UMA telecon 2009-12-10

UMA telecon 2009-12-10

Date and Time

- **Day:** Thursday, 10 Dec 2009
- **Time:** 9:00-10:30am PST | 12:00-1:30pm EST | 17:00-18:30 UTC (time chart)
- **Dial-In:**
    - Skype: +9900827042954214
    - US: +1-201-793-9022 | Room Code: 295-4214 (other local country numbers available on request)

Attendees

Quorum: 10 of 19.

Voting participants:

1. Adams, Trent
2. Akram, Hasan
3. Bryan, Paul
4. Carroll, Tom
5. Catalano, Domenico
6. Chadwick, David
7. Davis, Peter
8. Fletcher, George
9. Hanson, Michael
10. Lizar, Mark
11. Machulak, Maciej
12. Maler, Eve
13. Scholz, Christian
14. Smith, Bill

Regrets:

- Tom Holodnik
- Iain Henderson

Agenda

- Administrative
    - Roll call
    - Approve minutes of UMA F2F 2009-12-03
    - Action item review
        - Eve: "Hey, Sailor" scenario
        - Gerry: hData scenario
        - Hasan: "Protected status query" issue into Scenarios doc
        - Eve: (with Maciej, Hasan, Dom) Slide deck
        - Mark W.: Shindig contacts
        - Eve: Reach out to OAuth consumer devs
        - Paul: Strawman claims-handling spec
        - Eve: Terms-negotiation scenarios
- Review and approve/defer/reject scenarios and use cases
    - E-commerce
    - Personal loan
- Claims spec review
- AOB

Minutes

Administrative

Roll call

Quorum was achieved.

Approve minutes of UMA F2F 2009-12-03

Minutes of 2009-12-03 APPROVED.

Action item review

- Eve: "Hey, Sailor" scenario: still pending, though partly covered by the terms negotiation scenario writeups.
- Gerry: hData scenario: Eve will take an AI to ping Gerry to get this done.
- Hasan: "Protected status query" issue into Scenarios doc: to be done next week; we're pleased with the diagrams so far; Paul notes that some of the arrows do vs. don't represent protocol interactions, so maybe we need to have conceptual vs. "protocol-accurate" versions. Swimlane diagrams are best for strict protocol accuracy.
- Eve: (with Maciej, Hasan, Dom) Slide deck: still in process: consider doing a webinar early in the new year.
- Eve: Reach out to OAuth consumer devs/Mark W.: Shindig contacts: Mark uncovered two appropriate Google and Shindig contacts, including one person intimately familiar with the Dropbox OAuth implementation. Eve will follow up with Mark's contacts, and talk with the JanRain RPX guys.
- Paul: Strawman claims-handling spec: still pending.
- Eve: Terms-negotiation scenarios: still pending; David suggests that the "requester identification" and general "statement" scenarios might bleed together. There is little-to-no difference in implementation between a uniquely identified vs. a non-uniquely identified requester. This is precisely the issue that is hanging Paul up.

New AIs collected during the meeting:

- Eve to reach out to Gerry
- Slide deck team to work out a plan to host a status update webinar
- Eve: contact Mark's names
- Eve: soften "prove in court" language in e-commerce scenario
- Eve: remove "payment privacy" use case from e-commerce scenario
- Paul and Mike: comment on Dom's latest diagrams on the list
- Eve: capture potential requirement about independently verifiable access-agreement claims

Review and approve/defer/reject scenarios and use cases

The criteria are:

- Does this scenario belong in the problem space for UMA V1? (if not, defer or reject)
- If so, does it clearly articulate its distinctive aspects? (if not, revise)
- If so, does it appropriately steer clear of technical detail? (if not, revise)
- If so, then approve

E-commerce

Mike: "If Staplers behaves badly (gives out her data against her rules or allows a data breach to occur), she wants to be able to prove so – in court, if necessary." should be out of scope. Paul: Agrees that it should be out of scope for the protocol to make this literally/technically provable, but wants to consider the terms as an agreement. That is, the terms and the requester's agreement should be admissible in court somehow.

Mike: So is non-repudiation in scope? Eve: "Deep" non-repudiation (with key escrow etc.) is too hard. Mike: But how do we protect Staplers against Maya? What if Maya changed the terms after Staplers agreed? Paul: Agreed that we do have to provide the option to make claims independently verifiable, where this is what contracting parties want. Mike: This might end up being a matter of security considerations advice where we say the AM has to log things appropriately. Eve: This may want to be a new requirement somehow.

David: The trend in Europe is not to accept systems that won't provide this level of verifiability, e.g. around user credit card info. George: We're talking about two different kinds of claims here – there's user information that might be stored in a "personal datastore", and there's claims used to achieve an **UM A access agreement**.

Perhaps we can illustrate this scenario with Dom's multiple-hosts picture. We will try and do the disposition of this scenario next week.

We discussed Eve's notion of a "relationship manager" application, which at a minimum implements an AM endpoint but: (a) has to implement a number of UX functions to interface with the user, (b) has to implement a number of internal functions such as event logging that are not "visible" to protocols, and (c) may in addition implement other UMA endpoints, such as a Host and even a Requester! The concept of a relationship manager is discussed more in this blog post. Is **relationship manager** the right term for this? This is still not decided (it came up in this week's Kantara Info Sharing call as well), but we do need to account for it in at least one of our terminology diagrams, so that we can discuss on-board Hosts that might help package several multi-hosted resources.

Personal loan

Deferred.

Claims spec review

Recap: Paul couldn't find an expressive enough format in existing work that could avoid a "claims explosion" to cover, for example, every possible age and age range. (Age information could be an "UMA access agreement" claim, e.g., if you want to ensure that the requesting party is old enough to receive adult material.) This is why he delved into the parameter mechanism.

His current approach uses JSON, and he's feeling more and more confirmed in this approach. JSON structures can be serialized into objects in numerous languages with no ambiguity, and they are widely supported. An alternative could have been a flat format, but then some structured info would have to be crammed into flat string values. The other extreme would be XML, which isn't that "extreme" really, but it would introduce ambiguity due to impedance mismatches with programming data structures (this is why JSON was invented, after all).

Due to the conversations with David on the list, Paul has added a notion of "qualifications" on claims, including "critical" vs. "advisory" ones. This is akin to SAML's notion of Conditions vs. Advice.

The CouchDB folks have come up with a straightforward method of normalizing and signing JSON structures, which Paul has been inclined to use. We pinged the WRAP list to see what their plans are around JSON web tokens, and it could be that their alternative is better.

Bill: Do we plan to use the same mechanism for promises? Paul: Yes. Eve: Expects that most Internet-scale use cases will have a simple structure that just mentions the URL of the standard agreement terms that you're promising. E.g., Creative Commons copyright licenses could be used today – without having to invent any new terms! – to ensure that a requester *promises* to adhere to your CC terms before it gets access to your CC-licensed Flickr photo.

Paul proposes to use an extra-simple structure that adheres to "one statement per claim". This would mean that it's easier for a requester to subset claims coming from an original issuer before remanding them to the AM (which is the "relying party" in this case).

If the protected resource is a survey, and you want to limit takers of the survey to people who are between the ages of 18 and 35, the AM might demand a claim from the requester saying that the requesting party is between those ages. Or if the protected resource is some adult material, the AM might demand a claim from the requester saying that the requesting party is over 18 or 21. This is akin to the "identity oracle" concept that Bob Blakley has proposed; the data is "cooked" to achieve minimal disclosure before being released, rather than the "raw" birthdate being shared.

Eve: This is where a "relationship manager" application that houses not only an AM endpoint but also a Requester endpoint could help mediate the providing of such verified information. It could even have a parallel process to the UMA allowance for real-time consent by authorizing users, to let requesting parties consent to providing "UMA access agreement" claims.

Last Meeting of 2009: UMA telecon 2009-12-17

- **Day:** Thursday, 17 Dec 2009
- **Time:** 9:00-10:30am PST | 12:00-1:30pm EST | 17:00-18:30 UTC (time chart)
- **Dial-In:**
    - Skype: +9900827042954214
    - US: +1-201-793-9022 | Room Code: 295-4214 (other local country numbers available on request)