UMA telecon 2012-12-13

UMA telecon 2012-12-13

Date and Time

- Focus meeting on Thursday, 13 Dec 2012, at 9am PT (time chart) – educational, technical
  - Skype: +9905100000481

Agenda

- Activate join.me with code to be supplied
- Meeting schedule review: legal/all-hands meeting is next week due to legal all-stars' availability
- Action item review
- Review of changes suggested by George to make UMA fully compliant as an OAuth profile
- Discuss/resolve new issue 74: dynamic client registration config data
- Spec modularization and terminology review (join.me)
- Discovery metadata registration proposal (make one up if we don't have one in front of us)
- Sometime in second half of meeting: demo of Gluu's OX UMA support
- AOB

Minutes

Meeting schedule review: legal/all-hands meeting is next week due to legal all-stars' availability

Action item review

Domenico has begun to send security considerations comments to the list. Let's plan to spend a meeting in January on this topic.

Thomas would like to get somewhere with the higher-ed UMA profile before the next IETF meeting (March in Orlando). His MIT colleagues don't seem to require this to be a submitted I-D in order to pay attention to it.

Sal and Mike have discussed the "UMA for enterprise" case study, and Will is going to be working on it.

Eve has closed her item on editing the Implementations page.

Keith has closed his case study AI.

Review of changes suggested by George to make UMA fully compliant as an OAuth profile

Thomas has kept the ticket in a JSON body in the error response so as to be as backwards-compatible with existing UMA implementations as possible. The only change, then, in this picture is that we've started to use the official OAuth error code.

For now, we've decided to use an "UMA1.0" keyword in the WWW-Authenticate header to indicate that the "UMA 1.0 profile of OAuth 2.0" is in use. Maybe there's a better place for this; we'll open an issue to discuss this.

George has recommended: "It may be useful to look at all calls that use 'Authorization: Bearer' and ensure they match RFC 6750 as well." We need to follow up on this (can George take the AI?).

Thomas and Eve need to do some rhetorical work to ensconce this "profile" view of UMA into the spec in a way that doesn't confuse people.

Discuss/resolve new issue 74: dynamic client registration config data

We agreed with the proposal. Thomas will incorporate. The issue is now closed.

Spec modularization and terminology review (join.me)

Thomas walked us through the new module. The definition of "permissions" was removed because it's UMA-specific. He also removed "requesting party" because OAuth doesn't have that; it doesn't talk about the operator of the client in the same way as talking about human RO end-users.

The section describing the resource set registration endpoint can be folded into the Terminology section entirely now. Likewise, the section describing extended scopes can be moved into the Terminology section.

A bunch of endpoints got deleted from the config data. The AS config data section can take the opportunity to engage the proposed spec from elsewhere on AS config data. Also, it can sync up with Justin's proposal for token introspection, so that it's no longer "rpt_status_endpoint" anymore but whatever Justin calls it.

We should reactivate the issue about an "implicit resource set". Thomas should point/refer to that issue from the spec.

The Protecting a Resource intro should discuss the two use cases we know of for trust establishment between the RS and AS, namely: for many generic OAuth deployments, it's static and OOB, and for IdP/AP/RP scenarios, it may need to be dynamic.
The Kantara URI for the scope should be changed to something generic, and we need a new issue asking what URIs IETF specs use for this.

The description of Protecting a Resource should accommodate use cases where there is no human end-user (that is, 2-legged flows). Referring to the RO rather than the "end-user" helps a lot. In fact, we think Sections 2.1 and 2.2 need to be strongly curtailed and even possibly made non-normative.

We think that the third para in Section 2.3 should be moved to the UMA profile of this module.

There are a few instances left of the word "host", primarily in section headers, that need to be changed to RS.

Several mentions of "user" should probably say "resource owner", e.g. in Section 2.4.

(Let's say "an RS" rather than "a RS")

It's time for Thomas to make a formal pointer from the UMA core spec to the module; we'll publish this as rev 06a, and ask Nat and others for comments soon thereafter.

**Discovery metadata registration proposal (make one up if we don't have one in front of us)**

Scopes should be known as "scope types" in the module. The icon_uri properties for scopes and resource sets should be in the UMA core spec, not this module. Resource set descriptions need to have an added property called "resource_type", which contains a URI. We will define a reserved value that stands for "this resource set has implicit/application-defined semantics that are not exposed through this interface".

Currently, we say in Section 2.4.2 that the AS has to refresh its scope descriptions at certain junctures. Maybe for module purposes, this needs to be softened a bit to be more of a "health warning".

**Attendees**

- Eve
- Alam
- Keith
- Domenico
- Sal
- Thomas

**Regrets:**

- George
- Lukasz

**Next Meetings**

- All-hands meeting on Thursday, 20 Dec 2012, at 9am PT (time chart) – legal, all topics
- NO MEETINGS for the rest of 2012 – happy new year/end-of-the-world!