2021-04- 15 - Trust Registries Drafting Group Meeting Notes

<DAY> March <#>

Attendees

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

Participants:

- Marie Massery (
- Marcos Allende Lopez
- Patrice Van de Velde
- Stephan Baur
- RJ Reiser
- Sid Mishra
- Viola ICTS
- Marcos Loiez
- Sankarshan Mukhopadhyay
- Drummond Reed
- Savita Farooqi
- Scott Perry
- Kaliya Young

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

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

Recording - *Link*

Meeting Notes

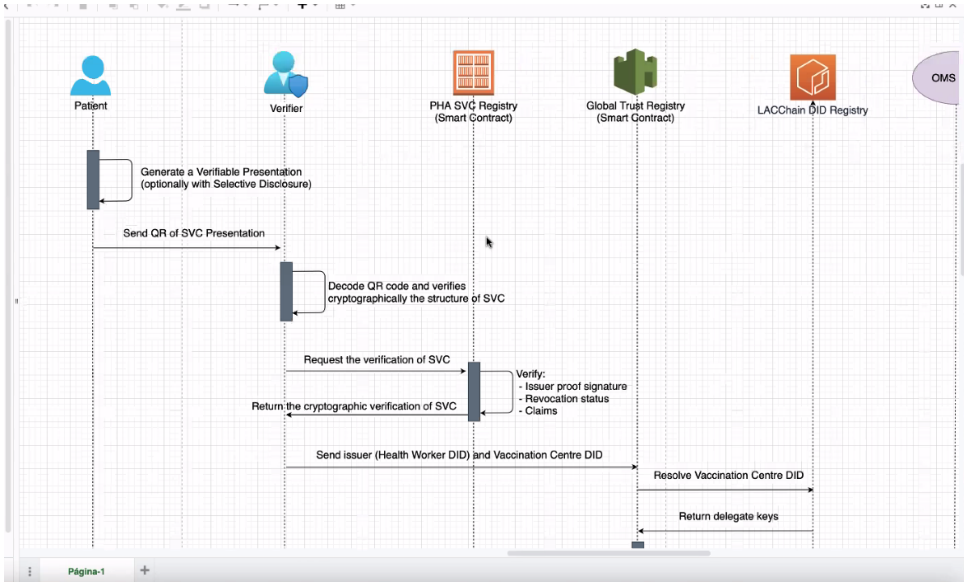
1. [Darrell] Start with present the diagram
    a. Sergio from LACChain and we are working with Marcos
    a. Introductions
    b. I think we're starting to get to the point of what are the real problems that we need to solve.
    c. In the initial phases, at least have good health pass, short term long term is really not our problem, the problem shouldn be solving the trust registry side.
    d. The concept here is Julian is not able to make it today, but Julian is fulfilling a role in the UK, and other countries where, in essence, his company helps you get access to your data from your own health system, it does some local processing knows, for example in the UK, that this particular vaccine.
    e. there's nothing precluding trust here, as you were in a world where if iI can get a verification form and verify myself or I can choose to trust the digime to do it for me
    f. Digi.me model makes the TR simple.
2. [Stephan] We want to be care with recommend a model that prompts a monopoly
    a. This could cause liability. I just want to be a little more careful. I think then that it's a toss-up. Agencies have one that's true in a particular situation where a verify trusts an APP.
    b. I'm I think what we need to we should have enough foresight to make sure that this is not, falling into their own rapidly building.
    c. Stephan Baur: And, and so I think there is a situation where somebody can actually verify that you still have transparency to the entire validation chain or trust chain. That a vendor to trust-anchor that started, this would provide will be of immense value.
    d. The delegation to such an APP is not the issue. It's only saying check that other necessarily registry, or trust framework is the authority, users have to be cognizant about the borders.
3. [Drummond] outputs, meaning a credential or pass that we're talking about that's what you're saying right there oh yeah yeah.
4. [Darrell] yeah you know if I received from the government of Ontario that I got a credential. But downstream if digi me was able to turn that into something that a verify would say yeah Darrell is vaccinated.
    a. [Darrell] this might be something that we start with for the 30 days. . .
    b. Some groups might want the simplified where someone assume responsibility
    c. Keep in mind “what does good look like”

    d. A lot of people will likely be doing stuff that's really not good enough, but we don't even have a norm to look at.
    e. We teach the world what good looks like so that we can't have that oh I just did this buddy over here has an APP and I just use it for the rest of time.
5. [Darrell] How do we handle counties that are 100% PKS WHO and others that are 100% DID based
    a. How do we handle a ecosystem with both Centralized PKI and Decentralized PKI
    b. Marcos will also share diagrams
6. [Drummond]
    a. Couple diagrams that outlines the trust architecture
    b. <diagram>
7. Starting points - roots of trust
8. We specify the requirements for each ecosystem to assign a DID
    a. This helps us resolve both x509 and DID based registries
    b. Any authority that wants to be a root of trust MUST comply with this model
    c. This is wrps the x509 with a DID / DID-document
    d. Standardize a protocol
    e. We don’t know if WHO is going to be publicly verifiable. They likely won’t assign a DID to their root servers. There might need to be somebody that acts as a proxy to resolve DIDs to x509.
9. [Todd] We should present this plan at IIW and get others considering the DID-x509 resolution
10. [Drummond] <verification protocol assumptions slide>
11. Stephan] should that not be a chain of VCs rather than DIDs? Or at least reference DID docs
    a. This breaks a whole model in my mind
    b. I wonder how difficult it would be to change x509 to use a DID
12. [Darrell] @Stephan - I’ve debated this a lot and there are pros/cons both ways. One is walking up 5 levels through VerCreds to finally get to a DID and needing to look them up anyway.
13. [Drummond] I have a couple quick slides to discuss
    a. They have a DID they publish the DID document wherever they choose, or in multiple places right, this is how they can say this is really you know the ID for our service and that document will expose again i'm just saying.
    b. Either there's two types of endpoints for resolution. Resolution DIDs, that simple, or key based, and they can support one or both. And then the other assumption this protocol is that a good health pass compliant vc or verify.
    c. verifiable credential and verifiable presentation, the distinction is getting more and more important what is going to be verifying is usually a presentation.
    d. This includes three things the DID for the EGF, and the credential type, so they know how to start resolution the DID for the or X

1. [Drummond] Of the verified clincher or present type presentation type and that's so that the verify or can only verify the issuer is.
    a. The type is needed to be sure that the issuer is authorized for that kind of credentials, so you don't have a testing lab issuing a vaccination certificate, or vice versa, or anything else, so those are the starting points at which point the protocol.
    b. The trust registries are either going to say, in the case of DID, register is basically saying yep registered and valid for that type
    c. In which case the final step is to resolve the DID to the document to get the key you need to do verification.
2. [Marcos] Presenting LACChain diagrams
3. <insert ppp>
4. [Marcos] I work in the American Development Bank, the Inter American Development Bank is like the World Bank.
    a. Innovation of these countries is coming from the IDP so basically my conversations are with a specialist of my institution That are managing loans and with the counterparts from the region that are deciding which projects, they want to do
5. [Marcos] In the topic is around vaccination credentials, the problem is that there is no clear solution. What we are doing is different than the proposal Drummond showed.
    a. Drummond was describing the problem that I'm facing; in order for people to understand what that is the solution, I needed them to understand the problem we are trying to solve.
6. The problem that we are facing
    a. We are introducing technology
    b. What is the
    c. What are the identifiers
    d. What are teh trust frameworks thet we need to make all this possible
    a. We need a flexible way to connect all entities to
    b. With regard to the certs centralized vs decentralized both have pros and cons
    c. Decentralized is better because it enables the owner of DID to rotate keys. This is difficult in the centralized model because id is slow andburrden with process

[Drummond] What Marcos just explained is exactly why DID architecture was created.

1. [Marcos] Now let's go to the diagrams and to see how we are proposing this to work in alignment with the World Health Organization.
    a. We are trying to convince WHO that verifiable credentials are the right way to specify these things, and DIDs were created because verifiable credentials needed some kind of identifiers and registries first.



2.
3. [Kaliya] CCI is trying to convince Europe of this - Marco - maybe you can share this with us in that group too and it can build on the work the Greek guys are doing in this area
4. Some countries don't have a PKI infrastructure but they at least have a HSM

1. [Drummond] So you are saying that you are using smart contracts maintained by the government? Checking cryptographic proof of the cred on chain
2. smart contracts maintained by root of trust

1. [Stephen] We need to talk about the what then moving into solutions of the how.
    a. Agreed - this is just one possible solution
    b. This gives hope that there are multiple approaches to solving. What is the min than needs to be in a TR?
    c. How do we get it to work both ways x509 and DID
    d. Comparing the identifiers DID in one and the public key in the other
    e. True if we are talking about self-signed x509 certs
2. [Sergio] So basically the process of education is being presented in a general way, so information is structured and verified by of cryptographic. and we ensure the issuer is authorized issue this type of credential
3. [Marcos] Then authorized by the Ministry of Health right, so we create that root of trust through the ids, so it is not necessary to use verifiable potential for these root of trust, and this was a conversation that was going on the chart because, if we have a smart contract.
    a. The DID register it's not exactly a smart contract, we use other things like events in order to register, in order to have the idea of what are the kinds of smart contracts for different purposes.
4. [Stephan] Is it, is it possible to find it out on Friday next week to sort of synthesize from yeah that trouble you as well,

Presentations

- Initial Presentation (Google Slides)

Key Resources:

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

Action Items

1. TBC