UMA telecon 2010-09-02

Date and Time
- WG telecon on Thursday, 2 Sep 2010, at 9-10:30am PT (time chart)
  - Skype line "C": +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214

Agenda
- Administrative
  - Roll call
  - Approve minutes of 2010-08-26 meeting
  - Action item review
  - Status reports from the wider UMA world
- Scenarios and use cases
  - Current plans for revising the document
  - Select "canonical scenario" for next phase of design work
  - Rest of scenario work docket: CCTV, real-time, TaxMonkey, "morning after", terms negotiation, PDS, custodian...
- Resource/scope registration
  - UX wireframes and scope string examples
  - Client credentials problem in step 3
  - Dynamic registration I-D
- Consider offering to "own" discovery and registration in the OAuth group? Eran not working on it
- AOB

Attendees
As of 02 Sept 2010, quorum is 6 of 10.

1. Catalano, Domenico
2. Hoffmann, Mario
3. Machulak, Maciej
4. Maler, Eve
5. Moren, Lukasz

Non-voting participants:
- Anna Ticktin (staff)
- Kevin Cox
- Alam
- Aaron Titus
- Mark Lizar
- Herve Ganem
- Gerry Gebel

Regrets:
- Tom Holodnik
- Thomas Hardjono

Minutes

New AI summary

| 2010-09-02-1 | Mário | OPEN | Categorize all existing scenarios by their distinctive aspects by 2010-09-09. |
Roll call

Quorum was not reached.

Approve minutes of 2010-08-26 meeting

Deferred due to lack of quorum.

Action item review

- 2009-12-03-4 Eve Open Add terms-negotiation scenarios to Scenarios document. Now OBE.
- 2010-08-12-1 Eve, Mario Closed Meet to discuss how to move forward on the Scenarios and Use Cases document.
- 2010-08-12-2 Mario OBE Revise the Scenarios and Use Cases document by end of August.
- 2010-08-26-1 Mark Open Write up CCTV scenario. In progress. Draft by next Thursday.
- 2010-08-26-2 Mark Open Set up the next Legal subteam call. In progress.
- 2010-08-26-3 Herve Closed Write up real-time scenario(s). He'll send it to the list.
- 2010-08-26-4 Eve, Domenico Open Write up generic Alice/Bob trust framework scenario. In progress; Eve will revise on top of Dom's new revision and send to the list.
- 2010-08-26-5 Eve, Iain Open Eve to ask Iain to write up personal data store scenario. Still open.
- 2010-08-26-6 Eve Open Ping Denise Tayloe of Privo to see if she has interest in taking custodian scenario forward. Still open.
- 2010-08-26-7 Eve, Domenico Open Do some screenshots showing what scope management on the host and AM might look like. In progress; Eve has forwarded her scope-related email to the list.
- 2010-08-26-8 Christian Open Extract spec issues from 2010-08-26 minutes.

Scenarios and use cases

- Current plans for revising the document
- Select "canonical scenario" for next phase of design work
- Rest of scenario work docket: CCTV, real-time, TaxMonkey, "morning after", terms negotiation, PDS, Kevin's user story, custodian...

Eve and Mario met earlier this week, discussing the current document structure and publication mechanisms, the nature of approved/pending/rejected scenarios, and all of their distinctive aspects. He will start to edit the scenarios to characterize their aspects in more organized fashion, for example highlighting whether the scenario is person-to-person or person-to-service or machine-to-machine, etc., and he will also rationalize the terminology used throughout. They also discussed how to choose a canonical scenario. The theory is that choosing a single example to design and implement would help speed up our protocol work.

Eve proposes to choose a scenario that is roughly OAuth-like (person-to-service on the same person's behalf, and has a very small set of API endpoints) and Web 2.0-like (it's relatively low-security). Her thinking is that we have many real examples in the world today of such services, and so it will lower the bar to solving the basic problems that still remain, though she still wants to illustrate all the UMA design principles with it. Mario mentions the idea of creating an integrative scenario that has elements of all the distinctive aspects in one way or another. Herve likes going from the simple to the complex. Kevin speaks in favor of starting simple and moving to more complexity.

Goal: Next week we will definitively decide on the "canonical scenario" to target.

Resource/scope registration

- UX wireframes and scope string examples

The group discussed Eve's "scope thoughts" email. With the Flickr use case, it's obvious that a single scalar list of scopes can quickly get unwieldy when there are multiple "dimensions" of scope that might want to be applied (where "nouns"—resource URLs—and "verbs"—actions—are the two most obvious dimensions). Indeed, Herve points out, semantic incompatibilities could lead people to get very confused. E.g., what does it mean to "edit" a bank account? (Does Tom H. have thoughts on this related to the TaxMonkey scenario?) It's seemingly uncomfortable to have a single list of scopes that bundles together things of different types (such as Flickr "sets" and "tags"). Herve points out that sensor actions can get arbitrarily complex.

Mario suggests that we accept that the scope writeup (which goes from simple to complex) highlights the challenges around scope, but also recognize that it shows a way forward for simpler cases. As long as it's kept to a bilateral communication between a user and a host that has a specific API, it seems to be fine. The "moving resources" scenario might have challenges because even two hosts that do the "same job" might have completely different scope offerings, but this is a problem for another day.

So the central proposition is that scopes and their semantics are entirely host-specific. Do we agree with this proposition? It would be perfect if we can get Domenico to illustrate the issues with having multiple host-specific scopes come together in an AM interface.

Goal: Next week let's confirm our understanding of scopes and their role in the UMA flows.

Client credentials problem in step 3

Domenico has been working on solving this problem, using a digital-signature approach. The basic idea is to reuse the SAML "sender-vouches" method, which allows the host to confirm that the subject (the requester presenting an access token in step 3) is correctly bound to the access token being presented.

Eve poses a brainteaser to the group: Can we invent, in addition, a lightweight way to solve the problem that doesn't require digital signatures? Could we have the AM provision the requester with something that only the requester can use for wielding access tokens?

Dynamic registration I-D
Consider offering to "own" discovery and registration in the OAuth group? Eran not working on it

Maciej is interested in taking this forward. Eve notes that Christian started cataloguing comments that people in the OAuth group made on the spec draft, and he started incorporated a few fixes to his draft in github.

Next Meetings

- Legal subteam telecon on Wednesday, 8 Sep 2010, at 8-9am PT (time chart) on line C
- WG telecon on Thursday, 9 Sep 2010, at 9-10:30am PT (time chart) on line C