UMA telecon 2021-05-27

UMA telecon 2021-05-27

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 2021-04-22, UMA telecon 2021-04-29, UMA telecon 2021-05-06, UMA telecon 2021-05-13, UMA telecon 2021-05-20
- Relationship Manager Review, discuss credential concept
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

- Approve minutes of UMA telecon 2021-04-22, UMA telecon 2021-04-29, UMA telecon 2021-05-06, UMA telecon 2021-05-13, UMA telecon 2021-05-20

Deferred

Genomics is a very interesting topic as the data always have multiple subjects. There are many complex layers to genesis data, chunk, sequence, images, etc. Eve has heard of a group working on set of permissions around the use of genomics data, could be made into APIS. Nancy notes another group, PP2PI (patient privacy 2 promote interoperability). Reach out to Nancy if you want to see the group

Charter Review/Refresh

(2) purpose

"For example, working with the Kantara Consent and Information Sharing Work Group" Kantara or external consent-oriented work groups (add some examples, eConsent)

"To promote interoperability of independent implementations of UMA", (keep this and add:) could this support wider interop? such as with HEART/OIDC

- "To promote interoperability between UMA and other related
- "To promote the use of UMA to provide authorization capabilities to

- Consider 3rd party requests to standardize profiles and extensions where there is wider applicability of the profile
  - Review, evaluation and recommendation of submitted implementation profiles of UMA
  - (already covered by point 1)

(3)

(4)

remove "Business Model Clause Templates for User-Managed Access (this may be a report instead; final title to be determined)"

add Relationship Manager/Policy Manager/Resource Definition drafts

(5)

- GNAP / OAuth 2.1, (sender constrained tokens, no implicit, pkce) we're there other oauth extensions pulled in, or 2.1 is only OAuth2 + BCP?
- would we accept an UMA profile based on GNAP instead of OAuth? Should UMA be GNAP-ready when it is released?
    - transition from Oauth to GNAP?
    - evaluation of UMA-like things on different authorization protocols, profile of GNAP
- evaluation of claims token beyond IDTokens (VCs?)

DO we need to define the different between implementation(/deployment profiles and guidance**

- implementations = the vendors who have UMA impls
- deployments = 'fully baked' systems that use UMA (PDP, FPX)

UMA + X, profiles

- HEART, FAPI, Consent Receipt

```
* This draft consolidates the functionality in OAuth 2.0 [RFC6749], OAuth 2.0 for Native Apps ([RFC8252]),
Proof Key for Code Exchange ([RFC7636]), OAuth 2.0 for Browser-Based Apps ([I-D.ietf-oauth-browser-based-
apps]), OAuth Security Best Current Practice ([I-D.ietf-oauth-security-topics]), and Bearer Token Usage
([RFC6750]).
* Where a later draft updates or obsoletes functionality found in the original [RFC6749], that functionality in
this draft is updated with the normative changes described in a later draft, or removed entirely.
* A non-normative list of changes from OAuth 2.0 is listed below:
* The authorization code grant is extended with the functionality from PKCE ([RFC7636]) such that the default
method of using the authorization code grant according to this specification requires the addition of the PKCE
parameters
* Redirect URIs must be compared using exact string matching as per Section 4.1.3 of [I-D.ietf-oauth-security-
topics]
* The Implicit grant ("response_type=token") is omitted from this specification as per Section 2.1.2 of [I-D.
ietf-oauth-security-topics]
* The Resource Owner Password Credentials grant is omitted from this specification as per Section 2.4 of [I-D.
ietf-oauth-security-topics]
* Bearer token usage omits the use of bearer tokens in the query string of URIs as per Section 4.3.2 of [I-D.
ietf-oauth-security-topics]
* Refresh tokens should either be sender-constrained or one-time use as per Section 4.12.2 of [I-D.ietf-oauth-
security-topics]
```

UMA + Consent Receipts

City University Birmingham have a demo showing how UMA works with Consent Receipts. Was in a healthcare context

Is there interest in setting up a joint UMA + CR WG call to review this? yes.

Sal is going to dig up the link and share on the mailing list

OIDF Liaison

Any one interesting in creating an UMA FAPI profile?

There was a draft shared, but never signed. Do we need to finish this, and what is the purpose? To support maintenance of HEART + future FAPI UMA profile

Relationship Manager Review

Deferred

AOB

Attendees

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

Voting:

1. Steve
2. Michael
3. Eve
4. Thomas
5. Alec

Non-voting participants:

1. Colin
2. Scott
3. Tim
4. George
5. Zhen - learned about group from ONC AGM. Training in biomedical informatics, interested in genomic privacy. Patients hardly ever in the use of their data!
6. Nancy
7. Sal

Regrets:

1. Domenico