Peer DID Method Specification Report

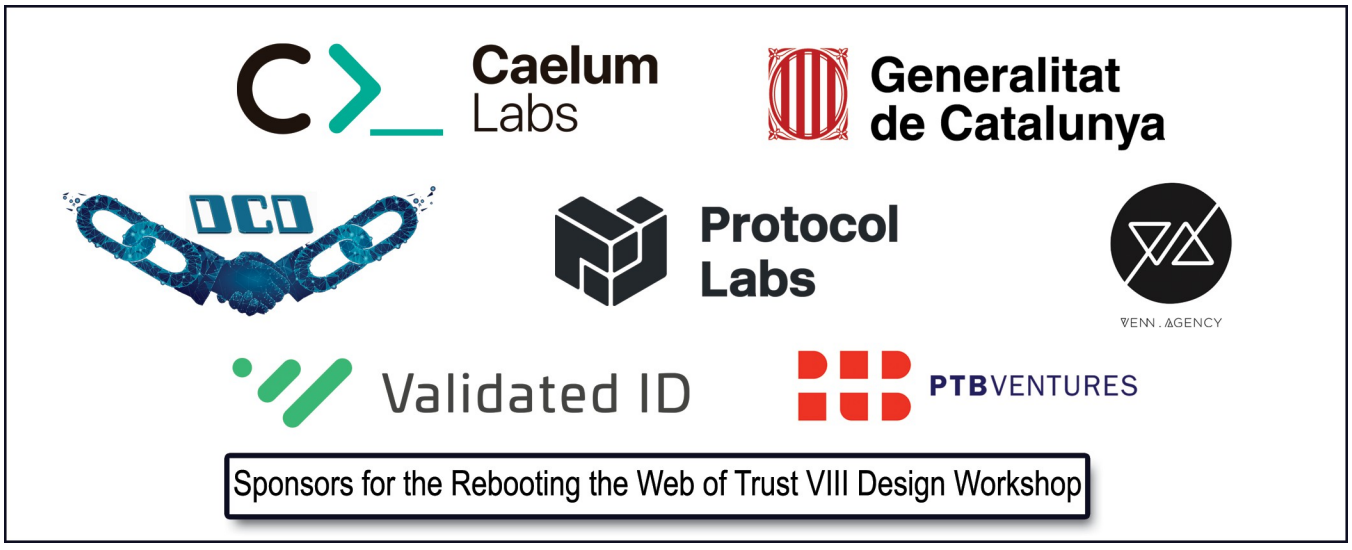
a white paper from Rebooting the Web of Trust VIII

by Brent Zundel, Timo Welde, Mike Varley, and Marton Csernai

ABSTRACT

This paper consists of objectives, use cases and observations around a "peer" DID method, based off a draft specification submitted to RWOT8. The following abstract is from that draft specification, located here.

> *"This DID method spec conforms to the requirements in the DID specification currently published by the W3C Credentials Community Group. For more information about DIDs and DID method specifications, please see the DID Primer and DID Spec.*
>
> *"This document defines a 'peer' DID Method that can be used independent of any source of truth external to the relationship in which it is used. The method is cheap, fast, scalable, and secure. It is suitable for most private relationships between people, organizations, and IoT things. DIDs associated with this method are also promotable to a more public context. That is, blockchains with different DID methods can graft some or all peer DIDs into their namespace(s) with no risk of accidental collision, and no loss of meaning. Peer DID will have a recognizable and consistent identity in all of them."*



OBJECTIVES

- Peer DID resolution does not require a Universal Resolver: documents are self-contained in a message protocol.
- Peer DID exchange is for the purpose of establishing secure communication, but Trust in the peers must be established at another level (in person, out of band, using Verifiable Credentials, using other attestations).
- Peer DIDs may be created on the fly for each new session between parties. This enables privacy and anonymity features.
- Peer DIDs may be persisted for subsequent sessions between the parties. This enables a persistent trust relationship between parties.
- Peer DID communication protocol is not bound to any specific ledger-based DID service or design model. (Someone who wishes to use a peer DID is not bound to any 'anchor,' such as a ledger).
- Peer DIDs may be interoperable with ledger-backed (anchored) DIDs; the peers group do not all need to be using peer DIDs (e.g. Alice wants to use a did:sov DID, and Bob wants to use a did:peer DID).
- Create an n-wise peer DID spec, of which one use case is pairwise DID exchange.

USE CASES

- Two or more individuals can create DIDs “without any overhead” such as infrastructure, registry costs, time penalty, or even network requirement.
- Two service entities wish to communicate in an "anonymous but trusted" way for a data exchange transaction, but do not need this relationship persisted beyond the transaction lifetime.
- In a doctor/hospital/patient context these three entities may wish to establish trusted communication channels for delegating care or sharing information (securely) regarding the other parties (the hospital sharing a record with the doctor and the patient seeing the exchange has occurred).

SPEC REVIEW OBSERVATIONS

Groups Section

- It should be made clear that if Alice and Bob are already connected (through peer DIDs), but wish to add another party, they should first create new peer DIDs with one another then invite Carol to that group.
- Removing participants from a Group is basically recreating the group without the person who is 'removed'.

Namestring Generation: keyfmtchar

- We understand the need for keyfmtchar, but it needs a definition, and an example of when to use it (i.e., when to make a "2") would be helpful.

Protocol: Message Format Section

- Indy HIPE message protocol is referenced - what extensions are required (multiplexed encryption) and why? The observation here is that pure JWE may be better for adoption, so understanding the need for extensions would be helpful.

Comments on the Spec

- The language of the abstract is "marketing speak". We would suggest changing it to state just the intent.
- "The method is cheap, fast, scalable, and secure" -> "The method is intended to be cheap, fast, scalable, and secure".
- Section 2.1 links to a non-existing section "cross-registration" at the end.
- Section 2.3 could be better structured with subsections (e.g. for `keyfmtstring` and `idstring`).
- Section 3.4 contains a lot of prose, which doesn't fit the structure of the rest of the document. Also it is not clear, what is meant by "The significance of the error situation described above, ..."

NEXT STEPS

The next step is to form a working group and establish a regular cadence of meetings to continue working.

The working group will work to:

- Address the issues outlined in this document.
- Continue to refine the objectives for peer DIDs.
- Iteratively modify the draft Peer DID Method Spec to reflect the objectives.
- Seek feedback on the draft Peer DID Method Spec from the community.
- Identify further issues with the Peer DID Method Spec.

CONCLUSION

The authors established a communication channel in the DIF slack and held a series of meetings. The issues introduced in this report (where still valid after significant changes to the Peer DID Method Spec) will be created in the github repo where the method spec is being refined.

The peer DID method has great promise. We feel that many of the interoperability concerns in the DID space may be addressed by wide adoption of a peer DID. We invite the SSI community to provide feedback on the Peer DID Method Spec reviewed here, and to participate in interoperability testing of implementations of the spec as they mature.

Additional Credits

Lead Author: Brent Zundel

Authors: Timo Welde, Mike Varley, and Marton Csernai

Sample APA Citation:

Zundel, B., Welde, T., Varley, M., and Csernai, M. (2019). Peer DID Method Specification Report. *Rebooting the Web of Trust VIII*. Retrieved from https://github.com/WebOfTrustInfo/rwot8-barcelona/blob/master/final-documents/peer-DID-method-spec-report.pdf.

About Rebooting the Web of Trust

This paper was produced as part of the Rebooting the Web of Trust VIII design workshop. On March 1st to 3rd, 2019, over 80 tech visionaries came together in Barcelona, Spain to talk about the future of decentralized trust on the internet with the goal of writing at least 5 white papers and specs. This is one of them.

RWOT Board of Directors: Christopher Allen, Joe Andrieu, Kim Hamilton Duffy

Silver Sponsors: Caelum Labs, Digital Contract Design, Generalitat de Catalunya, Protocol Labs, Venn Agency

Additional Sponsors: Validated ID, PTB Ventures

Community Sponsors: Blockchain Commons, Digital Bazaar, In Turn Information Management Consulting, Learning Machine, Legendary Requirements

Workshop Credits: Christopher Allen (Founder), Joe Andrieu (Producer and Facilitator), Shannon Appelcline (Editor-in-chief), and Carlotta Cataldi (Graphical Recorder)

Thanks to our other contributors and sponsors!

What's Next?

The design workshop and this paper are just starting points for Rebooting the Web of Trust. If you have any comments, thoughts, or expansions on this paper, please post them to our GitHub issues page:

https://github.com/WebOfTrustInfo/rwot8/issues

The ninth Rebooting the Web of Trust design workshop is scheduled for September 3rd-6th 2019 in Prague, The Czech Republic. If you'd like to be involved or would like to help sponsor the event, email:

rwot-leadership@googlegroups.com