UMA telecon 2020-07-02

UMA telecon 2020-07-02

Date and Time

- **Alternate-week Thursdays 10am PT**
  - Screenshare and dial-in: https://global.gotomeeting.com/join/485071053
  - United States: +1 (224) 501-3316, Access Code: 485-071-053
  - See UMA calendar for additional details: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Approve minutes of UMA telecon 2020-06-11, 2020-06-25
- Wallet profile
- Webinar work (if any discussion needed)
- Conformance test suite project (if discussion needed)
- AOB

Minutes

Roll call

Quorum was not reached.

Approve minutes

- Approve minutes of UMA telecon 2020-06-11, 2020-06-25

Deferred.

Identiverse authorization panel

Eve and George are on an authorization panel to be aired on July 14, 10am MT. Here's the description for looking it up:

Next-Gen Authorization Throwdown: It's Not Your Grandfather's OAuth

Speakers: Daniel Fett, George Fletcher, Eve Maler, Justin Richer, Jake Feasel

OAuth has seen several iterations over the last decade as the expert community has worked to solve difficult security, authorization, delegation, and consent challenges on behalf of both enterprises and end-users. We're now in "interesting times" as OAuth 2.0 is being stretched – some might argue to a breaking point – to cover new use cases. How should we enable fine-grained authorization? How similar should our handling of consent and authorization be? Can enterprise authorization and cross-domain authorization use the same model efficiently? Where do authentication inputs end and authorization decisions begin? And what about Alice? Join our panel of experts to hear their differing perspectives on OAuth innovation and how its next wave(s) of iteration must proceed for success

Wallet profile

We're continuing to analyze the swimlane that Alec sent out in email.

The wallet client and the first alt box satisfies the part that is normally out of scope in UMA FedAuthz. Line 9, with resource owner credentials, posts private keys and gets a list of pseudonymous subjects that can be used for policy writing later. Remember that in this context the RqP that appears there is really the RO. So the RO is at their wallet. They are redirected to their RS, where they authenticate. The wallet gets an access token. The wallet thus functions as an OAuth client. Identos thought about making this a pure OAuth client but didn't go that far.

RO policy is lines 11-14. Similar to the wallet-RO relationship, the wallet is a client to the AS, and the wallet uses lines 11-12 to register a public key. The RO is registered with an OAuth client-type relationship. In lines 13-14 it's really the RO using all of that key material and subjects and resource IDs to create policy at the AS. That could stay out of scope, but the AS is offering some kind of policy API.

So these make the "manage" and "control" lines in the spiral-is diagram above into defined interfaces.

What was the user agent that created the policies in the wallet? How was the wallet informed about what choices to offer the RO? In the Identos case, the AS has no interface, but it has a list of RS's and the resources available to that person through the resource definitions. This is the "out of scope but asynchronous policy management" part. Adrian notes that this is a terminology issue. Wallets hold private keys and hold credentials, and disclose them as appropriate. He doesn't see them as presenting policy interfaces.

So can we pick a name that isn't anything they use, perhaps including "wallet" and "agent", and move on for now – and maybe inform that community of what we do on a periodic basis in case it contains good ideas? Maybe "UMA wallet" will be sufficient to distinguish it. Eve suggests "policy pocket". 🙂

There are three delegation scenarios, the first two being new.

1. The RS offers delegation directly, a la the Google Docs Share button capability, after line 9. The use case here is a hospital custodian use case – the RO is the patient and they delegate to their doctor and the doctor authenticates as themselves.

2. The second place delegation can happen is directly from Alice to Bob, wallet to wallet. This is more of an impersonation case. An AS or RS couldn't audit or trace that this happened. The simplest way for this to work is to transfer a private key, and that's why Alec mentions impersonation, though some constraints could be imposed on the capabilities of the RqP (recipient of the key). But there are other possibilities, and that's where you could get into DIDs and VCs. It's then governed by the agent-to-agent world and its possibilities and constraints.
3. The third place this can happen, not marked on the diagram, is the stuff after line 14, is policy-based asynchronous access. That's the existing UMA-based delegation model.

Next steps for everyone, with Alec starting it: Start a "user stories" email thread. A user story is in the form "As a <<role>>, I want <<outcome>>, so that I c an <<benefit>>." Here are the really old user stories for UMA1.

Webinar work (if any discussion needed)

Deferred.

Conformance test suite project (if discussion needed)

Deferred.

Attendees

As of 23 Jun 2020, quorum is 5 of 9. (Domenico, Peter, Sal, Gaurav, Thomas, Andi, Maciej, Eve, Mike)

1. Domenico
2. Peter
3. Sal
4. Eve

Non-voting participants:

- Stephen
- George
- Gaurav (15 years in identity management, lots of products – heard about UMA and is aware of all the challenges – would like to help shape solutions)
- Alec
- Adrian
- Bjorn
- Colin
- Anik