecon 2018-05-31
- Decoupled flow: continue discussion
  - "Force authentication"?
  - Poll with interval vs. use a notification endpoint?
- Enterprise use cases and Gluu Gateway
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

Approve minutes of UMA telecon 2018-05-31: APPROVED by unanimous consent.

Decoupled flow: continue discussion

- "Force authentication"?
- Poll with interval vs. use a notification endpoint?

The CIBA spec has both a polling mechanism and a client notification endpoint. Mike is concerned that the token passed here is duplicating the function of the state parameter. When the client calls the notification endpoint, it gets back the equivalent of a permission ticket. Then it can present that ticket at the equivalent of the token endpoint and get back a token, or register a callback URL and say it authenticated the person. But isn't this "backwards UMA", because it would say it authenticated Alice vs. Bob?

Mike also has a concern about the /bc-authorize endpoint defined in the CIBA spec, which is basically a new API but not pulled out as a proper API definition.

UMA has a claims redirect URI. But it doesn't have any other redirect/callback URI. CIBA suggests another callback URI, that for us might be called an "RPT grant": You get a ticket, you present it at the AS, it returns "OK", and then sometime later, the AS says "I have your RPT" and it sends it back to the client. The comment Mike sent to the MODRNA list about CIBA was: "In section 6.4. "Token Error Response", There is no way for the user to fix the error if the back channel communication fails. Although you are kicking off the authentication via backchannel, if the user can switch to front channel, she may be able to resolve a problem. For this reason, I would suggest you define a "claims_gathering_endpoint" which can be returned to the client, and in which the user could then interact with the AS. Your claims gathering endpoint could be like an airline quickcode. For example, if I'm working with airline ABC, then the agent could tell me to direct my browser to https://abc.com/ciba/G5JQ2 Then you have a lot more options to fix the problem (especially if this claims gathering endpoint is on the OP, and you could put the subject through a multi-step authentication workflow)."

Justin notes that CIBA gets that it's not a complete solution. It's identity-focused. UMA is also not complete; it's authorization-focused, and runs in the other direction (Alice to Bob). So the two hurdles to applying UMA-as-it-exists-today to decoupled are a) it runs "backwards" (a big challenge, presumably) and b) it doesn't have a notification endpoint (a smaller challenge, presumably). Justin has been collecting "what do you hate about OAuth2" items. In the chat, Cigdem noted that currently the RO authenticates to the AS for permission purposes and the RS for resource management purposes separately; these are outside UMA's scope. What decoupled seems to look for is authentication of the RO by the AS. Maybe someday there would be a "grand unified theory" version of various specs (OAuth, OIDC, UMA...) that would offer some kind of complete solution for the requirements of decoupled, but today they don't seem to.

Mike imagines UMA-protecting the bc-authorize endpoint (effectively the RS role). What would happen? It's an API. It has parameters. They define a permission ticket equivalent (the identifier for the session), and what happens if the person doesn't authenticate (similar to UMA's error responses). Part of what they did was needed. What they made up that isn't as "well made up" as UMA, in Mike’s estimation, is what happens if the access token is not issued: the authentication error response. UMA allows both back-channel and front-channel loops (this is with the RpP, not the RO, though).

Mike is thinking of proposing a "revised CIBA" that uses UMA. To do that, he may need to solve the "backwards" problem! But it would be very interesting to see such a proposal.

Enterprise use cases and Gluu Gateway

Deferred to next week!

Identiverse
Justin, Eve, Thomas, Mike, Maciej, Sal, Mark, Colin, and likely other UManitarians and Kantarans will be there. 2000 people are expected. They target CxOs and identity architect types. Mark, Sal, and Eve are doing a Privacy 2.0 masterclass. Mike and Eve are doing an UMA2 masterclass. Ping Identity runs it but it’s very “ecumenical” in terms of sponsorship. It’s in Boston this year. It moves around every year. ZZ Auth and the Love Tokens (featuring Eve, Justin, and others you may know this year 😊) are playing at the closing party.

Attendees

As of 7 Mar 2017, quorum is 4 of 7. (Domenico, Sal, Andi, Maciej, Eve, Mike, Cigdem)

1. Domenico
2. Andi
3. Maciej
4. Eve
5. Mike
6. Cigdem

Non-voting participants:

- Justin
- Nancy
- Thomas
- Colin
- Tim

Regrets:

- Sal
- Adrian