UMA telecon 2020-03-12

UMA telecon 2020-03-12

Date and Time

- **Thursdays 6:30am PT (new time – and we are in "summertime skew" so it's one hour earlier for UK and CET)**
    - 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 2019-10-03, 2019-11-21, 2019-12-05, 2019-12-12, 2019-12-19, 2020-02-13
- Extensions
- Interop
- Publishing the relationship material
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

- Approve minutes of UMA telecons 2019-10-03, 2019-11-21, 2019-12-05, 2019-12-12, 2019-12-19, 2020-02-13

MOTION: Approve minutes of UMA telecons 2019-10-03, 2019-11-21, 2019-12-05, 2019-12-12, 2019-12-19, 2020-02-13. APPROVED.

Extensions

Alec and Anik: About a year ago, Alec shared how they were using UMA, and particularly modifying it. They have extended and profiled it for their use cases. They are going to share those with the group to get feedback. The first is for "RS Interoperability". This is to enable RS's to have a standard API. If there are, say, five FHIR servers, there can be discovery. Alec will send an email to the WG later today. This has been getting a lot of traction in healthcare in Canada. The second is about splitting the AS. The concept of a "cascading AS" has come up previously, and also a "personal AS" and potentially with a wallet component. This is related to that. The AS in this case doesn't deal with any personal information; it is delegated to a personal authorization server component. This goes into the world of SSI and wallets. The user can bring their own wallet that they can have a stronger relationship with than a "community" AS. This can solve some compliance challenges. This might just be one use case of UMA, or could potentially have broader implications. Alec will share at least the first one.

Currently, "compliant UMA" has the client going "RS-first": the first thing it does it to "hit a resource". What they are doing still supports that flow. But they have extended the flow to have the client ask for a permission ticket first. "I'm a client and I need this kind of a service." Does this solve for a "classic" resource protection use case where the RO can protect any (arbitrary) resource? It constrains to a set of well-known resources.

This isn't solving for Alice-to-Bob sharing. CanImmunize is an example of an app that gets access to immunization records. They can avoid integrating with every single "RS" (host of immunization records), by integrating with the AS that knows about all the actual RS's. Bob's client goes to the AS and looks for an immunization record. It could be at four RS's. It's told "It's at hospital C, and it looks 'standard' for some definition."

George comments: "This sounds a lot like a trust-framework mechanism that manages authorizations of clients and which RSs that client is authorized to access." Resources get statically registered. The user gets to choose what scopes get shared, in an asynchronous policy-based way. The client is registered at the community AS. After Alice (the RO) is in the picture, the RqP presents (SSI-style) credentials (that is, VCs) to Alice's personal authorization server ("PAS"). (In other words, Alice's PAS is a verifier and the RqP is a holder of VCs.) The PAS is an agent managing policy at the community AS.

Which extension features are to achieve privacy enhancement and which are to achieve resource standardization? Let's see if we can tease that out when we see the extension details.

Adrian notes that there is a prescription monitoring law that seems to overlap with these requirements.

Interop

ForgeRock has a new "Secure Sharing" open-source RS implementation out. Eve will add it to the Implementations page. This is in addition to Gluu's Gluu Gateway RS implementation.

Nancy's FHIR-based UMA implementation has been engaged in the healthcare connectathons. FHIR V4 is what's been generally targeted now. HEART now profiles UMA2.

It would be a very good time for us to test and demonstrate interop. AS interop is the first step. Nancy suggests that we need a plan to test all the components. A HEART client would be valuable. HEART is just a superset of SMART. It could be valuable to work with the FAST people and that connectathon community.

Our previous interop discussions led to this landing page (and a bunch of discussion and conclusions in previous notes). We've had offers previously to develop a test harness. Colin will research funds availability.

Any reason *not* to choose a healthcare use case for a first interop? Financial services is the other obvious one. Scott notes that in the Secure Sharing implementation, the idea was to start with a generic / abstract reference environment to help communicate the UMA concepts and value proposition, then move into industry-specific requirements. it's always somewhat cumbersome have an example in one industry and having to explain it to another. The implementation provides sample resources and scopes for several industries to reduce the need to say "imagine if you will ...".

Fastest route to publishing current UMA relationship material?

Relevant docs:

- Business-Legal Framework and Use Cases (GDoc)
- Mapping Graphics (GSlides)
- Legal Role Definitions (GSlides)
- Definitions and Use Cases Spreadsheet (GSheet)

Deferred, but interest continues in these use cases and potential solutions.

Attendees

As of 17 Feb 2020, quorum is 5 of 8. (Domenico, Peter, Sal, Thomas, Andi, Maciej, Eve, Mike)

1. Domenico
2. Sal
3. Thomas
4. Eve
5. Mike

Non-voting participants:

- Nancy
- Scott
- Adrian
- George
- Alec
- Colin
- Tim
- Anik – IDENTOS – guest expert – helping to bring some UMA extension thinking into our realm today