# 2021-04-06 - Trust Registries Drafting Group Meeting Notes

<DAY> March <#>

## Attendees

- **Co-Leads: Darrell O'Donnell**
- **ID2020 PM:** Todd Gehrke

**Participants:**

- Marcos Allende Lopez (LACChain/IADB),
- Stephan Baur (Kaiser Permanente),
- RJ Reiser (Liquid Avatar Tech)
- Sid Mishra
- Steve Megennis
- Marcos Loiez
- Sankarshan Mukhopadhyay
- Drummond Reed
- Julian Ranger
- Savita Farooqi
- Scott Perry
- Kaliya Young
- Jim StClair
- Sergio Ceron
- Tony Rose
- Steven Milstein

## Agenda Items

| Time | Item | Who |
|---|---|---|
| 2 min | Welcome & Antitrust Policy Notice | Chair |
| 10 min | Introductions | Chair & PM |
| 5 min | Backgrounder | Chair |
| XY min | Good Health Pass Blueprint Review | TBC |
| XY min | WHO Registry Guidance | TBC |
| 5 min | Tooling | Chair |
| 3 min | Wrap up | Chair |

## Meeting Notes

## Presentations

- Initial Presentation (Google Slides)

Key Resources:

- GHPC Blueprint Outline v2 - The Trust Registries section is detailed on pages 25-26.
- WHO SVC Guidance

## Recording - *Link*

## Notes

1. [Darrell] Steven Magennis and Darrell have worked on some topics to unpack. The Key Interoperability Questions document has Drummond around the Ecosystem of Ecosystems Governance Framework (EoEGF). People who are doing the early systems on the ground are doing a good amount of the hard work. There are a lot of credential formats among the various kinds of things to be done. There are a number of Levels of Assurance among other things.

a. One key thing that keeps coming up - for a verifier persona at an airport or a national border or even should I let you into the restaurant at this point in time. One of the questions is "if I am told that this is the vaccination credential and that is false, who will I stop that individual" also, "is it part of my job". If there is no identity binding (and additional business links)
b. How do we know that this lab is real and has a real test kit?

2. [Scott Perry] An organization can take responsibility to assert and they cannot verify their own assertion - that is a requirement from a different party.
    a. 'Attest' is done by an entity or a 3rd party who does the matching from a registry
3. [Stephan Baur] Assertion levels are a proven mechanism for identity. Attestation that the issuer does in the context of vaccination - this is unlikely is done right at the time of the vaccination event. This is done post. So, which type of data do we base the credential - thus do we need assurance level from the point/source of the data ie. EMR system or otherwise including self-reported.
    a. [Darrell] Self-reporting is likely a place where a lot of fuzziness will arise. The hope is that instead of having people assert data, the system will be able to enable a 'gold standard' through identity binding. [Stephan] Self-reporting and assertions around that can possibly have an extreme ripple effect when considering real life scenarios at this point in time.
    b. [Tony Rose] The difference between self-attestation and printing out a CDC card has to include the level of assurance to address the topics arising for fraud and forgery around the records.
    c. [Drummond] One of our big issues is level of assurance - both in the health data assertion and in the identity assertion. It appears all we can do is accurately describe the LOA that we have for the health data and the identity data.
    d. [Todd] One of our big issues is level of assurance - both in the health data assertion and in the identity assertion. It appears all we can do is accurately describe the LOA that we have for the health data and the identity data.
    e. [Darrell] A trust registry should have the ability to assert specific levels of assurance for the downstream organizations and entities to be able to make sense of that assertion and assurance level. The answer to the question of 'What is Good' and 'what is good enough' [Todd] Would the assurance level need to be an attribute in the data model? Marcos I agree. I think that assurance here does not rely on the technology at all but on the authorities responsible for the trust frameworks (in general governments, at least when speaking about verifiable credentials). Each government will define what are the entities authorized for the issuance of credentials and will require these entities to accomplish identity proofing in a certain way or with a certain LoA but this is (in my opinion) something that will not be able to be verified. Each verifier will have to decide which issues are trusted by them, and maybe this will come from countries or regions recognizing other countries or regions procedures/trust frameworks.
    f. [Scott] The initial floor is self-reporting (which has risks associated with it). The motivation to create fraud increases with incentives associated with the results of such forgery. Raising the level across all the systems, roles and processes is what is desirable rather than specific/ad-hoc. This reduces the risk including risk of collusion.
    g. [Tony] LOA belongs defined by the rules engine, supported in the schema, Issuer's in a trust registry can be bound by the governance framework to adhere to certain LOA. The whole point of a trust registry and a governance framework is to help the verifiers arrive at decisions
    h. [Steve Magennis] It is problematic if there is too much focus on what the verifier needs to be confident. The verifiers are going to determine what is sufficient to arrive at decisions based on specific levels of assurance. Do we need to go in and explain to the verifiers around the context in which they will be taking the decisions? The mechanisms by which information can be surfaced for the verifiers to make decisions based on business rules might be a good way to make progress. [Darrell] Verifiers are going to be told by 'someone' as to what is 'good enough' for them [Marcos] If you are an airport in Belgium you are never really gonna be able to verify that a lab in Panama followed a specific procedure for the identity proofing of an individual that was certified. What would typically happen is that Belgium and Panama will agree on recognizing all the certificates issued in each other country. [Tony] that's the point of the governance framework to define the rules to be in the trust registry. [Darrell] similarly, using that example - a country may have a more broad "we don' t accept X from this country" based on whatever reasons they have.
    i. [Drummond] Topics from Stephan are interesting and a use case that needs to be understood completely. What kind of rules/policies should exist in issuing a credential based on self-assertion? [Stephan] One foresees a challenge when there is hesitancy in the systems to issue VCs based on self-assertions thus having an impact on what exactly the issuers are attesting. Assurance of the quality of the data and provenance of the data to make the decision is what triggered off the conversation. [Drummond] Level of assurance in the health data and we'll have to allow for type of data ie. self-reported or otherwise. [Steve] That by itself is a complex and quite the aspect of 'trusted source' of data.
        i. [Scott] There is a difference between LoA when an individual reports and self-asserts in contrast with when an organization / institution asserts. [Darrell] An example 'a testing lab located outside of the airport'
        ii. [Steve Magennis] At the point of verification, it is important to know if the issuance trust chain is current
    j. [Scott] 'Trust' 'Registries' implies a level of trust and thus a level of assurance. [Stephan] what kind of practices does the issuer have to manage the private keys? [Darrell] We do not want to set the bar so high that no one is able to achieve that level.
        i. [Marcos] Key management is an important topic as we are not used to managing them in the context of decentralized registries. Similarly for individuals. Two main topics (a) what needs to be registered (b) how do we verify the information in the registry.
            1. Drummond adds an additional point (c) what can be described by the registry
            2. [Todd] What are the purpose and mechanics of a trust registry?
            3. [Drummond] What is the relationship between a Trust Registry and Governance Framework (or, Trust Framework)?
                a. The GF WG there is an assumption that there is no GHP certified Trust Registry that is not compliant with the GF. This is how transitive trust is enabled across the different ecosystems
                b. [Jim St.Clair] And the "actors" in the GF constitute the governance authority for those registries
                c. [Darrell] Even in a single system a trust registry makes the processes simpler and transparent
                d. [Stephan] Are we envisioning different registries for different types of attestation - test, immunization and recovery from COVID-19. [Todd] we will have to consider different registries in context of ongoing activity with WHO and EU and interoperability will mean that multiple registries will become necessary.
                    i. [Drummond] Stephan's question is precisely why the proposal of the "DID triple": 1) DID for the governance framework, 2) DID for the credential type, 3) DID for the issuer - a GF can thus have a single registry that describes all types of credentials issued under the GF. It can also be split up under multiple registries. [Stephan] are these flat or chain-of-trust design eg. WHO has root and then other countries participate [Drummond] These will be federated [Marcos] in LATAM these trust registries will be operated by the government [Drummond] or will be designated who can operate and maintain such registries. With the WHO Smart Vaccination Credential infrastructure, 100% of the public key issuers are governments [Marcos] But shouldn't it be necessary to have a DID registry onchain where the DID can be resolved, so therefore when the presenter signs the presentation with one of the keys associated to the DID, the verifier can go on chain, resolve the DID, get the keys associated and verify the signature?
                    ii. 2 dimensional plurality - what type of credentials and within each type there will be for nationality and similar.

4. [Todd] The Key Interoperability Questions document would be a place to comment. How can we be productive between now and Thursday?
    a. More focus on what we need to do from a trust registry standpoint - an interoperable trust registry ecosystem
    b. what we would propose to present at IIW should be another topic

1. Welcome and Linux Foundation antitrust policy - http://www.linuxfoundation.org/antitrust-policy

2. Topic A

3. Topic B

4. Topic C

5. Wrap up

- Next steps

**Action Items**

1. TBC