2021-04-01 - Trust Registries Drafting Group Meeting Notes

Thursday April 1

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

Agenda Items

Time	Item	Who
2 min	Welcome & Antitrust Policy Notice	Chair & PM
5 min	Introductions	Chair & PM
5 min	Backgrounder	Chair
+	Open Discussion	Group
2 min	Wrap up	Chair & PM

Meeting Notes

1. [Darrell] Anti-trust and membership policy introduction
2. [Todd] Work at this group and GHP was reflected in conversations at the WHO call of 31Mar
3. Key interoperability questions - [Darrell] some opening remarks on the topic of trust registries as a solution and where they fit in (are they a solution or a challenge?)
    a. Is there a way to establish transitive trust between different parts of the GHP digital trust ecosystem
        i. [Todd] establishing a globally scalable, jurisdiction specific registry is a challenge eg. X.509 trust registries - how do we work with those?
        ii. [Darrell] analogy of lanes/queues to describe the nub of the issue
        iii. [Julian] 'who is being registered in these registry' - assumption is people making the tests and vaccines (this massive trust registry is impossible) a short term solution is that the people who provide the trust (the app providers) provide it directly when presenting credentials.

Suggested registering the apps that issue as a possible approach

1. [Darrell] We still have to ask and validate 'who is the issuer' - is the issuer trusted? There is likely to be many trust registries - we'll need to get access to 'a credential' and answer the question 'can we trust the issuer'
    a. [Steve Magennis] How does one certify and qualify the issuer so that the data assertion can be accepted by the verifiers
    b. 'Who gets into the registry and how'
    c. [Scott Perry] The part of trust registries which we do care about is interoperability - we can make some difference by understanding the requirements of credentials required at border crossing
2. [Drummond]
    a. Proposal #1: verification of trust of the digital health credential issuer has to be "federated" or "decentralized" in some way.
    b. Proposal #2: each trust ecosystem needs a governance framework that explains how it handles delegating trust.
    c. Proposal #3: we need one protocol for cryptographic verification across governance frameworks.
3. Discussion around self-assertion topics
    a. [Scott Perry] biggest issue in the ecosystem is trust in the verification process of the data (unlikely to be solved by these WGs). Perhaps there is a necessity to say 'let us just accept things, so that we can have good interoperability models'
    b. [Kaliya] aren't there a lot of existing networks/lists - don't we need to connect these up.
        i. [Drummond] We cannot assume a single root of trust. Any proposed root of trust will manage its ecosystem with its governance frameworks. GFs will help form the basis of the trust decisions
        ii. [Marcos] Agrees with Drummond's proposals. Designing a trust registry in 3w is not possible. Best to focus on identifying the different types of trust registries - the taxonomies - which are going to be recommended. (see additional notes from the previous meeting around the set of questions introduced by Marcos). Some of Marcos' points:
            1. The issuer will typically choose which registries they consider good for them
            2. Defining trust registries from scratch is something very ambitious and takes a long time

3. If we can identify which things in the verifiable credentials that we are proposing need to be verified against the trust registries, maybe we could propose how to verify those things against each of the trust registries we can anticipate that are going to be used by issuers
4. I think two things that are very important to verify against a trust registry are (i) is the issuer authorized to issue this credential? Or do I trust the issuer for the issuance of this credential? (ii) has the credential been revoked? …. In this sense, I think it would be amazing to be able to define a specification on how this can be verified against any API or against any smart contract that an issuer decides to use
5. This will lead us to the definition of this trust and governance frameworks that establish how to leverage DIDs to orchestrate it
6. There are other things to be verified in a credential but not necessarily against the trust registry, such as the presenter matching the holder, and the integrity of the content (by resolving the digital signature of the hash by the issuer)

1. [Drummond] If we agree about: 1) multiple roots of trust, 2) each root of trust has a governance framework, then 3) is that we need a common protocol for an issuer to locate and query a trust registry using metadata from the governance framework.
2. [Todd] 'verifying the holder' is a part of the Identity Binding WG; contents of the credential is also out of scope for this WG. Agreement on the discrete questions would help make progress - we are still talking 'big picture' in the discussions. It is time to focus on the questions we are trying to solve.
    a. [Scott] Todd raises a challenge in the fact that every individual working group wants to solve all problems. It is up to Todd and leaders to keep us focused on our unique challenges to solve
3. [Stephen Baur] Just a point from the issuer perspective: the # of registries becomes an issue when large and issuers need to "register" with each separately.
    a. suggest to formulate what "registering" means, like quality processes and audits of the issuer. One big concern: if the private keys are leaked trust vanishes quickly
4. [Savita] using the framework of 'necessary' and 'sufficient' may be a way to find the direction and focus of the work output - 'what is the verifier looking for'
    a. [Stephan] suggest to keep focus on registries of issuers and leave verifier to a separate concern.
    b. [Drummond] Marcos proposed that verifiers need 3 standard items: 1) is the issuer authorized, 2) what is the issuer's public key for verifying the credential, 3) how do I check if the credential is revoked.
5. [Drummond] Proposal: delegate the question of whether a governance framework supports "verifying the verifier" to the governance authorities for the governance frameworks.
6. [Drummond responding to Julian] there exist interdependencies between different drafting groups. There's a meeting of Credential formats and exchange protocols coming up and so there is yet no clear answer is it 'just W3C VCs etc'

1. [Steve Magennis] see below
2. [Drummond] Creating a document to have key/specific questions up for answering. Each member goes in to provide detail/links/thoughts to the approaches to the questions. To get a collective view of the key questions and preliminary thought about the answers.
    a. [Todd] document of key questions https://docs.google.com/document/d/1mVZ5pRGBhb7VK5pSPsaZwaDo9hRjlZiQmCdggknP4ec/edit#heading=h.bqnrtc8kz7hb
3. [Kaliya] - what are the other systems doing - the "closed loop" (Wave1)

1. Recommended technical architecture
2. How does this reflect in GHP EGF

1. Forward looking plans
    a. IIW - opportunity to present a product for early feedback; what sessions would we like to host at this event
    b. Draft of the document which is the WG deliverable/product - as soon as the template is finalized and we'd want to get to a place where we can produce a document that makes clear recommendations and actionable information

There are a lot of existing networks/lists - don't we need to connect these up. We will likely have a network of networks

From 30 MAR 2021 meeting - input from Marcos:

What form can practical trusted registries take?

- Centralized
- Decentralized (Permissioned, Permissionless, Federated)
- Other?

Which information is necessary to register in a trusted registry by an issuer when a verifiable credential is issued?

- Hash of the content
- Status of the credential
- Link to the issuer (DID + digital signature)
- Link to the subject

Which information is necessary to verify against a trusted registry when they are presented to verifiers?

- The issuer as an authorized entity
- The status of the credential
- The content/claims of the credential

Who is responsible for defining or maintaining lists of entities authorized to be issuers of specific verifiable credentials in specific contexts or jurisdictions (i.e., the laboratories authorized to issue certificates of COVID-19 tests in Honduras)

How do we specify in the verifiable credential the trusted registry where the proofs are registered?

How do we establish a standard for both centralized and decentralized registries to store and make available the proofs in a way that is common to everyone, so once the verifier figures out the trusted ledger to be checked and the access point to it (which should be able to do directly from the credential), the protocol to accomplish verification is standardized

Steve Magennis : I believe items 5-11 below is where our focus needs to be and where we can offer real value. Items 1-4 are deep, complex issues that need to be resolved well in advance of the actual act of verification. These decisions will almost certainly be fluid and driven by a complicated mix of policy makers, corporate lawyers, industry advocates, public health professionals and public opinion.

Looking at the processes associated with the act of Verification:

1. MUST have **predetermined** knowledge of the range of decisions the verifier intends to make (e.g. fly / no fly, secondary check, isolate)
2. MUST have **predetermined** knowledge of what specific claims or credential(s) are acceptable for use as input to making said decision(s)
3. MUST have **predetermined** knowledge of the rules by which the range of decisions should be made
4. MUST have **predetermined** knowledge of which issuers are acceptable as a source for the predetermined claims or credentials

OR, if the issuer is not / cannot directly be deemed acceptable:

MUST have **predetermined** knowledge of which certifying authorities are acceptable to 'vouch' for the acceptability of an issuer as the source for the claims or credentials that are pre-determined to be acceptable

At the moment of verification:

1. MUST have a means of recognizing the issuer or certifying authority that is bound to the claim or credential presented (e.g. CDC issued credential or CDC authorized credential)
2. MUST have a means of verifying that the issuer or certifying authority is who the verifier thinks it is (e.g. Centers for Disease Control and Prevention NOT Coronavirus Disease Consortium)
3. If the verifier intends to rely on a certifying authority rather than the issuer directly the verifier SHOULD also have a means of verifying that acceptable certification is active and properly bestowed upon the issuer - for the given context and intended purpose.
4. MUST have a means of comparing the issuer or certifying authority to a predetermined list (internal list)
5. MUST have confidence the claims or credentials are sufficiently current at the time of presentation
6. MUST have confidence the claims or credentials presented have not been altered since they were issued
7. MUST have the ability to verify holder and principle of the credential is the same

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. 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