MOBI

Building the
New Economy of Movement

March 2021

CONNECTED MOBILITY DATA MARKETPLACE

TECHNICAL SPECIFICATIONS

MOBI CMDM0003/TS/2021
Version 1.0

INTRODUCTION

MOBI (Mobility Open Blockchain Initiative) is a global smart mobility consortium established to accelerate the adoption of blockchain, distributed ledger, and related technologies in the mobility industry through the creation and promotion of standards.The work of preparing standards is carried out through MOBI working groups. Each member of the consortium interested in a subject for which a working group has been established has the right to be represented and participate in that working group. Mobility providers, technology companies, governments, and NGOs, in liaison with MOBI, take part in this work.

The procedures used to develop this document and those intended for its further maintenance are described in the working group charter. In particular, the different approval criteria needed for the different types of MOBI documents should be noted. Approvals of MOBI Steering Committee and Board of Directors are obtained upon the final document release.

Attention is drawn to the possibility that some of the elements of this document may be the subject of intellectual property rights. In accordance with MOBI IPLR policy, a 60 day review period is provided to the MOBI community to disclose any and all IP matters pertaining to this standard. MOBI shall not be held responsible for identifying any or all such rights. Details of any IP rights identified during the development of this document will be contained within the Introduction upon public release of this standard.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement. The working group responsible for this document is the Connected Mobility Data Marketplaces (CMDM) Working Group.

Sincere thanks and appreciation are extended to those who contributed their unique insights to this report.

Authors

Griffin Haskins, MOBI
Rajat Rajbhandari, MOBI

CMDM Working Group Co-Chairs

Roger Berg, DENSO
Michal Filipowski, General Motors

CMDM Working Group Team Members

Loren Adams, Accenture
George Ayres, IBM
Tim Bos, ShareRing
Joshua Cartellone, Accenture
Benjamin Diggles, Constellation Network
Arjun Hassard, NuCypher
Thomas Hulse, Fifth9
Jerry Kim, AMO Labs
Suresh Kumar Sundararaj, Ford
Duy Linh Nguyen, Cognizant
Chalid Mannaa, Ocean Protocol
Jim Mason, DMX
Pramita Mitra, Ford Motor Company
David Noack, Continental
Evripidis Paraskevas, GM
Manan Patel, Ocean Protocol
Derek Pierre, NuCypher
Anthony Salamone, RouteOne
Liu Shaowei, CPChain
Sudha Sriram, Ford
Sukesh Tedla, Swedish Blockchain Association
Wanda Wang, Toyota Insurance Mgmt Solutions (TIMS)
Chris Wood, Filament

MOBI Team

Chris Ballinger, Founder + CEO
Tram Vo, Founder + COO
Rajat Rajbhandari, Working Groups Lead
Robin Piling, Technical Lead
Griffin Haskins, Fellow
Kelly Clark, Communications Manager

TABLE OF CONTENTS

Executive Summary

Blockchain, or distributed ledger technologies, play a significant role in ensuring that data exchange preserves privacy and keeps the data secure.

With advances in short and long range low latency, peer-to-peer communication technologies, data exchanges between vehicles and the roadside infrastructure is an obvious use case. For example, data exchange in a low latency environment is beneficial for vehicles to share braking or lane preference information with other vehicles. Vehicles can receive information from roadside and cloud infrastructure regarding road conditions. Single vehicle drivers, or fleet owners, can monetize by selling a vehicle's performance data to algorithm developers, road condition providers, and more.

MOBI working group members believe that blockchain, or distributed ledger technologies, play a significant role in ensuring that data exchange preserves privacy and keeps the data secure from outside tampering.

Use of blockchain/DLT would not scale without coherent and standardized methods adopted and implemented by the industry stakeholders

MOBI working group members believe that the use of blockchain/DLT would not scale without coherent and standardized methods adopted and implemented by the industry stakeholders who manufacture and service the vehicles. The lack of interoperability in the absence of industry standards becomes problematic at scale.

The Connected Mobility Data Marketplace (CMDM) standards at its core provides blockchain/DLT as a trust layer for V2X data exchange. This standard prescribes reference architecture, data schema, certificates, etc. for vehicles and infrastructure to be able to exchange data by leveraging blockchain/DLT.

MOBI CMDM TECH. SPEC. SCOPE

The CMDM standard specifies high-level system design. The provided CMDM-specific data structures can be utilized throughout the ecosystem.

The CMDM standard specifies the high-level system design, reference architecture, multi-party processes, and the CMDM specific data structures that are utilized throughout the ecosystem. Finally, this document provides guidance to implementation of the CMDM Standard, covering three primary use cases and their process flows.

With the systems for identity, data, and permissioning referenced above, it is possible to outline a variety of use cases. Each use case is broken down into three main categories which are Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2X), and Infrastructure-to-Infrastructure (X2X). In all of these use cases, a connected device, such as a vehicle or a sensor device, has connectivity through the same network, to other devices. These devices are able to authenticate each other's identities, securely share data, and securely record transactions. Their ability to communicate well enables a rich array of functionality.

This document provides reference implementation covering three primary use cases and their process flows broken down into Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2X), and Infrastructure-to-Infrastructure (X2X).

Note that while this standard references certain underlying technologies, it provides no opinion on what specific technologies are to be used. Such details are left as an option at implementation. In particular, the following underlying systems choices are not covered:

- Blockchains/DLT Protocols
  - Ethereum, Bitcoin, Hyperledger, IOTA, Corda etc. Settlement mechanisms (Ethereum, Bitcoin, PayPal, wire transfer, etc.)
- Usage of layer 2 technologies such as side-chains or state channels
- Communication protocols
  - Link layer protocols (WiFi, 5G, etc.)
  - Transport layer and above protocols (REST, gRPC, etc.)
- Trusted key-value store
  - Ethereum, Distributed Hash Tables, DNS, etc.
- Cryptography/Security
  - TLS, SSL, Hashing/MACs, Signatures, etc.
  - Best practices such as recommended key lengths or deprecated protocols
- Bootstrapping trigger
  - Triggers for creating a new entity, certificate, data source, or other should be handled by the implementer, not the standard.
- User interfaces
  - Users are assumed to have Entity IDs (EIDs) and can interact with the system. This standard provides no opinion on how an interface is abstracted away. In many situations, users may interact with a system through an intuitive user interface without knowledge of the underlying system and its technical details.

Glossary of Terms

AC

Access Certificates (ACs) are documents providing the ability for a particular entity to access a particular endpoint in the network's data layer.

Accessor

An entity is an Accessor if it attempts to access a resource's URI endpoint. An Accessor may need to go through security and authentication processes in order to access said endpoint.
A list that specifies entities that are allowed to access a particular resource.

Allow List

A list that specifies entities that are allowed to access a particular resource.

Block List

A list that specifies entities that are not allowed to access a particular resource.

Blockchain

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). Examples of blockchain include Ethereum and Hyperledger.

Data Host

A Data Host is an entity that stores data and is trusted with authenticating requests to access and distribute the data as needed.

Data Owner

The Data Owner is the owner of a particular piece of data. This owner is usually the same entity that generated said data (referred to as the Data Generator).

DBC

The Data Host Bootstrap Certificate (DBC) is a certificate that provides a cryptographic proof that a particular entity (Data Host) is allowed to serve a particular type of data from a specific URI.

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.

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) enables consensus regarding the state of replicated, shared, and synchronized digital data widely spread across multiple sites, countries, and institutions. A peer-to-peer network is required as well as consensus algorithms to ensure replication across all nodes is achieved. Blockchains are the most common and well-known example of DLT. General practical byzantine fault tolerant systems fall under this category as well.

Data Bucket

A logical data abstraction for a persistent data store. Data written to a Data Bucket can be used repeatedly over time.

Glossary of Terms

Data Stream
A logical data abstraction for data buffers. Acts as an ephemeral "stream" of data and persists for a set period of time in the network until it is purged within the online systems. Afterwards, it is moved to nearline data systems, then ultimately sent to offline data systems.

EC
An Entity Certificate (EC) is the certificate that represents all of a particular entity's network-level information and metadata. This includes, but is not limited to, identifiers about who they are, the URIs to delegate trust to, and their public keys. An EC is always paired with a corresponding EID.

EID
An Entity Identifier (EID) is a unique alphanumeric string that uniquely identifies any entity within the system's network described in this document.

Entity
An entity such as a vehicle, corporation, or individual, is a network participant that interacts with the system by reading/writing data, enforcing permissioning, or otherwise supporting the network in a particular manner. An entity is identified using an entity certificate anchored within a distributed ledger.

GPC
Group Permission Change Certificates (GPCs) are certificates signed by a data owner, prompting a Data Host to change the permissioning information of the group.

ISO
International Organization for Standardization.

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 associated with the unique identifier(s).

KV Store
A Key-Value Store (KV Store) is a system that stores (key, value) pairs. The key is used to obtain access to the value in some way. Distributed KV stores are KV stores spread across multiple machines and can effectively maintain a global state table.

KYC
Know Your Customer (KYC) is the process of verifying the identity, risks, and other pertinent information associated with a customer before initiating a business relationship.

Network
A group of entities that all participate in a digital system with a specific goal in mind. For example, a group of entities that participate in a distributed ledger such as Ethereum would be considered a network.

Node
A node is a computer connected to other computers which follows rules and shares information. 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 generally a vehicle manufacturer.

Personally Identifiable Information (PII)
PII is any information that (1) identifies or can be used to identify, contact, or locate the person to whom such information pertains, (2) has identification or contact information of an individual that can be derived, or (3) is or might be directly or indirectly linked to a human being.[ISO/IEC 29100:-1]

RC
Revocation Certificates (RC) revoke AC permissions if the AC has not expired automatically.

Glossary of Terms

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	Administrator for users and roles. On/Off-boarding of entities is facilitated by the network governance in Section 6.
UUID	Universally Unique Identifiers (UUIDs) are unique identifiers that are associated with pieces of digital information and can be used to address and identify each one.
URI	Uniform Resource Identifiers (URIs) ensure that a named URI will always point to the same resource it was assigned to. This example is similar to the addressing system on many blockchain platforms and represents one way to implement a URI.
URL	A specific type of URI referencing web resources.
Tokenized Carbon Credits (TCC)	This refers to a collection of use cases that center around digitizing carbon credits for ease of transfer and auditability. In particular, TCC's are digital, tradable certificates or permits that represent the right to emit a specified amount of greenhouse gases.
Vehicle-to-Grid (V2G)	V2G refers to a collection of use cases that center around the coordinated unidirectional or bidirectional energy exchange between vehicles and the grid.
Peer-to-Peer (P2P)	P2P refers to a collection of use cases focused on direct energy exchange between energy peers (equally privileged entities that transact electricity) in a decentralized manner.

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 CMDM@dlt.mobi.

dlt.MOBI

@dltMOBI

MOBI

@dltMOBI

CMDM@dlt.MOBI