UMA telecon 2014-09-11

UMA telecon 2014-09-11

Date and Time

- **Focus** meeting Thu Sep 11 9-10am PT (time chart)
  - Voice: Skype: +99051000000481 or US +1-805-309-2350 (international dial-in lines), room code 178-2540#
  - Screen sharing: [http://join.me/findthomas](http://join.me/findthomas)

Agenda

- Upcoming schedule
  - No meeting next week
  - Game plan for V1.0: Can we strive for quorum in meetings generally through the fall to get solid issue-resolution consensus?
  - Interop planning meeting
  - No telecon Oct 30 due to IIW (and open implementors’ meeting Oct 29)
- Quick Utrecht workshop report
  - Introduce Domenico's delegation use case: capture issue?
- Speaking opportunity Nov 25-27 at Alexandra Institute ID conference
- RSA conference submission coordination
- Issues 88 and 99: conclude today if possible
- Choose next issues to focus on
- AOB

Minutes

All-hands meetings

Game plan for V1.0: Can we strive for quorum in meetings generally through the fall to get solid issue-resolution consensus? We'll try!

Interop planning

We have a planning meeting on Sep 29.

No telecon Oct 30 due to IIW (and open implementors’ meeting Oct 29).

Utrecht workshop report

Mark reports: He liked it and learned a lot. He presented the Kennisnet use case. The feedback was good and useful. He took away that Mark Lizar's Consent Receipt work is an important missing piece in the Kennisnet work. Mark L put together a dashboard view of consent. So Mark D took away an AI to look into this, and there's going to be a followup discussion. There's a concept of a Notice Registry that could be a co-located function of an UMA authorization server.

Adrian notes that, in healthcare, there's a need for "Accounting for Disclosures" that needs to be accessed at individual relying parties for privacy reasons. Would the consent receipt play a role in pointing to where the resource owner could find the AIDs? It appears yes. Eve notes that, by default in UMA, the RS never does tell the AS that it did give access to some client/RqP on request – she'd seen this as a "bug" in that you can't (without further extension of what the RS tells the AS about actual access having been granted) centrally know what access was given, but maybe it's a "feature" for healthcare data in that this is kept decentralized.

Domenico presented an IoT use case where: The doctor needs share patient’s heartbeats data with EHR system and an external party. The sharing policy should be inherited by the mediator client (smart device) which will act as resource server for the EHR system and external Requester. The idea is that the granting of access comes with the right to grant further sharing "downstream". Adrian notes that in healthcare (which this example uses as the scenario!), the patient's identity is very important to be clear about! Is the patient pseudonymous, or what? So it could be that the granting of further sharing must be under deidentification controls of some sort. Domenico's wireframe example has an "anonymous data" checkbox, in fact.

Mark L notes that a patient dealing with a hospital has granted certain kinds of consent to the hospital. The user’s authorization system could query the hospital system for consent information.

Speaking opportunity Nov 25-27 at Alexandra Institute ID conference

Andi may be available for this.

RSA conference submission coordination

AI: Mike, Eve, Joni, Sal, Maciej, George: Coordinate on RSA talk submissions.

Issues 88 and 99: conclude today if possible
Rev 04 was the last time we had the eager permission registration, the short flow, and fewer protection API endpoints. We discussed this in depth last week. Mike speaks in favor of a change to the short flow. There isn't a general concern about a denial-of-service attack perpetrated by the client on the RS and AS by asking them to do work, because this is a constant concern in loosely coupled protocols with initially untrusted requesting entities anyway. This is such a generic security concern that we're wondering if it needs to be mentioned at all. A write to an in-memory database constitutes less of a threat, from a scalability perspective, than a persistent data store; a permission ticket likely falls into this category. The AS could even encode all the necessary state into the permission ticket itself, say, in encrypted form; there's no back-end write, just introspect whatever it's handed back.

Giving the RS the option to choose to register the permission eagerly or lazily is still possible; this is the lazy flow:

1. Client approaches RS with no RPT
2. RS gives as_uri without registering a permission
3. (Assumes AAT gotten by now) Client goes to AS authorization data request endpoint with no RPT and no ticket
4. AS gives client RPT
5. Client goes back to RS with RPT
6. RS registers permission
7. AS gives RS permission ticket
8. RS gives as_uri and permission ticket
9. Client goes to AS with RPT and permission ticket
10. AS does claims-gathering...

This is the eager flow:

1. Client approaches RS with no RPT
2. RS registers permission
3. AS gives RS permission ticket
4. RS gives as_uri and permission ticket
5. (Assumes AAT gotten by now) Client goes to AS with RPT and permission ticket
6. AS does claims-gathering...

We generally try to avoid optionality, so picking one would be nice. Note that the client does have to have an AAT to interact with the AS, but not with the RS.

What if we choose the eager flow once again, but resurrect the SHOULD language that we used to use (inconsistently) for all the response message language in the spec, motivating those SHOULDs with some health-warning security considerations language saying that it is the responder's "right to refuse service" in case of a DoS attack or other suspicious motives on the part of the requesting entity?

AI: Eve, Thomas: Propose text for eager permission registration and associated spec changes and float on the list for final decision in the Sep 25 all-hands call.

AI: Eve: Stimulate discussion of the single-RS eager binding question and the RPT expiration question on the list leading up to the Sep 25 all-hands call.

Attendees

- Eve
- Mark D
- Domenico
- Susan
- Adrian
- Andi
- Mike
- Sal
- Mark L
- Yuriy
- Jin
- George
- Maciej

Susan Schweiner works for MITRE. She has done some work on identity management and credentialing.

Regrets:

- Abhi
- Ryan

Next Meetings

- No meeting Thu Sep 18 - Eve, Mike regrets
- All-hands meeting Thu Sep 25 9-10am PT (time chart)