UMA telecon 2021-07-22

UMA telecon 2021-07-22

Date and Time

- **Primary-week Thursdays 6:30am PT**
  - Screenshare and dial-in: https://global.gotomeeting.com/join/485071053
  - United States: +1 (224) 501-3316, Access Code: 485-071-053
  - See UMA calendar for additional details: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Approve minutes of UMA telecon 2021-06-10, UMA telecon 2021-06-17, UMA telecon 2021-06-24, UMA telecon 2021-07-01, UMA telecon 2021-07-08, UMA telecon 2021-07-15
- Relationship Manager - user stories
- AOB

Minutes

Roll call

Quorum was NOT reached.

Approve minutes

- Approve minutes of UMA telecon 2021-06-10, UMA telecon 2021-06-17, UMA telecon 2021-06-24, UMA telecon 2021-07-01, UMA telecon 2021-07-08, UMA telecon 2021-07-15

Deferred

Relationship Manager - user stories

Challenges:

- *Alice must know the RS exists*

- *The RS may not be able to trust ANY AS*
- The RS MUST provide UX for the user to receive URLs
- The AS MUST provide UX to establish policy
- Alice must collect and share resource URLs with Bob
- The Client must understand the type of the resource at the URL
- The RS must determine the acceptable scope for the client from a URL
- The AS may not be able to trust ANY Client

Which motive these stories:

Alice=RO, Bob=RqP, RM=Relationship Manager, RSO=Resource Server Operator, ASO=authorization server owner

Medical Records has a complex joint-custodian/owner situation. Alice is the subject of the record, however the RS has a responsibility to protect the records. Today all EMRs do typically have authorization setup for internal (ie staff) access to information. A separate UMA AS could be used to manage patient access to their records to other consumer health applications. This AS can be trusted by more than one EMR so that the health apps dont' have to integrate with each EMR (and vice versa).

What does this mean for Bob, Hosp 1 trust ASa and ASb, and Hosp 2 trusts ASb, ASc. Bob needs to understand which AS's can facilitate his access to which Hospitals, and therefore may use different ASs.

1. As Alice(RO), I need a way to discover available RSs, in order to learn about resources I own
    a. Today in UMA, it 'assumed' that Alice i) knows of the RS, and the the RS can expose ii) those URLs to Alice in some way
    b. Is this analogous to the web without search engines? you have to know explicit links to all your documents
    c. There are two challenges, Knowing custodian of resources and knowing the specific locations of those resources
    d. In the RM draft,
        i. it assumes that Alice knows the custodian. However the list of custodians are registered either at the AS or with a different registry (discovery information for RM, can facilitate Dynamic Client Registration, eg RS trusts AS, so RS trusts RM) the relationship manager can also be a conformance profile manager for the RS
        ii. the custodian tells Alice the specific urls of her resources through the API
2. As an RSO, I need to trust a limited set of compliant ASs, in order to meet my obligations to protect resources
    a. Today, An RS is meant to trust any AS brought forward by a RO (ByoAS) over that RO's resources
    b. For a 'regulated' RS/custodian, it can't delegate authorization to ANY AS.. The RS may have 1 AS that allows edit scopes, while it may be more open to patient read
    c. In the RM draft
        i. The RS doens't need to register every specific resource with an AS, the specific resource information is conveyed to the RM and then to the AS. Instead the RS has a more general trust in the AS "I trust you to issue access tokens at all".
        ii. There are two bits of an RS given our a resource i) the access token was issued by an AS it trusts ii) the access token conveys information that was given the to the RM (the return trip to the RS includes proof from the RO) (ALEC MAKE A PICTURE)
3. As Alice, I need a way to work with many ASs, in order to use ones required by my RSs
    a. Today in UMA, Alice works with her AS and brings it to each RS that holds her resources. In a world where the RS restricts or sets the available ASs, Alice has a greater need to work with more than one AS. If Alice does work with multiple ASs, it's implied that each AS offers it own UX/authentication, this is not ideal for Alice.
    b. In the RM draft,
        i. a RM has an API with the AS, and can work with multiple ASs by design
        ii. The RM is the RO nexus between RSs and ASs, which the AS is the nexus between RSs and RPs (ALEC MAKE A PICTURE)
4. As an RSO, I want to allow Alice to bring a resource management UX, in order to not provide this myself
    a. Today, the RS must provide some interface for Alice to see her available resources (uri) and which resource is registered at each AS
    b. We're talking about the UXO=user experience owner
    c. this might be a good place to put into use the blinding identity taxonomy https://docs.kantarainitiative.org/Blinding-Identity-Taxonomy-Report-Version-1.0.pdf in relationship manager... it could check to see if these are necessary and if possibly blinded..
    d. In the RM,
        i. *Alice has a single place to manage all her resource i) see all available resources across all RS ii) see all registered resources at which ASs iii) manage policy of those registered resources at each AS*
5. As an ASO, I want to allow Alice to bring a resource management UX, in order to not provide this myself
    a. Today, the AS must provide some interface for Alice to see her registered resources (uri) and the policy for each resource->RqP
6. As Alice, I want a way to grant Bob access to my resources without knowing the URLs, in order to a) not deal with URLs b) share more complex resources (ex not a PDF, a health record)
7. As Bob(RqP), I want to be able to discover resources available/shared with me, in order to not need URLs sent by Alice
8. As a Client, I want to be able to declare types I understand, in order to successfully use complex APIs
9. As an RS, I want to defer permission ticket creation, in order to a) not have to understand the Client b) not make authZ decisions (tell me don't make me think)
10. As an ASO, I want to pre-register Clients, in order to assess their appropriateness, capability and complete non-technical activities
11. As a Client, I want to pre-register with ASs, in order to a) test my UX and technical integrations b) declare my capabilities

AOB

Sal touched up the ANCR notes from last week UMA telecon 2021-07-15

Attendees

As of October 26, 2020, quorum is 5 of 9. (Michael, Domenico, Peter, Sal, Thomas, Andi, Alec, Eve, Steve)

Voting:

1. Steve
2. Alec
3. Sal
4. Andi

Non-voting participants:

1. Kay
2. Scott

Regrets: