Blockchain PSIG Call Notes

*16 July 2020*

# Attendees

* Neil Aeschliman
* Robert Stavros
* Michael Bennett
* Bobbin Teegarden
* Rencher, Robert J
* Ian Stavros

## Apologies

* Rob Nehmer

# Agenda

* Ephemeral SSID

# Meeting Notes

## The Story so Far…

Disposable IDs (EU funded project)

Now called DispID

Telegraph channel

Rob von Kranenberg (sp?) has left DispID

Wanted to join OMG to be a submitter for this. Have not done so.

This PSIG group discussed applicability of Disposable IDs already – positive conclusions.

### Criteria

* Business case / potential users
* Other competing standards

### Other standards:

* W3C DID
  + DispID is an application of that

### Usage:

**Our conclusion:** this is unique and does fulfil a business need. GDPR etc.

We discussed how to bring our ontology approach to:

* Identify context as a thing
* Be able to next contexts

### OMG QM Discussion

Conclusion: Useful, maybe needs an RFI.

The original folks were looking to have something to submit (as an RFP response) in a month or so. So we were reluctant to slow things down with an RFI.

Now things have slowed down from their end, maybe RFI is a good idea?

### Points in Favor of RFI First

Unlike many standards proposals this one is not obvious until you understand it.

SSID is relatively new and most of the scenarios we see are for vanilla DID implementation.

So an RFI might be a way to see how people might use the thing

### Discussion

NS: One push-back we are seeing is identification controlled by Facebook or Google. Also Microsoft and Apple. And Twitter.

When you sign in to something it is often assumed you would use a Google ID. So there are additional privacy issues to be aware of.

When they start talking about splitting up the hi tech companies, the main thing that needs splitting up is the identity managememt side.

Some sites now are assuming Google without giving you the choice as others do. Most give a choice. Zoom seems to be doing this.

**Example:** hospital requiring log-in using a Microsoft credential.

This gives the credential provider knowledge about your activities.

So any RFI should also talk about privacy. Even if e.g. Google were to offer something would there be a firewall between this and the rest of their business.

**Conclusion:** Agree we should do an RFI. Also include Claude’s group on Data residency.

### GDPR / Data Residency

See also article on EU not being satisfied with US arrangements.

* See GDPR

Walled garden arrangements

* Questions of accountability (e.g. ISO 9000 audit trail)

### Credential Management versus SSID / DID

Login credentials. Do these have anything to do with SSID / encryption based identity?

SSID still requires you to trust someone.

The separate issue that NS is articulating here is the 3rd party being trusted to know stuff about you.

Are we diverging a bit to talk about Google and Microsoft etc. since these are not SSID as far as we know?

Yes – see Drummond Reed (Evernym): started with everyone needing individual credentials for every site. So you owned your own identity 1:1 with each site. Then as our interactions proliferated, we all had too many password and identities. So that’s where 3rd Party ID providers came (the Google etc. example above). Using a more predominant credential provider, as a platform we use more frequently – so we outsourced the authorization to them. Then define the APIs and standards or releasing that authorization. But, there are now privacy concerns:

* Whether that org is entitled to that data of yours
* How they use that data
* How this plays with GDPR

So the concept of W3C DID (SSID) is that that spec plus the verified credentials, with decentralized team management, gives 3 standards coming together to offer a new means of decentralized ID that does not depend on a 3rd party, which is a better way to be GDPR compliant.

So this is the business driver for DID.

Q: Is what we are pursuing about the GDPR Privacy question, or the initial hypothetical for DispIDs – e.g. exchange info after a car accident so your insurance companies can settle but you don’t want them to have that data after the context is ended.

Perhaps the RFI needs to take people over the jumps.

See <https://www.youtube.com/watch?v=Jcfy9wd5bZI&t=225s>

### What we Have So Far

So we have:

* Evolution of the ID solution
  + 1:1
  + Centralized e.g. Google
  + W3C DID
  + Ephemeral (Disposable) SSID – our potential RFP
* Privacy directions
  + Bypass the need for trust in 2nd party (online provider, insurance company, bar)
  + Bypass the trust in the ‘trusted’ 3rd party?
    - Disposable SSID – lets you choose an ID per Context
    - Also lets you choose a DIFFERENT 3rd party per context
* Different ID ecosystems
  + Credentials (Google etc.)
  + Cryptographically enabled e.g. W3C DID

W3C DID is peer to peer. Establishes a channel and identity between you and an organization – it does not require a 3rd party. Verified Credentials (VC) is where that comes in – this is about what things that party is allowed to do (e.g. the drinking age example). DID spec itself does not cover that, it primarily defines a private channel between 2 parties. Caveat: from an initial reading of this.

Maybe other applications use DID in different ways?

### Identity versus Permissions / Credentials

Distinction between:

* Saying you are who you say you are
* Saying you are allowed to do a given thing (requires specific data e.g. DoB)

The DispID thing also focused on what you are allowed to do.

**Decision:** Are we looking to do an RFI first, or carry on with the RFP idea?

#### In Favor

Would have better distribution to industry by starting with an RFI.

Also we can use the RFI to articulate what is possible in order to then ask about it.

So it provides an informative direction to industry – signaling direction on where we think this needs to go.

### RFI Ideas

#### Model Formats and ilustrations

Consider including a BPMN model as part of the RFI – identifying what is or is not covered. Rather than just asking questions.

Good graphics.

Use of BPMN? Or something less they (depends on audience)

* Use UML Activity diagram – anyone can understand those if we use the simplest notation (same as Visio and the rest).
* Maybe use multiple views
* Pictographs and things

Put this into the RFI so we show we have thought of each thing, asked if they are aware of it, and can then ask questions:

* Why they don’t like it?
* What are the gaps?

#### Messages:

* Potential of ephemeral context specific RFIs
* Distinction between ID and Credentialing
  + Put some scenarios down
* Distinction between (whatever Google etc. do) and cryptographic has based SSIDs

### Identification and Authentication

If we do SysML or UML, everyone is confronted with this idea of IA

IA = Identification and Authentication. Where ‘Authentication’ cover the ability to use some product or service of feature or facility – therefore covers Credentialing.

Can we have reusable components like a black box that people can pick from. Encourage people to actually do it.

Consider IA as Non Functional Requirement (NFR).

So e.g. if I want to provide info on medical devices – that’s the use case focus. People get into a rabbit hole about IA but what if we show a sort of black box for this functionality and then show the menu of things that may be in that black box in the terms outlined above.

Allow modelers to be able to specify IA in a simple way

We need: a language in which to articulate the dimensions and features of ID including AI, credentialing and Identi**ty**.

See Slack. Also Microsoft and Skype. Since MS bought Skype, we end up with issues across their IDs. MS Office gives you a new Skype ID.

So the RFI should include some more background on Identity v Identification.

So that’s more background for an introduction to the RFI.

So the RFI could be a way of capturing quite a few problems we might not have known exist, or calibrating some.

### Conclusion

This needs to be an RFI

### Audience for the possible RFI

* Individual people (not the usual audience for an OMG RFI)
* Standards organizations
  + E.g. G31 SC / Aerospace Industry Assoc etc. would be v interested
  + IATA
  + SAE International (Society of Automotive Engineers)
  + Org that develop solutions relative to forward looking standards (SAP, MS, Oracle, Dassault, RSA etc.)
  + NIST, MITRE etc. government funded research orgs (and others in other jurisdictions); DARPA
    - Find someone and help them write a SBIR proposal
    - This (IA) is a real problem for government employees
    - US Gov uses CAC extensively (meaning the facility not another word for IA it’s another IA facility for identification – see <https://www.cac.mil/>
* Companies doing these things
  + Other industries
    - Retail / retail finance / insurance i.e. where members of the public interact
    - eCommerce,
    - Web based communities
    - Etc.
  + Travel (airlines etc.)
* DLT Ecosystems
  + IOTA
* DID and SSID providers

### Priorities for this Group

Is it a high priority (work every 2nd week on it)?

Then we can do one (or more) RFPs later depending on what comes out of the RFI

BT: There are so many activities going on in OMG and elsewhere on this that we would be walking into a large amount of activities. So it might be hard to fit in.

NS: Would spend time on this if there was likely to be a corporation that would do some implementation (e.g. is GS1 or someone were interested).

BT: OAuth has an audience in this area. Can do something with them?

NA: GS1 doesn’t have anything directly on this right now. Would they respond to such an RFI if we did one – unlikely. Meeting cycles – happy to have the discussion – seems a burgeoning area.

**Question:** Should we continue bi-weekly, or revisit this every month or so? Or at each Quarterly meeting?

We can’t determine if IOTA or anyone needs this until we can do such an RFP for Disposable ID or anything else.

The DispID might be hard to implement from a systems architecture point of view.

It would be interesting to put the idea out there and see who wants to do that.

NS: Propose we start building an area in the Blockchain Wiki to start collecting stuff that describes ephemeral IDs and see where it leads, rather than doing a formal RFI. Can use as material to put into an RFI. The topic is interesting and worth documenting.

We could do a white paper.

#### Conclusion

The concept is of interest

It needs maturation

A white paper would be a good precursor to an RFI

Q: How many steps do we want to invest our time to get there?

Could stretch it out over a longer period of time. But it is of interest and has value in e.g. the travel industry. Use case.

RR: Would be interested to invest time to help mature this.

So is MB, so is BT. So is NS.

**Conclusion:** Pick this up again in 2 weeks’ time. Continue to work on a bi-weekly basis at least for now.

## Next Meeting

**Next week:** LETS RFP.