UMA telecon 2010-10-14

UMA telecon 2010-10-14

Date and Time

- WG telecon on Thursday, 14 Oct 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 2010-10-07 meeting
    - Agenda-bashing for both upcoming F2Fs
    - Action item review
    - Bounty proposal review and approval
    - Updates from the wider UMA world
- Second review of proposed scenario dimensions
- New trusted claims proposal?
    - Domenico's previous trusted claims writeup and UX wireframes
- Revisit scope discussion and plan for its conclusion
    - Thomas's access control proposal
- AOB

Attendees

As of 11 October 2010, quorum is 7 of 12.

1. Adams, Trent
2. D'Agostino, Salvatore
3. Fletcher, George
4. Hardjono, Thomas
5. Hoffmann, Mario
6. Holodnik, Tom
7. Lodderstedt, Torsten
8. Machulak, Maciej
9. Maler, Eve

Non-voting participants:

- John Bradley
- Kevin Cox
- Herve Ganem
- Mark Lizar
- Cordny Nederkoorn
- Mike Seilnacht
- Anna Ticktin (staff)

Regrets:

- Domenico Catalano
- Lukasz Moren

Minutes

New AI summary

2010-10-14-1	Eve	Open	Revise bounty program proposal and work with Dervla to announce it as soon as possible.

Roll call

Quorum reached.

Cordny is from Holland. He's a software tester, interested in authn and authz of web applications.

Torsten is a system architect for identity management for Deutsche Telekom, and is based in Germany. He's an active contributor to OAuth 2.0 standardization. He has a particular interest in our shared vision of where OAuth should be going.

Mike is a software architect at Intuit, and has just moved into a security architect role.

Approve minutes of 2010-10-07 meeting

Minutes of 2010-10-07 meeting APPROVED.

Agenda-bashing for both upcoming F2Fs

Eve publicized the F2Fs, particularly the IIW one, on her blog; everyone please feel free to do the same and to retweet @UMAWG postings.

What should the goals be for the Paris F2F next week? Attending will be Herve, Maciej, Mario, Alam, John Bradley, Fulup Ar Foll, Trent, and possibly others. Let's set these the goals:

- Conclude resource/scope registration decision-making (Maciej will plan to present on this topic)
- Drill down into the location scenario and its constituent use cases
- (optional) Push forward trusted claims if possible

Action item review

- 2010-09-02-1 Thomas Open Categorize all existing scenarios by their distinctive aspects. Progress made.
- 2010-09-16-1 Mark Closed Update main trunk of the Legal Considerations document with Legal subteam input.
- 2010-10-07-1 Eve, George Closed Draft/review a bounty announcement that identifies clear rules of engagement and near-term deadlines.
- 2010-10-07-2 Sal, Domenico Open Propose the next version of the trusted claims solution, making appropriate simplifying assumptions.

Bounty proposal review and approval

Draft 0.3 was sent to the list.

Regarding the **requirements** bullets:

John comments that perhaps OSIS should host the testing code, rather than KI. John and Joni have been discussing possible KI/OSIS synergies here. So we should soften the wording in the third requirements bullet to add "...or another agreed-upon site".

We should also clarify in the same bullet that testing code must be made available under a well-recognized open-source license. This is usually the assumption with bounty programs, but Eve forgot to say it anywhere. Trent notes that the only license that is currently acceptable to be contributed to KI is Apache 2.0, and recommends that we assess license suitability (for example, regarding the ability to incorporate the tests into a commercial offering) at evaluation time.

Tom wonders if we should mention positive and negative test cases, to test error conditions. Cordny and John wonder if the specs would simply drive this, since they describe error conditions, but then again, sometimes specs leave negative conditions un-remarked-on. Let's state both.

Regarding the **bounty program details** bullets:

John suggests that we need a period for interaction with submitters to get the submissions into shape. Since we can't vote on the submissions any later than Dec 16, we should bake into the program details a suggestion that submitters provide draft submissions for the WG's review and feedback no later than 6 Dec 2010. Let's do that.

Bounty program proposal draft 0.3 APPROVED with the four amendments noted in the UMA telecon 2010-10-14 minutes.

Second review of proposed scenario dimensions

Nature of protected resource dimension: This includes the API endpoint vs. content-oriented distinction, and also captures any known scope details. We have a technical issue to solve when there's a unified API endpoint that doesn't distinguish between particular users (like Twitter's and FireEagle's endpoints today). We'll defer discussion of this issue for a moment.

Sharing models dimension: The purpose of this one is primarily to figure out what sort of OAuth interaction is required on the authorizing and requesting sides. It also impacts the type of policies and claims that might be seen. Person-to-rep sharing would probably drive identifier claims about the company name, not the representative's name. The company would have delegated some rep to do an Alice-authorized task, though this may be outside the view of UMA. Mark has been continuing to work on the Legal Considerations document, which is where we have currently captured quite a lot of these distinctions. He'll work on including more of this conversation into that document.

Nature of policies and claims dimension: This has a dependency on the sharing model. Earlier, we were trying to make "person-to-self" into "person-to-service-on-Alice's-behalf" so that Alice can impose privacy and data portability policies on parties like Google Calendar, but can this really work? Can we privilege the requester app as an intermediary that's "nearly at the end of the line" as far as a sharing agreement is concerned? Does our ability to do this differ depending on whether the requester app is, say, a mobile app vs. a web-server-capable app (that is, based on OAuth client types)? Ideally, in Alice-to-Bob sharing, Alice might have policies around "only bob@gmail.com can subscribe to this calendar" *and* "Google Calendar must not use my calendar data for purposes unrelated to letting Bob interact with my calendar". But we haven't seen a way to do that yet. Once again, delegation rears its ugly head.

There is one other place in the UMA protocol where a requester *could* be made to provide claims about adherence to various policies, which is in Step 1 – in other words, our embedded OAuth flow could be an embedded UMA flow! However, any such claims would apply to the requester app with respect to the AM as a whole, not per authorizing user at that AM.

Mark asks: How could notice be given about the policies being adhered to by the requesting side? Eve observes that OAuth (and therefore UMA) let you expire refresh tokens, forcing a requesting party to re-supply claims (the nature of which may have changed in the interim). John points out that the window of token validity may be longer than the period where you want to have such an opportunity; he also observes that in an OAuth world, the concept of "notice" may not apply very well.

Next Meetings

- WG F2F on Wednesday, 20 Oct 2010, at 9am-noon CET (time chart) - no dial-in, and no telecon this week
- WG telecon on Thursday, 28 Oct 2010, at 9-10:30am PT (time chart) on line C
- WG F2F on Monday, 1 Nov 2010, at 11am-5pm PT (time chart) - no dial-in, and no telecon this week
- WG telecon on Thursday, 11 Nov 2010, at 9-10:30am PT (time chart) - Maciej to chair?