HEART March 23 agenda and notes

Steinar: HelseID

Adrian: Separation of Concerns

Adrian: HIE of One Trustee

Tom: Kantara Workgroups

Nancy: PatientShare

Eve: handling delegated permission “grain”

Eve: Improving btg scope profiling

Stephen: Secure Sharing

Attending:
Debbie Bucci
Eve Maler
Nancy Lush
Thompson Boyd
Tom Jones
Daniel Fett
Steven D
Stephen Payne
Steinar Noem
Dan Wirz
Kieron McGuire
Andrew Zander
Wesley Dunnington
Rita T
Alan Viars
Carlos Garcia
Adrian Gropper
Jim Kragh
Julie Maas
Luis Maas
Danny

REMINDER: Please note that while anyone can join the mailing list as a read-only recipient and listen to the calls, posting to the mailing list or actively contributing (all spoken comments are considered contributions) to the specification itself requires the submission of an IPR Agreement. More information is available at http://openid.net/intellectual-property.

NOTICE: An OpenID IPR contribution agreement is not mandatory in order to participate in this workgroup call. If participants provide feedback, they (on behalf of themselves and any organization they represent) are deemed to agree that: Attendee gives the OIDF the right to use their feedback and comments. Attendee grants to the OpenID Foundation a perpetual, irrevocable, non-exclusive, royalty-free, worldwide license, with the right to directly and indirectly sublicense, to use, copy, license, publish, and distribute and exploit the Feedback in any way, and to prepare derivative works that are based on or incorporate all or part of the Feedback for the purpose of developing and promoting OpenID Foundation specifications and enabling the implementation of the same. Also, by giving Feedback, attendee warrants that they have rights to provide this feedback. Please note that feedback is not treated as confidential and that OpenID Foundation is not required to incorporate feedback into any version of an OIDF specification.

Agenda

- Brief greeting - take attendance
- Reminder: On April 6 we will round out the presentations with Justin Richer then devote the remaining time for next steps. We should use the time between meetings to start a dialog to focus April 6th discussion
- **Discussion**

    1. **Using OIDC and OAUTH in Norway's Health Sector —**
    2. **Separation of Concerns - IETF/transactional authorizations/SSI Standards - Adrian Gropper**
    3. **HIE of One Trustee - Adrian Gropper**
    4. **Kantara Workgroup focused on assurance and Healthcare - Tom Jones**
    5. **Patient*Share* illustration of a patient centric record in a practical health care use case - N Lush**
    6. **FHIR resource type design patterns - Eve Maler**
    7. **Demo - FHIR integration - Eve Maler**
    8. **Potential Scope addition - Eve Maler**

Steinar: HelseID

(See his slide deck. These notes try to capture what's different from notes content.)
He has been following HEART from afar.
Norway is subject to many laws, eIDAS and GDPR but also other specific ones.
Business-to-business scenarios require strong authentication and contextual info.
HelseID authenticates health personnel, so it's somewhat different from HEART use cases.
Certificates are used in the underlying registries.

It’s an authorization server for API-consuming parties across legal boundaries.
There are a lot of scenarios they cover.
Since their focus is security, they point to FAPI and will increasingly do so.
If an EHR system will join the federation, it must undergo code review.
Integrity and non-repudiation using request objects is a big strategy.
The OIDF E-KYC assurance spec is coming for them.
Eve Q: The group has previously discussed how FAPI and HEART should perhaps consider aligning more closely. You chose FAPI and have been following HEART. Any thoughts?
A: Steinar and Eve previously spoke. Mostly they were following UMA. It’s mostly applicable to the end-consumer use case, which they have not been solving yet.
Daniel: FAPI is indeed useful beyond financial services.
Steinar: What they need is covered in FAPI and the recent additions to OAuth [RAR and PAR] to make clients as safe as they’re required to be.

Adrian: Separation of Concerns

Use Cases

1. PDMP Access
2. Medication List access
3. HR for Homeless

Ideal - Recognize patient center source of truth - current records go directly into EHR -

Interpretation of recent rule release:
● Neither the data holder (Source of truth, RS) nor the Client is a data controller (patient has right to their own data)

- The Authorization Server does not see the data (isn't this preferred?)

● The Authorization Server assumes a subset of FHIR for scoping
● The Requesting Party credentials are separate and distinct from the Client credentials (can be federated or SSI, per AS policy)
● Authorization is based on RqP and / or Client credentials
● The RS can issue a warning to the Patient (RO) but cannot block Client Registration (data blocking)
● Patient identity proofing or matching is unnecessary and out of scope. RS and Client access credentials are sufficient.

Gaps
Write access to multi EHR may be a gap
[note] copy info from slides - paraphrase for context
Eve Q: Where does the “HEART on FHIR” name/phrase come from?
A: I made it up! :-)
Nancy comment: Sees HEART as a superset of SMART.

A: SMART is difficult to implement and use, and underspecified, so maybe don't build on it.

Adrian: HIE of One Trustee

Implementation that's not meant to be commercial; it highlights the current scenario gaps.
Handles Ethereum-based credentials.
uPort is the chosen SSI integration currently; others could port DID software to Trustee.
The "policy bundle" makes it so a patient doesn't have to make 50 checkmarks to set policy.

Tom: Kantara Workgroups

(Talked from this page.)
There are three groups of interest.
1, Kantara Identity assurance - deals with certification of CSPs.
2. Kantara Health Identity Assurance Identity group has put together principles.
3. Kantara federated identity group has put together a "distributed identity" spec. This is intended to be "blockchain-friendly".
https://kantarainitiative.org/confluence/display/WT/Draft+Recommendations
Taxonomies like UMA are too complicated for people to understand.
People need to understand at an 8th grade level.
Alan Q: Could putting information in the token be a better solution than UMA?
T: There's a two-step process: a consent to connect, and a consent to share user information. Fairly grossly grained information could be provided.
Eve Q: UMA doesn't have taxonomies of information, so how did you get the idea that it's complicated?
T: We looked at some implementations of UMA. They're complicated. They need to be patient-oriented, not lawyer-oriented. I did not intend to malign UMA itself.
We have a demo of a trust registry now. https://trustregistry.us/
I propose a formal liaison with this group to split up the work in some appropriate manner.

SM(chat)Have you looked at https://tools.ietf.org/html/draft-lodderstedt-oauth-rar-03 as part of a solution?
T. Yes - i participated in it until i discovered it was not oriented to provide any user privacy. We went a different way.

Nancy: PatientShare

Patient care is a team sport.
Avoid too much techno babble.
Clearly define technical aspects so that it is easy to understand.

Eve: handling delegated permission "grain"

(See slide deck.)
How fine grained should a request be? Separation of concern - i.e. resource server may be in separate domains - may be value add info . May be an opportunity to standardize labeling

Resource framing - some folks want to list in 3rd party services - not just health data but (there is term for this … IOT and contributions to social determinants of health

Eve: Improving btg scope profiling

(See slide deck.)
Tightly profile btg for authorization.
Tom Q: Could you implement the ability to ask if a claim is essential as OIDC does?
A: This isn't how UMA works. Essential-or-not is just one of many policy decisions you'd want to make as part of an internal authorization assessment; see, e.g., ForgeRock's "dynamic authorization".

Stephen: Secure Sharing

(See information about new open-source UMA resource server implementation.)
Carlos Q: If you want the resource owner to be able to set up sharing of test results before they're back, would you need to register a stub resource for it?
A: If you want to enable proactive policy setting vs. approval after the fact, yes.
On this, see the UMA Implementer's Guide: Considerations Regarding Resource Registration Timing and Mechanism.