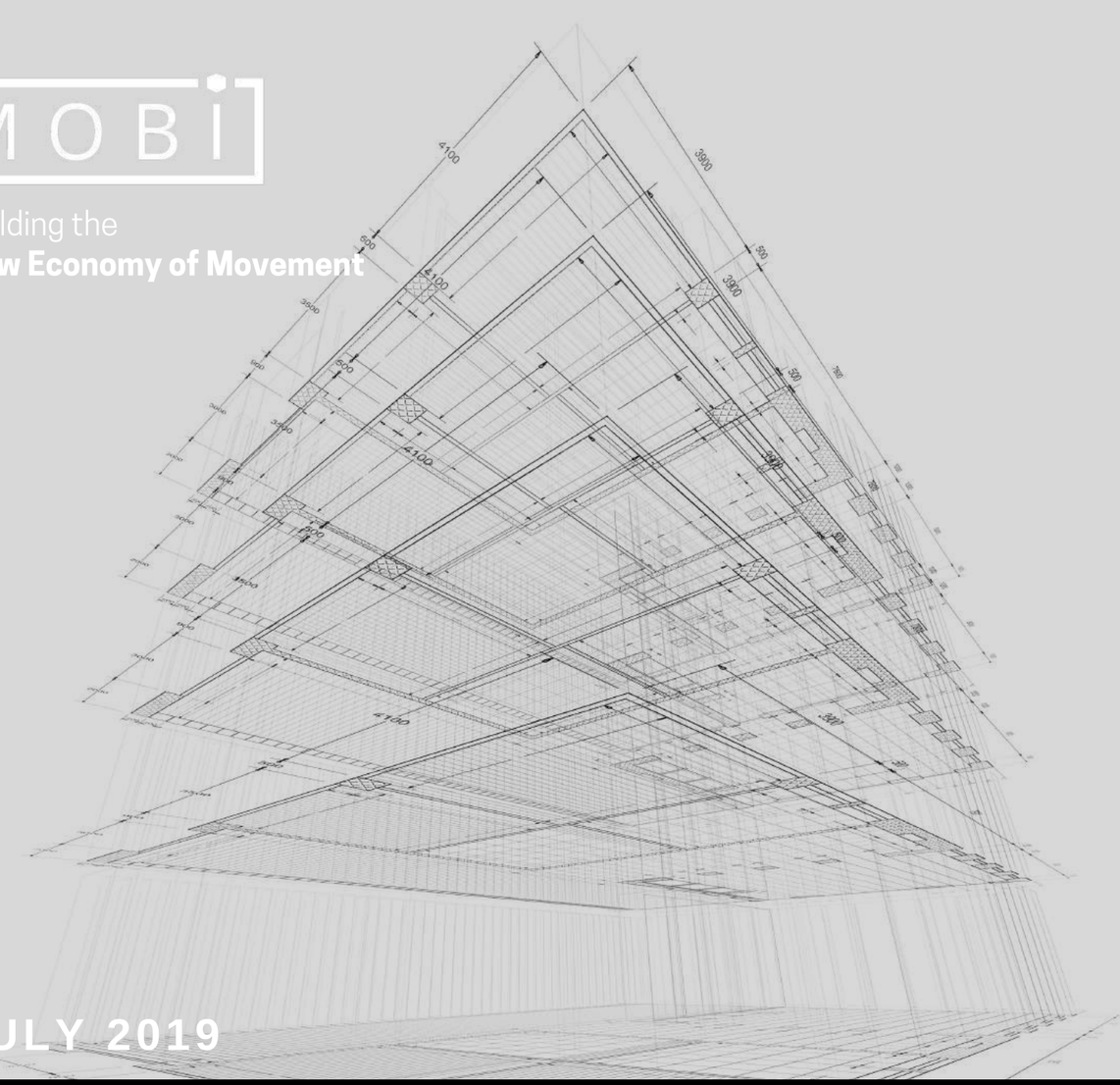
MOBI

Building the
New Economy of Movement



JULY 2019

VEHICLE IDENTITY I
TECHNICAL SPECIFICATIONS

MOBI VID0003/TS/2019
Version 1.0

INTRODUCTION

The Mobility Open Blockchain Initiative Vehicle Identity Working Group is a global, multi-stakeholder team, working to create blockchain- and distributed ledger technologies-based standards for the digital representation of a vehicle — its digital twin. The standards can be used to establish a vehicle's digital existence, manage access control, confirm ownership, and contain key events in the life of a vehicle for the connected mobility networks.

The team members' backgrounds span across the transportation value chain, including vehicle manufacturers, industry service providers, technology companies, governmental and non-governmental entities. This report is based on numerous discussions, workshops, and research. Opinions expressed herein do not necessarily reflect the views of individual members. Sincere thanks are extended to those who contributed their unique insights to this report.

Author

Sid Masih, MOBI

Reviewers

Joe Bannon, KAR Auction Services, Inc.
Todd Gehrke, Luxoft
Alan Gordon, Ford
Sebastien Henot, Groupe Renault
Don Ho, Quantstamp
Max Huang, Cerebri AI
Matthew Jones, IBM
Piyush Manocha, Accenture
Jim Mason, DMX
Richard Meszaros, Accenture
Boris Polania, Honda

VID I Working Group Co-Chairs

Alan Gordon, Ford
Sebastien Henot, Groupe Renault

VID I Working Group Team Members

Deepak Anand, Accenture
George Ayres, IBM
Murad Baig, Netsol
Sebastian Banescu, Quantstamp
Joe Bannon, KAR Auction Services, Inc.
Sean Batir, BMW
Asmita Bhattacharya, Accenture
Jennifer Blair, IBM
Jason Bolduc, RouteOne
Alain Briançon, PhD, Cerebri AI
Peter Busch, Bosch
Michael Casey, GM
Michelle Corson, On the Road Lending
Carlo Cruz, Toyota North America
Carlo Donadio, Accenture
Shyam Duraiswami, IBM
Michael Fischer, Aioi
David Freeman, DLT Labs
Andreas Freund, Consensys
Todd Gehrke, Luxoft
John Gerryts, Oaken Innovations
Muhammed Hamza, Netsol
J Barrington Hines, Accenture
Don Ho, Quantstamp
Max Huang, Cerebri AI
Divyesh Jadav, IBM
Matthew Jones, IBM
Ian Kendall, Volkswagen
Liang Kong, Volkswagen
Audrius Kucinskas, Car Vertical
Chengnian Long, CPChain
Dani Lopez, Accenture
Kanishk Mahajan, Accenture
Piyush Manocha, Accenture
Jim Mason, DMX
Lowell McComb , BMW
Richard Meszaros, Accenture
John Moon, Honda Innovations
Justin Oesterle, RouteOne
Iliana Oris, Accenture
Boris Polania, Honda
Nick Pudar, GM
Dan Rao, Toyota Financial Services
Wes Reid, DMX
Klaus Uwe Roehm, Bosch
Shyam Sundar, Faraday Future
Priya Tabaddor, Cognizant
Sajjad Thaika, Accenture
Christian Umbach, Xapix
Sowmya Varadarajan, IBM
Wanda Wang, Toyota Ins. Mgmt. Solutions
Juergen Wold, Bosch
Jonathan Yu, Toyota Financial Services
Joe Vander Zanden, Consensys
Bin Zhao, CPChain

MOBI Team

Chris Ballinger, Founder + CEO
Tram Vo, Founder + COO
Michael Vo, CTO
Lucy Hakobyan, Head of Program
Rajat Rajbhandari, Working Groups Lead
Robin Pilling, Technical Lead
Annabelle Sbarbatti, Fellow
Kelly Clark, Communications Manager

TABLE OF CONTENTS

01 Executive Summary

05 MOBI VID Technical Specifications Scope

07 Glossary of Terms

11 General System Description

1. System Overview
2. System Security and Identity
3. Key Management and Key Rotation Concepts
4. Addressing and Uniform Resource Identifiers

17 Certificate Data Format

1. Unique Vehicle Identifier (UVI)
2. Vehicle Birth Certificate (VBC)
3. Enum and Time Definitions
4. Entity Certificate
5. Revocation Certificate

22 Certificate API

1. Overview
2. Relationship Verification and Certificate Access
   - 2.1. Common Relationship API
   - 2.2. Role 4 to Role 4,3,2 API
   - 2.3. Role 3 to Role 4
   - 2.4. Role 3 to Creation and/or Revocation of Certificate, 4, 2API
   - 2.5. Role 2 to Self API
   - 2.6. Role 1 to Role 4,3,2

30 Entities

1. Overview
2. Entity Structure

33 System Requirements

1. Overview
2. Distributed Virtual Machine (DVM)

35 Bibliography

Executive Summary

The MOBI VID is the foundation of many new digital mobility services.

This document specifies the first standard for Vehicle Identity (VID), which represents the principal digital foundation of future mobility. The Vehicle Identification Number (VIN), a current vehicle identity system, is insufficient for the digitization of many mobility use-cases such as maintenance history, usage-based insurance, microtransactions, and, ultimately, the existence of a vehicle's digital twin. The complete VID and its immutable data can be employed by connected and future autonomous vehicles, and the IoT infrastructure that will support them. The VID is defined as an authoritative form of identity that can be cryptographically verified.

MOBI VID permits the vehicle to interact and transact directly with infrastructure, other vehicles, people, and entities in the mobility network.

Figure 1 shows a high-level architecture and a potential ecosystem of the distributed ledger network for the connected vehicle. At the center of this network is a vehicle with its associated Vehicle Identity (VID). The vehicle has a securely-stored electronic wallet (data-store) that contains digital certificates for things such as vehicle identification, ownership, warranties, and mileage. At the birth event, the VID consists of the vehicle birth certificate (VBC) and is indexed by a unique vehicle identifier (UVI). The left-hand side of Figure 1 shows (from bottom to top): the owner, lien-holder, the manufacturer (OEM), as well as government entities, e.g., Department of Motor Vehicles (DMV), that may also have wallets with their own digital certificates and unambiguously specify, their relationship with the vehicle. The VID allows the vehicle to identify itself to mobility networks (Figure 1 - Top Center) that provide services such as toll payments, parking, congestion pricing, etc. The VID may also be used to access vehicle data that may be stored on each OEM's network (right side of Figure 1). The advantage compared to current solutions is that the source and provenance of the data can be ensured through distributed ledger technology. The owner of the data may even

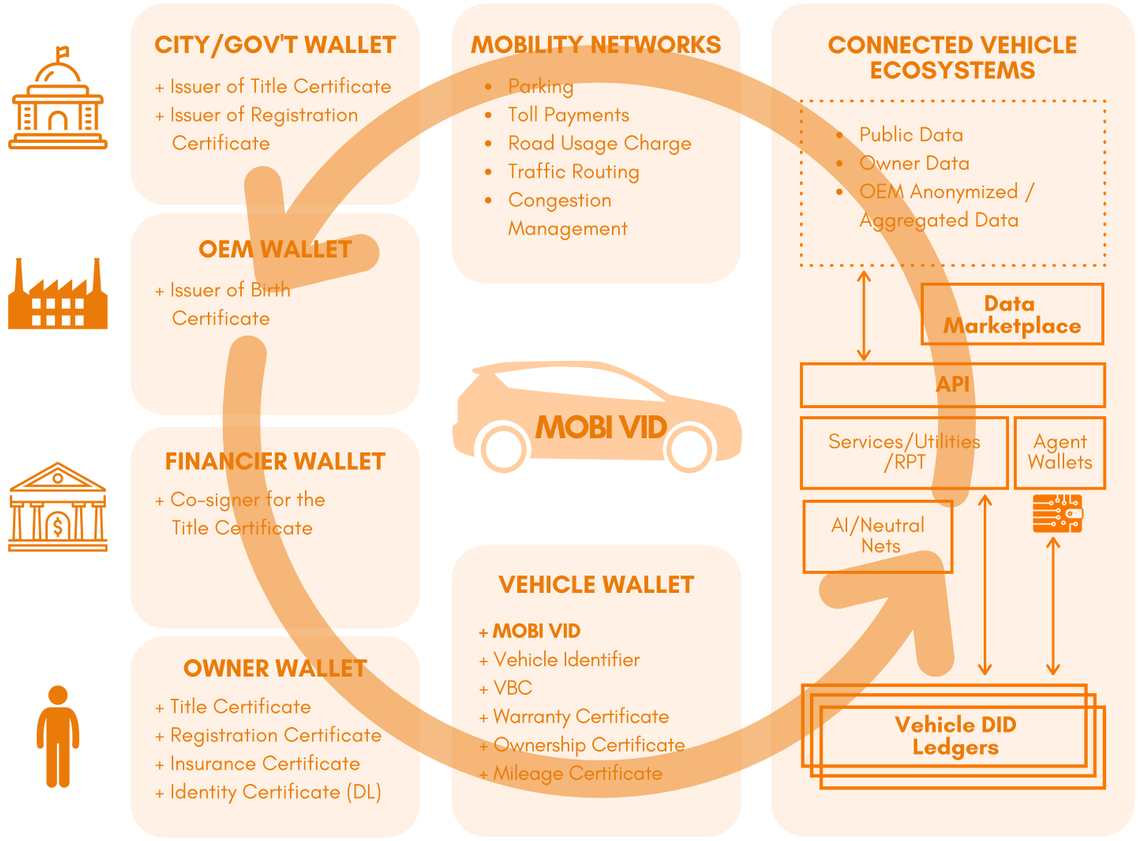


Figure 1 — A DLT-based Connected Vehicle Platform

choose to participate in a data marketplace, monetizing the vehicle data they choose to make available.

In contrast to a centralized architecture where each organization or entity would maintain a different view of the same vehicle, the decentralized architecture from Figure 1 offers an alternative where sharing and regulating vehicle data, as well as vehicle communication with infrastructure, are made possible.

The MOBI VID permits mobility stakeholders to verify identity, credentials, access, and associated metadata without relying on a third party.

This greatly simplifies the complex, trusted, single entity systems. This VID standard is designed to ensure that the data can be securely stored on a decentralized infrastructure with permissioned entity access. This allows mobility providers to verify identities, credentials, and associated metadata, enabling vehicles to be securely connected with infrastructure, consumers, and ultimately, to store digital currency; in essence, enabling secure transactions with the external world.

MOBI VID TECHNICAL SPECIFICATIONS SCOPE

This technical specifications standard focuses only on the digital information available when the vehicle is manufactured, its digital “birth certificate."

This VID technical standard specifies the methods and requirements to implement a vehicle identification system utilizing distributed ledger technology. This VID standard, in this initial release, will focus solely on the vehicle birth event, as depicted in Figure 2. This birth event along with the data structure and all required technical details are described within this document.

This VID technical standard, in its initial release, does not address:

- Complete implementation of the mobility network or ecosystem as shown in Figure 1
- Ownership transfer mechanism.

Future supplements to this technical standard will expand the scope to include the elements above.

Note 1: This VID standard should be consumed and implemented in conjunction with the following documents:DLT-Based Vehicle Identity Business ReviewVID Standard Implementation Specification

Note 2: While certain key methods and requirements are explicitly called out, other implementation-specific elements are left purposefully ambiguous in order to preserve optionality at implementation. One example is the use of Decentralized Identifiers (DIDs) as per the W3C specification vs. federated identity protocols.

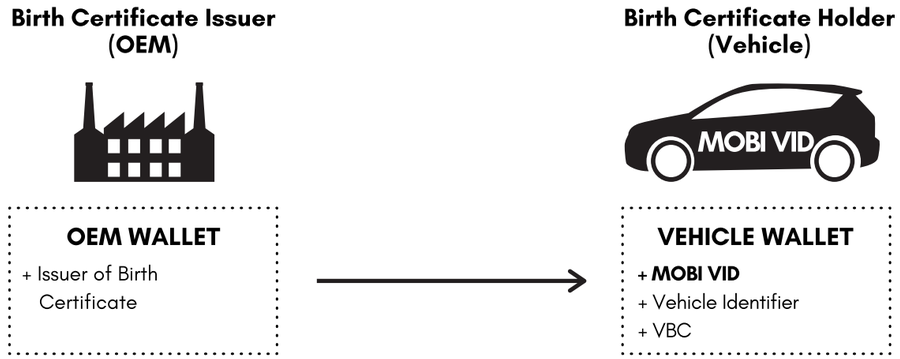
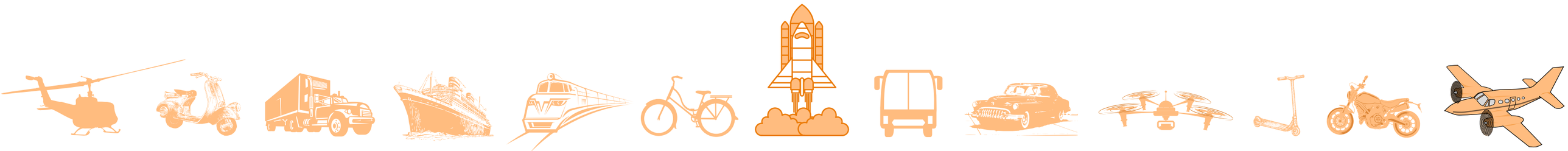


Figure 2 — VID Standard, Initial Release Scope (Vehicle Birth)



Glossary of Terms

Blockchain	A blockchain is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a cryptographically secure tree structure such as a Merkle tree.)
Decentralized Storage System (DSS)	A DSS is a non-static collection of data storage nodes with a global identifier where each node typically consists of a set of object revisions ("commits") which each represent a change (creation, update, or deletion) of a single node object. Each commit is signed, immutable, and content-addressable (typically stored and referenced by its hash). The set of commits representing an object is generally append-only, with certain exceptions made, for example, to allow garbage collection of older commits. Objects are associated with a permissioning structure (read/write) controlled by one or more DSS users. The set of data storage nodes utilizes a replication protocol that is deterministic and eventually consistent.
DID	W3C Decentralized Identifier (DID) represents a globally unique identifier that can be resolved to a DID Document, or de-referenced on a specific distributed ledger network, much like a URL on the Internet. DIDs resolve to DID Documents.
DID Document	A DID Document is a simple text document that describes how to use that specific DID. Each DID Document may contain at least three things: proof purposes, verification methods, and service endpoints. A DID Document can specify that a particular verification method, such as a cryptographic public key or a pseudonymous biometric protocol, can be used to verify a proof that was created for the purpose of authentication. Service endpoints enable trusted interactions with the DID controller.This document specifies a common data model, format, and operations that all DIDs support.
DLT	Distributed Ledger Technology (DLT) is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions. There is no central administrator or centralized data storage. A peer-to-peer network is required as well as consensus algorithms to ensure replication across nodes is undertaken.
DMV	Department of Motor Vehicles (USA). Government agency that administers vehicle registration and driver licensing.
Entity	An entity (e.g. vehicle, corporation, individual, etc.) is a network participant, that interacts with the system by reading and/or writing data. An entity is identified using an entity certificate (see Section 4.4 Entity Certificate) anchored on a DLT.
Entity Identifier	A unique alphanumeric string that uniquely identifies any entity within the system network described in this document.
ESN	The Engine Serial Number (ESN) is a unique number that identifies (within the context of a known manufacturer), an engine block.
Fuel Type	Type of fuel a vehicle uses (diesel, gasoline, fuel cell, electric, etc.).
Governance	Administrator for users, roles and certificate/UVI. On-/Off-boarding of entities is facilitated by the network governance in Section 6.
Identity	Identity is a combination of one or more unique identifiers having meta-data associated with them. Identity meta-data consists of certificates such as verifiable credentials (per the W3C definition) and other non-verifiable data objects

Glossary of Terms

Identity (Cont.)	generated by or on behalf of the unique identifier(s).
ISO	International Organization for Standardization
Network	The system's network is shared equally among network nodes such that no single node (within limits described) may gain an unfair advantage over the overall system.
Node	A node on the system network which is maintained by affiliates. A large number of nodes is meant to provide network availability and prevent collusion attacks.
OEM	An Original Equipment Manufacturer (OEM) is an organization that makes devices from component parts either made internally or sourced from other organizations. In the context of this document, this is synonymous to the vehicle's manufacturer and originator of the vehicle's birth certificate.
Role	Roles regulate creation of and access to data contained within the network.
SSL	(Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.
TLS	The Transport Layer Security protocol is the successor of SSL and aims primarily to provide privacy and data integrity between two or more communicating computer applications.
Trust Anchor	An authoritative entity that validates and qualifies entities on the network specific to the entity's corresponding role.
TSN	The Transmission Serial Number (TSN) is a unique number that
TSN (Cont.)	identifies (within the context of a known manufacturer), a transmission unit.
URI	Uniform Resource Identifiers (URIs) ensure that a named URI will always point to the same resource it was assigned to. Note that this is similar to the addressing system on many blockchain platforms and represents one way to implement a URI.
UVI	A unique vehicle identifier (UVI) is a unique alphanumeric identifier within the system described in this standard. Note that a unique vehicle identifier is not the same concept as a VID.
VBC	A Vehicle Birth Certificate (VBC) is a data structure of strings and integers that records information about a particular vehicle at its creation. See Section 4.2 Vehicle Birth Certificate (VBC) for definition and more details.
VID	A Vehicle Identity (VID) comprises of a UVI and its associated data (VBC being one source of this data).
VIN	A unique code, including a serial number, used by the automotive industry to identify individual motor vehicles, towed vehicles, motorcycles, scooters and mopeds, as defined in ISO 3779 (content and structure).

Full access to this Standard and other MOBI Standards are available to MOBI members.

If you are not part of the MOBI community and would like to become a member, please fill out our "Membership Inquiry Form" at dlt.mobi/join.

Members gain access to standards, working groups, and many other benefits. Join us in building the New Economy of Movement!

If you have any questions regarding the MOBI VID working group, please email vid@dlt.mobi.


dlt.MOBI


@dltMOBI


MOBI


@dltMOBI


vid@dlt.MOBI