UMA telecon 2014-01-09

UMA telecon 2014-01-09

Date and Time

- **Focus** meeting Thu Jan 9 8:30-10am PT (*time chart*)
  - Voice: Skype: +99051000000481 or US +1-805-309-2350 (*international dial-in lines*), room code 178-2540#
  - Screen sharing: [http://join.me/findthomas](http://join.me/findthomas)

Agenda

- UMA-dev list switching
- Interop participant planning: meeting Tue Jan 14 8am PT (see UMA calendar) – all welcome
- Twitter/Meshfire team: set up tutorial?
- Discuss Mark’s latest proposal for AS=C spec text
- Discuss next stage of terms of authz/binding obs work
- Q1 calendar and events
- AOB

Minutes

**UMA-dev list switching**

We have the option to move to a Kantara-hosted mailman-style mailing list, meeting our criteria for a) no IP requirements to sign up and b) no Google (or other "social"/organizational) account required! Not hearing any objections, Eve will ask Joni to create the list.

**Interop participant planning: meeting Tue Jan 14 8am PT (see UMA calendar) – all welcome**

We should have good attendance for this.

**Twitter/Meshfire team: set up tutorial?**

Eve will set this up, hopefully for next week.

**Discuss Mark’s latest proposal for AS=C spec text**

In "take 2", Mark refactored his proposal based on the discussion. He settled on the phrase "deployment profile" to describe these options.

*In section 1.3: APIs and Protection, add the following text to the end of the paragraph:

In specific optimization profiles in which different UMA roles are performed by the same entity, some communication requirements MAY change. The conditions for which this applies are described in (new) Section 4, **Optimization Profiles**.

This is meant to be a "global get-out-of-jail-free card" or "health warning" to soften some MUSTs that appear later. Mark notes that the language around "entities" is not explicitly defined in the UMA spec. Does it need to be? We'll think about it.

Don't change anything in section 3, where the communication between AS and C is specified.

The MUSTs still appear there, in other words. Do we actually want one more "health warning" in, say, each of the intros to Sections 2 and 3 now that we have this "optimization profile" name? Mark's reasoning for not doing this was to limit the impact to the existing spec. By creating a new section, we get the freedom to specify everything needed.

**At**: Thomas: Edit Core to do *s/Specifying/Specifying/* in the header of Section 5.

Instead, add new section after 3 and before 4: "Optimization Profiles"

*new* 4. **Optimization Profiles**

**When UMA compliant systems are deployed?** It can be desired to combine different UMA roles in one entity, for example when an authorization server also features dashboard-like functionality that requires actual access to resources. In this case, the authorization server would also act as a client. While the specification of the roles is unchanged, the particular optimization profiles may have impact on certain requirements for the communication between these roles.

Should this be between Sections 4 and 5, or maybe part of Section 5, or something else? Mark's reasoning for making it a separate section is that different x=y scenarios affect different parts of the phases 1-3 protocol flows of UMA, which stretch across Sections 2 and 3. We agree that this should be a separate section at the level of 2 and 3. Eve proposes that it go before the Error Messages section (currently 4), so that it's as close to regular protocol flows as possible. We have consensus.
What about the name "deployment profile"? Mark is using this to mean, specifically, multiple-colocated-entity profiles. Do we want to give these sorts of profiles their own name, and if so, what should it be? We could just pick something and then ask for feedback. Having a unique name allows us to put one or more clear "hooks" in text in Section 1.3 and possibly elsewhere. Eve notes that "deployment" is used already in the spec, in the description of profiling in the intro to Section 5: "For interoperability and to serve particular deployment scenarios, including sector-specific ones such as healthcare or e-government, third parties may want to define profiles of UMA that restrict these options." So reserving the word deployment for other things might be a good idea.

Along with considering "deployment profile", what about "optimization profile" or "protocol optimization profile" or "colocation profile" or ...? We have consensus that optimization profile is the right term for now. We agree that it is a special subspecies of the "profiles of UMA" currently discussed in Section 5.1.

(NEW) 4.1 Authorization Server = Client Optimization Profile

- Identifying URI:
  - http://docs.kantarainitiative.org/uma/profiles/uma-deployment-as-c
- Profile author and contact information: Mark Dobrinic
  - (mdobrinic@cozmanova.com)
- Updates or obsoletes: None; this profile is new.
- Affects communication between roles: authorization server and client
- Security and privacy considerations: As described below.

If an authorization server also acts as a client, the behavior for the communication between these roles MAY be optimized from the specified requirements.

To conform to this profile, the following conditions must be met:

* the authorization server is also acting as client in the same system entity
* the client role has a more direct means of access than using public communication channels to access the authorization server (i.e. a common datastore)

When these conditions apply, the client MAY use alternate (more optimized) means than TLS? or HTTP? or endpoints? to access the authorization API of its authorization server. When the client detects that it needs to request an AAT from itself, an AAT may be created directly without requiring an OAuth 2.0 flow to establish one.

The same exception may be made when issuing the RPT [section 3.4.1.], for when the authentication server is the same entity as the client, it can be directly issued without going through a TLS connection and requiring the client to present an AAT to an authorization API.

Finally, for requesting the suitable authorization data to be added to the RPT, the authorization server and client may choose their preferred means for acquiring the necessary claims? doesn’t this require getting the requesting party involved? note that the RqP necessarily = the RO in this case to satisfy the policies that are applicable for the required permissions. These permissions can be looked up from the ticket that the client obtained from the resource server.

Note that it is REQUIRED to create an AAT, because while it may not be used for authorizing requests to endpoints of the authorization API, the AAT does represent the particular conditions on which terms and obligations can be based.

Are we sure this rises to the level of being a profile that goes in the spec, vs. a third-party profile? It seems there are wide-ranging scenarios where this would be useful, so it seems "global" enough to be in the spec.

Do we see a need to add an uma_profiles_supported field in the configuration data? This case is different from rpt_profiles and claim_profiles, which directly affect the AS's operations. In an RS=C optimization profile, e.g., the AS has nothing to do with the change in communications! We don't seem to have any appetite for adding anything new to the configuration data for right now; we could always add it later.

We need to add a pointer to the spec-defined AS=C optimization profile in (old) Section 5.1, as an example of a profile of UMA. This should follow the same pattern as the other callouts to spec-defined RPT and claim profiles.

We also need to add a mention of Mark in (old) Section 10 as a co-author.

AI: Thomas and Eve: Confer on making spec changes.

Discuss next stage of terms of authz/binding obs work

Eve described the directions Dazza is taking with the Binding Obs.

Q1 calendar and events

Eve and Joni have been discussing a quarterly schedule of webinars, tackling different use cases, e.g.: Enterprise (access management 2.0), healthcare, OpenID Connect/PDS, research/edu... Some webinars might share early-stage results and some might share late-stage code. The rough calendar looks like this (slightly revised from what Eve and Joni talked about):

- Q1: Enterprise/AM2.0
- Q2: OpenID Connect/PDS
- Q3: Healthcare
- Q4: Research/Edu

Also, we're thinking of holding a drinks hour at RSA to find more potential UMAnitarians and buy them drinks. Eve, Joni, Dan, and Sal are likely "in".
• Mark
• Domenico
• Eve
• George
• Maciej
• Łukasz
• Thomas

Regrets:
• Adrian
• Keith (first half)

**Next Meetings**

• **Focus** meeting Thu Jan 16 8:30-10am PT ([time chart](#))
• **Focus** meeting Thu Jan 23 8:30-10am PT ([time chart](#))
• **All-hands** meeting Thu Jan 30 8:30-10am PT ([time chart](#))