Blockchain PSIG Call Notes

*21 May 2020*

# Attendees

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

# Agenda

* Updates on SSID RFP / Disposable IDs
* LETS RFP

# Meeting Notes

## SSID RFP

### Overview: MyData Webinar

MB shows a slide from a webinar today on the overall Covid-19 DLT-based identification landscape:

A screenshot of a cell phone

Description automatically generated

**Standards bodies and Technology Stack for Covid Applications – Greg Nadeau**

### Disposable IDs Initiative

MB gives an update of the recent conversations with the Disposable IDs folks. Some of this was brought up later in the call.

**Key points**

Identity is in a specific context. Context has a start and end time and is disposed of as soon as the context no longer applies.

The standard embodies each requirement of GDPR. At a simple view it takes each requirement of GDPR and ensures there is information / metadata to cover that requirement. That is, the Disposable IDs standard is effectively an implementation of GDPR itself.

The standard has a reference implementation already

The standard

Trusted party may be one of a number of kinds of entity chosen by the end user. These may include neighborhood professionals (e.g. solicitors/attorneys, accountant etc. as you would use to notarize something) or clubs and societies. They gave the example of the Automobile Association in the Netherlands. Such groups may offer this as a kind of service to their members.

A consequence of this is that users may choose to have different entities or individuals be thwir chosen trusted third party for different contextual disposable IDs – possible in the broader context of that entity (e.g. use AAA for all their automotive related contextual IDs) or not, as they choose.

(see notes on levels of context below: You would not have a Disposable ID for ‘Automotive’ as a context, since each Disposable ID would be for a specific and time limited context with a specific counterparty to whom you the user choses to identify yourself.

The end user is unlikely to choose to make a government or a large corporation their chosen third party for disposable IDs, and it is hoped that this simply doesn’t happen.

### Discussion and Comments

#### Defining Contexts

Who What When Where etc.: the Disposable IDs proposal explicitly defines

* Time window – when the context begins and ends (so it is discarded when the context no longer applies)
* Parties: there is always a party who the Disposable ID is about, and a party they are interacting with.
  + So this is a narrower sub-set of all the things that may be a context

#### Temporal Context

What if the time context changes? Does a user end up losing their contextual ID before they want it to be?

* This should not happen under GDPR: the context should be exactly what the user wants it to be
* It’s not like financial classifications of e.g. debt classified by maturity, in which the set of individuals moves in and out of a given category. Whatever category of things is the context, it must correspond to the reasons the user wanted that disposable ID.

NS: This needs to be Event not Time (or not only Time).

Define the context in terms of multiple events, e.g. event + time. Then it expires either after an expected event (trigger) happens or in the absence of that, after a given period of time.

Look at database triggers as a model for this.

REQUIREMENT: The context has to be how the user defines and understands that context.

Might be e.g. coming into contact with someone else.

GDPR: When you take someone’s data you have to describe it in certain formal terms and then demonstrate that will only use it in those terms. We need an ontology and a representation of the ontology to the end user in understandable terms (natural language). This natural language needs to correspond exactly to the ontology.

Don’t get hung up on the words e.g. discrete v continuous ‘event’ notions. If both continuous and discrete temporal concepts are needed it doesn’t really matter which one you choose to call ‘Event’. That’s a terminology problem.

BT: The ontology for the context is a simple named ontology.

You want to be able to stand up a simple named ontology (instances), that will need to have been derived from the broader ontology of the concepts that make up possible contexts.

Things moving in and out of time – should NOT be the basis on which a context is defined. User does not want their disposable ID thrown away in circumstances not of their choosing, as that would violate GDPR. So the ontology needs to reflect what they see as their context. See the possibility above of having multiple trigger events for disposal.

Who validates the elements of the context? Some governing entity.

MB: In terms of the slide below (from today’s MyData webinar), it looks like there are two things to consider:

* The standard itself (the RFP response) needs to define how the ontology is defined so that contexts are always coherent (and coherently and accurately represented to the user)
* The need for some governing body to oversee how the trusted third parties do what they do

A screenshot of a cell phone

Description automatically generated

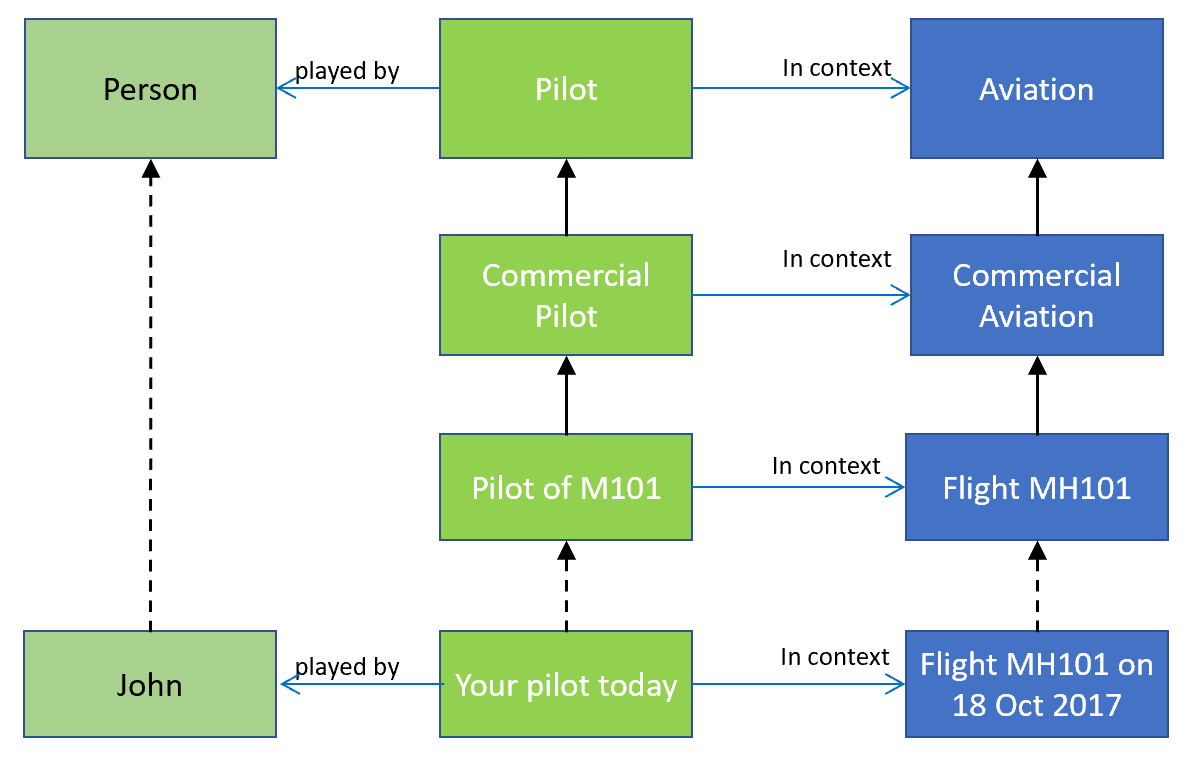
**Governance Slide from Greg Nadeau at the MyData Webinar of 21 May**

Note that this slide is for more general SSID scenarios, but the same notions of governance would be applicable to Disposable SSID, we think.

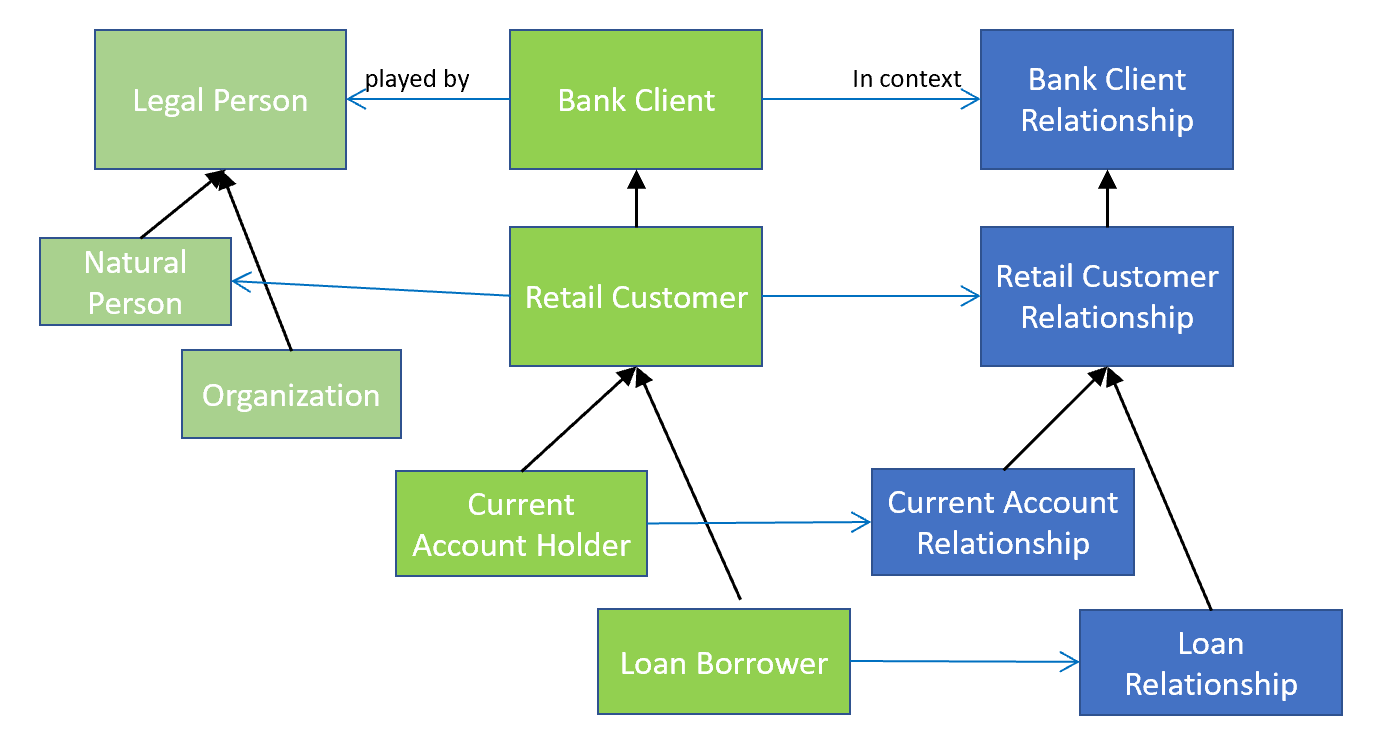
## Broad Context

Ontology allows for broad contexts e.g. flying, automotive, travel, as well as narrower contexts like a specific journey, flight or flight leg. Some of these may be nested within one another.

MB dug out this slide from the FIBO and post-FIBO / Semantic Shed activities:



**Hierarchy of Contexts: Pilot**



**Hierarchy of Context: Bank Client and Customer Relations**

**Comment:** these examples show single inheritance but this being an ontology, concepts in any one of these three partitions may use multiple inheritance (polyhierarchical or faceted classification).

#### Discussion

The user MAY choose to use e.g. an automobile club as the issuer for all their Disposable IDs in the broad context of motoring – or they may not. So there is a role for the broadest contexts in our ontology but it’s all optional.

The driving force for all this is the ability to exclude large corporations and governments.

For example a bar doesn’t need to know about the details on my driving license they just need to be able to verify that I am old enough to drink. They don’t need to know what vehicles I am allowed to drive. So already these documents are not being used for their native purpose. SSID reduces things to the information that someone is identified by, while disposable SSID reduces this to the use of the identification in a given context.

## LETS RFP

Sections rearranged as per April 30 call notes.

Content within those sections to be extensively re-written as they still describe the IOTA MAM exemplar (now called IOTA Streams).

There is nothing to review until that re-write has been done.

We will pick that up in 2 weeks

## Next Meetings

Next week 28 May we will draft the RFP for Disposable Self-sovereign Identity (and think of a name for it), using the ideas we talked about today. We will also discuss RFC versus RFP, since although this is a strong candidate for the RFP process, it is also already a mature standard with at least one reference implementation in place. So we should at least have that conversation (although it’s most likely we will end up deciding on the RFP route; the important thing is that that decision be seen to be made).

# Appendix: Chat Log

**Bobbin Teegarden (to Everyone)**: 1:18 PM: Are all of these 'disposable' personal IDs going to be as much as a chaotic personal activity as the plethora of personal passwords are now? Will we need a personal ID Safe?

**Bobbin Teegarden (to Everyone)**: 1:23 PM: We need to invent a ContextNut, a named context (little ontology) that contains the key important elements of whowhatwhen...

**Bobbin Teegarden (to Everyone)**: 1:29 PM: The SOWA example 'pilot' is a decomposition (less and less abstract, more defined). But level of abstraction is only ONE of many 'contexts' or 'points of view' where context changes

**Robert Stavros (to Everyone)**: 1:31 PM: I think that the Ontologies are additive

**Bobbin Teegarden (to Everyone)**: 1:31 PM: A hierarchy is a particular contextual POV (Point of View). There are others...

**Bobbin Teegarden (to Everyone)**: 1:32 PM: @Nick ontologies are additive: i.e. they merge? or some of the aspects of one context are preserved as they morph forward in time?

**Bobbin Teegarden (to Everyone)**: 1:43 PM: 'Event' is problematical -- e.g. does an event have a beginning and end and duration, or is a single thing in time...? Dave McComb and Mike Uschold have an ongoing argument about this (maybe triggered by me poking MikeU...)

**Bobbin Teegarden (to Everyone)**: 1:52 PM: If you're going to have disposable IDs, the mechanism needs to be simple (public key/private key like)...

**Bobbin Teegarden (to Everyone)**: 1:54 PM: In blockchain, one of the freeing aspect is that only the ID is known to the parties involved, and not wound up in the entrails of governance mechanisms (internal or external)

**Neil Aeschliman (to Everyone)**: 1:59 PM: Thanks for another interesting call, everyone!