Securing Emission Data of Smart Vehicles with Blockchain and Self-Sovereign Identities

Sofia Terzi
Centre for Research & Technology Hellas/ITI
Aristotle University of Thessaloniki
Thessaloniki, Greece
sterzi@iti.gr,
sofiaterzi@csd.auth.gr

Charalampos Savvaidis
Centre for Research & Technology Hellas/ITI
Thessaloniki, Greece
chsavvaidis@iti.gr

Konstantinos Votis
Centre for Research & Technology Hellas/ITI
Visiting Associate Professor, University of Nicosia
Thessaloniki, Greece
kvotis@iti.gr

Dimitrios Tzovaras
Centre for Research & Technology Hellas/ITI
Thessaloniki, Greece
dimitrios.tzovaras@iti.gr

Ioannis Stamelos
Aristotle University of Thessaloniki
Thessaloniki, Greece
stamelos@csd.auth.gr

***Abstract*— Modern Internet of Things (IoT) networks including vehicle networks face an increased demand for security and access control with respect to privacy for sensitive data. Data manipulation and tampering of emissions values due to the economic incentives and environmental and health issues require a tamper-proof solution with the use of blockchain (BC) where the integrity of data is ensured. In this paper, we propose the integration of a public permissioned Self-Sovereign Identities (SSI) framework with a permissioned consortium BC based architecture. This innovatively supports the decentralization of the authentication and authorization processes to overcome the single point of failure problems and the use of SSI to assign identities to IoT devices. Additionally, it gives full control to the holders for their identities, whether they are humans, organizations or smart vehicles. With the practice of advanced zero-knowledge proof (ZKP) cryptographic techniques, the exposure of sensitive and private information is minimized to the absolute necessary and gains in performance and scalability are achieved. Furthermore, the way this ecosystem of technologies is combined guarantees a trusted environment for enabling and automating vehicles' emissions certification according to emissions standards and regulations. Detailed descriptions of the processes required to integrate Hyperledger Indy (HLI) SSIs to authenticate and authorize entities on a Hyperledger Fabric (HLF) network are being quoted.**

Keywords*— *Self-Sovereign Identities, blockchain, zero-knowledge proofs, emissions, smart vehicles

Today, smart cars are equipped with multiple sensors and communication units in order to support the modern needs of connected vehicles, leading to what we call Internet of Vehicles (IoV) [1]. Along with the gains of this interconnected network of intelligent systems which include interchange of information for geolocation services, remote diagnostics, traffic data and human-computer interaction, security risks emerge as well in authentication, authorization and trust relationships [2]. Thus, smart vehicles are considered as cyber-physical systems, prone to attacks, exposed to threats, vulnerable to exploitation of weaknesses of such systems through cyber and physical attacks [3].

These attacks can cause social, economic and safety concerns to OEMs and car owners or even be the reason for life threatening situations. This was proved when attackers hacked a Jeep on the highway taking control of the ventilation, the in-seat climate control, the radio, the windshield wipers and finally the transmission system forcing the vehicle to immobilize in the middle of the road [4] resulting to a life threatening situation in real driving conditions. Additional to safety and security concerns, the environmental negative impact can be considered as high. The recently cheated emission tests by some OEMs [5] revealed that when there is an economic motivation nobody can be trusted.

Another frequent fraud tactic in the odometer tampering of second-hand cars, which as stated by European Parliament Research Service (EPRS) is hard to track and trace [6]. This results in hidden costs for maintenance to the buyers and in intercepted monetary values for the resellers between the odometer tampered and non-tampered cars [7]. In this context, in order to prevent the aforementioned tampering attempts, the European Union Agency for Cybersecurity (ENISA) suggests good technical practices regarding smart cars security, encouraging the use of cryptography, access control, self-protection and cyber resilience [8]. As attacks can be cyber or physical, prevention of such actions includes Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) [8], both at vehicle and infrastructure levels as well as pairs of digital keys and certificates used for authentication and end-to-end secure data exchange.

Distributed ledger Technology (DLT) technology, which takes advantage of cryptographic techniques, can be an answer to the required level of security concerning smart vehicles. Therefore, researchers have proposed frameworks and ecosystems using BCs as a solution for authentication, authorization, security, decentralization, tamper-proof records, firmware updates, traceability and transparency in

978-0-7381-0495-9/20/$31.00 ©2020 IEEE
DOI 10.1109/Blockchain50366.2020.00067

many smart cars and IoV related use cases [9][10][11][12]. Although some of them introduce innovative solutions for identity and access management on vehicles, none of them natively supports the use of SSI for decentralizing the authentication and authorization system in combination with zero-knowledge proofs (ZKP) for proving vehicle's verifiable claims regarding its sensor data.

The contributions of this paper are the following:

- Architecture design and implementation of a SSI and BC based access management system for smart vehicle's IoT and definitions of its actors and interactions between them
- Design and implementation of a decentralized identity management system for requesting, issuing and verifying identity verifiable credentials enabling data minimization
- Design and implementation of a decentralized system for requesting, issuing and verifying emissions verifiable credentials enabling minimum disclosure of raw data.

I. PRELIMINARIES

A. Blockchain for in Internet of Vehicles

Vehicle Networks and IoT networks in general are mostly non-trusted environments and the exchange of messages among the participants, either it is between cars or between cars and OEMs and service providers, can be relatively easy intercepted and tampered with unpredictable consequences [13]. Moreover, to establish a secure communication before transmitting to and accessing the various endpoints, despite if they are located in the vehicle or it is a backend server, proper authentication and authorization must take place [14]. BC technology has these features that along with SSIs can secure the messages exchanged between the participants with digital signatures and cryptographic techniques, provide a secure tamper-proof storage for transactions' data and guarantee the authentication and authorization processes follow high security standards for volatile IoT networks [15][16]. By using permissioned BCs and smart contracts for implementing the business logic the interactions needed to perform communication for sending and receiving data can be fully automated [17] without hindering performance and scalability.

B. Self-Sovereign Identities

Identity is a central aspect of life both in the real and online world and can be defined as the representation of an entity [18]. The rapid progress of technology has led to a wealth of digital identities as well as to the urgent need to manage them. So far, various approaches for digital identities and their management have been proposed [19][20][21]. However, they all share common drawbacks, the identity and access management is controlled by a central authority, thus a single point of failure is introduced. This further leads to performance issues and the violation of the privacy of entities in case the central database is compromised.

The SSIs can be used in order to eliminate the dependency on central authorities and enhance the privacy of the holders to which the identities belong [22]. The SSI approach focuses on security, controllability and portability of an identity, providing entities with the ability to fully control and manage their own identities and subsequently their relationships [23] without depending on a central authority, present it wherever they choose to share their personal information and disclose as many details as they wish. By combining SSI and BC technology a transparent, append-only and decentralized verifiable data registry maintaining the identities for untrusted entities is structured [24].

C. Decentralized Identifiers

Identifiers are a composition of a special category attributes that offer interrelation with a specific identity in a specific context [25]. Decentralized Identifiers (DIDs) [26] are a new type of unique global identifiers that are used in SSI solutions, they are uniquely resolved and fully owned by the entity that creates them. The association of a DID to an entity is cryptographically verifiable by using pairs of public and private keys. In addition, a DID may contain verification methods and service endpoints that are also linked with the DID owner [27]. There are two types of DIDs, public and private or pairwise DIDs. Public DIDs belong to entities which should be publicly queried and identified. For this reason, they are stored in a verifiable public data registry, making them visible to everyone. On the other hand, pairwise DIDs imply a private relationship among two or more entities and are used to establish secure trusted connections with each other and are stored locally and not in a public verifiable data registry. Their purpose is to provide a secure trusted communication channel for data exchange and minimize the time to start establish it while improving the privacy of the participants [27][28]. Each one of these pairwise secure communication channels can be terminated in case one entity decides it unilaterally.

D. Verifiable Credentials and Claims

Verifiable Credentials (VC) [29] constitute the machine-readable digital version of paper credentials, which are cryptographically verifiable and tamper-proof. An issuer issues a VC to a prover. The latter can present proof of the VC to multiple verifiers, as many times as necessary. The metadata of the VC include information for identifying the issuer which can be cryptographically verified by anyone presented with this VC, in order to decide whether they trust the issuer. There is no need for the issuer to mediate the presentation and verification of the VC, as this along with the verifiable data registry provide the cryptographic material for the authenticity of the claims it contains [30]. Moreover, as the VC supports revocation actions, thus an issuers can revoke them when appropriate [31].

E. Zero Knowledge Proof

Proof of knowledge is a major topic in cryptography. ZKP refers to proof that does not reveal anything more than the validity of claims [32]. Thus, by using ZKP, a prover can prove the truthfulness or possession of a claim to a verifier without conveying any further information about the claim itself or revealing the actual claim [33][34]. VCs can adopt

ZKP thus providing data minimization and privacy enhancement as provers can present proof with minimal disclosure of sensitive and personal data to the verifiers. [29].

F. Hyperledger Indy

HLI [35] is a public, permissioned BC infrastructure, that is purpose-built for identities, supporting the SSI concepts. As it is primarily focused on identity, it does not provide support for exchanging assets, nor any kind of smart contract. HLI nodes participate in the ordering and validation of transactions relevant to identities and VCs by running the Plenum [35] consensus protocol, which constitutes an implementation of the Redundant Byzantine Fault Tolerance (RBFT) protocol [36]. HLI nodes pool is an interconnected network of nodes that maintain the same state of the ledger by signing every communication using elliptic curve cryptography.

G. Hyperledger Fabric

HLF [37] is a private and permissioned Distributed Ledger with a modular design. HLF provides a completely new approach to transaction flow called the execute-order-validate architecture where transactions are first executed and their outputs are verified, then they are ordered into blocks using a consensus algorithm, validated and added to the ledger [38][39]. As a permissioned network, every participant (nodes and users) must have their own unique and known identity. HLF provides a membership identity service called Membership Service Provider (MSP) that manages identities and determines the privileges for each network participant, identify specific roles and sign or verify identities. The default MSP relies on Public Key Infrastructure and a hierarchy of X.509 digital certificates [40][41]. MSP can connect to commercial Certificate Authorities (CAs) and generate the required keys and certificates. It can identify which CAs are responsible for defining trust domain members, e.g., an organization, either by listing their members' identities or by identifying which CAs are authorized to issue valid identities to their members. Hence, It turns verifiable identities of a CA into members of a HLF network. HLF authentication and verification services as well as access control lists at different levels of the transaction flow contribute to reaching consensus. In the context of an algorithm that orders and broadcasts transactions to the nodes, HLF provides a modular ordering service. The ordering service can be implemented with a crash fault-tolerant (CFT) or byzantine fault-tolerant (BFT) protocol. In a permissioned network with trusted identities and multiple access controls, a CTF mechanism is preferable. The default implementations that provide CTF ordering services are kafka-based ordering service which utilizes Apache Kafka [42] and raft-based ordering service which utilizes Raft protocol [43].

II. Design Of The Proposed System

The proposed system aims to provide a secure BC ecosystem with respect to privacy to verify that the vehicle's emissions values have not been tampered and are between standard levels, making the vehicle eligible for receiving an emissions certificate and render the vehicle's after sales price worthy, avoiding second-hand resellers fraud. In this process, we designed a unique integration between HLI and HLF to fill the gap of enrolling for a certificate in HLF with a decentralized SSI. HLI has been added as an extra layer of security and privacy on the top of HLF and users are able to acquire a SSI and an IDVC and use them to authenticate and authorize on the HLF network while in parallel keeping all the advantages of ZKP, namely data minimization and privacy enhancements.

A. Use Case Implementation

Our system is built upon the rationale of restoring trust for emissions recorded values. We propose an architecture where a permissioned consortium administered BC - HLF in our case - keeps the emissions records immutable and enhances transparency, while in parallel decentralizes the management of authentication, authorization and access throughout the complete ecosystem with a SSI BC - HLI in our case. This architecture supports the scenario where the vehicles have been uniquely identified at the country they were imported through the local standard procedures and have been issued a registration certificate in hard copy proving their unique characteristics such as their car plate or their Vehicle Identification Number (VIN). The issuers of such certificates are the registration authorities (RAs) and are responsible for issuing any legal papers for the vehicle. The service providers (SPs) such as garages and workshops provide maintenance to cars whenever there is a problem with any of their systems such as an alarm light turned on or on a regular basis as a proactive measure such as checking their emission values. These SPs can be OEM authorized or independent professionals.

Next, we define the different parties that will participate on the network and the allowed interactions between them. There are three roles corresponding to three different kinds of identities, one for RA, the second for the car SP and the third for the vehicle. In a nutshell, RA is responsible for issuing Identities and Credentials to Vehicles and SPs, while the Vehicles and SPs are able to communicate and exchange data with each other directly, securely and with certainty. More specific, using the term RAs we refer to public entities - such as ministries of transport, environmental protection agencies, public authorities that are responsible for approving vehicle types - that can enter the market and in some cases, as ours, the OEMs. These RAs operate on the network as public identities, meaning they can be discovered by everyone, they have write access to the private permissioned BC and are in charge of issuing identities for the vehicles and emissions VCs (EVC) corresponding to the announced emissions values, as well as certify the vehicles for compliance with emissions standards. OEMs have read access on the HLF being able to verify the vehicle's EVCs and write access to certify the vehicle's emissions. Every vehicle participating at this network is transmitting its emissions values every twenty four (24) hours on a daily basis to the RAs in order to receive an EVC, which it then stores at its local secure storage location, also known as wallet. In order for the vehicle to be able to transmit emissions values and apply for an EVC, a trust relationship between the vehicle and the RA must pre-exist. This is accomplished via a pairwise DID, that is established the first time the vehicle accesses an internet connection.

Afterwards, the vehicle automatically receives an identity verifiable credential (IDVC) including claims and metadata specific to this vehicle, so it can use it for proving its identity to any other entity, as the SP, that participates on this network and requires to authenticate the vehicle before any further interactions occur. The IDVC is stored in the vehicle's wallet, eliminating the need for repeating the issuing process, unless any of the claims included in the IDVC change. To enhance privacy and security furthermore, the claims presented by the VC can take the form of a predicate ZKP (PRP) or selective disclosure ZKP (SDP). PRPs have the ability to hide a specific value but in the same time prove the requested claim. For example, if the SP wants to know whether the car adheres to emissions standards and requests a proof, the car can present a PRP proving that the CO2 levels are within acceptable limits without revealing the real values. In another case, if the SP wants to know the exact CO2 emissions values, the car can present the EVC using a SDP by showing only the necessary internal combustion engine water and carbon dioxide by-products CO2 field of the vehicle's EVC and not the complete list of claims included, such as the combustion process known as particulate matter [44]. This enhanced security features are made available under the ZKP support of the HLI framework.

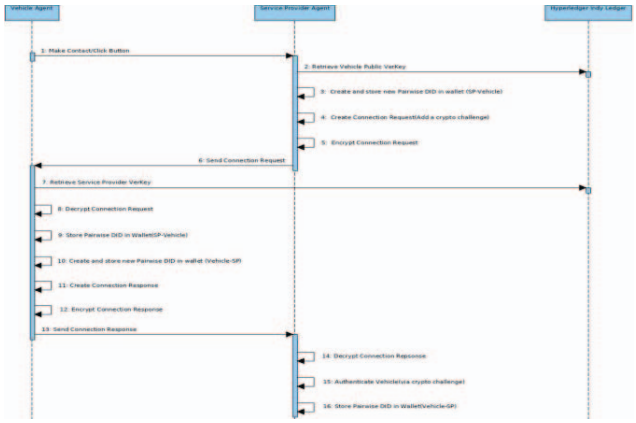

Fig. 1. Vehicle and Service Provider pairwise steps

As with the RA pairwise DID connection, when a vehicle visits a SP it establishes a pairwise relationship where a sequence of IDVC presentation and verification takes place, resulting in a permanent private communication channel between them, without the need to contact the IDVC issuer. Although, there is no need for contacting RAs who are the issuers, a trust between the SP and the RAs must pre-exist as well. After the authentication has been completed, the SP gains access to the vehicles onboard Engine Control Units (ECU) [10]. In the figure 1 flow chart the steps for the establishment of the pairwise DIDs are shown. After this phase the SP might request any additional VCs that are required for repairing the car or confirming its well state, such as the EVC.

{ "@context": ["https://www.w3.org/2018/credentials/v1",
"https://www.w3.org/2018/credentials/examples/v1"],
"type": ["VerifiableCredential", "EmissionCredential"],
"credentialSchema":
{"id":did:indy:cdf:Lk32LaoXp30fok20sLFO31Ak3FxpoR2A",
"type": "did:indy:schema:
{"id":did:indy:cdf:Lk32LaoXp30fok20sLFO31Ak3FxpoR2A",
"type": "did:indy:schema:
IONk7YM1YH43JLD7xdnWRinqWCEY5u5fK"},
"issuer": "did:indy:Qo213aE0FlxQ50Lpe82lPp4vLrT091oR",
"credentialSubject": {"co": "802","thc": "67","nmhc": "43","nox":
"51", "pm": "3"},"proof": { "type": "CLSignature2019",
"issuerData":
"5NQ4TgzNfSQxoLzf2d5AV3JNiCdMaTgm...BXiX5UggB381QU7
ZCgqWivUmy4D", "attributes":
"pPYmqDvwwWBDPNykXVrBtKdsJDeZUGFA...tTERiLqsZ5oxCo
CSodPQaggkDJy","signature":"8eGWSiTiWtEA8WnBwX4T259ST
pxpRKuk...kpFnikqqSP3GMW7mVxC4chxFhVs",
"signatureCorrectnessProof":"SNQbW3u1QV5q89qhxA1xyVqFa6jC
rKwv...dsRypyuGGK3RhhBUvH1tPEL8orH" }}

III. Integrated Architecture

The system's architecture is based on two kinds of BCs. The emissions data is recorded on a HLF private permissioned consortium BC [16] and the authentication and authorization is implemented with SSI on a HLI permissioned public BC. The choice of HLF allows to control the access to the system and fine-grain the rights for the various participants. The emissions transactions sent by RAs, contain the hash of the last unique identifier (UID) of the EVC they issued to the vehicle. This immutable record on the HLF can be used to prove the emissions values that have been announced by the vehicle to the RAs until a specific point in time, due to the fact that each record has a sequential timestamp.

A. Hyperledger Fabric Infrastructure

The vehicle stores the EVC containing the UID to its local wallet, which is accessible only by the vehicle's owner. Based on the above records, the vehicle is eligible to be certified for its compliance to emissions standards according to the HLF emissions records, through a straightforward automated procedure. A smart contract stored on the HLF BC checks every month whether the records are in between the standard emissions levels. If they are, then a certificate is encrypted with the vehicles public key and recorded on the ledger available for downloading. If the emissions are not compliant with the standards, then the smart contract notifies the car's owner by sending an email that it has to check vehicle's emissions with a legitimate authority. In figure 2, we assume the IDVC has already been issued.

B. Hyperledger Indy Infrastructure

The credential schemas and definitions as well as public DIDs of each entity are stored on HLI ledger. In our case, the HLI infrastructure consists of four nodes, which are participating in the same pool, running the Plenum consensus protocol and maintain the same transactions. HLI defines several roles each one with different privileges on the network. The specific role for each node is defined in the transaction by which the corresponding public DID has been written on the ledger. The Steward role is mandatory in any HLI network and is assigned to all HLI nodes. These nodes in our case are located at RAs premises.

Similar to Stewards, the participants holding the Trust Anchor role are the members of the network with the privilege to write transactions on the ledger. All the participating RAs on the system are assigned the Trust

Anchor role, inheriting the exclusive right to write the necessary data on the ledger. Additionally, SPs and vehicles are assigned the User role, which grants the strict permission to read the ledger.

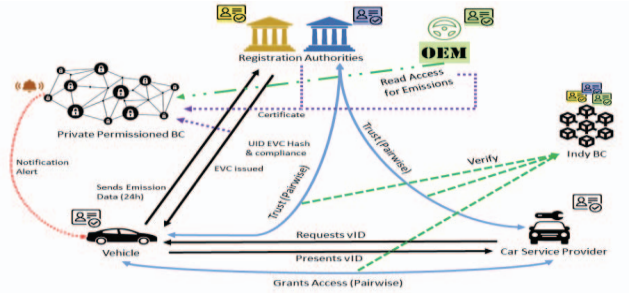

Fig. 2. Vehicle and Service Provider network interactions

As for now, HLI does not support any existing DID verification methods, hence, a generic "*indy"* method is used for the implementation of the system's DIDs.

C. Hyperledger Indy Anonymous Credentials

The VCs the vehicle possesses are implemented using the anonymous credentials format [45]. The main principle of anonymous credentials is to provide the entities with the ability to prove that their credentials include the requested proofs while ensuring that no identity attributes are disclosed. Anonymous credentials are based on Camenisch and Lysyanskaya (CL) credential [46] and enable non-interactive ZKP. The sequence for issuing a VC is described below:

1. RA as a trust anchor creates and writes the credential schema on the ledger. Schema defines the credential attributes and encapsulates the public DID of the RA.
2. Based on the schema, RA creates and writes the corresponding credential definition (CRD) on the ledger. The most important components of CRD are the type of signatures, CL in our care, as well as the RA public key which is composed of all the necessary crystallographic materials that are required for issuing and verification.
3. RA creates and sends a credential offer to the vehicle containing a nonce and a proof of correctness.
4. The vehicle receives the credential offer and creates a master secret. Based on the credential offer it assembles a credential request containing a blinded master secret that links to master secret as well as to its DID and sends it to RA.
5. RA received the credential request from vehicle and proceeds to issue and sign the credential. The credential contains raw and encoded vehicle-related values (e.g VIN, CO level). RA sends the credential to the vehicle.
6. The vehicle updates the credential signature and stores the credential in its wallet. The updated signature is the CL signature that is computed by both the RA and the vehicle throughout the process, from offering to storing, from this point, the vehicle is able to present proofs of the credential claims.

The verification sequence of a VC is described below:

1. The SP assembles and sends to the vehicle the proof request which includes a list of attributes regarding the published credential definition on the ledger thus requiring the interrelation between the vehicle claims with the issuer identity. The proof request may require self-attested attributes, issuer-attested attributes or predicates of attributes.
2. Vehicle searches and fetches the claims from the appropriate credentials that are stored in its wallet. Furthermore, it retrieves from the ledger the corresponding credential schemas and definitions. Then, the vehicle generates the proof with the following options a) hide its identifier, b) disclose selective claims of a credential, c) combine multiple claims for multiple credentials and d) involve predicates proofs to answer a true-or-false in order to satisfy a condition (e.g. staying in NOx levels). As soon as the vehicle assembles the proof, it sends the proof to the SP. The proof is computed, inter alia, using the CL signature.
3. The SP also retrieves the corresponding CRDs for each claim in the proof. Therefore, using the issuer's public key from the CRD in conjunction with the cryptographic components that derives from proof, the SP can verify each claim or predicate.

D. Hyperledger Fabric and Hyperledger Indy Integration

This architecture creates a system with end-to-end security, authentication and authorization as well as immutability in order to enhance the trust and enable the issuance of certificates that complement the car's identity with intention to prove its emission levels. Currently due to HLF features, the HLI SSI functionality cannot be embedded in the HLF BC. Thus, we added an extra layer of identity handling in our proposed architecture to integrate the SSI into the HLF system, so that HLF participants either they are persons, organizations or vehicles, gain full control and protection over their personal data.

The concept behind this lies in the fact that when creating a decentralized identity the holder is in charge of updating their information and only in one place, which is accomplished in our case by the HLI network, through a secure verifiable way. After that, any BC network that uses this identity is capable of contacting the issuer and if any change makes the user's identity invalid prohibits access into the network and prompts the holder for appropriate actions. This means that whoever intents to use this solution must make the appropriate modifications to the specific permissioned BC code, as we did with HLF, to become HLI verifiers and be able to communicate with the HLI clients, agents and servers. The vehicle must participate in the HLF network to get an emissions certificate and notifications when its emissions are out of acceptable levels. In any HLF network, clients must request from an HLF CA a X.509 certificate that is used to represent them on the network. The entity's credentials are sent to the CA because on permissioned networks every identity must be known. It is crucial to enable the SSI holder to send only the necessary claims and not all the credentials including in her/his/its wallet. The holder is able to conceal private data unnecessary for the certificate., without preventing the CA to be able to verify the holder's claims with the trusted issuing authority.

Figure 3 displays a simplified version of this process. The agents represent client software and network services running on the various actors.

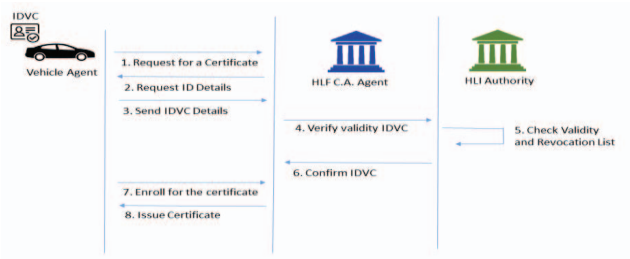

Fig. 3. HLF and HLI integration

At this stage, the vehicle has a digital certificate compliant to the X.509v3 standard and can be properly identified, authenticated, authorized to participate in the HLF BC network and receive notifications about its emissions.

Following is described our approach with two instances of HLF CAs, one acting as a root and the other as an intermediate CA [47]. Fabric-CA is a built-in HLF CA for issuing, revoking and managing X.509 certificates. It is supported by a backend SQLite database in order to store and manage registered identities and their certificates. These certificates are used to authenticate members and define their roles and access rights to the HLF network [48]. The first instance of Fabric-CA refers to the Root-CA hosted and managed by RAs, as they are trustworthy entities. Having this Root-CA, we define a second Fabric-CA instance as an intermediate CA hosted and managed by OEMs in order to provide X.509 credentials to their fleets, called OEM-CA. This "chain of trust" approach provides security by mitigating the exposure risk of Root-CA and deducts its overhead [49]. Thus, the corresponding OEM-CA can directly issue, revoke and manage the credentials for its fleet without contacting the Root-CA.

An additional software component needed for the implementation is an agent running along with the intermediate OEM-CA responsible for verifying the IDVC of each vehicle before it can acquire its certificate. The vehicle, after having an IDVC in its wallet, can request an X.509 certificate from the corresponding OEM-CA. Hence, the DIDs and VCs that are stored in HLI are used to gain access at the HLF network. Since X.509v3 is used, a custom extension with ASN.1 OID (Abstract Syntax Notation Object IDentifier) [50][51] of 1.2.3.4.5.6.7.8.1 must be defined to store an attribute called "indyuser" along with a boolean value for providing flexible management and audit services. The following table depicts the structure of this custom extension.

Version	3 (0x2)	
Serial No	1e:49:98:e9:f4:4f:d0:03:53:bf:36:81:c0:a0:a4:31:96:4f:52:75	
Sign.Algor.	ecdsa-with-SHA256	
Issuer	**CN=OEM-CA, O=OEM, OU=OEM, C=EU**	
Validity	Not Before	May 6 07:35:00 2020 GMT
	Not After	May 6 07:35:00 2022 GMT
Subject	**CN=4JGAB54E81A277648(vinNumber)**	
Subject Public Key Info	Public Key	04:e6:07:5a:f7:09:d5:af:38:e3:f7:a2:90:77:0e:32:67:5b:70:a7:37:ca:b5:c9:d8:91:77:39:ae:03:a0:36:ad:72:b3:3c:89:6d:1e:f6:1b:6d:2a:88:49:92:6e:6e:cc:bc:81:52:fa:19:88:18:5c:d7:6e:eb:d4:73:ce:51:79
	Algorithm	id-ecPublicKey
	Parameters/ASN1 OID	prime256v1
X509v3 extensions	Key Usage	critical, Certificate Sign
	Basic Constraints	critical, CA:FALSE
	Subject Key Identifier	D8:28:B4:C0:BC:92:4A:D3:C3:8C:54:6C:08:86:33:10:A6:8D:83:AE
	Authority Key Identifier	keyid:C4:B3:FE:76:0D:E2:DE:3C:FC:75:FB:AE:55:86:04:F0:BB:7F:F6:01
	1.2.3.4.5.6.7.8.1	**{"attrs":{"indyuser":"true"}}**

E. x.509 Certificate Issuing with Verifiable Credentials

Initially, the OEM-CA agent and the vehicle agent create a secure communication channel using pairwise DIDs. Taking advantage of pairwise DIDs, communication and messaging, data exchange is done exclusively through this channel. The vehicle's agent sends a request to obtain an X.509 certificate to OEM-CA agent. OEM-CA agent responds by sending a proof request to the vehicle's agent for its identity. The vehicle's agent fetches the credential from its HLI wallet, assembles and sends the proof back to the OEM-CA agent. The OEM-CA agent acts as a verifier and verifies the proof. If the proof is valid, it triggers OEM-CA server to issue the appropriate certificate for the specific vehicle. The actual issuance of a X.509 certificate is happening in two phases, the registration and the enrollment phase.

1) Registration

During registration, an Enrollment ID (EnID) and an Enrollment Secret (EnSecret) for a specific subject are generated by the OEM-CA. During the enrollment, the subject enrolls itself using the EnID and EnSecret. The OEM-CA server uses the vinNumber of the vehicle's IDVC as the EnID and generates the EnSecret for vehicle. In addition, it defines the attribute "indyuser" with the value "true" that will be encapsulate in the X.509 certificate. The EnID, the hashed EnSecret and the "indyuser" attribute are stored as a new entry in the OEM-CA SQLite database.

Afterwards, the vehicle is registered and known to OEM-CA. The OEM-CA server sends back to the OEM-CA agent the EnSecret. The OEM-CA agent is responsible for sending the EnSecret via pairwiseDID to the vehicle's agent which proceeds with the enrollment.

2) Enrollment

In the enrolment procedure, the vehicle's agent triggers the vehicle HLF client to generate a public/private key pair and a Certificate Signing Request (CSR) using the generated keys. The CSR uses ECDSA with curve prime256v1 and ecdsa-with-SHA256 as signature algorithms. The CSR along with EnID and EnSecret are submitted by the vehicle's HLF client to the OEM-CA server for the issuance of the certificate. The vehicle's private key is kept secret and never sent to the OEM-CA. The OEM-CA server authenticates the vehicle by finding the corresponding entry in its database. Subsequently, it issues, signs and sends an X.509 certificate

(in HLF called Ecert) to the vehicle, and the vehicle stores it in its HLF wallet. In parallel, the OEM-CA server stores the certificate in its database. The certificate includes the vinNumber from IDVC as CommonName and the custom field, which indicates that vehicle is a HLI user. Henceforth, the vehicle can participate in HLF using its credentials.

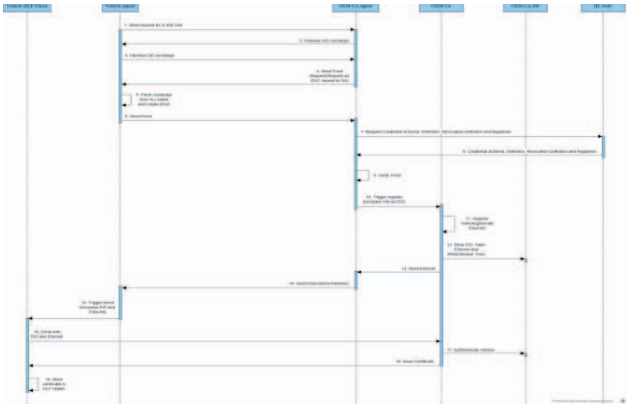

Fig. 4. HLF x.509 certificate issuing using IDVC

IV. Conclusions And Future Work

In this paper, we proposed a decentralized authentication and authorization system for securing access and emissions control based on BC technology and SSIs. With this ecosystem, access management for the vehicles can be decentralized while in parallel emissions transmitted values are immutable thus secured from tampering. Regulation authorities can take advantage from this tamper-proof system and enforce local and national laws protecting the environment. By taking advantage of ZKP techniques, the communication between the different stakeholders is private and secure, with respect to sovereignty for personal, private and sensitive data protecting from unauthorized exposure of this data. With the use of pairwise DIDs scalability and performance are ensured to a level. However, further studies are needed with specific metrics regarding performance and scalability actual gains. For example, our system uses four nodes for HLI and four nodes for HLF, but in real life scenarios, probably more nodes will be used for both of these networks, which might affect response times. Although our proposed architecture includes BC emissions certificates, we will include in our future work VCs for issuing and verifying these certificates easily from any third party service. We also demonstrated the importance of using only one HLI service for issuing SSI and VCs and making them available to any other BC such as HLF. In our future work, as both DID and X.509 are related to private/public key pairs, we intend to link the keys that are generated for the entity's DID to generate the corresponding X.509 certificate. In addition, we believe that apart from the correlation between DID and X.509, future research should look for extending the HLF MSP to directly manage identities and credentials from HLI without the need for X.509 certificates, thus by having a DID and an IDVC, entities can get directly involved in the HLF network.

Acknowledgment

This work was funded from the European Union's Horizon 2020 Framework Programme for Research and Innovation under grant agreement No 814951, project DIAS.

References

[1] F. Yang, S. Wang, J. Li, Z. Liu and Q. Sun, "An overview of Internet of Vehicles," *China Communications*, vol. 11, no. 10, pp. 1-15, Oct. 2014

[2] J. Contreras-Castillo, S. Zeadally and J. A. Guerrero-Ibañez, "Internet of Vehicles: Architecture, Protocols, and Security," in *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3701-3709, Oct. 2018, doi: 10.1109/JIOT.2017.2690902.

[3] A. Humayed and B. Luo, "Cyber-physical security for smart cars: taxonomy of vulnerabilities, threats, and attacks", *in Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems (ICCPS '15)*, pp. 252-253, 2015

[4] Hackers Remotely Kill a Jeep on the Highway—With Me in It, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, last accessed 06/14/2020

[5] How Volkswagen's 'Defeat Devices' Worked, https://www.nytimes.com/interactive/2015/business/international/vw-diesel-emissions-scandal-explained.html, last accessed 06/14/2020

[6] "Odometer manipulation in motor vehicles in the EU", https://www.europarl.europa.eu/RegData/etudes/STUD/2018/615637/EPRS_STU(2018)615637_EN.pdf, last accessed 06/14/2020

[7] P. Borkowski "Reducing Odometer Fraud in the EU Second-Hand Passenger Car Market Through Technical Solution", *Sierpiński G. (eds) Integration as Solution for Advanced Smart Urban Transport Systems. TSTP 2018*. Advances in Intelligent Systems and Computing, vol 844. Springer, Cham, 2019

[8] "ENISA good practices for security of Smart Cars", https://www.enisa.europa.eu/publications/enisa-good-practices-for-security-of-smart-cars, last accessed 06/14/2020

[9] N. Fotiou, I. Pittaras, V. A. Siris, S. Voulgaris and G. C. Polyzos, "Secure IoT Access at Scale Using Blockchains and Smart Contracts," *2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, Washington, DC, USA, 2019, pp. 1-6, doi: 10.1109/WoWMoM.2019.8793047.

[10] M. S. U. Alam, S. Iqbal, M. Zulkernine and C. Liem, "Securing Vehicle ECU Communications and Stored Data," *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, 2019, pp. 1-6, doi: 10.1109/ICC.2019.8762043.

[11] X. Wang, P. Zeng, N. Patterson, F. Jiang and R. Doss, "An Improved Authentication Scheme for Internet of Vehicles Based on Blockchain Technology," in *IEEE Access*, vol. 7, pp. 45061-45072, 2019, doi: 10.1109/ACCESS.2019.2909004.

[12] A. P. Christodoulou, K. Christodoulou, V. Vassiliou, and Z. Zinonos. "IoT Device Firmware Update over LoRa: The Blockchain Solution." In 2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS), pp. 404-411. IEEE, 2020

[13] Z. Yang, K. Yang, L. Lei, K. Zheng and V. C. M. Leung, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495-1505, April 2019, doi: 10.1109/JIOT.2018.2836144.

[14] K. L. Brousmiche, T. Heno, C. Poulain, A. Dalmieres and E. Ben Hamida, "Digitizing, Securing and Sharing Vehicles Life-cycle over a Consortium Blockchain: Lessons Learned," *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, 2018, pp. 1-5.

[15] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," in *IEEE Internet of Things Journal,* vol. 5, no. 2, pp. 1184-1195, April 2018, doi: 10.1109/JIOT.2018.2812239.

[16] N. Kulabukhova, A. Ivashchenko, I. Tipikin and I.Minin (2019) Self-Sovereign Identity for IoT Devices. In: Misra S. et al. (eds)

Computational Science and Its Applications – ICCSA 2019. ICCSA 2019. Lecture Notes in Computer Science, vol 11620. Springer, Cham

[17] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292-2303, 2016.

[18] J. Jensen , "Identity Management Lifecycle - Exemplifying the Need for Holistic Identity Assurance Frameworks," *Information and Communication Technology. ICT-EurAsia 2013.* Lecture Notes in Computer Science, vol 7804. Springer, Berlin, Heidelberg

[19] S. E. Haddouti and M. D. E. E. Kettani, "Towards an Interoperable Identity Management Framework: a Comparative Study," ArXiv abs/1902.11184 (2019): n. pag.

[20] Y. Cao and L. Yang, "A survey of Identity Management technology," *2010 IEEE International Conference on Information Theory and Information Security*, Beijing, 2010, pp. 287-293, doi: 10.1109/ICITIS.2010.5689468..

[21] M. Dabrowski and P. Pacyna, "Generic and Complete Three-Level Identity Management Model," *Second International Conference on Emerging Security Information, Systems and Technologies*, Cap Esterel, 2008, pp. 232-237.

[22] K. C. Toth and A. Anderson-Priddy, "Self-Sovereign Digital Identity: A Paradigm Shift for Identity," in *IEEE Security & Privacy*, vol. 17, no. 3, pp. 17-27, May-June 2019, doi: 10.1109/MSEC.2018.2888782.

[23] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018. ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2018.10.002.

[24] D.V. Bokkem, R. Hageman, G. Koning, L. Nguyen and N. Zarin. "Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology," ArXiv abs/1904.12816 (2019): n. pag.

[25] A. Jøsang, J. Fabre, B. Hay, J. Dalziel, and S. Pope. "Trust requirements in identity management," *Proceedings of the 2005 Australasian workshop on Grid computing and e-research - Volume 44 (ACSW Frontiers '05).* Australian Computer Society, Inc., AUS, 99–108.

[26] "Decentralized Identifiers (DIDs) v1.0", https://www.w3.org/TR/did-core/, last accessed 06/14/2020

[27] M. Davie, D. Gisolfi, D. Hardman, J. Jordan, D. O'Donnell and D. Reed, "The Trust over IP Stack," in *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 46-51, December 2019, doi: 10.1109/MCOMSTD.001.1900029.

[28] Y. Kortesniemi, D. Lagutin, T. Elo, and N. Fotiou. "Improving the privacy of iot with decentralised identifiers (dids)," *Journal of Computer Networks and Communications*, *2019*.

[29] "Verifiable Credentials Data Model 1.0", https://w3c.github.io/vc-data-model, last accessed 06/14/2020

[30] G. Fedrecheski, J.M Rabaey, L. C. Costa, P.C. C. Ccori, W. T. Pereira, and M.K. Zuffo. "Self-Sovereign Identity for IoT environments: A Perspective," *arXiv preprint arXiv:2003.05106*.

[31] Z. A. Lux, F. Beierle, S. Zickau and S. Göndör, "Full-text Search for Verifiable Credential Metadata on Distributed Ledgers," *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, Granada, Spain, 2019, pp. 519-528.

[32] Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press

[33] J. L. Canovas Sanchez, J. B. Bernabe and A. F. Skarmeta, "Towards privacy preserving data provenance for the Internet of Things," *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, 2018, pp. 41-46, doi: 10.1109/WF-IoT.2018.8355229.

[34] C. Huang, R. Lu, X. Lin and X. Shen, "Secure Automated Valet Parking: A Privacy-Preserving Reservation Scheme for Autonomous Vehicles," in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11169-11180, Nov. 2018, doi: 10.1109/TVT.2018.2870167.

[35] "Hyperledger Indy", https://www.hyperledger.org/projects/hyperledger-indy, last accessed 06/14/2020

[36] A. Abraham, K. Theuermann and E. Kirchengast, "Qualified eID Derivation Into a Distributed Ledger Based IdM System," *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, 2018, pp. 1406-1412, doi: 10.1109/TrustCom/BigDataSE.2018.00195.

[37] "Hyperledger Fabric", https://www.hyperledger.org/projects/fabric, last accessed 03/14/2020

[38] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger fabric," *Proceedings of the Thirteenth EuroSys Conference*, 2018.Association for Computing Machinery, New York, NY, USA, Article 30, 1–15. DOI:https://doi.org/10.1145/3190508.3190538

[39] M. Vukolić, "Rethinking Permissioned Blockchains," *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts - BCC 17*, 2017. Association for Computing Machinery, New York, NY, USA, 3–7. DOI:https://doi.org/10.1145/3055518.3055526

[40] A. Fuchs, D. Kern, C. Krauß, and M. Zhdanova, "TrustEV: : trustworthy electric vehicle charging and billing", *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, 2020. (SAC '20). Association for Computing Machinery, New York, NY, USA, 1706–1715. DOI:https://doi.org/10.1145/3341105.3373879

[41] M. Ring, D. Frkat and M. Schmiedecker. "Cybersecurity Evaluation of Automotive E/E Architectures," *ACM Computer Science In Cars Symposium (CSCS 2018)*. 2018.

[42] Thein, Khin Me Me. "Apache kafka: Next generation distributed messaging system." *International Journal of Scientific Engineering and Technology Research* 3.47 (2014): 9478-9483.

[43] D. Ongaro and J. Ousterhout. "In search of an understandable consensus algorithm*," Proceedings of the 2014 USENIX conference on USENIX Annual Technical Conference (USENIX ATC'14)*. USENIX Association, USA, 2014, 305–320.

[44] "Cars and Emissions", https://www.vehicle-certification-agency.gov.uk/fcb/cars-and-emissions.asp, last accessed 06/14/2020

[45] "Anonymous credentials with type-3 revocation", https://github.com/hyperledger/ursa-docs/tree/master/specs/anoncreds1, last accessed 06/14/2020

[46] J. Camenisch, A. Lysyanskaya "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation," *Pfitzmann B. (eds) Advances in Cryptology —* EUROCRYPT 2001. EUROCRYPT 2001. Lecture Notes in Computer Science, vol 2045. Springer, Berlin, Heidelberg

[47] "Hyperledger Fabric CA", https://hyperledger-fabric-ca.readthedocs.io/en/release-1.4/, last accessed 06/14/2020

[48] A. R. Thota, P. Upadhyay, S. Kulkarni, P. Selvam and B. Viswanathan, "Software Wallet Based Secure Participation in Hyperledger Fabric Networks," *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS),* Bengaluru, India, 2020, pp. 1-6, doi: 10.1109/COMSNETS48256.2020.9027445.

[49] Z. E. Uahhabi and H. E. Bakkali, "A comparative study of PKI trust models," *International Conference on Next Generation Networks and Services (NGNS),* Casablanca, 2014, pp. 255-261, doi: 10.1109/NGNS.2014.6990261.

[50] International Telecommunication Union – ITU-T Study Group 7: Abstract Syntax Notation number One – ASN.1. www.itu.int/ITU-T/asn1/(1995)

[51] J.K Hong, "PKI Management of cooperative intelligent transport system," *Indian Journal of Public Health Research & Development*. 9. 392. 10.5958/0976-5506.2018.00766.0.