UMA telecon 2019-01-17

UMA telecon 2019-01-17

Date and Time

- Thursdays 6am PT
  - Screenshare and dial-in: https://global.gotomeeting.com/join/857787301
  - See UMA calendar for additional details: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Approve minutes of UMA telecons 2018-12-06, 2018-12-13, 2018-12-20, 2019-01-10
- UMA business model
  - If Tim and David are available
  - Contributing the UMA2 specs and next steps
  - Sender-constrained RPTs
  - Comments on oauth-distributed draft
  - Attending IETF 104
- High assurance of the RO to the RqP
  - If Peter is available
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

- Approve minutes of UMA telecons 2018-12-06, 2018-12-13, 2018-12-20, 2019-01-10

MOTION to approve minutes of UMA telecons 2018-12-06, 2018-12-13, 2018-12-20, 2019-01-10: APPROVED.

UMA business model

The IEEE P7012 presentation that Tim and Eve did in August (listed on the home page) is a fairly thorough accounting of what we want to put into the mapping doc, but a doc needs to have full sentences. Eve, Tim, Andi, and Domenico are the subteam already working on the doc. Do we want to work on the tough questions during some subsets of the calls? This may also relate to what we called "trust attacks" in our analysis of the "OAuth/UMA short-circuit attack" about a year ago.

The gray boxes in the "railroad diagrams" in the back of the UMA Legal Role Definitions deck represent legal contracts or laws that are invoked by legal parties outside of/upstream of UMA technical entity interactions. There are business use cases, such as "little Johnny aging", where the UMA protocol doesn't understand the changes and we can conceive "messing with" UMA artifact bonds (such as revoking the PAT) to make the use case happen. Tim asks: Have there been criticisms/pushback on the presentation? Eve has talked with people who want to solve these use cases! This is where "IRM" comes in, on top of UMA. Alec's work in his UMA variation has an AS that is protected from knowing too much RO personal information, but there still has to be a legal/business relationship between the AS and RO.

An OAuth RS expects the client to go to the AS first. Adrian's HIE of One/Trustee business case is to build a directory of Subjects for both OAuth and UMA RS's to look up what/where their resources are. The Subject's AS determines what shows in their row in the Directory. Legal relationships come into picture in a more complex way. They use SSI (uPort) at the AS. So the credential issuer is separate from the credential holder, and that's separate again from the client. So in essence it's more loosely coupled still than the traditional federated identity model of IdP/RP.

The UMA Legal Role Definitions deck uses a paradigm of role boxes that could be very useful for illustrating a variety of business use cases.

IETF plans

- Contributing the UMA2 specs and next steps
- Sender-constrained RPTs
- Comments on oauth-distributed draft
- Attending IETF 104

We would want to stimulate a conversation at the IETF table, but also not entirely "blow up" the specs given the level of implementation seen in UMA2. The deadline for contributions is usually about two weeks before the meeting. IETF 104 is in Prague and the submission deadline is March 11. The OAuth WG has already asked for agenda items. Eve is speaking to Hannes T today and could ask for a slot. Andi could potentially attend for part of it. The remote attendance options are quite high-quality, so that's an option as well. The OAuth WG usually will have, say, a Tuesday 90-minute morning slot and a Thursday 90-minute afternoon slot. The actual contribution starts a serious conversation and whoever might present on the specs' behalf would have to be prepared.

What's the contribution timeline? The sooner, the better.
Might it be possible to have a conversation at the IETF table about use cases that Auth0 would like to solve? Certainly "enterprise UMA" use cases are ones we know are desirable to solve. Many consent-related ("Alice-to-x" sharing) use cases are proving to be valuable.

At: Eve: Reach out to Prabath and Pedro/John from RH to let them know our plans.

At: Eve: Reach out to Thomas and Justin to look into putting our specs into contribution-ready form by mid/late February based on WG agreement (we should vote on it).

At: Eve: Reach out to business model subteam ASAP for next steps on the draft report.

**High assurance of the RO to the RqP**

Deferred.

**Attendees**

As of 18 Oct 2018, quorum is 5 of 8. (Domenico, Peter, Sal, Andi, Maciej, Eve, Mike, Cigdem)

1. Peter
2. Sal
3. Andi
4. Maciej
5. Eve
6. Cigdem

Non-voting participants:

- Alec
- Thomas
- Tim
- Adrian
- James
- George
- Colin
- Nancy

Regrets:

- Domenico
- Mike