UMA telecon 2019-12-12

UMA telecon 2019-12-12

Date and Time

- Thursdays 6am 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 of UMA telecons 2019-10-03, 2019-11-21, 2019-12-05
- Discuss recent next-gen authz news
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

- Approve minutes of UMA telecons 2019-10-03, 2019-11-21, 2019-12-05
  
Deferred.

Reminder: IdentiVerse CfP is open till Jan 10

Keep those cards and letters coming!

Discuss RAR/PAR and UMA implications

Some handy links about RAR/PAR:

- Roundup by Aaron Parecki of IETF 106 artifacts, including spec links
- Brief discussion on the UMA WG list of RAR/PAR interest
- Medium article from Torsten L on the specs from Sep
- (Hyperledger Aries concepts about cross-“agent” communication (everything is an “agent” in their conception))

When Eve says ”RAR/PAR”, she really means the data structure that seems to underlie both of them. RAR is heavier, and in talking to Justin she has learned he believes it’s not really baked yet, while PAR is much lighter weight and is much more ready for prime time. RAR is sort of the “pull” version and PAR is the “push” version from the client side.

In the brief discussion thread, Eve said:

“Here was my observation. RAR manages to convey, in a just-in-time/one-time way (vs. registering ahead of time in an RO context), a lot of fine-grained authorization details. Some resemble what we do or have done in the past.

For example, it has individual resource “locations” à la our individual resources per RS that get an RO-specific resource ID. (We dropped our location uri parameter after V1.)

Its individual resources are able to have scopes associated differentially, the way we’ve been able to do for a long time.

Its main purpose is the one-time fine-grainedness (which we don’t do, but I’ve seen proposals for from time to time), but some of these other ideas seem sensible since, after all, we do something like them. Our version is more complicated. Is this a case of potential broader adoption of design ideas we could eventually “adopt back”, or of feedback we should provide on why the design needs more thought, or a mix, or...?”

In OAuth originally, the concept of scopes being simple strings was powerful but very coarse-grained, and too many entitlement types have gotten squished into scopes over time, which has resulted in overloading. UMA invented the concept of having different scopes per resource; because of its asynchronicity goals (Alice being able to set authorization policy at the AS separately from when Bob and his client seek access), we made resource registration happen prior to policy setting. It could be “dynamic” or “static” but must happen before that point. The consequence is that resource reg is in an RO context; the resource ID carries that context. The (common) RAR/PAR data structure goes beyond the detail of our resource reg/scope reg, but one thing that data structure and the UMA protection API’s resource description have in common is that resources (resource locations in RAR/PAR) can have unique scopes.
Maciej notes that in some past work, he found utility in a model similar to RAR/PAR, and Eve knows of several cases of this as well. In fact, the cases she's aware of were sort of "UMA-enabled". So it seems like the time has come for some standardization of this. Eve's recollection of the work to profile /extend UMA at Identos to privacy-enhance the AS reminds her a little bit of this overlap. They had a customer that apparently wanted to eliminate the particular trust vulnerability remarked on in the FedAuthz Privacy Considerations section: "The authorization server comes to be in possession of resource details that may reveal information about the resource owner, which the authorization server's trust relationship with the resource server is assumed to accommodate. The more information about a resource that is registered, the more risk of privacy compromise there is through a less-trusted authorization server." Of course, there could also be authentication data as well, but if the AS is an RP to some other IdP for that, then it doesn't even hold that.

AI: Eve: Reach out to Alec at Identos and see if there are any synergies with his "enhanced UMA" and the RAR/PAR approach to per-resource scopes (or anything else in there).

AI: Adrian (if he wishes): Put some questions/comments about capabilities models and comparisons on the list for further discussion there.

Eve asks: Is it worth exploring an extension to UMA (backwards incompatible) that reuses some portion of RAR/PAR so as to consider "sedimenting" more features down into OAuth? Cigdem thinks putting in place PAR could be fairly easy, but RAR needs to mature a lot and could be more involved. (Note that authorization_details is supposed to be able to be used anywhere scope is. UMA has resource_scopes for a reason, so we'd have to deliberately make the equivalence, if it indeed can be made.) Let's continue this discussion in our final meeting of the year.

Separately, Adrian asks: Is it worth the agent/wallet-y sort of approach we saw from Identos if it is more privacy-enhancing? Thomas points out that ecosystem pressures are still in play for the software used for wallets. We discussed an Amazon client app example and an example of a single-user "personal AS" service run in an environment of the RO's choice. It seems that both may only marginally improve on the "typical" situation of a web user choosing a large, powerful multi-user SaaS service to give them AS (or any other) services in terms of trust, vulnerability, level of fiduciary responsibility, etc.

Attendees

As of 16 Jul 2019, quorum is 5 of 9. (Domenico, Peter, Sal, Thomas, Andi, Maciej, Eve, Mike, Cigdem)

1. Sal
2. Thomas
3. Maciej
4. Eve
5. Mike
6. Cigdem

Non-voting participants:

• Scott
• Adrian
• Nancy