UMA telecon 2021-02-18

UMA telecon 2021-02-18

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 2021-02-04, UMA telecon 2021-02-11
- Reintroduce the relationship manager/policy manager/wallet profiles
- Pensions Dashboard, any updates
- AOB

Minutes

Roll call

Quorum was NOT reached.

Approve minutes

- Approve minutes of UMA telecon 2021-02-04, UMA telecon 2021-02-11

Deferred

LC Presentation Review

Another Common Theme:

- interop theme, need standards based implementations of the protocol (UMA) + the ability to apply specific profiling/configuration choices
  - example, how the RS would request a PAT (interactive/token push)
  - custom/implementation specific interop of data formats
- needs for conformance of specific implementations (protocol,data)

Should we rekindle the conformance suite/testing conversation?

Could we start with conformance to a specific implementation profile and generalize afterwards? This reduces the scope of the testing, provides something concrete

Reintroduce the relationship manager/policy manager/wallet profiles

Discussed the 4 potential profiles

Trusted claims is interesting in context to a public/private collaboration. Where data may need to move from public to private or vis-versa in known ways. There are challenges open public IDPS to private sector parties/use-cases. More public sector parties are creating identity/credential services. This also comes up in us health care as there is a need to exchange data between sectors, it's hard to agree on who's idp to trust.

There is a lot of push back against using "social" provider (eg Google) to provide end-user (ex Patient) credentials. This is a big industry challenge. Where is the push back? The lack of identity proofing, or the security of the credential? Google spend WAYYY more to secure that credential that any single hospital/impl likely could. Seems like a partner education challenge to the benefits: user convenience, increased (delegated) security, no need to manage user passwords.

As a (health acre) RP, they may end up need to support many many IDSP, this could push orgs the "other way" to centralize these features, if only for operational simplicity. Even if google is the CSP, each org that accepts it is building a new IDP and enriching the user account with local data/identifiers, useful to downstream providers.

Are healthcare providers building their own Identity stacks? This should be strongly discouraged. Most health care systems seems to buy and install their own, instead of relying on external.

Nancy & Alec's impl both federated authenticate and layer on identity proofing capabilities. The CSP does not have the *right* identifiers in every context, some proofing must be layered on. IDPS that come with proofing capabilities are beneficial, but can't meet all needs (eg to find/bind to a medical record number)

There is a lot of public sector effort to define national trust framework: eg in UK https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework

The interop of IDPs is the main focus of the Kantara Identity Assurance WG, which helps ensure the compatibility of different CSPs/IDPs against 800-63-3. If this topic interests, please checkout that WG!

Pensions Dashboard, any updates

Pensions Dashboard Program has released some documents as they build towards their procurement

https://www.pensionsdashboardsprogramme.org.uk/2021/02/11/passing-pensions-schemes-bill/

https://www.pensionsdashboardsprogramme.org.uk/2021/02/18/identity-call-for-input-data-providers/

Attendees

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

Voting:

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

Non-voting participants:

1. Vlad
2. Nancy
3. Ian
4. Scott
5. Colin
6. Tim
7. George

Regrets:

1. Eve