Blockchain PSIG Call Notes

*10 Feb 2022*

# Attendees

* Rob Nehmer
* Mike Bennett
* Bobbin Teegarden
* Marilyn Pineda

# Agenda

* Disposable SSI RFP

# Meeting Notes

## Actions from Last Time (20 Jan)

### Read paper:

<https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust>

Includes a definition of SSI and reference to the W3C DID Standard

Published last month

RN: Was not on the 20th call – will read the paper

RFP should state that this (proposals) should be an extension to what's defined in this paper, or be ancillary to it, or similar.

#### Notes

Possible tie-in with DIF – group responsible for DID extensions / usage etc. (building on W3C DID)

- payloads? In our RFP

Communities (e.g. DIF, Sovrin, other issuers etc.)

Funding initiatives e.g. Horizon 2020 (EU)

**Resolution:** We should do due diligence against the various standards, communities etc. mentioned in this paper.

- action to be done during this quarter

**Timing:** when RFP?

Meetings before March: this + 2 more (24 Feb, 17 March).

### Today's Agenda

**This call:** Go through that paper, and plan out how we talk about the relationshipo f the RFP to:

* That paper
* The things mentioned in that paper (as a comprehensive survey of the landscape)
  + And international (EU but cites things in other jurisdictions)

Then on Q2 planning we might e.g. focus on this RFP specifically (given the RFI will be in a different phase).

Also to note that we don't have a corporate sponsor on this group that is participating in thee efforts so there is a risk of putting out something that looks naïve.

Also cover concerns such as security.

#### Broader Issues (as well as what is in the paper)

* Security
* Consensus etc. (the usual DLT things)
* Governance

We should coordinate and reach out other active group we know of and have links with:

* GBA
  + NB SSI is very relevant in voting (Identity + VCs)
* Cloud Security Alliance (CSA)
  + 2 connections via Claude – follow up on possible presentations in Reston
* IIC?
  + Identity of objects (IoT Things)
  + Security

Identity of Things vers peoples – are SSI principles (privacy etc.) relevant there? Things have no lega standing?

* There is relevance: if Ihave a devide e.g. a thermostat, what is the relatioshp between the Thing (device) and th user as a person – with their privacy issues as well as security issues. And both – can someone grab info from a device and access part of your identity information?
  + Would be nice to standardize on these so that a vendor conforms to principles of SSI
  + Then devices use same underlying technology – can verify that commands to the device

Device as the thing to which you are identifying yourself.

Device owner ass the party with privacy consideration – i.e. need a link from the devices physical ID and the SS ID of the person.

**Context:** the device may be a context. Long-live (not disposable) but definitely contextual. Context = This Device (1-dimensional context, recalls context may have any number of dimensions)

See also eIDAS in terms of context changing sites. Crossing borders. For example if your age allows you to drink in one jurisdiction and not another.

So for some credentials, we don't need VC because existing information about you already determines credentials.

#### Scenarios:

Driving licenses – in e.g. Italy you can drive things you can't drive in the US, n a US license.

Similarly, in e.g. UK the credentials are often grandfathered in e.g. large vehicles, motorbikes.

So the credentials – what a given piece of info allows you for differ against the SAME information.

Same for **COVID**: Different jurisdictions accept different vaccines as being eligible for entering a given jurisdiction.

**Voting:** the same information about domicile would make you eligible to vote in one place and not in another (though only relevant in places where voting ID has been made mandatory)

**Leisure activities** e.g. scuba diving. Different jurisdictions recognize different credentials. Some places allow 1-day training for tanks use.

Similarly sailing, motorized boat usage.

However: the point of SSI is that you don't show the data.

So given that the credentials in the driving license are NOT shown to the person, but retained by the trusted 3rd party.

e.g. if I wanted to drive a 13 seater minibus in Italy, and the license I have in the US says I cannot drive the thing, but in Italy the same license says I could drive the thing – would the hash / Q Code thing from the T3P to the 2nd party (e.g. rental desk) say I can't drive the thing (because I can't at home) or that I can drive the thing?

But I also don't want to reveal to the person at the desk that I am from the US. How do we deal with cross-border differences in what credential information allows for what activities in another jurisdiction?

There needs to be some recognition of the relativity. E.g. if I am American with valid license at all, that's what is accepted by the Italian authorities – but then I need to give some aspect of my identity to the 2nd party.

So need for the trusted 3rd party

* This person is from the US and has this kind of license
* In this country that kind of license lets you drive a scooter
* Therefore this person can drive a scooter

That is, the T3P needs to be able to recognize the contextuality of credentialling.

**Action:** - in our reading of the EU paper and overall landscape, look for how this is handled for T2Ps today

Both the 2nd and 1st party trust the 3rd party.

So these are Contextual ID-based credentialling.

So context > time-based disposability; is in scope for this RFP as it is context.

e.g. context of: This person in this jurisdiction

Or This situation

i.e. any context (situation = context):

A nice test for how Context is defined in RFP responses, is whether it can include the context of a person from situation (e.g. jurisdiction) X in situation (e.g. jurisdiction) Y.

Disposable ID is like a token? E.g. purchase tokens. Where the token creates a context-free credential.

Token = the response from the T3P where it says e.g. 'old enough to drink' or 'young enough to drive' or 'entitled to scuba dive in these waters'

Statefulness: what is the activity diagram between these 3 parties.

### Notes on the Paper

EU Agency for Cyber-security

eIDAS – cross-border regulation

#### From the paper? (BT posted in the chat)

The past nearly two years have proven to be a globally challenging period, in which eIDAS has been under revision and the COVID-19 pandemic has urged the development of new models for social life, business, and administration of government. To address these challenges, this report explores the potential of self-sovereign identity (SSI) technologies to ensure secure electronic identification and authentication to access cross-border online services offered by Member States under the eIDAS Regulation. The maintenance of continuity in social life, businesses and administration has accelerated the reflection on the possibility of a need for such decentralised electronic identity.

### Next Call

Rob away on 24th – can we switch it?

Swap with 17th Feb i.e. next week is D-SSI RFP.

Read MB proposed Abstract in these notes (below).

#### Agenda for next call:

Map out the relationships between the 3 parties in a D-SSI exchange relationships (transaction).

Also please read this paper before coming – complete the walk-through cross reference etc. on that.

MB put out a mail with the change of sequencing and the reading / actions list for next weeks call.

# Homework for Next Time

*(Please read ahead of the next call and be prepared to comment)*

## Proposed Abstract

This RFP seeks proposals for standardization in the area of disposable self-sovereign identity. The term Self-sovereign Identity (SSI) refers to a cryptographically-enabled means for an individual to be able to provide proof of their identity without needing to divulge personal data to the party to whom they are proving it. An SSI is also able to be linked to credentials of the individual (verified credentials) for specific services or capabilities.

Disposable SSI defines an arrangement whereby a person may use the facilities of SSI as described above but in a way such that the identifier may be discarded once the user no longer has need of it, and at the user's discretion. In practical terms this kind of short-term, single-scenario use means that the Disposable SSI is used within and is valid for a specific defined context, such as a specific journey or course of treatment. D-SSIs may also be used in broader contexts, such as all travel or all healthcare, meaning that contexts themselves may be nested from very broad contexts such as travel, to narrower, more specific contexts such as a specific journey or specific activity within a journey, such as hotel check-in. The user may elect to appoint different trusted third parties for different kinds of context.

Proposals sought under this RFP must address the following three aspects of disposable SSI as a minimum:

* Context
* Identifier Payload
* User states and activities

As follows:

**Context:** A formal definition of context itself, along with details of how to manage and maintain definitions of context for each use of disposable SSIs. For example context may be defined as a combination of concepts of instances of concepts defined under a formal ontology and knowledge graph, or by some other means, with justification. Proposals must include provisions for maintenance of context information as defined under the proposed definition of Context

**Payload:** Assuming the use of a formal standard for SSI such as the W3C DID standard, proposals shall define the proposed payload structure for DID documents, to define or identify the formal context definition and deal with disposability / state. If the use of a standard for SSI other than the W3C DID standard is proposed, explanation and justification shall be given.

**State / User Activity:** Proposals shall consider the statefulness of the SSI solution as used for disposable SSIs, and provide formal definitions of the relevant states and how conformant applications are to deal with those states and the transitions between them, and the implications, if any, for the DID (or other SSI standard) payload.

The scope of this RFP does not include other identity or identification solutions outside the scope of cryptographically enable self-sovereign identity.

For the avoidance of doubt, the term 'Self-sovereign Identity' should be construed as defined in:

<https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust>