UMA telecon 2011-03-03

UMA telecon 2011-03-03

- **Date and Time**
- **Agenda**
- **Attendees**
- **Minutes**
  - New AI summary
  - Roll call
  - Approve minutes of 2011-02-17 meeting
  - Action item review
  - Review of trust model work and TODOs
  - Next steps for progress on core spec revisions related to scoped access
  - Review of previous day's Claims 2.0 discussion
  - Review reg changes and issues
- **Next Meetings**

**Date and Time**

- WG telecon on Thursday, 3 Mar 2011, at 9-10:30am PT (time chart)
  - Skype line "C": +9900827042954214
  - US: +1-201-793-9022 (other int'l numbers) | Room Code: 295-4214

**Agenda**

- Roll call
- Approve minutes of 2011-02-17 meeting
- Action item review
- Next step for progress on core spec revisions related to scoped access
  - Some details decided last week
- Review of trust model work and TODOs
  - New content and diagrams to consider?
- Review of previous day's Claims 2.0 discussion
- Review reg changes and issues
- AOB

**Attendees**

As of 24 Feb 2011 (post-mtg), quorum is 7 of 13.

1. Mohammad, Alam
2. Catalano, Domenico
3. D'Agostino, Salvatore
4. Hardjono, Thomas
5. Machulak, Maciej
6. Maler, Eve
7. Moren, Lukasz
8. Morrow, Susan
9. Wolniak, Maciej

Non-voting:

- John Bradley
- Kevin Cox
- Mark Lizar
- Cordny Nederkoorn
- Frank Wray

Observer:

- Bob Cope

Regrets:

- Paul Bryan
- Christian Scholz

**Minutes**

**New AI summary**

[2011-03-02-1 (http://groups.google.com/group/kantara-initiative-uma-wg/browse_frm/thread/00d866779be57fe1)](N) [Open](N) Put together JWT-compliant examples of Claims 2.0 and Simple Access Authorization Claims.
Roll call

Quorum was reached.

Approve minutes of 2011-02-17 meeting

Minutes of 2011-02-17 meeting APPROVED.

Action item review

- 2011-01-27-1 Paul Open Revise the Claims 2.0 spec to reference and profile JWT.
- 2011-02-10-1 Alam Open Share details of his planned UMA demo with the list. Very soon. Alam and Cordny are both presenting on UMA at the EEMA conference. They’ve been coordinating.
- 2011-02-24-2 Susan, Eve Closed Revise trust model according to the discussion from 2011-02-24.

Review of trust model work and TODOs

Jeff Stollman made some great comments on the list. One issue he brought up: Is "trusting" and "relying on" the same thing? In practical terms, should we switch to "trusting party" and, e.g., "User trusts host operator" (TR-1a)? Mark points out this could be described as a need for "confidence" in their actions, which has a social dimension. John warns about going in circles on terminology. Sal notes that we’ve got core relationship requirements that we need to record, and liability is a blunt instrument to be used only when things go wrong. Mark observes that indemnity is the other half of liability.

Let’s keep the language we have, track Rainer’s work over time in case the recommendations around "reliance" change, and scrutinize the verbs that currently appear in our “Expected behavior” column.

- See Domenico’s new diagramming trust graphic.

Thomas has long experience in defining technical trust (and other kinds of trust – social, business), including in hardware systems. He suggests labeling the arrows to say explicitly "A trusts B to...". Eve proposes that our TR-7a is really only talking about technical trust, and really the job of this document is to get as far as business trust. It seems like the layers go like this:

1. Technical trust (APIs "contracts" between software or hardware components – this approaches "compliance" to specs or profiles)
2. Social trust (expectations about responsibilities)
3. Business trust (a model of liability/indemnity that applies to parties whose responsibility rises to the level of "duty")

The matrix is generally agreed to be valuable. The requester is kind of hanging out to the side; what should this mean? It’s a good idea to remove the requester and keep the diagram just containing “parties”, and then consider making a whole separate diagram for “endpoints” that can illustrate the technical-trust layer.

The danger in labeling 0 through 3 is that people will think of NIST-like Levels of Assurance! Maybe we should call them Llama, Alpaca, Chinchilla...

Next steps for progress on core spec revisions related to scoped access

- Some details decided last week.

Right now, the implementer population is being held back by the lack of detail and accuracy in our core spec. We’ll probably need Paul’s help, but could also use other’s help, to remedy this. Let’s plan on doing a collaborative editing session for the week of Mar 14.

Review of previous day’s Claims 2.0 discussion

- See meeting notes.

The Claims 2.0 spec defines, and the Simple Access Authorization Claims spec utilizes, a "templating" trick where the claims-requested message that the AM sends to the requester looks like a wildcarded/regex version of the claims that are desired to come back in response.

The "( | )" trick seems really useful, particularly for issuers. The "*" trick seems useful but limited. John feels "<" and ">" operators would be very useful for privacy reasons, since it makes it easier to find out if a person is "over 18". And not having them available may lead to claims definition standards that are anomalous (a claim for "over 18", a claim for "over 13", etc.). But maybe we should be very cautious about adding new operators and adding data types. A lot of claims that we can imagine are relatively specialized or vertical; would requester software need to understand all of them, or would it have recourse to some kind of discovery service or catalog to find out where to go to get the needed claim? Discovery would be an added level of complexity. Then again, an OpenID Provider has to be a kind of discovery service, and so maybe we can point off to that.

OpenID ABC may be in the position of profiling or extending Claims 2.0! That sort of feedback would be important to listen to if we want Claims 2.0 to be a reusable modular for reasonable other purposes. JWT defines a "claims response message format", but is currently missing a request format. This is where our spec comes in.

We’ll bring this up for discussion again when we have Nat’s examples to look at.

Review rreg changes and issues

The SMART implementation enforces uniqueness of resource set identifiers among users at the host. We had made a decision not to require uniqueness of this sort, but maybe the book isn’t closed on this. We need to spec the scoped-access stuff to fully see the consequences.

Next Meetings
• WG telecon on Thursday, 10 Mar 2011, at 9-10:30am PT (time chart) – Eve regrets; Maciej to chair and publish agenda/minutes
• WG telecon on Thursday, 17 Mar 2011, at 9-10:30am PT (time chart) – Eve may need to miss first part; Maciej to chair?
• WG telecon on Thursday, 24 Mar 2011, at 9-10:30am PT (time chart)