UMA telecon 2020-04-02

UMA telecon 2020-04-02

Date and Time

- **Alternate Thursdays 6:30am PT (this ad hoc meeting was added in the series specially)**
  - Screenshare and dial-in: https://global.gotomeeting.com/join/857787301
  - See UMA calendar for additional details: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- IDENTOS extensions
- Interop

Minutes

Which week to meet

George points out that the "OpenID A/B" (OpenID Connect) meeting overlaps the latter half of this meeting if we meet last/next week vs. this week/2 weeks from now etc. No one attending today has a problem. Eve will investigate with others and voting participants who are not currently present and reschedule if no problem. (**UPDATE:** Sufficient positive responses established, so Eve will switch weeks in the calendar. We will start meeting Apr 16, Apr 30, etc. instead of continuing with Apr 9, Apr 23, etc.)

Online notarization

Tim raises the topic of the current worldwide situation and the fact that online notarization has suddenly become more important. Is this similar to remote proofing? These technologies have certainly existed for quite some time, and have been integrated to IAM stacks. But it got more notice in Okta's keynote this week, which mentioned use cases like employee onboarding. IT budgets seem overall negatively impacted in the current environment, though this is not evenly spread out. UMA and delegation use cases generally depend on identity solutions being in place, so that makes them relatively "sophisticated". On the other hand, telehealth and health data sharing are under more pressure now.

IDENTOS extensions

Alec provided a sequence diagram and we worked through it. To download, see the attachments to this page.

The resource IDs are static.

The "RS PAT" is not RO-specific.

The capability ticket is static. If you want to see a patient record with an immunization, you get a capability ticket that's sort of like a permission ticket but it doesn't change. This maps to terms of use. When a RqP authorizes the client to access resources and scopes, they review the ToS. This is Alice-to-Alice sharing right now. So the effect is Alice reviewing ToS for accessing her own stuff. What is in this ToS? It's the client's ToS for usage by the RqP, whoever it is (could be Bob in future). The client uploaded this to the AS for safekeeping, effectively. So the AS presents the ToS to the RqP on the client's behalf. Thus, instead of the possibility of the RqP having an independent relationship possible with that client outside of UMA and that AS, the RqP is assumed to use the same AS as the RO does, so it's a narrow ecosystem assumption. (See slide 36 in the UMA Legal role definitions for the "RqP-CO-ASO relationship train tracks" for how it could be built up in the widest possible ecosystem.)

Security-wise, is it okay for the capability ticket to be static? It's like requesting a scope, so it's okay for it to be static. So yes, it's safe. George describes the critical characteristics: If it's just an identifier, it's okay to be static. If it's a "binding agent" across multiple flows, then it needs to be rotate.

Is the capability ticket similar at all to OAuth resource indicators (now RFC 8707)? It's more general, but the analogy does apply. The client would use the resource definition in the URI instead of the resource server.

What happens if the API gets versioned? Is there a CRUD API or something? The capability API has something like the resource registration API. IDENTOS has implemented a dynamic version along with their static version, but they're not currently using it.

The **first flow** in the diagram is "standard UMA", RS first. The RS can still request a permission ticket, only using static resource IDs. The last leg is always a token endpoint call with either form of claims collection.

The **second flow** is the static capability ticket flow. The client goes to the AS first and then goes straight to interactive claims gathering. The RqP (currently the same person as the RO) is then at the AS after the redirect and can authenticate etc.

The **third flow** is a hybrid where the client, *not* using the static capability ticket, uses the permission endpoint as if it was the RS. This is perhaps a bit like OAuth Pushed Authorization Requests (PAR). Are there any security implications to this? The client is similar to an RS in that they have registered what they can do. Since a PAT is now no longer RO-specific, the client can go ahead and use their client credentials as a "PAT-equivalent". The AS can distinguish them from an RS because they have registered as a client.

After the three flow options, saying (say) that they're looking for a patient record, now the RS still has to be told which patient's resource to give out. So in introspection, the AS provides subject information explicitly in its response, along with the granted resource IDs and scopes. Or George notes that an encrypted access token could contain that information. The RPT is still used. (Last week Alec noted that it was in this step, providing the subject, that there is some potential overlap with the other extension they have defined. See his email to the list and the description of "step 8" for more detail.)

Thank you to Alec and IDENTOS for contributing this for the WG's consideration! The "narrow ecosystem" this use case serves does seem pretty common (shared AS between the RO and RqP, oftentimes the RO == the RqP, the design patterns of the resource need interop due to open APIs or other reasons).

Other questions and comments we didn't have a chance to address yet, maybe in future:

- George: Could you use Dynamic Client Registration of the mobile app to help with this? That would make the client_id specific to each mobile app instance
- Sal: trusted platform environment might also come into play

We seem to have interest in considering work on this as a WG. More to come.

Interop

Deferred, but some people are working on this as a separate thread.

Attendees

As of 17 Feb 2020, quorum is 5 of 8. (Domenico, Peter, Sal, Thomas, Andi, Maciej, Eve, Mike)

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

Non-voting participants:

- Cigdem
- Scott
- Alec
- Tim
- George
- Colin