Blockchain PSIG Call Notes

*14 May 2020*

# Attendees

* Mike Bennett
* Ian Stavros
* Neil Aeschliman
* Robert Rencher
* Rob Nehmer
* Nick Stavros
* Bobbin Teegarden

# Agenda

* SSID RFP Possibilities

# Meeting Notes

## Disposable IDs RFP

Previous discussion – via OMG introductions

Existing Spec: W3C DID: <https://www.w3.org/TR/did-core/>

### Disposable Identifiers Initiative:

<https://www.disposableidentities.eu/>

#### Definitions

DID allows you to allocate a trusted 3rd party to supply your credentials and the you can send some encrypted or hashed thing to anyone who needs to verify your identity – without giving away your own personal information in so doing.

Also lets you indicate that the identity has not been tampered with. Based on the party not being sure whether or not to trust who is sending the credentials but can verify the underlying information.

### Questions

Then what does the ‘Disposable IDs’ thing do?

Also who are they and are they a standard.

**Who:** NGI FORWARD CSA

The NGI.eu portal is run by NGI4ALL, which is part of the NGI initiative. NGI4ALL has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement no 825354. The content of this website does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

### Slide Deck (on DispIDs Site)

For the remainder of the meeting we went through the slides from the Disposable ID Project.

#### Slide 3

Slide 3: Introduces temporality of e.g. a car accident evet.

GS1 – persistent not disposable. Highlights the need for persistent ID so that you are talking about the same object each time between any 2 parties.

DID – likewise?

Temporary / non persistent v permanent.

Temporary if associated with an event, would have information specific to that event. Set of variables relating to creation of a non persistent ID.

Could like a persistent ID to a non persistent ID, or not, as required.

Framed on Slide 3 as an event. See GS1 RFI Response: the ETCIS ID. Objects that have a time stamp and a location and further context. The object and the locations are defined with the persistent IDs and then Time uses an ISO time standard while XML binding uses XML Schema date time concepts. Vocabularies from WGs provide grater context. If you are trying to trace the history of an object as it traverses a supply chain, then ETCIS provides those event. Locations and Objects use their persistent IDs. Provides the thread that holds it together.

In the car accident example: I want to be able to get hold of the other party but as soon as the thing is settled I don’t want them to be able to contact me again or vv. So I need to reach the as long as I need to (but no longer). There may be entities that need to retain that information (e.g. for a medical issue, turning into a lawsuit, going to an insurance company). Ho do you handle the requirement for how long I need to retain that.

Also GDPR.

If my ID is associated with another ID, that relationship needs to be held private. E.g. if I am associated with someone who is associated with some rehab center. So anonymity is a reason to use the DID standard.

This improves on e.g. giving a Microsoft ID to see your medical records.

Same for the Covid proposals – seem not to be making us of any DID, whereas Disposable ID is a step further.

So the challenge is how you provide a non persistent ID specific to the event it is associated with. How do you prevent people collecting these non persistent IDs and identify the corresponding persistent identification.

**Bitcoin:** not anonymous but anonymized. Can trace the txns and figure out the people doing the txns. So not a simple matter of 1 level of indirection. The ability to search an ID through the system lets me triangulate who you are.

So this remains a challenge.

So do these guys have a solution to that scenario?

What’s the opportunity: That when you define a disposable ID you design in the ability to not identify related persistent identifiers.

So we can do an RFP that lays out these requirements, including the ability not to triangulate against that ID.

#### Ontology view:

* Relative Thing (relative to any context)
  + Examples: Party in role
  + Temporary things (any relative thing has its own start and end)
  + Any contextual matter
* Independent Thing (identity bearing thing)

**The challenge:** Any Relative Thing refers to an Independent Thing.

* The challenge is to make that relationship inscrutable.

#### GDPR:

Disposable IDs has string claims on BDPR compliance. Effectively the individual requirements of GDPR are baked in to the solution (and the standard?)

GDPR comes out of EU. Replaces earlier DPA.

**Principle:** Any personal data about some person is the property of that person.

Any use of that data must be in accordance with your reasons for giving it.

**Disposable Identity:** defines context in which the data is given. Not used outside that context at all.

Provided that there isn’t an obvious link to persistent information about you.

Linking a disposable ID to a DID might resolve that problem.

#### Slide 8

Hardware chip based ID

Hardware oriented public / private key encryption. The chip holds the private key so you need the physical device to sign a thing.

If that is what slide 8 refers to – disposable because it uses hardware to create a temporary hash (for the context). That exists.

**Example:** Put your drivers license in a physical reader, then it validates that. That is independent to the facility that wants to do the txn with you. You get back an ID validating that this person is who they say they are, without you needing either the drivers license or any biometrics. Using external physical equipment.

That’s DID.

**Challenge:** once the validation of credential has been made, is there a requirement to retain details of the validation?

Might get a txn ID identifying the 3rd party agency with which it was verified. That org can always go back and verify.

Surely they need to keep a record that the ID was authenticated but would not need to retain a copy of the material used.

* What ‘who’ is being referred to above?
* 3rd party needs to keep track
* Direct counterparty does not.

Are we working with outmoded methods relative to the risk?

Cultural norms versus what is possible with technology. Can DLT liberate us where we can not be bound to the historical norms for how we validate, trust and prevent fraud.

In conjunction with this we should look at our legacy methods and see if they are still applicable. Expect emerging tech to reform how we do identity.

e.g. use of drivers license to prove our identity. Was never its purpose but has become its use.

The Person generates a one-time “disposable” DID for this specific connection, which is derived from one of her persona DIDs. Only this Person can make the correlation between her persona DID and her disposable DIDs

## Conclusions

* This is something unique.
* There are specific requirements we can put in an RFP about begin able to occlude the link between context ID and persistent ID
* The proposal here does cover that (so it makes a suitable RFP response).

So…

Shall we do an RFP for this?

(First check that W3C or someone else doesn’t already have this)

**Consensus:** Yes.

People would be interested in the outcome and in contributing.

Important in commercial aviation. Reason: Requiring individuals to demonstrate their health, or be put in a situation where their health is continually evaluation. So there is always an ID associated with that. If we can come up with a temporary ID that needs this need without giving away persistent personal data about the individual. Would last the duration of a flight.

e.g. if I have been through a health check 20 minutes earlier I don’t want to go back and do it again. Likewise if changing flights.

Also there are many entities that have an interest in the validation of your health.

However, they only need it while you are in contact with them

### Outcome - Proposal

**Proposal:** Ephemeral is a better way of putting it than Disposable.

RFP for Ephemeral IDs

Draft RFP we can bring to June QM.