UMA telecon 2010-03-25

UMA telecon 2010-03-25

• Date and Time
• Agenda
• Attendees
• Minutes
  • New AI Summary
  • Roll call
  • Approve minutes of 2010-03-18 meeting
  • Action item review
  • Eve report on IETF77 OAuth meeting
  • Maciej report on paper submissions and plans
  • Domenico report on UX progress and plans
  • TomH walkthrough of small-business scenarios
  • Resource-oriented scoping and how to expand scope (as discussed on 2010-03-18)
  • OAuth's "three use cases" for signatures: what are UMA's use cases?
  • Gerry report on news from the health data world
  • Other spec issues
• Next Meeting: UMA telecon 2010-04-01 (no, really)

Date and Time

N.B.: U.S. Daylight Savings Time is in force for this meeting, and UTC correspondingly "shifts". Locations that have not yet shifted to summertime will have a meeting-time skew.

• Day: Thursday, 25 Mar 2010
• Time: 9:00am-10:30am PST | 12:00-1:30pm EST | 16:00-17:30 UTC (time chart)
• Dial-in:
  • Skype: +9900827042954214
  • US: +1-201-793-9022 | Room Code: 295-4214 (other local country numbers available on request)

Agenda

• Roll call
• Approve minutes of 2010-03-18 meeting
• Action item review
• Eve report on IETF77 OAuth meeting
• Maciej report on paper submissions and plans
• Domenico report on UX progress and plans
• A user-experience testing victim has stepped forward! What next?
• TomH walkthrough of small-business scenarios
• Spec issues:
  • OAuth's "three use cases" for signatures: what are UMA's use cases?
  • Token profile questions (see also the Lexicon)
    • Any hard need for refresh tokens to be issued in all cases, due to positioning of claims-required?
  • Token validation models
  • Greater modularity given potential wider interest in selected pieces of our functionality?
  • Resource-oriented scoping and how to expand scope (as discussed on 2010-03-18)
  • Needs for "identity tokens" as previously proposed by George et al. for access authorization claims?
• If time, discuss custodian scenario input received
• AOB

Attendees

As of 19 Mar 2010, quorum is 7 of 13.

1. Adams, Trent
2. Armstrong, Brian
3. Bryan, Paul
4. Catalano, Domenico
5. Fletcher, George
6. Holodnik, Tom
7. Machulak, Maciej
8. McIntosh, Michael
9. Maler, Eve

Non-voting participants:

• Gerry Beuchelt

Regrets:

• Hasan ibne Akram
Minutes

New AI Summary

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Open/Close</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-03-25</td>
<td>Paul</td>
<td>Open</td>
<td>Send email giving examples of how a resource-oriented scope approach is necessary.</td>
</tr>
<tr>
<td>2010-03-25</td>
<td>Eve</td>
<td>Open</td>
<td>Add security consideration section to the spec with a placeholder for the &quot;TurboTax use case&quot;.</td>
</tr>
<tr>
<td>2010-03-25</td>
<td>Eve</td>
<td>Open</td>
<td>Create fresh protocol issues list based on 2010-03-25 agenda items.</td>
</tr>
</tbody>
</table>

Roll call

Quorum was reached.

Approve minutes of 2010-03-18 meeting

Minutes of 2010-03-18 meeting APPROVED.

Action item review

Everything is under way.

Eve report on IETF77 OAuth meeting

Eran will edit a new spec based on a draft written initially by David Recordon late last week that combined elements of OAuth 1.0a and WRAP.

Progress was made on describing the various use cases for signing messages; pockets of wider interest for various UMA extension piece-parts were uncovered.

Maciej report on paper submissions and plans

We have submitted a paper on UMA to the Web 2.0 Security and Privacy workshop, which is colocated with the IEEE Symposium on Security and Privacy. We'll distribute the paper to the mailing list as soon as we can. We also prepared a two-page abstract, which we'll submit to the Symposium as a "poster"; that deadline is still farther out.

In future, we hope to work on papers that include implementation experience, e.g. for the ACM Digital Identity Management workshop.

Domenico report on UX progress and plans

He has distributed a slide deck explaining the work to date and future plans. The newest wireframes (a few weeks back) explored some access analytics ideas. Maciej explained that Bath University is interested in studying how users perceive the user interface for an AM; we'll hope to partner with them. We plan to produce a new set of wireframes taking into account UX best practices, targeting the EIC workshop as a deadline.

- A user-experience testing victim has stepped forward! What next?

We'll get back to him later, when we have some new materials for him to react to.

TomH walkthrough of small-business scenarios

He feels there are a number of ways to implement his high-level scenarios, and in particular the delegated (custodian) models would likely be involved. The sorts of claims that a requester would have to present, and the kinds of policy a business owner would want to set, bring up additional complicating factors.

His scenario #1 is the most common: "Small business owner delegates to contractor. Small business owners often hire accountants to operate payroll and manage payroll taxes for their business. " Lots of small business owners try to stay away from the messy business of payroll management. The business owner would tend to interview accountants, and then would invite the chosen accountant to join the business "sandbox". The accountant would need to show some form of identification. Family businesses might have an informal arrangement with them, or it could be more formal.

Is it possible to ask for claims about "experience"? If they're just self-asserting their experience, it may not be very valuable. This is a bit like some parts of our CV scenario, where professors could write letters of recommendation.

Some fields in business applications are restricted from view in the accounting workflows, such as credit card information. If they become visible, special levels of authentication or access control might be required. This is fairly complex to achieve in the best of circumstances (e.g., sophisticated enterprise environments).

One accountant (requesting party) might have multiple business clients (authorizing users with hosts), and would need to be issued different access tokens per business client. UMA can probably handle this just fine.

The current way of doing things involves a business owner inviting an accountant in. This probably equates to an authorizing user provisioning a requester directly with a URL – perhaps the UX could involve niceties like the user telling the AM to generate an email message to some requesting party that launches them into an UMA flow. And indeed, the current practice of using "private URLs" could be used to bootstrap the UMA flow with strong-enough authentication for lots of purposes.
Eve issues a call for additional use cases that cover “ACL-building”, of which these are an example.

**Resource-oriented scoping and how to expand scope (as discussed on 2010-03-18)**

Can we actually force the scope parameter in UMA to be resource-oriented? Paul would like to, but Eve would feel more comfortable making our scheme advisory and hoping it will spread (“catching flies with honey” and appealing to those who are already practiced in thinking RESTfully). There’s a concern about artificially limiting our audience.

Paul feels that it shouldn’t be too foreign to require an HTTP-based way of expressing scope. George presents a counterexample: What if the parameters passed to the same endpoint with the same method change the semantics of access dramatically? Paul is concerned that hosts in a loosely coupled system need to be able to present their API in a way that’s as standardized as possible, or the ecosystem will have a serious interoperability barrier. Eve wonders if published/standardized APIs (amenable to being expressed in scope parameter form), even if they’re not RESTfully oriented, would help interop as much.

See the [Session Extension spec](http://nhindirect.org/session-extension-spec) proposed for OAuth to see a way to increase the scope of a token; even though the general idea of a refresh token was included in WRAP, the scope-change solution wasn’t included. We may want to extend OAuth 2.0 to do this if it’s not included.

**OAuth’s “three use cases” for signatures: what are UMA’s use cases?**

The proposition is that UMA benefits from the “third use case” for signed Client->PR messages in WRAP/OAuth 2.0, in which the client signs the message so that the server can tell, in a more “semantic” way, exactly who the client is (vs. just recording their IP address).

Brian Eaton had claimed that OAuth 1.0’s signature model doesn’t actually solve this problem, and Paul agrees. The issue is that the credentials backing up that signature might have aged (becoming less valuable), or might have been revoked. An UMA host with SSL trusts its own PKI enough to have a high level of assurance that the messages from the party on the other end (the UMA requester) haven’t been compromised, so that takes care of the “first use case” (where SSL isn’t strong enough). If they still want to identify the requester more strongly and rely on the requester’s signature of the message, they have to wonder if the requestor treated their own credentials with as much hygiene as the host would demand.

Thus, in the special UMA use cases where the AM (based on user policy) demands strong requester identification before issuing a token, the AM can sign a structured bearer token that the requester can carry over to the host, or issue a token that the host could use to make a back-channel query about the requester’s identity (currently not specified by UMA, but it could be if we saw a need). In either of these paths, the complexity is sequestered to (a) the AM and (b) the special use cases where requesters already have to be “smarter” because they have to get, store, and provide third-party claims or otherwise have to provide special claims.

And if the AM didn’t care enough (based on user policy) to ask for strong requester identification, then the host has no business knowing either, whether for auditing purposes or for its own idle interest.

Tom is concerned about cross-site attacks that might mess with the request. Is there a way for a malicious party to compel a client to give up something inappropriate? If the client has an embedded webkit/HTTP engine, are there cases where the client application would behave in a manner similar to a browser in injecting scripting into other applications? Moving funds from one domain into another, or other non-idempotent operations, would be a sensitive operation. (A la the TurboTax use case discussed at the recent F2F.) Paul suggests that bearer tokens need to be protected just like cookies, so the same security policies should be followed in this case.

Eve observes that the “UMA layer” seems to provide a potential solution to this third use case for signing, but this solution isn’t available to pure OAuth users.

**Gerry report on news from the health data world**

Project hData is a new, lightweight approach to electronic health records, which is now an HL7 project. It moves away from passing around large monolithic documents, making the data more modular. In addition, it enables more efficient exchange of the data using a RESTful approach. It needs to secure access to this information, and it has identified UMA as the likely solution. A number of user stories have been developed.

At the annual HIMSS conference they announced a new project called NHIN (Nationwide Health Information Network) Direct. NHIN has been around for a while and is currently rather SOAP-oriented and heavy. The new NHIN Direct project also wants to adopt a more RESTful approach. Contributions, including user stories, are being gathered on a wiki, and hData work is getting noticed here. In this forum, there’s interest in OAuth in managing access, and there is starting to be interest in UMA too.

Gerry invites UMANitarians to join the discussion and add their thoughts. Brian comments that these topics are core to his interest as well.

See, e.g.:

- [http://nhindirect.org/specifications-and-service-descriptions](http://nhindirect.org/specifications-and-service-descriptions)
- [http://nhindirect.org/hData+Mapping+to+User+Stories](http://nhindirect.org/hData+Mapping+to+User+Stories)

**Other spec issues**

- Token profile questions (see also the [Lexicon](http://nhindirect.org/lexicon))
- Any hard need for refresh tokens to be issued in all cases, due to positioning of claims-required?
- Token validation models
- Greater modularity given potential wider interest in selected pieces of our functionality?
- Needs for “identity tokens” as previously proposed by George et al. for access authorization claims?

Deferred.

**Next Meeting: UMA telecon 2010-04-01 (no, really)**

- **Day:** Thursday, 1 Apr 2010
• **Time:** 9:00am-10:30am PST | 12:00-1:30pm EST | 16:00-17:30 UTC (time chart)

• **Dial-In:**
  - Skype: +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214 (other local country numbers available on request)