UMA telecon 2014-05-29

UMA telecon 2014-05-29

Date and Time

- **All-hands** meeting Thu May 29 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

Agenda

- Roll call
- EIC report
- Upcoming meeting planning
- Webinar planning:
  - Date: June 19, 8-9am PT
  - Theme: UMA, OpenID Connect, and personal data stores ("You can't spell human without UMA" 🙂)
  - Key participants: Maciej/Cloud Identity, Thomas/Justin?/MIT-KIT, Dazza/MIT, and Nat so far
  - Hashtag: #UMApcloud
  - Sponsorships: MIT, who else?
  - Need to get registration page up
  - Do press release again this time?
- Leadership team ballots:
  - Chair, vice-chair, and spec editor positions are coming due
- Interop planning
  - In-person interop at CIS?
- Case study work
  - Personal loan/Life Management Platform case study
  - Personal cloud app architecture case study
  - IoT case study/discussion?
- Multi-AS policy sourcing (Gluu)
- Claim profiling work (Cloud Identity)
- Regex style of resource set/scope registration (Gluu)
- RS config data for publishing resource sets and required policies for client benefit? (Gluu)
- AOB

Minutes

Roll call

Quorum was reached.

Vivek is new to the calls. He works for Cisco on the security side on the cloud platform. He works on OAuth and SAML mediation, and JWE technologies.

Mike is new to the calls. He's the founder of Gluu. They have a service to help companies deploy open-source identity software. They have an UMA implementation that focuses on organizational use cases.

Yuriy is new to the calls. He works on Gluu as a developer.

Casey and Katie are new to the calls. They are at ForgeRock, and are working on an UMA implementation over the summer. Implementation questions should go to the uma-dev@kantarainitiative.org list.

Minutes approval

MOTION: Thomas moves: Approve minutes of UMA telecon 2014-04-24 and read into today's minutes all intervening ad hoc meeting notes. APPROVED by unanimous consent.

EIC report

This is the most important identity conference in Europe, organized by Kuppinger Cole. This year they focused on cloud, privacy, security, etc. There was a special track on "Life Management Platforms", a KC-innovated concept in 2012. It builds on the personal cloud/PDS vision. Domenico and Maciej presented. Nat S was there, and a vendor interested in the concept, Qiy. The cherry on top of the conference was UMA receiving an EIC award. Questions came up about how UMA controls data. Michelle Chibba expressed interest from the PbD perspective. We have written on UMA wrt PbD here: http://tinyurl.com/umapbd.

Next steps: Publish our LMP analysis formally.

Webinar planning

Mike suggests that his work on the Ubuntu Juju framework, for which UMA and OIDC are two-thirds of the underpinnings (and in which WSO2 and ForgeRock also participate), could be relevant to use in the webinar. Eve notes that the Maciej/Domenico presentation from EIC is also extremely relevant, and it already includes a demo component. (It's not so bad if we max out our line at 30 callers.)

AI: Thomas: Doublecheck that it's possible to record through MIT's WebEx account and that the line can support more than 30 callers.

AI: Eve: Coordinate a registration page and potentially a press release with Joni.

AI: Eve: Send out an email summarizing the state and a candidate webinar agenda to the list and other involved parties, including Nat and Dazza.

The hook for the press release and other marketing efforts could be: On the occasion of the EIC award, ICYMI, see the great personal cloud/LMP UMA story and demo.

We'll assume MIT is the sole sponsor.

Leadership team

MOTION: Jin moves: Approve Eve Maler for Chair, Maciej Machulak for Vice-Chair, Thomas Hardjono for Specification Editor, Domenico Catalano for User Experience Editor, Maciej Machulak for Implementation Coordinator, and Dazza Greenwood for Binding Obligations Specification Editor for a year: APPROVED by unanimous consent.

Interop planning

Who's planning to attend CIS? Not Mike; OSCON is on the same dates. He's thinking about reaching out to a new community at OSCON (which is being held in Portland, OR). He's not crazy about in-person interops, even for OIDC! There's already an ongoing virtual interop going on for OIDC. Roland's virtual interop style is more productive because it allows for a lot more interactive back-and-forth.

Allan F is apparently speaking on UMA at CIS, so those of us attending IRM can help prep him next week. This speaking opportunity at CIS is probably more valuable at this juncture for outreach purposes.

RS config data

Previously, we revised our requirements around what description the RS has to provide about its interface. Mike has brought up an interesting new topic: enabling discovery by a client of the RS's resources and required scopes over them. E.g., a WordPress RS that doesn't have super-secret protected resources might want to declare statically, in some RS-oriented configuration metadata, what's available. George notes that AOL has been looking at what you could use for the markup format for this. Swagger? We're already using hostmeta (the .well-known location) for AS configuration data, so we could presumably use this type of location for the RS as well. If we could leverage existing tool chains that know how to consume Swagger (or other) formats in building UMA-aware clients, that would be cool.

How specific or orthogonal is this idea to UMA? Ideally we can not reinvent something. This seems largely orthogonal. The RS-C relationship is something that preexists the UMA resource protection mechanism, and others are already looking at how to get better and better at smoothing this relationship.

Enabling static declarations that can take advantage of prearranged trust models is always a good idea, since static vs. dynamic is so popular. Would this help IoT use cases, e.g. around building permissions into proactively issued RPTs? We're not sure.

George hasn't done a full "competitive analysis" of candidate formats yet. He notes that the Swagger schema is underdefined (i.e., no official JSON Schema), but the format seems sufficient to the task, and it's all JSON.

AI: Mike and George: Put together a quick spec text proposal.

Mike notes that he's been talking about enabling discovery for SCIM as well, and he does support UMA protection of the SCIM API in Gluu, so this could kill two birds with one stone.

URL pattern matching issue

(This was the "regex" issue in the agenda above.)

The original crux of the issue was that there may be an unworkable infinity of resources to be managed and protected by the AS, e.g. **/auction/***. But a further question is how UMA can distinguish between the GET and POST methods on the relevant resource. The normal way UMA expects different scopes/methods to be handled is:

1. C makes access request to RS using, say, POST on the desired resource, /auction. (To create a new auction.) C has an RPT.
2. RS introspects the RPT to see if it's valid and has sufficient authorization data (permission) associated with it.
3. If it doesn't (e.g., the RPT only has GET and not POST scope for this C and RqP), then it registers a permission ticket for the POST scope with the AS.
4. The RS returns the ticket to the C.
5. The C goes to the AS and figures out how to "win" sufficient authorization data to POST to /auction.

If you had **/auction/1234**, a GET would be viewing that item, and a DELETE would be to cancel the auction. In this case, when the client makes a request to this resource, it would want to request what scopes it can get. A key difference from OAuth to UMA is that OAuth clients are expected to go to the AS first and to know everything necessary about the available scopes, and UMA clients are able to be "dumber" and not know about specific scopes while the RS has to make a decision about what the desired scope would be when registering the requested permission and getting the ticket. Our assumption is that there would be some mapping of methods to scopes (could be 1:1, or *n*:*n* in complex fashion).

In SiteMinder and other access management tools, there's no assumption that the web plugin is going to send you the operation type along with the authorization request; the policy server then wouldn't be able to switch based on that. The URL could be distinguished based on the method, but that seems anti-RESTful! But if the distinction is made only by the RS at the resource registration level, then the question of RESTfulness isn't relevant. This was Mike's proposal in email, e.g.:

post:http://example.com/auction
get:http://example.com/auction/*
delete:http://example.com/auction/*

The web container use case is one that we might want to optimize for, because there are so many web servers that are going to want a plugin for modern access management: Tomcat, NGINX, etc. This pattern looks like "a qualifier plus a resource set", which actually could have its own further unique set of scopes. In a web container world, the qualifier could be HTTP methods, but in another context, the qualifier might want to be different. The RS is in complete control of what the qualifier is.

If there's an XACML-based policy mechanism that needs to map to what's being provided by the RS, you wouldn't necessarily want to tie this to HTTP. We want to preserve the ability to map to whatever policy and resource paradigm is being used by the AS/RS ecosystem in question. Eve notes that OAuth privileges the scope level because it doesn't formally have the resource set level, and UMA privileges the resource set level because it's "above" the scope level. The goal is for the RS to provide sufficient context to enable the AS to search for the requisite policy.

Mike notes: Mobile clients are "smart" enough to be able to state the scope they desire when making a request; the challenge is with web app clients. Vivek comments: A hidden form in the web app could help flesh out this context.

Eve thinks UMA has a lot of capabilities and extension points to allow lots of different solutions, e.g. the resource set level, the scope level, the ability to name resource sets and (indirectly) scopes, the ability to leverage the optional "type" property when registering resource sets, and even the ability to extend the JSON structures for registering resource sets and scopes to accommodate additional context as needed. Mike will investigate these avenues for a solution.

The group may ensconce some eventual decisions along these lines as "best practices" writeups for implementation and deployment scenarios.

Attendees

As of 27 May 2014, quorum is 7 of 12.

1. Eve M
2. Steve O
3. Mark D
4. Keith H
5. Jin W
6. Thomas H
7. Domenico C
8. Mike S
9. Maciej M

Non-voting participants:

- Vivek
- Zhanna
- George
- Yuriy
- Casey

Regrets:

- Sal D

Next Meetings

- **Focus** meeting Thu Jun 5 8:30-10am PT (time chart) - Eve and Mike regrets; Maciej can chair and find a note-taker
- **Focus** meeting Thu Jun 12 8:30-10am PT (time chart)
- **Webinar** Thu Jun 19 8-9am (time chart) followed by **focus** meeting 9-10am PT (time chart)
- **All-hands** meeting Thu Jun 26 8:30-10am PT (time chart)