UMA telecon 2021-07-08

UMA telecon 2021-07-08

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
- 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

Deferred

Relationship Manager - user stories

Review the Diagram: https://groups.google.com/g/kantara-initiative-uma-wg/c/WAnizgl08Fg/m/YjflL1EbAwAJ

Discussion Recording (split into 4 parts)

2021-05-20 13.24 UMA Working Group Part 1.mp4

2021-05-20 13.24 UMA Working Group Part 2.mp4

2021-05-20 13.24 UMA Working Group Part 3.mp4

2021-05-20 13.24 UMA Working Group Part 4.mp4

Here's a token and here's where to go: OIDC distributed claims. Existing mechanism to pair and endpoint with a token

Want to be able to still share a URL and have flow work. This is a discovery mechanism, has many privacy implications, eg user understanding what the policy means. How does the user really know what will happen, do we need a notification mechnism to allow review ahead of the disclosure? We don't nessicarily want it to be a revocation after the data is shared. In this case the consent needs to be just in time, eg Alice is notified about the specific request based on the more general policy. This is back to the CIBA/liberty alliance interaction service, where the the AS can reach out to the RO. One the client side this is handled by the request_submitted token response.

How would discovery be layed on top of the existing protocol (vs overload). Discovery creates AS-first (or discovery server-first) flows

- exposing the UMA Fedz resource API to the client
  - two step process, the client/RqP are first identified to the AS, to get access to an AS hosted resource API
- A discovery endpoint, the client goes there first and then gets a ticket to use with a token endpoint
  - who hosts discovery endpoint? can is cross AS's, it is discovery only for the UMA protected URL, where each URL can be independantly protected.
  - pass in the resource id (eg resource indicators) to the token endpoint with a PCT

We are separating discovery from existing UMA flow/roles, it can be co-located with an AS or entire separate service, in future could be colocated with RM (Alice shares he RM url instead of specific URLS)

In UMA, I pick an AS, all of my/Bob's services go through my AS to get authZ to my resources. Reality has shown there are likely 3/4 different ASs this is one purpose of the RM, to be a layer that serves Alice directly. Comes down to where agreegation happens, and who knows about it, how this makes Alice's life easier to manage her distributed information.

We are seperating the policy of discoverability from the authorization to access, they have different policy needs. If these are different, why allow discovery? Because Alice wants transparency and want to understand the different risks. Knowing that Alice takes landscape photos may be discovery, while access to specific photos may want to be controlled. This goes back to a general policy around discvoery (all photographers can discover) vs the specific RqP (only selected photographers can access specific photos, tiered access)

Discoverability works well where there are a small amount of URLs, however in complicated APIS, there could be 100+. There can be expansion to 'wildcard' urls or types of resources vs the specific URI.

RS first access lacks mechanisms for intent. The RS must extrapolate from a single request the scope of resources to includes in the permission ticket. Discovery allows client/RqP to speak to there intent, eg as a client I can understand only specific resource types, however the RS can't know this ahead of time. We want to match the granted resources to the intent/capability of the Client. Bob can show up and declare what privacy obligations he'll uphold, and leave the notarized receipt with the AS for Alice to follow up with eg Data Controller information. Rather than audit trail, the receipt is meant to be one-time signal that be compared over time and allows the identification of policy change. On all resource accesses the AS receives a new and comparable-to-previous receipt.

I'm a health care system or photo sharing systems, the site needs to standalone. The could be cases where an RS is trying to add authz capabilities, this can be delegated to the UMA environment without major changes to the core RS. UMA needs to work for both scenarios.

The interesting questions always comes back to liability, if the AS is the authority and the RS releases the wrong data, the AS still needs to take the liability. The RS is the data custodian, and they always have liabity/responsibility to the RO. If company A uses UMA as technology for RS/AS/RM /Discovery, then there is little liability question, it's all in the same place. Once the ecosystem is wider, where company A holds the data, and delegates authZ to an AS of company B, now the liability split is less clear.

When PDP did the dashboard, there is an idea of consent boundaries. Anything happening at the RP on behalf of the RO, has a separate consent boundary, between teh client software and the RqP.

The ANCR would allow Bob/Client to create the notice receipt to the discovery mechnism so that Alice is able to see what terms we're accepted. From RqP perspective, access is based on presented claims, to meet Alice's policy. Bob wants to set his terms for sharing those claims with an AS(?) The policy within the AS is not-specified, the ANCR could be a profiled claim type for Alice/Bob to both understand the legal requirements/expectations for the claim handling. Purpose is to reduce the cognitive load on Alice/Bob to understand the terms, having a common vocabulary vs ad-hoc TOSs.

As an RqP, I can define an ANCR receipt, in order to specific my requirements for claims handling. THis could be a claims presentation to the AS. There are two privacy rights that need to be balanced: Alicearbitrary client vs Bobarbitrary AS. In ANCR, there is a cyber rights notary, when Bob wants access he see's Alice's preestablished policy.

AOB

Attendees

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

Voting:

1. Thomas
2. Alec
3. Domenico
4. Sal

Non-voting participants:

1. George
2. Ian

Regrets:

1. Eve
2. Nancy