UMA telecon 2017-11-30

UMA telecon 2017-11-30 (joint with CIS WG)

Date and Time

- **Special time, Thursday 8am PT** (scheduled for 1 hour, assuming it will run longer!)
  - Special dial-in for today: CIS WG GoToMeeting line (see calendar link below for additional details): https://global.gotomeeting.com/join/323930725
  - UMA calendar: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda for joint meeting

- Consent Receipts people present on Consent Receipts to UMA people
- UMA people present on UMA to Consent Receipts people, including reviewing the GitHub issues labeled "shoebox"
- UMA Legal people present on UMA Legal to all
- Enumerate the possible places in UMA where things would be useful to "record"/have a "receipt" structure
  - See also IIW XXI "Consent Receipts in UMA" session notes (also known as "pumpkin security theater") – page 38
- Enumerate places where the UMA resource owner and requesting party would find it useful to get a receipt ("repudiation" use cases)
- Enumerate relevant technical artifacts in UMA and their places of issuance and usage
- Record next steps
- AOB

Minutes

Joint meeting notes

- Consent Receipts people present on Consent Receipts to UMA people

(Eve and Domenico are the only "non-CIS WG" UMAnitarians on the call.)

CR V1.0 is fully published and downloadable now. The WG has developed V1.1 and has voted to move it to the public review period. That's due to go to the 45-day review shortly. The data structure inside the receipt has seen some structural changes (to allow multiples, e.g. of data controllers), and the spec has had editorial changes. V1.1 had a fundamental goal to make no breaking changes. There were a couple of minor such changes. The spec is for a data structure, not a protocol. It has implementers in various stages, mostly for internal use and with heavy extensions (which is compatible with the "MVCR" intention – "minimum viable"). Consentua, digi.me, JLINC (when it gets to V1.0 of its product), and Open Consent Group are all implementing. There are a bunch of random commenters on GitHub. There have been a lot of downloads of V1.0, more than UMA!

The informal roadmap includes what will likely be a V2.0 that focuses on interop issues. The new Consent Management WG would be able to feed best practices into the CR work at that point. The CR would be able to become something like a "personal data privacy receipt" that captures all the justifications for processing. Or maybe this is overstating future directions.

- UMA people present on UMA to Consent Receipts people, including reviewing the GitHub issues labeled "shoebox"

Eve showed the UMA V2.0 specs, and a quick demo of a "profile and privacy dashboard" that integrates UMA2. Mary asked who has built UMA-style sharing dashboard interfaces. ForgeRock has, and HIE of One has (on UMA1 so far).

CR has focused first on the notice requirements, not all privacy requirements. By contrast, UMA's design center is more about authorization/access control made convenient for humans. So it's a control mechanism. A regulation like GDPR has made "choice and control" more important and viable for data subjects, but there are a lot of consent flows outside UMA use cases.

- UMA Legal people present on UMA Legal to all

Mark notes: There is no obligation in privacy law for natural persons to protect other natural persons' data. It's about organizations. Companies have used individuals as a loophole to get around their obligations. The UMA Legal plan to use licenses can plug some loopholes.

Chris notes: It's not so much that people have a fear factor about sharing data, but we need to press for a unified identity+consent structure that is deregulated.

Andrew proposes: A "consent receipt" is a record that should be issued whenever a person agrees to something. Can we say that Alice (the resource owner) is definitely the data controller? Bob (the requesting party) is a data processor, because he's following the rules that Alice set out for him? But then he becomes a data controller (another data controller, with a different purpose) when he uses his access. CR today is about data privacy, not about IoT (though Eve notes the ePrivacy regulation mentions IoT). Let's find a use case that encompasses both CR and UMA. How about using the Aggregating and Sharing Pension Information UMA case study? (Sal notes it's similar to this Massachusetts search feature.)

We seem to have some gaps. What are the specific roles?

What is the role of timing? The time of consent is the time you must be prepared to issue a receipt. The data controller must be prepared to issue a receipt to the data subject – or rather, we think that would be nice; some of that data would be included in a subject access request, but "consent receipts" aren't included as such. But what if, as our analysis, the (a) data controller is the data subject, or at least their proxy?

Andi: When a resource owner decides who is going to have access and what kind, which could happen multiple times, presumably that's an occasion for generating a receipt. Similarly, when a resource server makes a decision on receiving an access token and a resource request. Andrew envisions the UMA roles flipping from data subject to data controller to data processor at different stages.

Can we capture state changes and each of the UMA roles, and try to pinpoint what their "data *" roles are supposed to be?

There are a lot of verbs that might work for "agrees to something", depending on the circumstances. Permits, approves, grants access, becomes a party to a transaction...! Robert: Every new subject/controller agreement needs a receipt. The receipt is just the metadata. Sal: It's a relationship!

- Enumerate the possible places in UMA where things would be useful to "record"/have a "receipt" structure
    - See also IIW XXI "Consent Receipts in UMA" session notes (also known as "pumpkin security theater") – page 38
- Enumerate places where the UMA resource owner and requesting party would find it useful to get a receipt ("repudiation" use cases)

Eve showed the Legal slides where the OAuth client credentials, ToS/PN, PAT, (optional) PCT, and RPT get issued. They can also be revoked.

- Enumerate relevant technical artifacts in UMA and their places of issuance and usage
- Record next steps

AI: Andrew, Eve, Robert, Andi: Work on UMA/receipt state changes spreadsheet. Put some thinking into the "relationship" angle.

AI: Andrew, Eve: Find next time for a joint meeting.

UMA agenda

- Update on spec timeline progress and GOTV efforts
- Update on new logo selection

Mike asked his colleagues and they don't like the new logo. 🙂 Regarding the "2", he points out that OAuth 1 was huge, and with a 2.0, he worries about a 3.0 and changing his client software. Jin likes the middle one. Adrian doesn't think the "2" is necessarily useful, and thinks having a distinctive design (e.g. with the circle) is useful. Having the blue and green does add cost in printing.

- Update on plan to switch to GoToMeeting in 2018

Eve will freshen up the calendar event invites in 2018 with this info; our current events don't extend past 2017.

Attendees

As of 7 Mar 2017, quorum is 4 of 7. (Domenico, Sal, Andi, Maciej, Eve, Mike, Cigdem)

1. Domenico (first hour)
2. Sal
3. Andi (second hour)
4. Maciej (second hour)
5. Eve
6. Mike (second hour)

Non-voting participants:

- John
- Mark
- Mary
- Andrew
- Adrian
- Jin (second hour)
- Bjorn (second hour)
- Tim (second hour)
- Robert (second hour)

Other participants from the CIS WG