JANUARY 2021

VEHICLE IDENTITY II

REFERENCE IMPLEMENTATION ARCHITECTURE

Use Cases

Vehicle Registration and Maintenance

MOBI VID0004/RI/2021
Version 1.0

INTRODUCTION

The Mobility Open Blockchain Initiative Vehicle Identity Working Group is a global and multi-stakeholder project working to co-design blockchain- and distributed ledger technologies-based standards for connected mobility ecosystems. The project engages stakeholders across the mobility value chain, including original equipment manufacturers, mobility 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

Johannes Sedlmeir, FIM Research Center

Reviewers

Alan Gordon, Ford
Johannes Klepsch, BMW
Jonathan Lautenschlager, FIM Research Center
Lukas Mueller, BMW
Robin Pilling, MOBI
Rajat Rajbhandari, MOBI

VID II Working Group Co-Chairs

Alan Gordon, Ford
Johannes Klepsch, BMW

VID II Working Group Team Members

Daniel Bachenheimer, Accenture
Sebastian Banescu, Quantstamp
Joe Bannon, KAR Auction Services
Manuel Bolsinger, BMW
Randy Cole, Ownum
Aaron Fong, Honda
Todd Gehrke, Luxoft
Dante Giancola, Ownum
Sebastien Henot, Accenture
Divyesh Jadav, IBM
Sumita Jonak, USAA
Sanjay Khunger, Ford
Will Maney, USAA
Piyush Manocha, Accenture
Jim Mason, DMX
Lukas Mueller, BMW
Hans Otten, Autodata Solutions
Dean Phillips, AWS
Boris Polania, Honda
Klaus Roehm, Bosch
Angela Ruthenberg, Autodata Solutions
Ryan Tabibian, CarIQ

MOBI Team

Chris Ballinger, Founder + CEO
Tram Vo, Founder + COO
Rajat Rajbhandari, Working Groups Lead
Robin Pilling, Technical Lead
Annabelle Sbarbatti, Fellow
Matt Shi, Fellow
Kelly Clark, Communications Manager

TABLE OF CONTENTS

Executive Summary

MOBI VID standards leverages distributed ledger and blockchain technology to provide foundation for the new economy of movement.

Distributed ledger technologies (DLT), including blockchains, and other cryptographic tools that enable decentralized applications, have become practical in recent years and accelerate and influence the digital transformation of the mobility industry.

The foundation and requirement of all activity is an interoperable vehicle identity. Shared ledger technologies, decentralized identifiers (DIDs), and Verifiable Credentials (VCs) for vehicle identities are crucial technical building blocks for the new mobility and transportation IoT ecosystems of the future. These ecosystems will disrupt the automotive and mobility sectors while changing the way that business is conducted. Mobility Open Blockchain Initiative (MOBI) Vehicle Identity (VID) is a tool that enables these ecosystems. MOBI VID supports dynamically defined, multi-stakeholder, interoperable mobility ecosystems, yielding increased transparency, coordination, control, privacy, and automation between the stakeholders.

MOBI VID acts as a trust anchor to support use cases across the full mobility value chain.

Use cases that depend on a secure digital vehicle identity include fully automatic registration, vehicle payments, supply chain, automotive financing, autonomous vehicle data marketplaces, and many more. This document introduces a technical standard for selected VID-based use cases, describing repeated information flows that serve as building blocks for more complicated use cases. Therefore it is the technical counterpart of the Vehicle Identity Use Cases and Business Requirements (MOBI VID0002/UC/2021) standard.[1]

1. "Vehicle Identity Use Cases and Business Requirements," Standards, MOBI, last modified January 2021, https://dlt.mobi/standards/.

MOBI VID STANDARDS

Vehicle identity is linked to the VIN and persistently maintains physical attributes of a vehicle.

A vehicle's identity, similar to a human's identity, begins at its birth. The issuance of the Vehicle Birth Certificate (VBC) marks the point in a vehicle's life cycle at which its identity comes into existence, and is the first use case on which the MOBI VID Working Group has focused. The vehicle's lifecycle covers the vehicle's complete history from the early stages of production, through usage, and to the destruction of a vehicle. The working group released its first technical standard related to VID focused on the birth of the vehicle in July of 2019.[2] Subsequent standards, such as the one at hand, build on this and complete the lifecycle of VID, exploring use cases such as transfer of ownership, repairs, and end of vehicle life.

The digital VBC extends the VIN to encompass relevant information and vehicle specs known when the vehicle is produced.

A VBC provides stakeholders the opportunity to receive verifiable information about the respective vehicle, allowing for benefits to be extracted by the VBC itself. Examples encompass automated vehicle tax computation based on fuel type, engine size, production year etc., or tax collection by the government from a vehicle owner's wallet. However, this document outlines technical workflows for further use cases that are made possible through a VBC in an open mobility ecosystem. Like the VBC itself, these further use cases build upon technical workflows that leverage the documentation of processes involving blockchains and other decentralized technologies.

2. "Vehicle Identity Standard," Standards, MOBI, last modified July 2019, https://dlt.mobi/wp-content/uploads/2020/04/Preview-MOBI-Vehicle-Identity-Standard-v1.0.pdf.

The VID can be used to prove its birth and existence in the mobility network, manage access control, and track events throughout its life.

In this standard, VID means the digital identity of a vehicle. The VID provides a bridge between the vehicle as a physical asset and a digital ecosystem connecting vehicles, owners, users, and IoT devices. The VID exists because the physical vehicle exists. Because the vehicle has a VID, it can digitally interact with the surrounding digital ecosystem. The physical vehicle and its VID are inextricably linked by the Vehicle Identification Number (VIN) imprinted on the vehicle, as well as several other persistent vehicle attributes such as an engine's serial number. The VID can be used to prove existence, manage access control, confirm product definition and ownership history, and track events during and after the life of a vehicle. As a result, it becomes a key to records for the vehicle's history and usage information.

VID is one key component of an open ecosystem for broader and more efficient collaboration. Stakeholders will be able to

ID to remain relevant and link to its physical attributes, stakeholders involved in producing, maintaining, and registering the vehicle must be involved to update the VID.

interact with the vehicle and verify the validity of its claims by referring to information that is stored on a tamper-evident decentralized ledger or a tamper-evident verifiable credential in the vehicle's or its owner's digital wallet. Access to the information is governed through read and/or write permissions on a DLT or access to an open, Decentralized Public Key Infrastructure (DPKI) that enables the verification of VC (provided that the vehicle's owner reveals it).

Information associated with the VID requires continuous input from multiple stakeholders to remain relevant. Controlled coordination between these stakeholders is enabled by highly standardized and decentralized bi- or multilateral peer-to-peer (P2P) information flow. In many use cases, centralized solutions would not scale or lack a trusted third party that all stakeholders can agree on, so a decentralized architecture leverages significant economic potential.

The VID is digital, immutable, verifiable, tamper resistant and machine readable, making it ideal for V2X transactions.

VID elevates the VIN in the following three areas:

- The VBC describes a subset of the vehicle's overall digital identity. It allows the identification of a vehicle through the individual parts that constitute it. It is immutable through the manufacturer's digital signature. Other systems of record (i.e., ownership, vehicle history, etc.) can relate back to the VBC. Hence the VBC is the immutable anchor for an extensible and verifiable system enabled by VID. It thus constitutes an essential building block for other services.
- The VID is digital, standardized, and tamper-resistant, making it machine-readable and machine-verifiable. This is essential for Vehicle to Vehicle (V2V) or Vehicle to Infrastructure (V2I) communication, as well as future extension to support centralized or decentralized payments. The VID and its associated metadata are not only verifiable but also revocable, reducing the risk of fraud and protecting data integrity.
- VID data is secured and stored in a decentralized infrastructure with permissioned user access. Multiple roles can be created with dedicated read and write access fostering privacy where it is desired, while creating a single source of truth for vehicle attributes. During the lifecycle of a vehicle, these attributes might be subject to change. Authorized entities in the ecosystem can account for this fact by making suitable changes to the VID. Consequently, a dynamic vehicle identity allows for associated business cases which require up-to-date information about time-dependent vehicle attributes.

Glossary of Terms

Agent, Cloud Agent or Software Agent

A software component that is able to control an entity's digital wallet (to an extent that is typically defined by the entity) and the communication to other agents in order to send or obtain information stored in the digital wallet. The agent software can be deployed on an edge device or server that is run by the entity itself or a service provider on behalf of that entity. In the former case, all VID data is stored on the vehicle, giving the vehicle owner maximum control. However, when the vehicle does not have an internet connection or is completely shut off, this means that the vehicle could not communicate with the digital vehicle ecosystem.

In the latter case, the agent running in the cloud alone or additional to the agent on the vehicle can store incoming data and be permanently available. In this case, the agent can be compared with an email hosting provider, which runs an inbox 24/7 while an edge device like a smartphone or computer is not necessarily always available online. When the vehicle (the edge device) comes online again, information can be forwarded from the cloud agent to the edge agent and vice versa. On the other hand, running an agent directly on a vehicle can be very useful in scenarios with purely bilateral communication between entities in the digital vehicle ecosystem where there is no access to the internet or latencies during communication need to be extremely low.

Agents as a service provided by specialized providers could also help with data backup and recovery functionalities, advanced security and availability requirements, and enhanced confidentiality through herd privacy at the agent's endpoint. Running an agent outside the vehicle requires a certain amount of trust of the entity with respect to the cloud provider as in this case the agent is not run on hardware that the entity fully controls. Summarizing, edge agents and cloud agents have

Agent, Cloud Agent or Software Agent (Cont.)

different attributes in regard to performance, control, and availability. Combinations of edge and cloud agents can be utilized to adjust to use-case specific privacy, control, and usability requirements.

For simplicity, we will often use the term "wallet" to describe any application that provides the functionalities of a digital wallet, but also manages permissions and ensures availability for the purpose of the respective use case, which might involve one or multiple agents that act on behalf of the wallet.

Binding

In general, it is difficult to prevent private keys and verifiable credentials from being copied and shared across multiple entities such as vehicles or customers when the vehicle or customer intends to, as long as a digital wallet does not run in a hardware or software enclave. This is similar to passwords, where preventing someone from intentionally revealing them to other entities poses challenges. When a process relies heavily on authentic verifiable presentations (VP), strong confidence may be required that no sharing (or also theft) of a wallet's contents has occurred.

Hence, it is often desirable to establish an additional binding of credentials to the subject that they refer to (in general there is a distinction between the entity that has the credential in their wallet - the holder - and the entity whose attributes and permissions are described by a VC - the subject.) Binding methods include, e.g., using secure hardware that protects a secret key where the associated public key is referenced in a verifiable credential. For example, a registration document might refer to a vehicle as subject but be stored in their owner's wallet, who is then the holder. The requirement of the verifier being convinced that a verifiable presentation really gives information about the subject under consideration is sometimes

Glossary of Terms

Binding (Cont.)

called “authenticity”. Traditionally, binding can often be achieved by multi-factor methods, which can include physical tokens that are hard to copy. Similar approaches can also be used in VPs, which then refer to additional credentials (something the subject knows, is, or has). In the case of a VC that is issued to a vehicle, this could be achieved by including some of the vehicle's characteristic attributes in the VBC, such as VIN, color, type, etc., in the VC. One can then already establish a good binding if the vehicle is physically involved in an interaction (this is similar to “biometric data” in physical credentials issued to humans, e.g., a passport). For example, in a process that involves reading from a physical license plate, a verifier can readily check the vehicle’s biometry (color, manufacturer, ...) and compare it to some claims in attributes referenced in the VBC that is involved in a VP.

In a purely remote interaction, the verifier cannot do so and might therefore expect other evidence that the credential has not been secretly moved to or shared with another vehicle. Economic incentives and so-called “all-or-nothing non-transferability” are essential building blocks for such consistent credential usage with sharing and theft protection. An example for an economic technique is including a private key that can be used to unlock a valuable external secret key, e.g. a bank account, in the VC under consideration. This only works when during a VP, attributes from a VC are only selectively disclosed (e.g., via Zero-Knowledge Proofs). Alternatively, a trusted third party such as the bank could sign the subject another VC that confirms that certain information included (in a blinded way) in other VCs can be used to unlock a certain amount of money at the bank.

All-or-nothing non-transferability, on the other hand, is a technique that binds each credential that is issued to a wallet

Binding (Cont.)

to all other credentials that are already contained in it. One implementation of all-or-nothing non-transferability is the so-called link secret in Hyperledger Ursa/Indy/Aries. It is a random number that is initially created on the subject’s hardware and included in blinded form into all the credentials that are issued to the subject. A verifier can then require that all proofs of attributes that they get in a VP are derived from VC that include the same link secret. In Hyperledger Ursa/Indy/Aries, this can be achieved without the verifier learning the link secret itself.

This protects the subject’s privacy because otherwise, the link secret would serve as a globally unique ID and thus a strong correlator. An example of authenticity and consistency checking using a link secret would be the verifier’s requirement “provide a proof from the VBC that the vehicle’s engine serial number is xyz and that the link secret that is included in the VBC in blinded form is the same as the link secret in two other credentials in your wallet that are issued by one of the issuers from the list ABC”. This method can, therefore, be used to prevent selective credential sharing, making sharing only useful for the recipient when they get all (or at least many) credentials from the sharer.

Constructions like including “biometrics”, putting economic value into VCs, or all-or-nothing non-transferability can help to lower the incentive of the sharer to do so, and in some cases (e.g., when the link secret or a private key that are necessary to create a VP from the VC are contained in an enclave with higher security) also a theft’s utility from stealing VCs or even a wallet. More details on the two latter constructions and the problems associated with credential sharing in general can be found, e.g., in Camenisch and Lysyanskaya 2001. [3]

3. Jan Camenisch and Anna Lysyanskaya, “An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation,” International Conference on the Theory and Applications of Cryptographic Techniques, (2001): 93-118, https://doi.org/10.1007/3-540-44987-6_7.

Glossary of Terms

Binding (Cont.)

However, one must take into account that stronger binding will in general induce additional complexity in processes where credential transfer is necessary or desired. Note that this should not be mistaken with VP, in which the validity of a subset of the claims in a VC are proved (this also emphasizes why selective disclosure or an unlocking mechanism of VC through private keys is necessary, since otherwise, the verifier could copy the VC and use it on their own). For example, credential transfer might be necessary when the owner of a vehicle changes and some of the vehicle-related credentials, e.g., maintenance records, are stored in their owner's digital wallet, or when a user with a mobile wallet wants to switch to a new smartphone.

One possible solution for transferring VCs with a strong binding to a device or owner (e.g., through one of the previously mentioned mechanisms) is to establish a workflow in which the old wallet asks the issuer for revocation and re-issuance to the new holder's wallet. This, of course, requires interaction with the issuer, which in some scenarios is not desirable.

In general, binding is a complex but necessary topic. It is important to note that binding this is not an intrinsic problem of VC and a decentralized or privacy-oriented identity management, but holds for conventional mechanisms such as usernames and passwords as well. Binding is, therefore, rather a consideration that is relevant as more (security sensitive) use cases are made digital, and not a specific complexity of the identity management that is proposed in this standard.

Certificate of Conformity (CoC)

A CoC or Certificate of Conformity is a declaration of conformity with the type approval of the European community. It ensures the free movement of vehicles within the European Union, specifically for those vehicles that are subject to

CoC (Cont.)

homologation or registration. A CoC is a producer's declaration that a vehicle complies with the given approved type. This document contains information about the vehicle and its producer's identification, type approval number, and other technical specifications.

The content of a CoC is defined by the European regulation Amendment IX, Regulation 92/53. Vehicles which do not comply with the EU specification (such as vehicles manufactured for the U.S. or Japanese market) and older vehicles that have not been given the type approval of the EC yet cannot have a valid CoC. Similarly, it is not possible to issue a CoC for converted vehicles; in this case other technical documents need to be referred to when registering a vehicle.

Only cars and motorcycles are eligible for a CoC. The CoC will be used as an example of a registration document that is required by authorities but directly derived from vehicles' and their manufacturer's attributes. The process is comparatively similar in the United States, which also uses a CoC to check, for example, whether a vehicle meets the requirements of the United States Environmental Protection Agency (EPA) for a light-duty vehicle within the scope of the emission standards.

Credential Issuance

Credential issuance describes the process by which an authority ("issuer") creates and transfers ("issues") a VC to a holder in bilateral communication. This requires different communication steps to include and verify associated data. Consequently, credential issuance is frequently preceded by a verifiable presentation in which the prospective holder convinces the issuer of their eligibility.

Glossary of Terms

Credential Issuance (Cont.)

As for the VP, we abstract from the certificate-based and DLT-based perspective. For the certificate-based workflow, the credential typically requires some blinded secrets from the prospective holder to bind the credential to their wallet or other credentials (see also binding). Hence, the issuance process often starts with a credential offer by the issuer in which the issuer states its intention to issue a credential to the prospective holder. Afterward, the prospective holder sends a credential request containing data such as a random number (nonce) and blinded values (commitments) of linking information to the issuer.

The credential request can also include further, verifiable or self-attested information that the holder wants the issuer to include in the new credential. The issuer then creates a VC, which might involve updating a (positive) revocation registry on a distributed ledger or another verifiable data registry (e.g., a trusted third party's server) with broad (preferably public) read access. The issuer can also batch updates resulting from multiple issuance processes and apply them on-chain in a compressed way, e.g., once per day. Finally, the issuer sends the credential to the holder, who stores it (and may immediately want to check its validity, i.e., whether they can create a proof from it).

In the DLT-based case, as illustrated in the description of a VP, the credential consists of or refers to an entry on a blockchain, which is typically not required to include blinded information. Therefore, the issuance process simply consists of a transaction that the issuer performs on-chain. The transaction contains information about the claims that the issuer certifies. The issuer then sends the transaction address as "credential" to the holder, who can immediately store this record and check its

Credential Issuance (Cont.)

validity. Note that in this case, we somewhat abuse the term VC because according to the W3C VC standard, VCs have a very specific form. It is, however, a reasonable assumption that the proof methods for W3C VCs could be generalized to include references to entries in a verifiable data registry in general or a DLT in particular, which would then justify the choice of terminology used in this technical standard.

Decentralized Identifier (DID)

The W3C DID Standard describes a "new type of identifier that enables verifiable, decentralized digital identity. A DID identifies any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) that the controller of the DID decides that it identifies. In contrast to typical, federated identifiers, DIDs can be decoupled from centralized registries, identity providers, and certificate authorities. Specifically, while centralized or decentralized ledgers might be used to help enable the discovery of information related to a DID, the design of the DID standard enables the controller of a DID to prove control over it without requiring permission from any other party.

DIDs are URLs that associate a DID subject with a DID document allowing trustable interactions associated with that subject. Each DID document can express cryptographic material, verification methods, or service endpoints, which provide a set of mechanisms enabling a DID controller to prove control of the DID. Service endpoints enable trusted interactions associated with the DID subject. A DID document might contain semantics about the subject that it identifies. A DID document might contain the DID subject itself." A specific vehicle's DID in the context of this and previous MOBI standards is the UVI.

4. Drumond Reed, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, and Markus Sabadello, "Decentralized Identifiers (DIDs) v1.0," last modified December 20, 2020, https://www.w3.org/TR/did-core/.
5. Ibid.

Glossary of Terms

DID (Cont.)

A DID's and its associated DID document's main purpose is to provide a standardized way to establish end-to-end encrypted and, thus, repudiable and secure connections between identities, with an identifier that outlasts key rotations, and changes of domain or controllership policies. It can be anchored on a public, verifiable data registry such as a DLT for discoverability reasons and collecting reputation, but the default for vehicle owners and vehicles should be so-called pairwise or peer-DIDs that are only stored locally on their controllers' devices for privacy reasons (see also section 2). In particular, DIDs should not be regarded as the only means to establish trust in a bilateral interaction - establishing trust through the presentation of verifiable data (attributes) is the main purpose of VPs using VCs, which relies on establishing a secure communication channel in the first place.

Vehicle Registration Authority (VRA)

Vehicle registration authorities (e.g., Department of Motor Vehicles in the US) typically are government agencies that administers vehicle registration and driver licensing.

Digital Wallet

A software application that runs, for example, on a user's mobile phone, a laptop, server, or on a vehicle's hardware. A digital wallet contains private keys that can be used to encrypt messages, prove control over a DID, permissions or property on a distributed ledger, or eligibility to use a VC. A digital wallet typically also contains VCs. If binding is relevant, a digital wallet can also contain a link secret or similar constructions that should never leave the wallet in unblinded form. Frequently, digital wallets also contain information about (private) peer-to-peer connections with and references of other entities in the digital identity ecosystem.

In the following technical standard, we assume that a vehicle is not yet capable of deciding fully autonomously when to use its

Digital Wallet (Cont.)

capabilities. We have the following intermediate model in mind: the vehicle runs a reactive wallet (or agent) that can be authorized by its owner or user to respond to specific requests, such as digitally signing a message using its private keys, reading from a ledger or another public data registry, providing sensor information or proving attributes about itself using its VCs in a VP on request. Entitled entities, such as manufacturers, owners or users, can have specific and customizable permissions to limit access to these functionalities to selected entities in the digital VID ecosystem.

In other words, the permissions to access the wallet and decisions when to trigger the execution of specific methods will not be managed by the wallet or the vehicle fully autonomously but according to vehicle manufacturer-, owner- or user-defined policies. A wallet that is not exclusively reactive would then only mean that certain communication steps - those that trigger an event - can be removed, or that the digital wallet manages read and write permissions autonomously, simplifying the process further. Access to a digital wallet can be provided via API endpoints and providing permissions to the wallet, e.g, through a VC that can be created when managing permissions through an interface for the vehicle manufacturer, owner, or user.

This hypothesis implies that the triggers for calling the wallet's functionalities will be activated by other entities in the digital VID ecosystem, such as the vehicle manufacturer, the vehicle owner or a service provider that interacts with the vehicle owner or vehicle. Methods that a vehicle owner can call on the wallet's endpoint should be limited to increase security and to prevent some undesirable side-effects of privacy and control in specific scenarios, such as undesirable selective disclosure of maintenance records (see also section 4.3.3).

Glossary of Terms

Digital Wallet (Cont.)

A vehicle's wallet could run on:

- A vehicle owner's smartphone: The digital wallet can be unlocked through a PIN, password, fingerprint scan, face scan, or other biometric data. In this case, the vehicle owner would act as a custodian for the vehicle's keys (and further data that is stored inside the wallet as described in above).
- A vehicle's hardware, where again it can be unlocked via a username/password combination or a VP with the vehicle as verifier. Access policies can be regarded the vehicle wallet's "authorization list" in this case.
- An OEMs server: This is similar to the previous case where the wallet runs on the vehicle's hardware. However, changes might also be triggered by a customer's account at the OEM (which is not necessarily interoperable, of course). In this case, the OEM would act as a custodian for the vehicle's keys.

It is unlikely that the majority of vehicles will provide the previously described capabilities in a digital wallet that runs on the vehicle soon. An agent that runs on a cloud instance controlled by the vehicle manufacturer or vehicle owner is more realistic in the medium term from a resources requirement perspective (and regarding vehicles that are already on the road and where retrofitting is difficult).

For a discussion of the tradeoffs regarding control, performance and availability associated with the location of a wallet and its agent, see also the discussion of agents). Since overall, the location of the digital wallet does not considerably change the process from a conceptual perspective, and distinguishing between all scenarios that one can imagine in the real world is beyond the scope of the standard, we will not further elaborate on this in detail in the specification at hand.

Distributed Ledger Technology (DLT)

DLT describes physically distributed and logically decentralized shared databases. Key components of DLT are a peer-to-peer network where all data is replicated across multiple peers, and an associated consensus protocol operated by specific nodes to ensure the validity of state modifications ("transactions") and to synchronize the shared state. Distributed Ledger Technology (DLT) is, therefore, 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.

Authentication of transactions on DLT makes use of public key cryptography, which allows participation in consensus mechanism and interaction with the network and authorizes transactions to be added to the ledger. DLTs are regarded as resistant against single points of failure and malicious behavior of a small subset of participating nodes. These capabilities make DLTs highly available as a decentralized digital infrastructure. However, they also exhibit drawbacks in terms of scalability and privacy/confidentiality due to the redundant storage and execution of transactions.

Among many varieties of DLT, blockchain is the most widely used. The key characteristic of blockchain architectures is batching transactions into blocks, with each block of data containing the hash value of the previous block. The blocks therefore form a chain to establish a tamper-resistant historical record of transactions. Examples of blockchains include Bitcoin, Ethereum, Fabric, Indy, and Quorum.

Glossary of Terms

Entity

An entity (e.g. vehicle, corporation, individual) is a network participant that interacts with the system by communicating, reading and/or writing data to/from another entity. An entity is identified using an entity DID. This DID (and the associated DID document) can either be anchored on a DLT if it is of public interest (e.g., due to reputation and credential issuance activities, see also section 4.4.1) or kept private. In the latter case, for being trusted without a trust relationship with the entity, a DID controller must give a VP by means of VCs issued by another trusted third party, such as a Certificate Authority or another institution with a reputation (that can be anchored on a DLT). An entity often has one or multiple of the roles of an issuer, a holder, or a verifier.

Original Equipment Manufacturer (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.

Proof Creation

In a VP, based on a proof request, the prover searches references (VCs or addresses of DLT transactions/smart contracts) in their digital wallet that allow them to present their attributes or permissions, together with a proof of their validity. As stated, this proof might be derived from one or several VCs in the prover's digital wallet, the correctness of which can be verified based on the issuer's signature on it, or the address of a DLT smart contract or transaction that testifies the claim.

Proof Request

In a VP, the verifier typically tells the prover at the start of the interaction which information they need, and what kind of proof they expect (a positive list of issuers that the verifier trusts, restrictions regarding the timeliness of a proof of non-revocation, ...). A proof request is then followed by the creation and transmission of a suitable proof by the holder. The proof verification by the verifier then completes the VP.

Proof Request (Cont.)

Proof Transmission

In a VP, after creating the proof, the holder sends it as a message to the verifier. The proof might be a Zero-Knowledge Proof derived via selective disclosure from one or several VCs, or a plaintext presentation of a VC that the holder has in their wallet, or a DLT transaction or smart contract address on a distributed ledger that the verifier can read and trust.

Proof Verification

In a VP, the verifier checks the correctness of the proof based on the requirements that they previously stated in the proof request and the proof that the prover sends. This can involve one or multiple read operations on a DLT or another verifiable data registry. In the VC-based case, downloading the issuer's public signing key, a schema, a credential definition and a revocation registry state (if they are not up to date or not cached) could be required. In the DLT case, the verifier must check whether the original transaction for credential issuance is still valid on the DLT. Hence, by construction, the verifier can verify the proof without the need for interaction with the issuer. Typically, the proof can also be verified by the verifier without requiring further interaction, i.e., the exchange of further messages, with the prover.

Registration Certificate / Vehicle Registration Document - VRD (Part I)

The registration certificate or vehicle registration document gives the driver the official permission to participate in road traffic with the vehicle. The document contains information about the owner and the vehicle, such as the owner's name, the date of its manufacture, and the engine and chassis numbers. The registration certificate must always be carried by the driver and must be available at a traffic stop. In this way, the vehicle can be identified. A registration certificate is required for all vehicles subject to registration.

Glossary of Terms

Registration Certificate / Vehicle Title Document - VTD (Part II)

The vehicle owner is referenced in the registration certificate part II (Vehicle Title Document). In some legislations, it also indicates ownership of the vehicle. If the vehicle is financed (credit/leasing), the VTD typically remains with the lender.

Revocation

When entities use VCs or entries of a DLT to prove their claims in a VP, there must be a means to disable their capability to create proofs from this when the reason why the issuance had happened ceases to be legitimate. For example, a driver's license should be revoked when its holder was caught driving drunk. Similarly, it might be useful to revoke some registration or other documents of vehicles that are reported stolen. Revocation is generally possible by two different methods:

- If the credential issuance consisted of conducting a transaction on a DLT, it must be possible to operate a transaction that updates the status of this transaction (or a respective state controlled by a smart contract) to "invalid."
- Since VCs are digital documents in a wallet under the vehicle's or vehicle owner's control (for a detailed discussion of this topic also see section 4.5.), the issuer cannot force the credential holder to delete it, or check this when the vehicle owner claims to have done so. Consequently, revocation lists need to be used, which display information that issuers announce publicly to allow validity checks of previously issued credentials. In this case, a valid VP should convince the verifier that the underlying VCs have not been revoked. This can be ensured by one of the following ways:
  - Private revocation lists: If there is a trustworthy issuer of credentials which exposes an API that can be queried for the validity of certain credentials, this can be regarded an (interactive) private revocation list. In this case, however, every VP involving a VC with such a revocation list will involve an interaction of the verifier with the issuer, which can be considered problematic from an availability and privacy perspective.
  - Public revocation lists:
    - Non-privacy preserving revocation: a public revocation list might be published on a public verifiable data registry, such as a distributed ledger. However, the naive approach of listing inactive credentials in plain text or listing all the active credentials can raise serious privacy and confidentiality issues.
    - Privacy preserving revocation are typically cryptographic accumulators ("compressed cryptographic gibberish") in a public verifiable data registry, maintained by the issuer, which is often the only entity with write access to a revocation registry that refers to credentials that they issue. Based on such an accumulator, a proof of non-revocation can be created by the VC holder without revealing any information about the VC except it's non revoked state. Thus, no such thing as a unique serial number or the value of a signature must be revealed. This avoids the danger of correlation from repeated proofs of non-revocation involving the same VC.

Revocation (Cont.)

Unique Vehicle Identifier (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. The UVI is a special case of a DID for a vehicle. It is a unique alphanumeric string that is verifiably mapped to a specific vehicle through its associated VBC. It is a minimum

Glossary of Terms

UVI (Cont.)

representation of that vehicle's digital identity. It can be used to establish existence, enable access control, confirm product specifications, etc. If we abstract the view of the system to a key-value store, then the UVI is the key. It may hence also be used as a lookup key (identifier) to access vehicle data that may be stored on each OEM's network.

Vehicle Birth Certificate (VBC)

A Vehicle Birth Certificate (VBC) is a data structure of strings and integers that records information about a particular vehicle at its creation. A digital vehicle ID's life cycle begins with a birth certificate. The birth certificate is a subset of the vehicle's overall digital identity (VID) that identifies a vehicle along with individual parts that constitute it. It is described in more detail in the VID I Standard.[6] It is a VC that contains attributes such as the VIN, serial numbers of core components, color, fuel type, etc.

All vehicle's attributes that rarely change during the lifetime of a vehicle are confirmed by the OEM in the VBC. It can therefore be used to prove claims about the vehicle. The VIN (and also the assembly of the vehicle, which corresponds to biometric data for people) establish a tight bond between the physical and digital identity of the vehicle (yet, crypto chips are not included in the major components, but this might be an option in the future).

Vehicle Identity (VID)

A Vehicle Identity comprises a UVI and its associated data and particularly VCs, the VBC being one source of this data). It is hence an authoritative form of identity that can be cryptographically verified and allows the vehicle to identify itself in mobility networks in general and the digital VID ecosystem in particular.

6. "Vehicle Identity Standard," Standards, MOBI, last modified July 2019, https://dlt.mobi/wp-content/uploads/2020/04/Preview-MOBI-Vehicle-Identity-Standard-v1.0.pdf.

Vehicle Identification Number (VIN)

The Vehicle Identification Number (VIN) is a unique 17 character code (digits and capital letters), including a serial number, that acts as an identifier for a specific vehicle. The VIN serves as a fingerprint, as no two vehicles in operation have the same VIN. It is used by the automotive industry to identify individual motor vehicles, towed vehicles, motorcycles, scooters and mopeds, as defined in ISO 3779 (content and structure).

Verifiable Credential (VC)

The W3C VC Standard defines VC as "a part of our daily lives; driver's licenses are used to assert that we are capable of operating a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable us to travel between countries. This specification provides a mechanism to express these sorts of credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable."[7] In this document, VCs will be abundant, e.g., the VBC, (verifiable) registration documents, service records, etc.

Verifiable Data Registries

This is an abstraction of databases whose content is considered reliable and trustworthy by a large subset of stakeholders. A verifiable data registry might be a GitHub repository if GitHub is considered reliable and trustworthy by the involved stakeholders, or an Interplanetary File System (IPFS). Typically, a verifiable data registry will require strong integrity guarantees and timestamps, so blockchains or other distributed ledgers are an exceptional example of verifiable data registries.

7. Manu Sporny, Dave Longley, David Chadwick, "Verifiable Credentials Data Model 1.0," last modified November 19, 2019, https://www.w3.org/TR/vc-data-model/.

Glossary of Terms

Verifiable Presentation (VP)

In many interactions, it is necessary for an entity (the prover) to convince the counterparty (the verifier) of the validity of statements regarding some of their attributes, so-called claims. Sometimes, trust with respect to the counterparty is sufficient to be convinced. However, there are many situations, in particular when there is only little or no trust between the parties, that a proof of the validity of the claims needs to be given. For example, in an application process, one can claim to have a diploma with distinction, or in a traffic control, one can claim to have a driver's license, but the counterparty wants to have a confirmation by the issuer of the related documents, i.e., a university or a federal government.

In the analog world, a VP would consist of showing evidence in the form of documents (signed diploma) or plastic cards (containing, e.g., watermarks or crypto-chips) that are difficult to duplicate and manipulate. In the analog word, therefore, also some secure or tamper proof mechanism is required. There are different ways to achieve this - we will focus on two slightly different approaches, one referring to data that is stored on a verifiable data registry (such as a DLT), and the other based on VCs, which can be regarded as a digital analog of the paper-based documents or the plastic cards. A verifiable presentation consists of the following sequential steps: proof request, proof creation, proof transmission, and proof verification.

Vehicle Registration Workflow (VRW)

The process of (digitally) registering a vehicle through interaction of a vehicle (and typically other stakeholders such as the vehicle dealer or owner) with an authority.

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 MOBI VID working group, please email vid@dlt.mobi.

dlt.MOBI

@dltMOBI

MOBI

@dltMOBI

vid@dlt.MOBI