RWoT8 DID Specification Refinement

a white paper from Rebooting the Web of Trust VIII

by Dan Burnett, Ken Ebert, Amy Guy, Drummond Reed, and Manu Sporny

ABSTRACT

The Decentralized Identifier (DID) specification describes a new type of URL that is globally unique, highly available, and cryptographically verifiable and which has no central authority. The DID spec document describes the expected ecosystem, data model, and syntaxes for DIDs. In December 2018, the W3C held a Strong Authentication and Identity Workshop that determined that a reasonable next step would be to create a W3C Working Group to standardize the DID specification. As a result, the W3C Credentials Community Group, which has been incubating the specification, will eventually need to hand the specification over to the newly formed W3C DID Working Group. In preparation for this hand off, a group at Rebooting the Web of Trust triaged issues related to the DID specification, refined existing proposals related to the specification, and gathered new features and requirements from the community. The result of this work is outlined in this document.

INTRODUCTION

In a recently published W3C Workshop Report on Strong Authentication and Identity, it was suggested that the DID Specification should be considered for standardization at the W3C via a new group called the W3C Decentralized Identifier Working Group (DID WG). The current Decentralized Identifier Specification maintains a list of issues that have been growing over the past year. Amy Guy and Dmitri Zagidulin performed an initial

Sponsors for the Rebooting the Web of Trust VIII Design Workshop
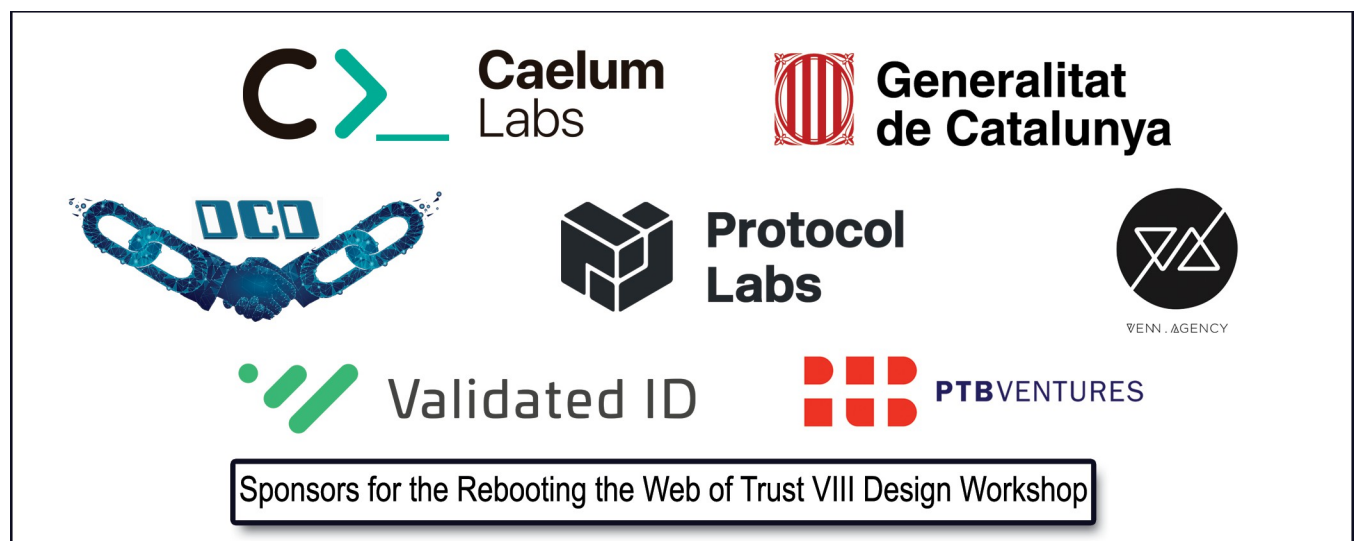
[triage of the DID specification](#) issues as an advanced reading topic paper for Rebooting the Web of Trust 8 (RWoT8).

In an attempt to provide the DID WG with a good foundation to build upon, the W3C Credentials Community Group, with aid from the Rebooting the Web of Trust community, worked on the specification at the Rebooting the Web of Trust 8 (RWoT8) event in Barcelona, Spain in early March 2019. The group processed issues related to the DID specification, refined existing proposals related to the specification, and gathered new features and requirements from the community. The state of the work as of the end of the RWoT8 event is outlined below.

The first day consisted of triaging issues that resulted in three broad categories:

1. Issues that are editorial and did not require debate.
2. Current features that required debate and refinement.
3. New features and requirements that needed to be captured.

The second day consisted of communicating open questions and answering them so that the group could divide the work up into different work tracks that could progress independently. The third day consisted of executing on the work tracks and making as much progress as we could.

The group had wanted to produce a document to detail a plan for the W3C Credentials Community Group to summarize discussion or propose one or more PRs that add the feature to the specification

ISSUE TRIAGE

One of the results of the issue triage was the desire to restructure the specification in order to communicate the concepts in the document more cleanly. The following structure was agreed upon by the group as an improvement that would need to be further refined:

- Intro
- A Simple Example
- Terminology
- Core Data Model (simple, short, overview) (~~151~~)
- Decentralised Identifiers (ABNF etc)
- DID Documents (detail on core concepts)
- DID Document Syntax
- DID Methods
- DID Resolvers
- Security Concerns
- Privacy Concerns
- Accessibility

The result of the issue triage follow. Issue numbers with strike-throughs were resolved during the event.

- Update relationship between DID spec and URI spec: https://github.com/w3c-ccg/did-spec/issues/81
- Does the did-spec need to be specific about which parts of the URI RFC it is conformant with? https://github.com/w3c-ccg/did-spec/issues/169
- Intro overhaul
  - ⇨ Improve abstract 115, 112
  - ⇨ Define target audience of the DID spec: https://github.com/w3c-ccg/did-spec/issues/157
  - ⇨ Terminology and explanations, what is a DID?
    - ▢ ~~122~~ (Motivations)
    - ▢ ~~121~~ (Purpose, terminology)
    - ▢ ~~117~~ (entities in Overview)
    - ▢ 156 & 155
    - ▢ ~~123, 124~~ (management of identifiers, Design Goals, terminology)
    - ▢ 130 title - close this once definition of DID and related parts are solidified throughout the rest of the spec
    - ▢ 127
- Remove uses of 'entity' and other fluffy terms when we mean DID Subject:
  - ⇨ ~~125, 145 139 154~~
- Clarify language about keys:
  - ⇨ 147 143 105 166
- Clarify language around ledgers:
  - ⇨ 150 119 149
  - ⇨ ACTION: ledger -> Verifiable Data Registry (with clarification that there are multiple registries, see VC spec)

  - ⇨ Michael>> You mean Verifiable Data Registry (VDR), n'est pas?
- Quick fixes: ~~137~~, ~~144~~, 133, ~~116~~, ~~118~~, 129, ~~140, 141~~
- Clarify language about requirements: ~~120~~

FEATURE REFINEMENT

- MIME Types 1: https://github.com/w3c-ccg/did-spec/issues/84
- MIME Types 2: https://github.com/w3c-ccg/did-spec/issues/82
- ABNF for DID Syntax
  - ⇨ Use case: changing file hosting providers
  - ⇨ Use case: fragments continue to function after moving a resource that supports fragments (DB: and what, precisely, is *the resource*?)
  - ⇨ Use case: change ActivityPub from one provider to another provider
  - ⇨ Use case: I want to advertise a legacy URL (Twitter, Linkedin, etc.)

- ⇨ Use case: Citations
- ⇨ Use case: Timo???
- ⇨ Use case: MS services by type??? Need more details.
- Semantics of DID URL vs DID
- Which URL spec? https://github.com/w3c-ccg/did-spec/issues/163
  - ⇨ If we don't need WHAT WG URL spec features, then cite only the RFC3986.

NEW FEATURES AND REQUIREMENTS

The following new features and requirements were identified at RWoT8

- The need for a place to express keys that are used to digitally sign Verifiable Credentials (e.g. a "credentialIssuer" property)
- The need for a place to express keys that are used to digitally sign legal agreements (e.g. a "legalAgreement" property)

Michael Herman's Key Feedback:

- DID Resolution Technical Use Cases: https://github.com/w3c-ccg/did-resolution/issues/32
- Check that small-e "entities" references are removed or better qualified
- Verifiable Data Registry - DID Resolver Architectures: https://github.com/mwherman2000/indy-arm/blob/master/images/HBB-DID-Resolver-Architecture%20v0.2.png
- DID Data Object References feedback: https://github.com/WebOfTrustInfo/rwot8-barcelona/issues
- DID Namespaces feedback: https://github.com/WebOfTrustInfo/rwot8-barcelona/issues

Editorial work - WIP:

- https://github.com/w3c-ccg/did-spec/commits/rwot8-editorial

---

ADDITIONAL CREDITS

Lead Author: Manu Sporny

Authors: Dan Burnett, Ken Ebert, Amy Guy, Drummond Reed

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 2019 in Europe. If you'd like to be involved or would like to help sponsor the event, email:

> rwot-leadership@googlegroups.com