Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

FuSeCar

Future generation Security for smart and connected Cars - FuSeCar

Deliverable D2.2: Privacy-enhanced authentication protocols based on Zero-Knowledge approaches that support attribute-based authentication and authorization through dynamic policies

WP2: Privacy enhancement of current vehicular communication protocols and architectures

Authors:
Author 1[1] and Author 2[2]
giampaolo.bella@unict.it

Department of Mathematics and Informatics
University of Catania

Current revision: R0.1
Delivery date: December 4th, 2024

Revision history

Authors	Changes	Date	Revision
Giampaolo Bella	First draft of the deliverable structure	April 12th, 2024	R0.1
Giampaolo Bella	First draft of the deliverable	July 20th, 2024	R0.1
Giampaolo Bella	Refinements and update	October 6th, 2024	R0.5
Giampaolo Bella	Revision of document and minor fixes	December 4th, 2024	R1.1

Contents

1 Introduction

This deliverable presents a detailed account of the use of Identity-Based Authentication combined with Attribute-Based Authentication over a specific case study drawn from the automotive sector in the area of dematerialised payment, hence without the use of smart cards discussed in Deliverable D2.1. The case study is drawn from the real world, also thanks to the external consultancy benefited from during the project.

This Deliverable continues by modelling the privacy landscape of the Internet of Vehicles (IoV) by starting off with the older paradigm of Intelligent Transportation Systems (ITS) (Section 2). It does so with the aim of distilling out relevant attributes to later adopt through Attributed Based Authentication (Section 3). It then investigates on the technologies that may be relevant to digital fuel distribution, such as Zero-Knowledge Proofs (ZKPs) to enable a prover to confirm knowledge of relevant items to a verifier without disclosing additional information to the verifier (Section 4). It continues with a relevant case study on dematerialised payments for fuel (Section 5) and terminates with its enhanced, innovative version by the use of ZKPs, Attributed Based Authentication and dynamic policies (Section 6).

1.1 Context, challenges and motivation

It is evident that, for the present work to progress effectively, the initial and indispensable step consists of identifying and defining the set of attributes that will serve as the foundation for the design of Attribute-Based Authentication (ABA) techniques and protocols. Establishing these attributes provides the semantic and operational backbone upon which authentication decisions can be consistently and securely made. In pursuing this objective, we recognise that our investigation naturally situates itself within the broader framework of the Internet of Vehicles (IoV) — a paradigm that represents a substantial evolution beyond the traditional scope of Intelligent Transportation Systems (ITS). The IoV extends the capabilities of ITS by embedding pervasive connectivity, decentralised intelligence, and dynamic data exchange among vehicles, infrastructure, and cloud services, thereby introducing new challenges and opportunities for attribute-driven security mechanisms.

Accordingly, the primary objective of this phase is to disentangle the inherent complexities of the domain by systematically analysing the existing gaps, overlaps, and redundancies found within current standards, regulatory frameworks, and academic literature [4]. This analysis encompasses both the well-established domain of Intelligent Transportation Systems (ITS) and the emerging paradigm of the Internet of Vehicles (IoV). By doing so, we aim to construct a coherent representation of their respective privacy landscapes — identifying not only where current approaches fall short in addressing data protection requirements, but also where unnecessary duplication or conceptual ambiguity may hinder the development of unified, privacy-preserving models. Such a comparative exploration provides the foundation for a more integrated understanding of how privacy risks evolve as vehicular networks transition from the centralised architectures of ITS toward the more decentralised, data-intensive ecosystems characteristic of the IoV.

2 Modelling the privacy landscape of the Internet of Vehicles

In the field of Intelligent Transportation Systems (ITS), the integration of cutting-edge communication technologies has been pivotal in enhancing traffic management, safety, and the environmental sustainability of transportation networks. ITS leverages a broad array of technologies to facilitate the dynamic exchange of information between vehicles, infrastructure, and pedestrian devices, aiming to improve the efficiency and responsiveness of the transportation ecosystem [8]. The European Telecommunications Standards Institute (ETSI) has been instrumental in developing standards that underpin various applications and technologies constituting ITS.

A notable example is ETSI ITS G5 [6], which focuses primarily on vehicular communication systems designed to ensure interoperability and reliable performance across European roads. These standards encompass protocols, application guidelines, and communication frameworks that dictate the efficacy of ITS deployments.

Despite the comprehensive framework provided by ETSI, rapid advancements in vehicular technology and the rise of the Internet of Vehicles (IoV) [27] present new challenges and opportunities. IoV extends beyond traditional vehicular communication, incorporating more extensive data exchange and connectivity that promise enhanced vehicular services and automation. However, this evolution also introduces complexities in privacy, security, and data management, areas where existing standards may not fully align with current technological capabilities and societal expectations [25].

As an example of privacy issues for IoV, the wireless transmission of data between vehicles and infrastructure is vulnerable to interception, compromising personal and operational confidentiality. Furthermore, continuous tracking of vehicles by malicious actors can expose sensitive personal information, such as location habits and routines. Data aggregation across ITS and IoV networks can inadvertently create detailed individual profiles, potentially leading to unintended privacy breaches [13]. Moreover, the complexity of these networks introduces vulnerabilities that could be exploited, threatening data integrity and the overall security of transportation systems [12]. Additionally, attempts to use a temporary identifier instead of the station canonical's one, as stated by ETSI [7] to prevent linking attacks, often fall short as the detailed nature of the data being transmitted between vehicles and between vehicles and infrastructure allows for possible re-identification [1], a risk intensified by the increasing volume of data in IoV.

This modelling aims to dissect these complexities by analysing gaps and redundancies in current standards and academic literature with respect to both traditional ITS and the nascent IoV paradigm to model their privacy landscapes.

2.1 Context

The Internet of Vehicles (IoV) represents a significant evolution in the domain of Intelligent Transportation Systems (ITS), encompassing a large-scale distributed system for wireless communication and information exchange between vehicles, roads, humans, and the Internet. This system needs standardised communication protocols and data interaction guidelines to facilitate intelligent traffic management and Vehicle-to-Everything (V2X) communication [27].

The integration of 5G and edge cognitive computing (ECC) [5] has significantly advanced intra-vehicle communications, enhancing the speed, intelligence, and stability of interactions between wearable and vehicular devices. This improvement plays a critical role in ensuring the safety and comfort of individuals within vehicles and enhances the overall safety of the traffic system.

Inter-vehicle networks, which include all communicative vehicles sharing resources, add another dimension of complexity. On a larger scale, the Cognitive Internet of Vehicles (CIoV) [5] analyses data from a comprehensive network that includes intra-vehicle, adjacent vehicle, and environmental road data to bolster road traffic safety. The complexity of these systems necessitates stringent network reliability to prevent issues like personal data

breaches and traffic system failures, highlighting the importance of joint physical and network space cognition. Furthermore, the IoV paradigm faces considerable challenges in privacy and security, underlined by the need for robust measures against potential cyber threats. Promoting a human-centred approach [5] helps to ensure service safety and the protection of personal information across these vehicular networks, thus addressing essential security aspects such as confidentiality, integrity, availability, and privacy [22].

Moreover, the absence of universally accepted standards presents considerable challenges in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications, impeding the scalability and integration of IoV systems across different regions and technologies [22]. The staged roll-out of IoV systems, beginning with low-risk implementations and advancing towards broader, systemic deployments, highlights the critical need for robust regulatory frameworks and widespread population adaptation. The integration of IoV with other infrastructures is imperative to create a holistic Internet of Things (IoT) ecosystem, enhancing collaboration and interconnection across various sectors.

In Europe, the ETSI ITS G5 standards serve as a cornerstone for ITS, aiming to ensure reliable V2V and V2I communications [6]. Formulated by the European Telecommunications Standards Institute (ETSI), these standards utilise technology based on IEEE 802.11p — a modification of the Wi-Fi standard tailored for automotive applications. This forms the basis for the Dedicated Short-Range Communications (DSRC) system, which operates within the 5.9 GHz band and is engineered for low-latency, high-reliability communications critical to automotive safety applications. The ETSI ITS G5 standards encompass protocols for various applications, including Cooperative Awareness Messages (CAM) and Decentralised Environmental Notification Messages (DENM). CAMs facilitate the regular exchange of basic vehicle information to enhance situational awareness, while DENMs alert drivers and automated systems to hazardous situations or emergency conditions in real-time. Comparatively, the US counterpart to ETSI ITS G5 is Wireless Access in Vehicular Environments (WAVE) [15], which also operates under the IEEE 802.11p standard and is institutionalised by the US Federal Communications Commission within the DSRC framework.

2.2 Motivation

Given the above context, we seek out to model the current privacy landscapes of both ITS and IoV in order to distil the relevant attributes to be later employed through Attribute Based Authentication. With the term "privacy landscape", we refer to the intricate scenario of privacy concerns, regulations, and practices within a specific domain or technological ecosystem. It encompasses the dynamic interplay between technological advancements, regulatory frameworks, and societal expectations regarding the protection of personal data and privacy rights. This understanding is essential for evaluating the applicability and sufficiency of standards in addressing the privacy and security requirements of both ITS and the forthcoming IoV contexts.

There is a pronounced need to evaluate how the privacy landscape influences the development and implementation of standards within ITS and IoV. This involves conducting a systematic review of the protocol stack, key message types such as CAM and DENM, and the various application classes defined within these standards. For these reasons, it becomes imperative to provide a comprehensive overview of where the standards successfully support ITS and IoV functionalities and where they may fall short or exhibit inefficiencies, particularly from a privacy perspective.

This analysis is not only critical for assessing current capabilities, but also for anticipating the adjustments required to ensure that privacy considerations are adequately addressed as we transition from ITS to IoV.

2.3 General contributions

We observe that there is a lack of standards in the IoV domain, due to the novelty of this new paradigm. In fact, existing standards are limited to the IoV predecessor, i.e., the ITS framework. Hence, this modelling

first investigates the privacy landscape of ITS, in particular at the European level, analysing the ETSI ITS G5 standards. Furthermore, with the IoV paradigm emerging to replace ITS, this modelling extends the initial exploration on ITS by analysing recent academic literature, so as to comprehensively obtain an overview of the privacy landscape for the IoV.

The main contributions of this modelling are summarised as follows:

- A relational model that illustrates the privacy landscape of ITS, grounded in the ETSI ITS G5 standards.
- A relational model that illustrates the privacy landscape of IoV, informed by available academic research and potential standardisation gaps.
- A contrastive analysis between the privacy landscapes of ITS and IoV, highlighting the continuity and divergence in privacy as the technology transitions from ITS to IoV.

2.4 Motivation

Given the above context, we seek out to model the current privacy landscapes of both ITS and IoV in order to distil the relevant attributes to be later employed through Attribute Based Authentication. With the term "privacy landscape", we refer to the intricate scenario of privacy concerns, regulations, and practices within a specific domain or technological ecosystem. It encompasses the dynamic interplay between technological advancements, regulatory frameworks, and societal expectations regarding the protection of personal data and privacy rights. This understanding is essential for evaluating the applicability and sufficiency of standards in addressing the privacy and security requirements of both ITS and the forthcoming IoV contexts.

There is a pronounced need to evaluate how the privacy landscape influences the development and implementation of standards within ITS and IoV. This involves conducting a systematic review of the protocol stack, key message types such as CAM and DENM, and the various application classes defined within these standards. For these reasons, it becomes imperative to provide a comprehensive overview of where the standards successfully support ITS and IoV functionalities and where they may fall short or exhibit inefficiencies, particularly from a privacy perspective.

This analysis is not only critical for assessing current capabilities, but also for anticipating the adjustments required to ensure that privacy considerations are adequately addressed as we transition from ITS to IoV.

2.5 General contributions

We observe that there is a lack of standards in the IoV domain, due to the novelty of this new paradigm. In fact, existing standards are limited to the IoV predecessor, i.e., the ITS framework. Hence, this modelling first investigates the privacy landscape of ITS, in particular at the European level, analysing the ETSI ITS G5 standards. Furthermore, with the IoV paradigm

2.6 Related Work

The convergence of Intelligent Transportation Systems (ITS) and the Internet of Vehicles (IoV) has precipitated numerous privacy and security concerns addressed in various research studies. This Section reviews notable works in the field.

Ometov et al. [19] provided a comprehensive overview of positioning information privacy within ITS, highlighting the impact of European Union regulations and suggesting directions for future privacy strategies. Their discussion encapsulates the regulatory landscape and its implications for privacy in ITS.

Sadiku et al. [21] explored the ITS standards in relation to IoV. They discuss the privacy issues that emerge when tracking vehicles and individuals, emphasising the need for robust privacy-preserving mechanisms in ITS developments.

Butt et al. [3] reviewed privacy management challenges within the social aspects of IoV. They proposed the use of blockchain technology as a novel solution to enhance privacy and security in vehicular networks, providing a detailed analysis of blockchain's potential to address inherent privacy issues.

Hahn et al. [14] classified and analysed prevalent security and privacy issues in ITS. Their study employs a model-driven approach to better understand and mitigate the challenges faced in securing ITS architectures.

Sun et al. [24] focused on the integration of security and privacy requirements in IoV systems. They provided insights into the necessary frameworks that need to be established to support the safe deployment of ITS services.

Boualouache et al. [2] examined pseudonym changing strategies in Vehicular Ad-Hoc Networks (VANETs), identifying them as essential for protecting location privacy. Their review categorises these strategies and discusses their effectiveness against pseudonyms linking attacks, highlighting the ongoing need for robust solutions to prevent adversaries from tracking vehicles.

Petit et al. [20] systematically categorised and compared pseudonym schemes based on cryptographic approaches. They also offered insights into the state of standardisation in the field, along with identifying open research challenges that need to be addressed.

Zavvos et al. [28] explored privacy and trust challenges inherent in the IoV, emphasising the need for a holistic approach to address privacy concerns at the service level. As we shall see below, our deliverable builds on this work for the design of the relational model for the privacy landscape of IoV.

Each of these studies contributes to the state of the art by proposing frameworks, identifying challenges, and suggesting potential solutions to enhance privacy and security in ITS and IoV ecosystems. However, to the best of our knowledge, this modelling presents the first work that uses relational models to analyse the privacy landscape of the Intelligent Transportation Systems and the Internet of Vehicles, and the first to perform a contrastive analysis between them.

2.7 Our Modelling Method

Our literature analysis covers the available European standards and recent scientific contributions that are relevant to both the ITS and IoV domains. In our modelling method, we adopt the Crow's foot notation [26], which is a standard diagramming technique used for representing relational database structures. The distinguishing feature of this notation lies in the graphical symbols denoting the "more" (one or more) side of relationships. Resembling a crow's foot, these symbols are the hallmark of this notation, hence its name.

A brief recall of the key components and their meanings in Crow's foot notation is given below:

- *Entities*: Represented by rectangles, entities are the objects or concepts about which data is stored, such as "Customer" or "Order". The entity's name is positioned at the top of the rectangle.
- *Attributes*: Below the entity's name, attributes are the properties or details of an entity, such as "Customer Name" or "Order Date".
- *Relationships*: Depicted by lines connecting entities, relationships illustrate how entities interact with one another. The nature of the relationship is indicated by symbols at each end of the line.
- *Cardinality*: Specifies how many instances of one entity can or must be associated with each instance of another entity. Cardinality is indicated by symbols such as:
  - A single line (|) for "one".

  - A three-pronged "crow's foot" for "many".
  - An optional circle or zero (O) to represent "zero or more".
  - A vertical bar (|) combined with a crow's foot to indicate "one or more".

- *Participation*: Denotes whether the relationship is optional or mandatory. Mandatory participation is shown by a line without a circle, whereas optional participation is indicated by adding a circle.

Briefly, our modelling method examines the relevant entities and their relationships in state-of-the-art documents, focusing on potential privacy gaps.

2.8 Modelling the Landscape

This Section presents the relational models for the privacy landscape of the Intelligent Transportation Systems and the Internet of Vehicles, hereafter referred to as the (relational) models for ITS and IoV. The description of our relational models is conveniently structured into two subsections below.

2.8.1 A Relational Model for ITS

The relational model for Intelligent Transportation Systems comprises a total of ten entities, each representing a distinct aspect of the ITS ecosystem. The model builds upon the ETSI ITS G5 standards [6] and is depicted in Figure 1.

The choice of standards at the European level clearly affects the resulting model, as we shall detail below, and is founded upon two key factors: firstly, the significant similarities between ETSI ITS G5 and its American counterpart IEEE WAVE, particularly in their fundamental aim of enhancing road safety and facilitating intelligent transportation systems; and secondly, the profound influence of GDPR within the European Union, emphasising the paramount importance of privacy and data protection.

The first entity that we consider is Intelligent Transportation System (ITS) Domain, which represents the overarching context of the model, encompassing all components related to transportation systems that utilise information and communications technology to improve safety, efficiency, and the environment.

ITS Domain has two relationships with the ETSI standards that are conveniently divided into two separate entities. One is ETSI ITS G5 Basic Set of Applications [7], which contains a catalogue of V2X applications and use cases, grouped respectively by Applications Class and Application. The other is ETSI ITS G5 Other Standards, which gathers the list of documents that specify the five layers of the ETSI ITS G5 Protocol Stack, as presented by Fernandes et al. [10]. Both the ETSI ITS G5 entities refer to ITS Domain.

Finally, since ETSI has standardised two fundamental types of messages, we specialise the entity Message with CAM and DENM entities, both supporting more than a Use Case. Notably, all entities have no attributes, with the only exception for CAM and DENM.

2.8.2 A Relational Model for IoV

The relational model for Internet of Vehicles includes a total of five entities, each representing a distinct aspect of the IoV ecosystem. The model relies on the list of IoV services, information categories and privacy concerns presented by Zavvos et al. [28] and is depicted in Figure 2.

The choice of Zavvos et al. as the only document for IoV clearly affects the resulting model, as we shall detail below, and derives from the comprehensiveness and depth of their analysis regarding privacy concerns in IoV services and the absence of consolidated IoV standards. Their work offers valuable insights into the potential risks and implications associated with the collection, processing, and sharing of vehicular data.

The first entity is Internet of Vehicles (IoV) Domain, which encapsulates the interconnectedness of vehicles, infrastructure, and devices through network technologies to enhance transportation efficiency and safety.

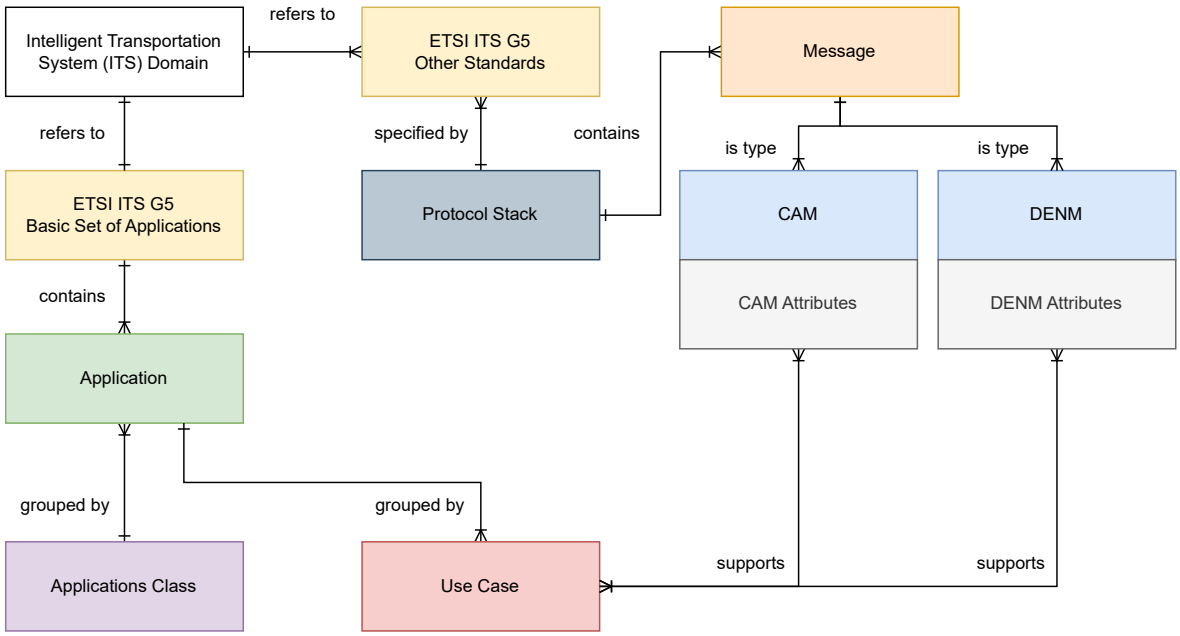


Figure 1: Relational Model for ITS.

The Zavvos et al. entity refers to the IoV Domain entity and also has a relationship with the IoV Service entity, as the work by Zavvos et al. [28] contains a list of services whose privacy concerns are systematically categorised by the authors into four basic categories: personal information privacy, multi-party privacy, trust, and consent to share information [28]:

- **Personal information privacy** raises significant challenges as users are required to share personal data to access IoV services, while facing risks of exploitation due to extensive data collection and storage. Achieving a balance between the provision of high-quality services and the minimal use of user data becomes a complex and nuanced endeavor.
- **Multi-party privacy** arises as a pressing issue, since the interconnected nature of the IoV heightens fears of breaching third-party privacy. In fact, the seamless exchange of information across multiple entities can lead to inadvertent privacy violations, and the monitoring of activities across IoV networks could severely undermine trust in the system.
- **Trust** assumes various forms within the IoV ecosystem, encompassing user-provider trust, inter-user trust, and trust in the IoV infrastructure itself. Ensuring trust is vital for the widespread adoption of IoV technologies, as a lack of trust may impede users from sharing information or engaging with IoV services.
- **Obtaining consent for data sharing** presents a complex challenge, as users grapple with unclear privacy trade-offs and the need for real-time consent management, which potentially disrupts user experiences in the IoV environment.

The last entity of the model for IoV is called Information Category. In fact, information has been arranged by Zavvos et al. according to its typical uses and into categories that, when combined, may present hazards to the user if not properly managed.

For example, the ID category pertains to uniquely identifying elements, such as vehicle details, user credentials, or third-party entities. Said identification is crucial for the functionality and security of IoV services. The

GPS category offers insights into geolocation, velocity, direction of the vehicle at any point in time, and it is crucial for tracking movement. The Route Information category encompasses the origin, destination, and path of travel for a vehicle. The Multimedia Feeds category encompasses visuals and audio obtained from onboard sensors or external devices, and can enhance situational awareness and safety. The Profiles category is built from diverse data like behavioural patterns, health records, and emotional states. The Interests and Relationships category sheds light on personal preferences and social connections, enriching the user experience. Finally, the Other category encompasses information from sensors like RADAR or LIDAR, expanding the scope of data collection beyond the mentioned categories.

These facets collectively provide a thorough understanding of individuals, vehicles, and their interactions within various contexts.

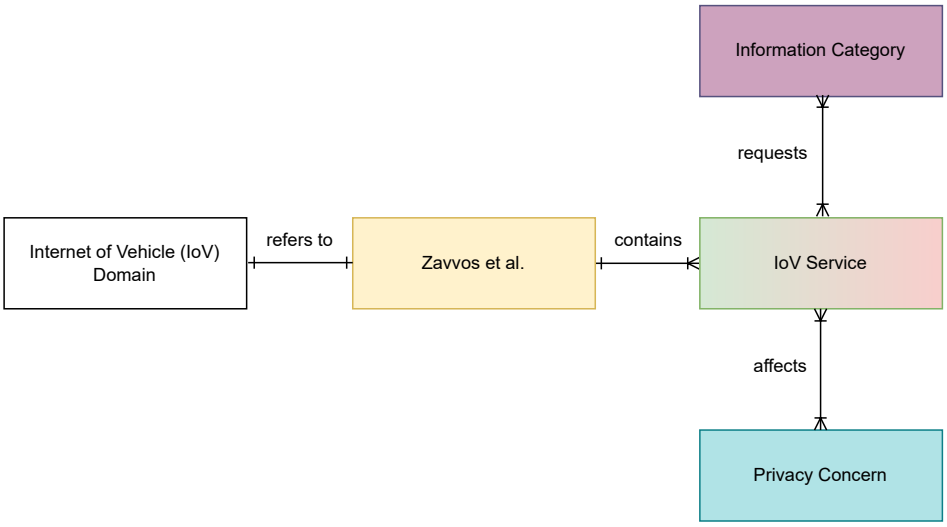


Figure 2: Relational Model for IoV.

2.9 Contrastive Analysis

The relational models presented in Section 2.8 serve as the foundation for conducting a contrastive analysis between the privacy landscapes of ITS and IoV. For the sake of clarity, this Section is conveniently structured into two subsections. The first subsection provides a contrastive analysis of the two relational models at a macroscopic level, outlining their broad structural and thematic differences. The second subsection delves into a detailed contrastive analysis, examining the specific elements and implications of each model in depth, along with privacy considerations.

2.9.1 Macroscopic Analysis

We undertake an initial comparative analysis at a macroscopic level between the relational models. As stated in Section 2.8, both the relational models are affected by the selected documents, i.e. the ETSI standards and the work by Zavvos et al., which clearly imply some restrictions in terms of completeness, a well-known open problem in the field of modelling. In particular, the model for ITS reflects the European landscape as it leverages the ETSI ITS G5 standards. By contrast, the model for IoV is based on the contribution by Zavvos et al. Both choices introduce inherent limitations to the models, as they may not fully encapsulate global ITS and IoV privacy issues. Additionally, the relational models depend on the availability and accuracy of current literature, which may not completely represent the rapidly evolving IoV landscape. Nevertheless, their structured approach

facilitates a comprehensive understanding and analysis, enabling effective navigation through the complexities of ITS and IoV, and ultimately fostering innovation in these domains.

Moreover, a disparity in dimensionality between the two models exists, attributable to the comprehensive structure provided by ETSI standards in contrast to the nascent IoV paradigm. The relational model for ITS exhibits a considerable breadth of entities and relationships, indicative of a robust and well-defined structure. Conversely, the relational model for IoV, existing solely as a paradigm, lacks the formalised structure and depth characteristic of established standards such as those promulgated by ETSI.

The originality of the model for IoV lies in its capacity to adapt within the evolving landscape of transportation technologies, leveraging the embryonic state of IoV to pioneer novel approaches and address emerging challenges with agility and foresight.

2.9.2 Detailed Analysis

By analysing the relational models for ITS and IoV at a microscopic level, both similarities and disparities emerge. A first similarity is the inclusion of the documents in both the models: in the model for ITS we have the ETSI standards, while in the model for IoV just the contribution by Zavvos et al.. In Figures 1 and 2, the entities representing these documents are highlighted in yellow.

It is noteworthy to highlight that the entities Application and Use Case, included in the model for ITS, are missing in the model for IoV. In fact, both these entities are integrated into the IoV Service entity. For example, the IoV service "Driver Assistance" is comparable with the application "Driving assistance". By contrast, the IoV service "Safety Warnings" can be mapped to the use case "Wrong way driving warning". The double nature of IoV Service is illustrated in Figure 2, where the entity has a double colour of green-red, with green representing the equivalence with Application and red with Use Case. Hence, the lack of rigour in the classification of the IoV services from Zavvos et al. finds a mitigation in our relational models. The remaining entities of the models for ITS and IoV are coloured differently, as we cannot identify any similarities.

Moreover, a notable absence in the relational model for IoV is the concept of Application Class, which holds significance in the ITS framework. In fact, the ETSI ITS G5 Basic Set of Applications groups Applications into distinct classes, i.e., Active road safety and Cooperative traffic efficiency, Co-operative local services, Global internet services, to facilitate organised categorisation. However, in the IoV context, the conventional notion of an Application undergoes a transformative shift. As described above, Application is redefined under IoV Service, encompassing a broader spectrum of functionalities and services tailored to the IoV ecosystem.

Unlike the ETSI ITS G5, where the delineation and standardisation of a Protocol Stack play a pivotal role, the IoV paradigm lacks a definitive network architecture. While numerous researchers propose various design schemes for IoV architectures [17], a unanimous consensus remains elusive. Consequently, the absence of an accepted Protocol Stack precludes its inclusion in the relational model for IoV.

Furthermore, in contrast to the relational model for ITS, where Message types, such as Cooperative Awareness Message (CAM) and Decentralised Environmental Notification Message (DENM), serve as integral components within the Protocol Stack hierarchy, their absence in the relational model for IoV is conspicuous. This omission is intrinsically linked to the absence of an established Protocol Stack in the IoV domain.

Finally, the entity Privacy Concern is present only in the model for IoV, reflecting Zavvos et al.'s inclusion of privacy concerns in their treatment of IoV. By contrast, the ETSI ITS standards lack of a thorough consideration of privacy, as evidenced by the missing Privacy Concern entity in the model for ITS.

When observing the specific applications and use cases included in the ETSI ITS G5 Basic Set of Applications alongside the IoV services provided in Zavvos et al., the transition from ITS to IoV translates to an increase in the number of applications, which in turn implies an extension of the use cases. Consequently, we identify a set of IoV services with no counterpart in the ITS domain. These IoV services are: Parking Finder, Intention-aware routing, Cooperative charging, Vocal warnings, Sensing tasks, Voice chat.

2.10 Categorisation of the Relevant Attributes

By leveraging the analyses outlined above, several privacy issues that require attention can be identified:

- *Data collection and storage*: In the transition from ITS to IoV, there arises a pressing need for the collection of an expanding volume of data. This encompasses a spectrum ranging from vehicle location and speed to driver behaviour and environmental conditions. However, the proliferation of connected devices and sensors in IoV exacerbates concerns regarding the scope and sensitivity of data being gathered. This influx of data raises questions about the necessity and proportionality of data collection practices, as well as the adequacy of measures to anonymise or pseudonymise personally identifiable information. Furthermore, storing this data poses risks of security breaches leading to unauthorised access, and raises concerns about long-term retention.

- *Data sharing and access control*: The seamless connectivity inherent in IoV facilitates the sharing of data among various stakeholders, including government agencies, transportation operators, and third-party service providers. While data sharing holds promise for enhancing traffic management and fostering innovation, it also heightens concerns about data security and privacy. Issues such as inadequate access controls, insufficient encryption, and unclear data ownership rights can lead to unauthorised data access and misuse, potentially compromising individuals' privacy.

- *Privacy policies and consent mechanisms*: Effective privacy protection requires clear and comprehensive privacy policies that outline how data will be collected, used, and shared within IoV ecosystem. Addressing the lack of transparency and specificity in these policies is crucial [3]. Moreover, consent mechanisms for data collection and processing may be insufficient, leaving users unaware of the extent to which their data is being utilised and without meaningful options to exercise control over their personal information.

- *Privacy-by-design*: Privacy-by-design principles advocate for the integration of privacy safeguards into the design and development of IoV systems from their inception. While such principles hold promise for mitigating privacy risks, their implementation remains uneven across different applications and contexts. Inadequate attention to privacy considerations during system design can result in vulnerabilities and loopholes that undermine individuals' privacy rights.

- *User awareness and control*: Central to ensuring privacy in IoV environment is the empowerment of users with awareness and control over their personal data. Yet, user awareness campaigns and educational initiatives regarding privacy risks and protective measures are often lacking. Moreover, the absence of user-friendly tools and interfaces for managing data preferences and consent settings further diminishes users' ability to exert control over their privacy.

These privacy issues can be addressed simultaneously by considering the following CAM and DENM categories

CAM Categories

- **Protocol and Message Management**: It manages the protocol-specific information necessary for ensuring the correct decoding and identification of messages. It may include the *protocolVersion*, *messageID* fields;

- **Vehicle Characteristics**: It describes the physical and operational characteristics of the vehicle originating from the CAM. It may include the *stationID*, *stationType*, *vehicleRole*, *specialTransportType*, *dangerousGoodsBasic* fields;

- **Vehicle Positioning**: It relates to the geographical location and lane placement of the vehicle. It may include the *referencePosition* and *lanePosition* fields;
- **Vehicle Control and Status**: It provides information on the control mechanisms and status indicators of the vehicle. It may include the *accelerationControl*, *exteriorLights* and *embarkationStatus* fields.
- **Timing**: It relates to the timing aspects. It may include the *generationDeltaTime* and *performanceClass* fields;
- **Vehicle Movement**: It provides detailed information about the vehicle's movement and dynamics. It may include the *speed*, *pathHistory*, *driveDirection* fields.
- **Interference Mitigation**: It manages and mitigates potential interference with other systems, particularly those operating in similar frequency bands. It may include the *protectedCommunicationZoneRSU* field.
- **Road and Traffic Conditions**: It relates to the current state and regulations of the road network and traffic environment. It may include the *closedLanes*, *emergencyPriority*, *speedLimit* fields.

DENM Categories

- **Vehicle Characteristics**: It describes the physical characteristics and specific configurations of the vehicle involved in the detected event. It may include the *carryingDangerousGoods*, *vehicleMass*, *vehicleIdentification* fields;
- **Vehicle Occupancy**: It describes the presence and distribution of occupants within a vehicle. It may include the *numberOfOccupants* and *positionOfOccupants* fields;
- **Event Spatial References and Positioning**: It refers to the geographical data and positioning details associated with an event. It may include the *eventHistory*, *positioningSolution* fields;
- **Event Environmental Conditions**: It refers to the external factors that describe the physical state of the surroundings at a given location and time. It may include the *externalTemperature* field;
- **Event Dynamics**: It refers to monitoring and analysing the dynamic behaviour of detected events. It may include the *eventSpeed*, *relevanceTrafficDirection* fields;
- **Road Type**: It provides information about the specific type of road at the event's location. It may include the *roadType* field;
- **Event Types and Causes**: It encompasses the types and causes of detected events. It may include the *eventType*, *incidentIndication* fields;
- **Transmission Details**: It provides details about the transmission of DENM messages. It may include the *transmissionInterval*, *requestResponseIndication* fields;
- **Information Reliability**: It indicates the likelihood of detected events being accurate and reliable. It may include the *informationQuality* field;
- **Timing**: It relates to the timing aspects of detected events. It may include the *detectionTime*, *referenceTime* fields;
- **Event Identifiers**: It uniquely identifies events across different DENMs. It may include the *actionID* and *referenceDENMs* fields;

- **Protocol and Message Management**: It manages the protocol-specific information necessary for ensuring the correct decoding and identification of messages. It may include the *protocolVersion* and *messageID* fields;
- **Roadwork Details**: It refers to the specific conditions and regulations associated with roadwork zones. It may include the *trafficFlowRule*, *speedLimit*, *closedLanes* fields.

2.11 Intermediate Findings: the Attributes

It is now reasonable to appeal to CAM and DENM message types to define an innovative and privacy-preserving approach to authorising users to refuel their cars based on a hybrid identity-based + attribute-based authentication approach. In short, we observe that the uniqueness of CAM and DENM messages that characterise a specific vehicle can be profitably leveraged to authorise the vehicle throughout the evaluation of dynamic policies.

3 General Background

3.1 Attribute-Based Authentication (ABA)

Attribute-Based Authentication (ABA) is an approach to authentication and access control in which access is granted not based on the identity of the user, but on the possession and verification of specific attributes. These attributes can be static (e.g., age, role, membership level) or dynamic (e.g., account balance, usage history, time of access), and are evaluated at the time of the request. Unlike identity-based models, ABA does not require the user to reveal or prove their personal identity; instead, access is authorised based on contextual or behavioural conditions. In many cases, credentials are non-nominal and associated with tokens, devices, or sessions rather than individuals. This method supports privacy-by-design principles by minimising personal data exposure, avoiding unnecessary profiling, and enabling selective disclosure of information. ABA is particularly suited to environments where personalisation, eligibility, or conditional access are required—such as in digital services, marketing systems, or IoT networks—offering a flexible and privacy-preserving alternative to traditional identity-centric authentication.

3.2 Dynamic Policies

Authentication and authorisation mechanisms often rely on dynamic policy models to govern access. Dynamic policies evaluate contextual factors during each access attempt—such as device posture, geolocation, time of access, or recent activity—to make real-time decisions. This enables more granular, risk-aware authorisation aligned with zero trust principles. For example, a user might be authenticated successfully, but access to sensitive resources could be denied if the request originates from an untrusted device or an unusual location. Dynamic policy enforcement is particularly valuable in environments with fluctuating threat landscapes or distributed workforces, allowing security systems to adjust access decisions on the fly without manual intervention.

3.3 Zero Knowledge Approaches

Zero-knowledge approaches aim to minimise the amount of sensitive information exposed or stored during authentication and authorisation processes. Functionally, a zero-knowledge authentication system allows a user to prove their identity without revealing actual credentials, reducing the attack surface for credential theft, replay attacks, and insider threats. From a security perspective, this means systems can verify access rights without having to centrally store secrets such as passwords or private keys. In zero-knowledge authorisation, the principle extends to verifying that a user or device is allowed to perform a specific action without disclosing why or under what identity—useful in privacy-preserving architectures and zero trust environments. Emerging implementations, especially in decentralised identity systems, leverage these approaches to ensure that neither the verifier nor intermediaries learn more than necessary, aligning with the principle of least privilege and enhancing overall system resilience.

4 Main Relevant Technologies in the Digital Fuel Distribution Sector

Over the last decade, the fuel distribution sector has undergone a significant process of plant automation and computerisation of management systems and related administrative procedures. Suffice it to think of the so-called "ghost" service stations, which remain operational even in the absence of operators, the computerisation of excise duties, or electronic invoicing, which saw the sector among the "early adopters". The main technologies and operational flows involved in payment systems in the automotive sector, and involved in various ways in the processes referred to in this analysis, are described in the following subsections.

4.1 SmartCards

SmartCards are payment and loyalty tools specific to the automotive sector. For a functional description, please refer to the following paragraphs. From a technological point of view, they can be divided into two types: "physical" and "virtual." Physical cards are plastic cards equipped with a magnetic strip and contact chip (SLE44442) or NFC (NTAG 213). Virtual cards are dematerialised cards that can only be used via mobile apps.

4.2 EFT POS Terminals

EFT-POS (Electronic Funds Transfer at Point of Sale) terminals are devices capable of reading payment cards from various circuits and establishing a secure connection and communication with authorisation servers that verify the availability of funds on the card read, authorising or denying payment, and updating balances at the end of the transaction.

4.3 OPTs – Outdoor Payment Terminals

OPTs are payment instruments now found in almost all service stations. They allow payments to be accepted using smart cards issued by various providers, enabling fuel to be dispensed without the need for an operator, thus ensuring that the point of sale is operational 24 hours a day.

4.4 Trackfuel

Trackfuel [23] is an innovative technology designed to monitor and manage fuel refills for company vehicles, ensuring safety, traceability, and accuracy in consumption. The system consists of a device installed on the car and a gateway located at the fueling point, which together verify that fuel is dispensed only into the authorised tank. With Trackfuel, companies can automate fuel management, prevent fraud and waste, monitor consumption in real time, and simplify fiscal accounting, making fleet management more efficient.

Trackfuel offers a fully automated and contactless payment system for fuel refills. Users do not need to present any card, app, or cash at the time of fueling. The system verifies the vehicle and authorises the transaction electronically, simplifying the payment process and reducing administrative overhead. This allows companies to streamline fuel management while ensuring secure and efficient operations.

4.5 Mobile APP

Users are also given the option of using a mobile app that makes it easier to manage certain operations while on the road. For example:

- Identify the points of sale that accept smart cards in your area, as a means of payment or recognition.
- Check the credit availability on your account.

- View details of the latest transactions.
- Make payments in both "Self" and "Served" modes.

4.6 General Cybersecurity properties

The described technologies are strictly related to the following cybersecurity properties:

The following security properties are mapped from the MSC flows.

- **Confidentiality (C)**: for protecting data.
- **Integrity (I)**: for prevening tampering.
- **Authentication (A)**: for terminal identification.
- **Non-repudiation (NR)**: useful in disputes.

4.7 General Privacy Properties

The privacy principles discussed in this work are grounded in a set of internationally recognised frameworks, standards, and legal instruments. At the core lies the European Union's General Data Protection Regulation (GDPR) [9], particularly Article 5, which defines the fundamental principles of lawful data processing, including data minimisation, purpose limitation, and storage limitation. Complementing the GDPR, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [11] provide a foundational soft-law reference, influencing global privacy regimes by articulating key principles such as collection limitation, use limitation, and accountability. Additionally, the ISO/IEC 29100 Privacy Framework [16] offers a formalised set of privacy principles designed for implementation in information systems, aligning technical and organisational measures with data protection requirements. In the North American context, the NIST Privacy Framework [18] further supports these principles by offering a risk-based, outcome-oriented approach for managing privacy risks in alignment with cybersecurity practices.

By integrating the common principles of these documents, we obtain the following privacy properties:

- **Collection Limitation:** Personal data must be collected only for specific, legitimate, and necessary purposes.
- **Data Minimisation:** Only the minimum necessary personal data should be processed.
- **Purpose Limitation:** Data must only be used for the purposes explicitly specified at the time of collection.
- **Transparency:** Individuals must be informed about how their data is collected, used, stored, and shared.
- **Individual Control:** Data subjects must be able to access, correct, or delete their personal data.
- **Accountability:** Data controllers must demonstrate compliance with privacy regulations and principles.
- **Storage Limitation:** Personal data must not be kept longer than necessary for the intended purposes.
- **Security of Processing:** Appropriate technical and organisational measures must be applied to protect personal data.

5 Case Study: dematerialised payment system

This deliverable analyses a case study that is fundamentally different from that of Deliverable D2.1, despite the fact that the two case studies share the same functional objective, that is, to refuel securely. While the previous deliverable focused on the use of fuel cards and loyalty cards as a payment means, the present case study delves into the notion of dematerialised payments, which are meant to enable users to refuel and pay later without showing a specific payment card. The car becomes completely smart thanks to a refuelling system called Trackfuel [23], which allows the vehicle to be recognised, identified, and paid only for the amount of fuel emitted, without presenting a specific card. Payments would become completely smart as well as digital, with the car itself becoming the means of making the payment.

The case study is illustrated in Figure 3.

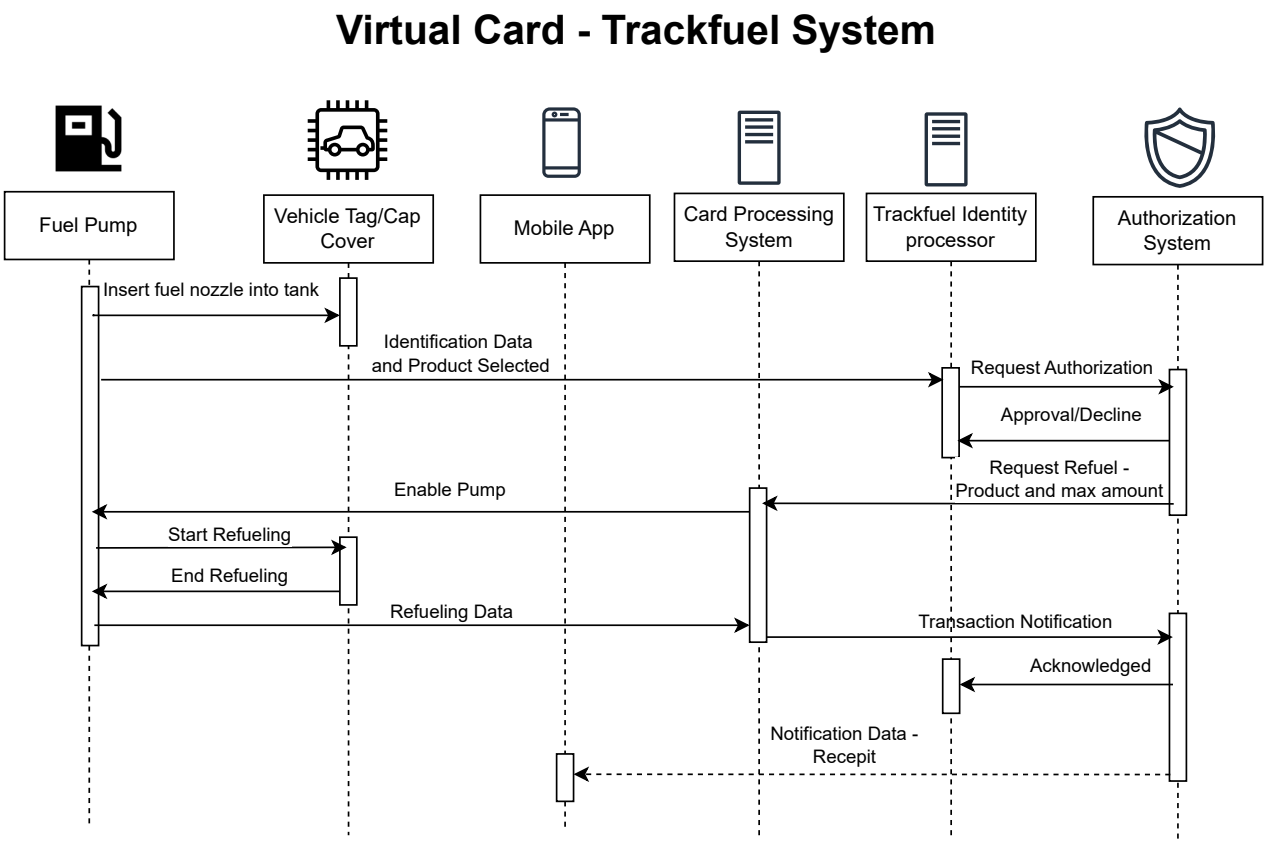


Figure 3: Fuel refilling and payments within smart cars

As done for Deliverable D2.1, for the case study, we describe the actors and operations involved with MSC diagrams, along with a cybersecurity and privacy analysis.

5.1 Actors

- **Fuel Pump** (dispenser controller).
- **Vehicle Tag/ Cap Cover** (object for the identification through Trackfuel).
- **Mobile App** (system for payment).
- **Card Processing System** (CPS; payment/acquirer gateway for transaction orchestration).

- **Trackfuel Identity Processor** (system for identity processing).
- **Authorisation System** (issuer/authoriser or network service providing approval/decline).

5.2 Steps

- **Fuel Pump → Vehicle Tag/Cap Cover:** ***Insert fuel nozzle into tank.*** This action initiates the fueling process.
- **Fuel Pump → Mobile App:** ***Trackfuel Identity.*** Customer identity is transmitted via the vehicle tag or fuel cap.
- **Mobile App → Card Processing System:** ***Identification Data and Product Selected.*** App sends user identity and selected product type.
- **Card Processing System → authorisation System:** ***Request authorisation.*** Processor requests payment approval.
- **authorisation System → Card Processing System:** ***Approval/Decline.*** authorisation system replies with transaction decision.
- **Card Processing System → Fuel Pump:** ***Enable Pump.*** Fuel pump is enabled for authorized transaction.
- **Fuel Pump → Customer:** ***Start Refueling.*** Customer begins dispensing fuel.
- **Fuel Pump → Customer:** ***End Refueling.*** Customer completes fueling by returning nozzle.
- **Fuel Pump → Card Processing System:** ***Refueling Data.*** Pump sends fuel volume and product data.
- **Card Processing System → authorisation System:** ***Transaction Notification.*** authorisation system is notified of completed transaction.
- **authorisation System → Card Processing System:** ***Acknowledged.*** Receipt issuance is confirmed.
- **Card Processing System → Mobile App:** ***Notification Data – Receipt.*** Customer receives a digital receipt in the mobile app.

5.3 Cybersecurity and privacy analysis

Table 1: Communication Steps, Protocols, and Security Properties

Step	Protocol	Guaranteed Properties
POS → Cloud (direct)	TLS mutual + AES/3DES	C, I, A, NR
APP mobile → API cloud	TLS 1.2 + JWT	C, I, A, NR
API cloud → Third parties	TLS mutual	C, I, A, NR

Table 1 summarises the main communication steps within the system, the protocols employed at each step, and the security properties they guarantee. The first step involves the direct communication between the POS and the cloud, secured using mutual TLS and symmetric encryption via AES or 3DES. This channel ensures the properties of confidentiality, integrity, authentication, and non-repudiation (denoted as C, I, A, NR). The

second step occurs between the mobile app and the cloud API, where the connection relies on TLS 1.2 and JWT for authentication. All major security properties are guaranteed in this channel as well. Finally, the third step concerns the communication between the cloud API and external third parties, also protected by mutual TLS, again ensuring confidentiality, integrity, authentication, and non-repudiation.

Table 2: Overview of Data Types, Purposes, and Legal Bases

Data	**Type**	**Purpose**	**Legal Basis**
Vehicle Plate Number	Personal Data	Vehicle identification	Contractual (Art. 6.1.b GDPR)
GPS Position (APP)	Sensitive Data	Location-based services	Explicit Consent (Art. 6.1.a)
VIN (PAN-like)	Pseudonymised Data	Authentication and authorisation	Contractual
PIN	Sensitive Data	Transaction security	Contractual + Security

Table 2 provides an overview of the different types of data collected in the system, their purposes, and the legal bases for processing them.

The first entry refers to the vehicle plate number, classified as personal data, which is used for vehicle identification. Its processing is based on a contractual obligation according to Article 6.1.b of the GDPR.

The second entry concerns the GPS position collected by the mobile app. This is considered sensitive data and is used to provide location-based services. Its processing relies on explicit consent from the user (Art. 6.1.a GDPR). The third entry is the VIN (Vehicle Number Identifier), which is treated as pseudonymised data. It is used for authentication and authorisation purposes, and its processing is justified on a contractual basis. Finally, the PIN is classified as sensitive data and is used to ensure transaction security. Its processing is necessary for contractual and security purposes.

6 Combining Identity-Based Authentication with Attribute-Based Authentication over a dematerialised payment system

6.1 Approach

In a system, Identity-Based Authentication (IBA) is used to verify the driver or the vehicle, often through card IDs, PINs, or registered vehicle information. While this ensures operational accountability, it can expose sensitive identity information.

In an Attribute-Based Authentication (ABA) system, access and authorisation are determined by evaluating specific attributes rather than fixed identities. These attributes can include vehicle characteristics, operational roles, or contextual parameters such as time, location, or fueling capacity. Unlike traditional identity-based approaches, ABA allows for a more flexible and privacy-preserving model, where authorisation depends on whether the entity satisfies predefined attribute conditions, not on who the entity is. When integrated with a zero-knowledge (ZK) framework, ABA enables verification of attribute possession without exposing the underlying data, thus minimising privacy risks. Dynamic attribute policies, such as fuel quotas per vehicle type or adaptive authorisation levels, complement this model by providing fine-grained, context-aware control over fueling operations.

In the Trackfuel system, where fuel payments are fully dematerialised and occur without physical cards or manual input, authentication and authorisation are achieved through a combined Identity-Based Authentication (IBA) and Attribute-Based Authentication (ABA) model. Initially, IBA is used to authenticate the vehicle through its unique Vehicle Identification Number (VIN), ensuring that only registered and trusted entities can initiate a fueling session. Once authenticated, the system transitions to an ABA stage, where dynamic policies are evaluated against contextual and operational attributes derived from vehicular communication standards such as Cooperative Awareness Messages (CAM) and Decentralised Environmental Notification Messages (DENM). These attributes were identified and widely discussed in Section 2.10. In particular, we note the use of categories that discriminate against allowing a user to refuel. Among these, from CAM and DENM, we might consider the following fundamentals: *specialTransportType*, *dangerousGoodsBasic*, and *carryingDangerousGoods*, which determine the type of material a vehicle can transport.

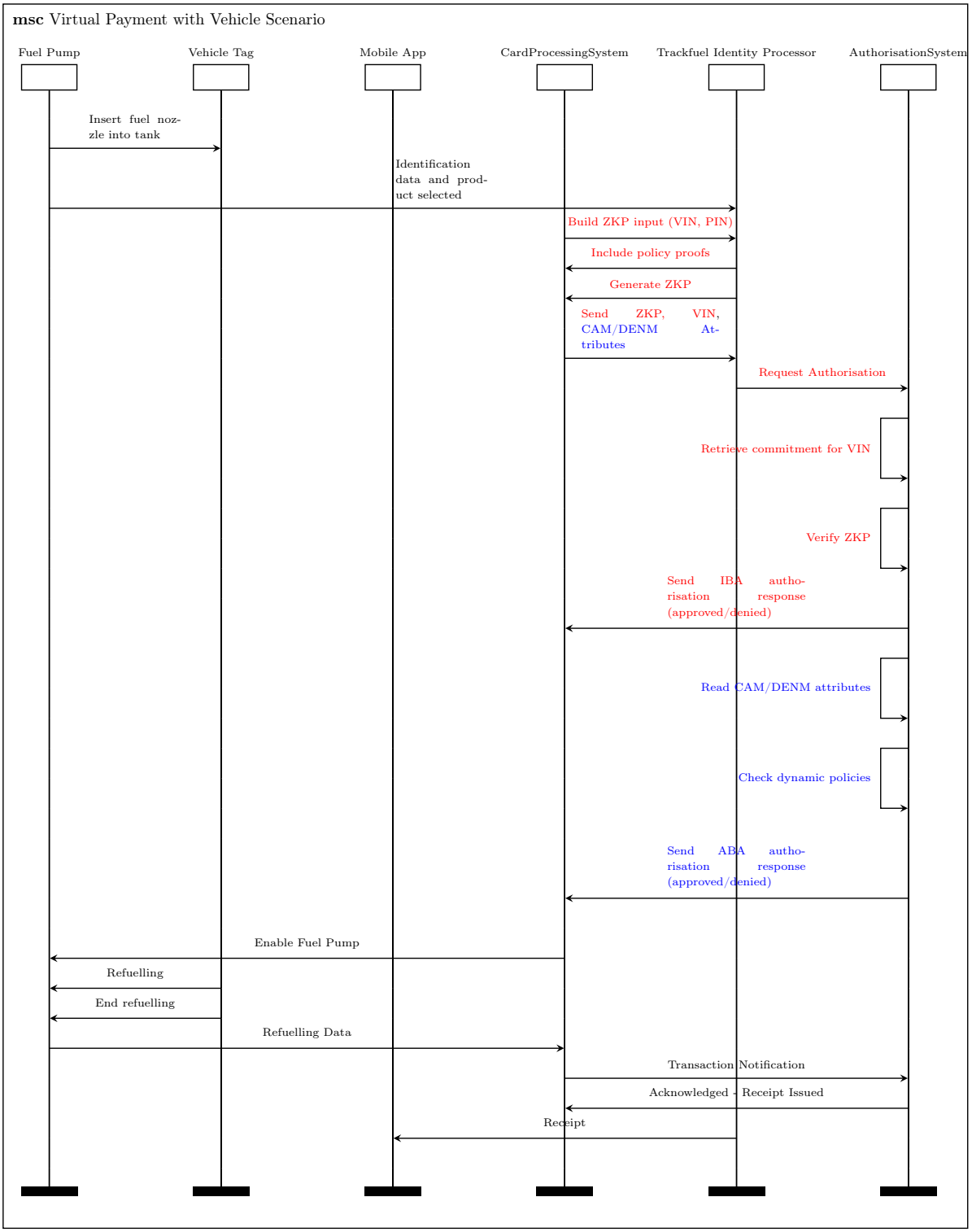
Based on these factors, the system authorises or denies the refuelling request in accordance with policy rules and safety constraints. This layered approach ensures that authentication establishes identity, while authorisation enforces compliance with adaptive, context-aware attribute policies. Relying solely on ABA would be insufficient, as attribute verification alone cannot guarantee entity legitimacy; hence, the combination of IBA and ABA provides both strong identity assurance and flexible policy enforcement.

To preserve privacy and security during these processes, Zero-Knowledge Proofs (ZKPs) are employed to protect sensitive data, such as vehicle identifiers and operational attributes, from disclosure. Each vehicle or user is issued a credential by a trusted authority, which embeds signed attributes and static constraints, such as authorised service categories or refuelling permissions. During each transaction, the vehicle generates a ZKP that proves compliance with dynamic policies without revealing the underlying values. Numerical constraints (e.g., fuel amount $\leq$ 100 L) are verified using *range proofs*, whereas categorical or membership conditions are validated via *equality* or *set membership proofs*.

6.2 Design

The message sequence chart in Figure 4 highlights two main operational stages in the Trackfuel virtual payment scenario: the **Identity-Based Authentication (IBA)** phase, indicated in red, and the **Attribute-Based Authorisation (ABA)** phase, shown in blue. The following list details the logic and purpose of the main interactions in both stages.

Figure 4: Trackfuel system augmented with zero-knowledge proof and dynamic policies



- **Build ZKP input (VIN, PIN):** The Trackfuel Identity Processor collects the vehicle's unique Vehicle Identification Number (VIN) and any confidential identifiers (e.g., PIN or private key) to construct the input for the Zero-Knowledge Proof (ZKP). This step establishes the link between the physical vehicle and its digital identity, without disclosing sensitive data.
- **Include policy proofs:** Static rules, such as maximum refueling quantity or vehicle role, are embedded within the credential as signed attributes. These constraints are included in the ZKP to ensure that subsequent authorisation is consistent with pre-defined operational limits.
- **Generate ZKP:** The Identity Processor generates the ZKP locally, proving the vehicle's authenticity and compliance with embedded policies. This guarantees that the authentication is privacy-preserving and non-interactive.
- **Send ZKP, VIN, and ABA attributes:** The vehicle sends the generated proof together with its VIN and preliminary operational attributes to the processing infrastructure. This transmission initiates the verification process by the Authorisation System.
- **Request authorisation, retrieve commitment for VIN, and verify ZKP:** The Authorisation System retrieves the stored cryptographic commitment associated with the VIN and verifies the received ZKP against it. Successful verification authenticates the vehicle (IBA), proving that it is registered and authorised to participate in the Trackfuel network.
- **Send IBA authorisation response (approved/denied):** Once the ZKP is validated, the Authorisation System returns the authentication result to the Transaction Processor. This marks the end of the IBA phase and enables the start of dynamic attribute evaluation.

Following successful authentication, the process transitions to the **ABA (Attribute-Based Authorisation)** phase, represented by blue messages in the MSC. Here, the system evaluates contextual data and dynamic conditions before enabling fuel delivery.

- **Read ABA attributes:** The Authorisation System collects operational and contextual data derived from vehicular communication standards such as CAM and DENM messages. These attributes may include the vehicle's category, cargo type (e.g., goods transport, hazardous materials), or mission status.
- **Check dynamic policies:** The system evaluates adaptive policies against the received attributes — for example, authorising refueling only if the vehicle is engaged in an approved transport mission or located in a designated fueling area. This enforces contextual compliance and safety rules at runtime.
- **Send ABA authorisation response (approved/denied):** After evaluating all conditions, the Authorisation System issues the final decision, approving or rejecting the refueling request. Only vehicles satisfying both identity verification (IBA) and dynamic policy constraints (ABA) are allowed to activate the fuel pump.

Through this two-layered mechanism, Trackfuel achieves a secure and privacy-preserving dematerialised payment process, ensuring that each refueling transaction is both legitimate (IBA) and contextually compliant (ABA).

7 Conclusions

This deliverable modelled the privacy landscape of the Internet of Vehicles by grounding the analysis in the established Intelligent Transportation Systems paradigm and extracting the core entities, trust assumptions, and general data-flow that shape modern vehicular ecosystems. Building on this structured landscape, the deliverable motivated an attribute-centric approach to identity and authorization by identifying which contextual and operational properties are most relevant for privacy-preserving access control. The work then assessed enabling cryptographic and system technologies for digital fuel distribution, such as Zero-Knowledge Proof techniques as a rigorous means to prove possession of required information without revealing it. The deliverable continued by consolidating the findings in a concrete case study on dematerialised fuel payments, hence without a traditional payment means such as a credit card.

In its final section, the deliverable introduced an enhanced, innovative security protocol for dematerialised fuel payment and access workflows by tightly combining Attribute-Based Authentication with Zero-Knowledge Proofs of knowledge and dynamic, context-aware policies. This design supports selective disclosure and unlinkability by allowing a prover to demonstrate compliance with policy-required attributes (and/or knowledge statements) while minimizing information leakage, and by enabling policies to adapt over time and context (e.g., station rules, regulatory conditions, risk posture) — most notably, everything without re-issuing static credentials. Within our framework, suitable and operationally meaningful attributes can profitably include the vehicle's category as well as the cargo type, thereby enabling fine-grained authorization decisions that remain privacy-preserving yet fully supporting safety, liability, and compliance needs.

References

[1] Sebastian Bittl and Arturo A Gonzalez. Privacy endangerment from protocol data sets in vanets and countermeasures. In *Smart Cities, Green Technologies, and Intelligent Transport Systems: 4th International Conference, SMARTGREENS 2015, and 1st International Conference VEHITS 2015, Lisbon, Portugal, May 20-22, 2015, Revised Selected Papers 4*, pages 304–321. Springer, 2015.

[2] Abdelwahab Boualouache, Sidi-Mohammed Senouci, and Samira Moussaoui. A survey on pseudonym changing strategies for vehicular ad-hoc networks. *IEEE Communications Surveys & Tutorials*, 20(1):770–790, 2018.

[3] Talal Ashraf Butt, Razi Iqbal, Khaled Salah, Moayad Aloqaily, and Yaser Jararweh. Privacy management in social internet of vehicles: Review, challenges and blockchain based solutions. *IEEE Access*, 7:79694–79713, 2019.

[4] Ruben Cacciato, Mario Raciti, Sergio Esposito, and Giampaolo Bella. Modelling the privacy landscape of the internet of vehicles. In *Proceedings of the 19th International Conference on Availability, Reliability and Security*, ARES '24, New York, NY, USA, 2024. Association for Computing Machinery.

[5] Min Chen, Yuanwen Tian, Giancarlo Fortino, Jing Zhang, and Iztok Humar. Cognitive internet of vehicles. *Computer Communications*, 120:58–70, 2018.

[6] ETSI. ETSI ITS G5.

[7] ETSI. ETSI TR 102 638 V1.1.1 (2009-06); Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions.

[8] ETSI. Intelligent Transport Systems.

[9] European Parliament and Council. Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (general data protection regulation). `https://eur-lex.europa.eu/eli/reg/2016/679/oj`, 2016. Official Journal of the European Union.

[10] Bruno Fernandes, Joao Rufino, Muhammad Alam, and Joaquim Ferreira. Implementation and analysis of ieee and etsi security standards for vehicular communications. *Mobile Networks and Applications*, 23:469–478, 2018.

[11] Organisation for Economic Co-operation and Development. Oecd guidelines on the protection of privacy and transborder flows of personal data. `https://www.oecd.org/privacy/oecd_privacy_framework.pdf`, 2013. Updated Guidelines.

[12] Tanvi Garg, Navid Kagalwalla, Prathamesh Churi, Dr. Ambika Pawar, and Sanjay Deshmukh. A survey on security and privacy issues in iov. *International Journal of Electrical and Computer Engineering (IJECE)*, 10:5409, 10 2020.

[13] Catalin Gosman, Ciprian Dobre, and Florin Pop. Privacy-preserving data aggregation in intelligent transportation systems. In *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pages 1059–1064, 2017.

[14] Dalton Hahn, Arslan Munir, and Vahid Behzadan. Security and privacy issues in intelligent transportation systems: Classification and challenges. *IEEE Intelligent Transportation Systems Magazine*, 13(1):181–196, 2021.

[15] IEEE. Ieee standard for wireless access in vehicular environments–security services for applications and management messages. *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, pages 1–240, 2016.

[16] International Organization for Standardization. Iso/iec 29100:2011 - information technology — security techniques — privacy framework. `https://www.iso.org/standard/45123.html`, 2011. International Standard.

[17] Baofeng Ji, Xueru Zhang, Shahid Mumtaz, Congzheng Han, Chunguo Li, Hong Wen, and Dan Wang. Survey on the internet of vehicles: Network architectures and applications. *IEEE Communications Standards Magazine*, 4(1):34–41, 2020.

[18] National Institute of Standards and Technology. Nist privacy framework: A tool for improving privacy through enterprise risk management. `https://www.nist.gov/privacy-framework`, 2020. Version 1.0, U.S. Department of Commerce.

[19] Aleksandr Ometov, Sergey Bezzateev, Vadim Davydov, Anna Shchesniak, Pavel Masek, Elena Simona Lohan, and Yevgeni Koucheryavy. Positioning information privacy in intelligent transportation systems: An overview and future perspective. *Sensors*, 19(7), 2019.

[20] Jonathan Petit, Florian Schaub, Michael Feiri, and Frank Kargl. Pseudonym schemes in vehicular networks: A survey. *IEEE Communications Surveys & Tutorials*, 17(1):228–255, 2015.

[21] Matthew N. O. Sadiku, Nishu Gupta, Kirtikumar K. Patel, and Sarhan M. Musa. *An Overview of Intelligent Transportation Systems in the Context of Internet of Vehicles*, pages 3–11. Springer International Publishing, Cham, 2021.

[22] Lion Silva, Naercio Magaia, Breno Sousa, Anna Kobusińska, António Casimiro, Constandinos X. Mavromoustakis, George Mastorakis, and Victor Hugo C. de Albuquerque. Computing paradigms in emerging vehicular environments: A review. *IEEE/CAA Journal of Automatica Sinica*, 8(3):491–511, 2021.

[23] 3IVM S.r.l. Trackfuel. `https://www.trackfuel.it/`, 2025. Accessed: 2025-10-13.

[24] Yunchuan Sun, Lei Wu, Shizhong Wu, Shoupeng Li, Tao Zhang, Li Zhang, Junfeng Xu, and Yongping Xiong. Security and privacy in the internet of vehicles. In *2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)*, pages 116–121, 2015.

[25] Hamideh Taslimasa, Sajjad Dadkhah, Euclides Carlos Pinto Neto, Pulei Xiong, Suprio Ray, and Ali A. Ghorbani. Security issues in internet of vehicles (iov): A comprehensive survey. *Internet of Things*, 22:100809, 2023.

[26] Wikipedia. Crow's Foot Notation.

[27] W. Wu, Z. Yang, and K. Li. Chapter 16 - internet of vehicles and applications. In Rajkumar Buyya and Amir Vahid Dastjerdi, editors, *Internet of Things*, pages 299–317. Morgan Kaufmann, 2016.

[28] Efstathios Zavvos, Enrico H. Gerding, Vahid Yazdanpanah, Carsten Maple, Sebastian Stein, and m.c. schraefel. Privacy and trust in the internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 23(8):10126–10141, 2022.