MOBI

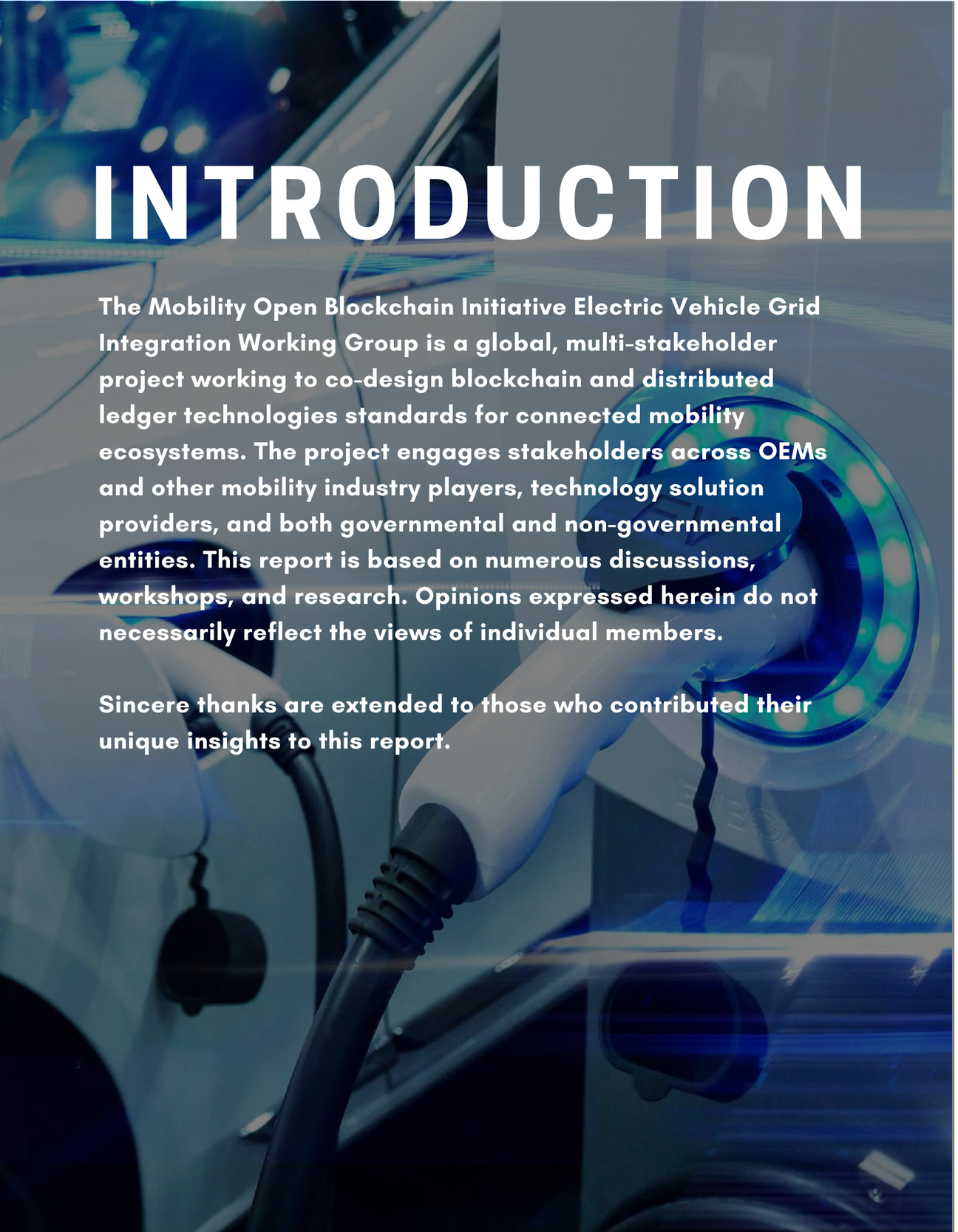
Building the
New Economy of Movement

AUGUST 2020

ELECTRIC VEHICLE GRID INTEGRATION

TECHNICAL SPECIFICATIONS

MOBI EVGI0003/TS/2020
Version 1.0



INTRODUCTION

The Mobility Open Blockchain Initiative Electric Vehicle Grid Integration Working Group is a global, multi-stakeholder project working to co-design blockchain and distributed ledger technologies standards for connected mobility ecosystems. The project engages stakeholders across OEMs and other mobility industry players, technology solution providers, and both 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

Eric Hou, MOBI

Reviewers

Andreas Freund, Consensys
Matthew Yarger, IOTA

EVGI Working Group Co-Chairs

Christian Koebel, Honda
Massimiliano Melis, GM

EVGI Working Group Team Members

Joe Bannon, Kar Auction Services
Amy Fisher, R3
Valentina Gatteschi, Politecnico di Torino
Sebastien Henot, Accenture
Divyesh Jadav, IBM
Richard Kim, Pacific Gas & Electric Co
Shaowei Liu, CP Chain
Krasina Mileva, DOVU
Jaywardhan Sawale, Koinearth
Anne Smith, IOTA Foundation
Carsten Stoecker, Spherity
Priya Tabaddor, Cognizant
Sukesh Kumar Tedla, Swedish Blockchain Asso.
Mohamed Thaika, Accenture
Wayne Tian, CPChain
Kate Tomlinson
CK Umachi, Pacific Gas & Electric Company

MOBI Team

Chris Ballinger, Founder + CEO
Tram Vo, Founder + COO
Michael Vo, CTO
Lucy Hakobyan, Head of Program
Griffin Haskins, Fellow
Matt Shi, Fellow
Kelly Clark, Communications Manager
Eric Hou, Technical Writer

TABLE OF CONTENTS

01 Executive Summary

03 Scope

05 Glossary of Terms

10 System Overview

18 Infrastructure Subsystems

1. Identity Subsystem
2. Data Subsystem
3. Permissioning Subsystem

3.1 Permissioning Subsystem Program Flow

39 Actors and Identity

1. Decentralized Identifiers Framework
2. EIDs 40

2.1. Common Entity Certificate (EC) Structure

2.2. User

2.3. Physical Assets

2.4. Service Providers

2.5. Data Hosts

2.6. Trust Anchor

49 Registering Data

52 Permissioned Access

1. Data Host Bootstrapping Certificate (DBC)
2. Access Session Setup (Unlock)

2.1. Session Request Packet (Unlock Request)

2.2. Session Rejection (Unlock Response)

2.3. Session Acceptance (Unlock Response)

3. Groups
4. Allow Lists

4.1. Access Certificates (ACs)

5. Block Lists

65 EVGI Extensions of Infrastructure

1. EVGI Entity Certificate

1.1. Communication Bootstrapping

69 EVGI Processes

1. Infrastructure Subsystem Processes
2. Misc. Sub Processes

76 EVGI Use Case Processes

1. Vehicle to Grid (V2G)
2. Tokenized Carbon Credits (TCC)
3. Peer-to-Peer (P2P)

96 EVGI-Specific Information

1. Vehicle ID
2. User ID/Entity ID
3. Battery
4. Meter
5. Time Dependent and Smart Energy Tariffs
6. V2G Communication
7. Credit Systems
8. Charger Identity
9. Communication Protocol Standards

107 Appendix A: Certificate Structures

111 Bibliography

Executive Summary

Electric vehicles are expected to dominate global roadways. Charging availability must not only be widespread, but also interoperable in order to reduce range anxiety and enable seamless (e)roaming. Systems for calculating, generating and managing carbon offsets must be scalable. As more EVs are used by households, new ways of storage and even interaction with the grid are made possible, such as selling energy back to the grid, and in the long run peer to peer services. Critically, as the number of EVs increases, the number of charging sessions will, in turn, increase significantly. The charging sessions and grid interactions generate a wide variety of data, which will reach enormous volumes. A disjointed response from utilities, charging infrastructure providers, automakers, and the manufacturers supporting them would produce a series of incompatible systems for managing that data. This lack of interoperability becomes problematic at scale.

To speed adoption of green mobility, standards are needed to ensure interoperability, scalability, and security.

For these systems to be interoperable, there must be standards that govern their structure and interactions. Without such standards, core functionality like identity, permissioning, and data sharing would exist in a walled garden, which necessitates integration costs, increases manual processes, disregards opportunities to support the grid with the help of electrified mobility assets and most importantly, reduces charging availability for electric vehicle drivers. Governments, utilities, and the mobility industry are well aware of the need for such standards, and have invested in their development over time. Standardization organizations like ISO, IEEE, and MOBI are working to produce standards that will ensure the interoperability, scalability, and security of systems that power charging sessions, manage energy exchange, carbon credit generation, and other initiatives.

Blockchain offers several advantages to improve interoperability, reduce frictional costs, and enable new services in electric mobility ecosystems.

For eMobility, the grid, and carbon offset markets, blockchains offer a variety of value propositions. At its core, blockchain provides a trust layer, which is key for eliminating manual processes and third party intermediaries. Ultimately, these blockchain applications result in reduced costs, new revenue opportunities, and new services for players on all sides of the EVGI ecosystem. By providing a secure, immutable, singular source of truth, blockchains enable the orchestration of a secure and trusted marketplace where energy transactions can be facilitated without intermediaries through automated business logic in smart contracts.

MOBI EVGI TECH. SPEC. SCOPE

This EVGI Technical Specification Standard specifies high level design, processes, reference implementation, and system architecture for electric mobility networks.

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

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

- Blockchains/DLT Protocols
  - E.g.: 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
  - E.g.: Link layer protocols (WiFi, 5G, etc.)
  - E.g.: Transport layer and above protocols (REST, gRPC, etc.)
- Trusted key-value store
  - E.g.: Ethereum, Distributed Hash Tables, DNS, etc.
- Cryptography/Security
  - E.g.: TLS, SSL, Hashing/MACs, Signatures, etc.
  - Best practices, such as recommended key lengths or deprecated protocols

The Technical Specification Standard provides no recommendation as to blockchain protocols, digital IDs for vehicles or infrastructure, data sources, and interfaces.

- Bootstrapping trigger
  - Triggers for creating a new entity, certificate, data source, or other should be handled by the implementer, not the standard.
- Interfaces to users
  - E.g.: Users are assumed to have Entity IDs (EIDs) and can interact with the system, but this standard provides no opinion on how the 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 of a resource if it attempts to access the URI endpoint. An Accessor may need to go through security and authentication processes in order to actually access said endpoint.

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 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). Examples include Ethereum and Hyperledger.

Data Host

A Data Host is an entity that stores data and is trusted with properly administering it, authenticating requests to access the data, and distributing the data as needed.

Data Owner

The Data Owner is the owner of a certain piece of data, usually the same as the 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 about the state of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions. A peer-to-peer network is required as well as consensus algorithms to ensure replication across nodes is undertaken. Blockchains are the most well-known example, though 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.

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 in the online systems, thereafter, moved to nearline data systems and ultimately moved to offline data systems.

Glossary of Terms

EC	An Entity Certificate (EC) is the certificate that represents all of a particular entity's network-level information and metadata, including but 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 network described in this document.
Entity	An entity (e.g. vehicle, corporation, individual, etc.) is a network participant that interacts with the system by reading/writing data, enforcing permissioning, or otherwise supporting the network in some way. An entity is identified using an entity certificate anchored on a DLT.
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 information associated with a customer before initiating any business relationship.
Network	A group of entities that all participate in a digital system, generally with a specific goal in mind. Ex: A group of entities that participate in a distributed ledger such as Ethereum.
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 (generally) a vehicle manufacturer.
Personally Identifiable Information (PII)	PII is any information: (1) that identifies or can be used to identify, contact, or locate the person to whom such information pertains, (2) from which identification or contact information of an individual can be derived, or (3) that is or might be directly or indirectly linked to a natural person [ISO/IEC 29100:-1]
RC	Revocation Certificates (RC) revoke AC permissions if the AC has not expired automatically.
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

Glossary of Terms

TLS (Cont.)	and aims primarily to provide privacy and data integrity between two or more communicating computer applications.
Trust Anchor	Administrator for users, 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 them.
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.
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, auditability, etc.. In particular, TCCs 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, either uni- or bi-directional energy exchange between vehicles and the grid.
Peer-to-Peer (P2P)	P2P refers to a collection of use cases that focus on direct energy exchange between energy peers 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 evgi@dlt.mobi.


dlt.MOBI


@dltMOBI


MOBI


@dltMOBI


evgi@dlt.MOBI