Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

Future generation Security for smart and connected Cars - FuSeCar

Deliverable D2.1: Privacy-enhanced authentication protocols based on Zero-Knowledge approaches that support identity-based authentication and authorization through dynamic policies

WP2: Privacy enhancement of current vehicular communication protocols and architectures

Authors:
Giampaolo Bella
`giampaolo.bella@unict.it`

Department of Mathematics and Informatics
University of Catania

Current revision: R0.1
Delivery date: September 23st, 2024

Revision history

Authors	Changes	Date	Revision
Giampaolo Bella	First draft of the deliverable structure	May 17th, 2024	R0.1
Giampaolo Bella	First draft of the deliverable	July 19th, 2024	R0.1
Giampaolo Bella	Refinements and update	November 14th, 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 on the use of Identity-Based Authentication over four case studies drawn from the automotive sector in the area of payment and loyalty cards. The case studies are drawn from the real world, also thanks to the external consultancy benefited from during the project.

Moreover, the document continues by investigating the use of Zero-Knowledge Proofs (ZKPs) to enable a prover to confirm knowledge of relevant items to a verifier without disclosing additional information to the verifier. It follows that the Customer, who is the credit card holder, manages to prove that their card is genuine to the transaction's Authorisation System.

1.1 Context, challenges and motivation

Digitisation and fleet automation in fuel logistics are reshaping how dispatching, monitoring, and billing work. Electronic bills of lading (eBOL), telematics, and cloud dispatch platforms remove phone calls, paper, and manual reconciliations. Large 3PLs have begun rolling out standardized eBOL based on the NMFTA Digital LTL Council's API, proving that digital documentation can scale across carriers and customers while improving real-time visibility [1].

This modernization brings efficiency—and fresh risk. Fuel distribution is tightly coupled to national resilience, so cyber incidents quickly turn into supply problems. In 2022, a ransomware attack on Oiltanking/Mabanaft disrupted terminal operations in Germany and forced major suppliers to reroute product, with knock-on effects across parts of the Netherlands and Belgium. The case showed how a logistics operator's IT outage can ripple into physical flows [9]. In 2023, a cyberattack in Iran temporarily disabled a large share of petrol stations nationwide, again illustrating the dependency between digital platforms and fuel availability [10].

Fleet automation adds another layer: connected trucks now expose new attack surfaces. CISA warned that popular low-cost GPS trackers (e.g., MiCODUS MV720) had vulnerabilities allowing attackers to track vehicles, tamper with alarms, and in some configurations even trigger *fuel cut-off* commands—an obvious safety and business risk for hazardous-goods fleets [2]. These realities make cybersecurity a core operational control, not an afterthought.

On the privacy side, digitisation means more data about drivers: precise location histories, driving behaviour, shift patterns, even in-cab video. Regulators increasingly expect governance around such monitoring. The UK Information Commissioner's Office (ICO), for example, issued specific guidance in 2023 reminding employers that worker monitoring must be lawful, necessary, and transparent, with Data Protection Impact Assessments where risks are high—especially for remote or in-vehicle tracking [6]. For EU operators, the NIS2 Directive expands obligations for essential/important entities, emphasising supply-chain security, incident reporting, and risk management that now reach into third-party platforms used for dispatching and telemetry [3].

Putting this together, a digitised fuel-logistics program should pursue four tracks:

1. **Secure the platform stack.** Treat dispatch, billing, and eBOL systems as Tier-1: MFA everywhere; network segmentation between office IT, terminal OT, and vehicle telematics; rigorous patching and backup/restore testing. The Oiltanking/Mabanaft incident underlines why tabletop exercises must include “IT-only” failure modes that still halt product movement [9].

2. **Harden vehicles and devices.** Maintain an inventory of in-vehicle devices and their firmware; disable remote functions you don't need (especially any “fuel cut-off”); change default credentials; and procure telematics from vendors with a vulnerability-disclosure program. CISA's advisory shows what's at stake [2].

3. **Protect documentation flows.** Standardised eBOL reduces manual errors and fraud opportunities, but also centralises risk: authenticate API calls, sign documents digitally, and monitor for anomalous

routing or consignee changes. The current industry adoption wave provides a blueprint for secure-by-design implementation [1].Trackfuel

4. **Respect drivers' privacy.** Limit data to what's necessary for safety and operations; define clear retention periods; provide notice and access rights; and conduct DPIAs for new monitoring tools. Align driver policies with regulator expectations to protect trust and reduce legal exposure [6].

Strategically, digitisation is no longer optional: eBOL and telematics improve on-time delivery, billing accuracy, and utilisation, while enabling dynamic rerouting during terminal outages. But recent, real-world incidents—terminal ransomware and nationwide pump outages—prove that cyber risk now *is* logistics risk. The winners in fuel distribution will be those who pair automation with robust security engineering, rigorous vendor governance, and privacy-by-design for their workforce [11].

2 State of the art

2.1 Identity-Based Authentication (IBA)

Privacy-Preserving Identity-Based Authentication (IBA) is an authentication paradigm that enables the secure verification of a subject's identity without directly exposing their personal data. Unlike traditional models—where identity is represented through explicit identifiers such as usernames, email addresses, or other personal information—IBA relies on pseudonymous identifiers uniquely associated with an entity, combined with strong authentication mechanisms such as PINs, digital certificates, or cryptographic keys. The identity is thus implicitly recognised through the validation of credentials uniquely linked to a subject, without revealing their actual identity in plain text. This approach minimises the collection and processing of personal data while ensuring the confidentiality, integrity, and authenticity of the transaction or service access. IBA is particularly well-suited for scenarios where both traceability and privacy protection are required, such as in regulated digital services, secure payments, or distributed system architectures.

2.2 Static Policies

Authentication and authorisation mechanisms often rely on static policy models to govern access. Static policies define fixed, pre-configured rules—such as user roles, access levels, or IP whitelisting—that determine who can access which resources, and under what conditions. These policies are typically defined by administrators and remain unchanged unless manually updated. For example, a user assigned an "admin" role may always have full access to a system, regardless of when or where they log in.

The primary advantage of static policies is their simplicity and predictability. Because the rules are explicitly defined and do not depend on external factors, they are easy to understand, audit, and enforce. This makes them well-suited for environments with stable requirements and low variability in user behaviour or security threats.

2.3 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.

3 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.

3.1 SmartCards

SmartCards, hereinafter referred to as Fuel Cards and Loyalty Cards, 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 (SLE4442) or NFC (NTAG 213). Virtual cards are dematerialised cards that can only be used via mobile apps.

3.2 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.

3.3 OPTs – Outdoor Payment Terminals

OPTs are payment instruments now found in almost all service stations. They allow payments to be accepted using both bank cards and fuel 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. They also allow customers to be identified at the end of a transaction by scanning their loyalty card.

3.4 Cloud

All payment transactions are handled in real time, so it is essential that authorisation servers are always available and responsive.

3.5 Web Applications

All system users can access a web-based management and reporting platform. Several access levels are available, described below in ascending order of functional limitations:

- **Network Level (3)**: This is the level accessed by employees of the company that manages the issuance and administration of its own brand of Fuel/Loyalty Cards. The task of network-level users is to manage all operational and administrative aspects of the Fuel/Loyalty Card management process, with visibility of data from all service stations belonging to the private card acceptance network.
- **Manager Level (2)**: This is the level accessed by those responsible for managing a single point of sale, allowing them to monitor and report on purchases made using Fuel/Loyalty Cards at their service station.

- **Enterprise Level (1)**: This access is reserved for owners of vehicle fleets who are assigned Fuel Cards, allowing them to request, monitor, and suspend their use. At this level, all payments made using the company's cards can be viewed, regardless of the service station where the fuel was purchased. Loyalty Card holders can also access this level to view details of purchases made and the degree to which they have achieved the rewards offered in the promotional initiative.

- **Driver Level (0)**: This is the level accessible to the holder of one or more Fuel Cards, enabling reporting and/or transaction functions for the assigned cards only.

3.6 FEP

Data transmission, protocol conversion, error checking, and other network and peripheral activities are handled by a Front-End Processor (FEP), a specialised computer that manages communications for a primary host computer. By relieving the host of communication overhead, FEPs increase a system's efficiency and free up the host to concentrate on its core processing tasks. They serve as a bridge connecting the host to other networks or gadgets.

3.7 Mobile APP

At the "Company" and "Drivers" levels referred to in the previous paragraph, 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 Fuel/Loyalty Cards in your area, as a means of payment or recognition.

- Let yourself be guided by the "Navigate to" function.

- Check the credit availability on your cards

- View details of the latest transactions

- Make payments in both "Self" and "Served" modes

3.8 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)**: PIN encrypted with symmetric keys → guaranteed by HSM, AES/3DES.

- **Integrity (I)**: HMAC SHA512 signature of messages between OPT and FEP → prevents tampering.

- **Authentication (A)**: Mutual TLS between POS and cloud → terminal identification.

- **Non-repudiation (NR)**: Traceability of operations via centralised logs → useful in disputes.

3.9 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) [4], 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 [5] 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 [7] 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 [8] 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.

3.10 Types of Cards

Fuel Cards In the fuel distribution sector, Fuel Cards are defined as payment cards that allow the purchase of products and services on sale at a group of service stations belonging to the same brand, or, using more sector-specific terminology, stations that display the same flag. These filling stations constitute a “network” of sales outlets managed by a company referred to in the sector as a “network operator”. These are “limited-use” payment instruments, i.e. cards that allow the purchase of only certain types of products and only within a closed loop of affiliated sales outlets. This feature makes them both payment and loyalty tools. They can work in ‘credit card’ mode, i.e. allowing purchases with deferred payment, or as ‘prepaid cards’, which must be topped up before use. Fuel cards can be ‘physical’ or ‘virtual’. Physical cards are plastic cards equipped with a magnetic strip and contact chip (SLE4442) or NFC (NTAG 213), while virtual cards can only be used via mobile applications on smartphones or tablets. Physical cards are also automatically virtualised in the mobile app. In the fuel distribution sector, they are widely used because they have functional features that make them much more convenient for cardholders to use than the more common bank payment cards.

Loyalty Cards In the fuel distribution sector, Loyalty Cards are defined as cards that allow customers to be identified to grant them benefits following the purchase of products and/or services, exclusively for those who participate in a loyalty programme. In order to attract new customers to their service stations, network operators of all sizes usually launch loyalty programmes regularly. The promotional mechanics may vary, from reward schemes with a points collection mechanism to prize competitions with a final draw, from the recognition of immediate discounts or accumulation on an electronic wallet, all loyalty programmes share the aim of attracting new customers and retaining old ones, and the method: providing customers with a card (physical or virtual) that allows them to be quickly recognised. Like payment cards, loyalty cards are recognised within the network of service stations managed by the card issuer, typically all displaying the same logo, but they can also be recognised at other brands' points of sale, not necessarily fuel distributors, when cross-marketing campaigns are launched to make the initiative more attractive to end customers. Unlike Fuel Cards, which are mainly used for business purposes, Loyalty Cards are primarily intended for the consumer market and cardholders.

Unlike Fuel Cards, which are mainly used for business purposes, Loyalty Cards are primarily intended for the consumer market, and cardholders are normally private individuals. Like Fuel Cards, Loyalty Cards can also be "physical" or "virtual". Physical cards are plastic cards equipped with a magnetic strip and contact chip (SLE4442) or NFC (NTAG 213), while virtual cards can only be used via mobile applications on smartphones or tablets. Physical cards are also automatically virtualised in the mobile app.

3.11 Operational Flows

This Deliverable focuses on two main operational flows: one about the ecosystem surrounding fuel cards, the other about loyalty cards. The main phases of the two ecosystems are described below, also leveraging the main technological components introduced above.

Fuel Cards A typical operational flow concerning fuel cards is described below.

- **Phase 1**. The personal and tax details of the requesting company and its legal representative are sent for the purposes of correct identification and subsequent invoicing. The details of the vehicles that make up the company fleet and to which the payment cards will be associated are also provided. The details of the vehicles that make up the company fleet are also provided, and these will be associated with the payment cards. Other information is also requested on an optional basis, such as the number of kilometres travelled in a year, the type of fuel normally used for each vehicle, etc. The payment cards are then issued and delivered to the applicant company. The cards are valid for one year and can be renewed upon expiry.

- **Phase 2**. With or without the support of a credit insurance company, the network operator carries out an analysis of the applicant company's creditworthiness. If the outcome of the investigation is positive, it grants a credit line, i.e. a maximum limit in pounds sterling within which the company can make purchases "on credit", i.e. without paying for the products purchased at the time of purchase, but at a later date. Fuel cards are protected by a PIN code, so when the cards are delivered, the network operator must provide the company with the PIN for each card. The confidentiality of the PIN is a key feature in the security of the entire infrastructure.

- **Phase 3**. Fuel Cards can be either 'physical' (plastic cards with a magnetic strip and NFC tag) or 'virtual' (usable only via a mobile app). In both cases, when used, the card data (identification number and PIN code) are widely transmitted across various systems. However, this data is anonymised, as it can never be directly traced back to individuals.

- **Phase 4**. Through a dedicated web portal or mobile app, companies that hold one or more cards can obtain detailed reports on all purchases made using their cards, modify certain card usage limits, block cards in the event of theft or loss, etc. The data managed at this stage includes all the details of individual purchase transactions and the remaining credit that can still be used before payment with the cards is denied. When using the mobile app to make payments via virtual cards, the cardholder may choose to share their geographical location.

- **Phase 5**. Through a dedicated web portal, the network operator, or someone appointed by them, can analyse all payment transactions recorded in real time at their points of sale at any time. The network operator can also view the transaction history for each point of sale, including the time and date of each transaction, the amount paid, the type of payment method used, and the name and surname of the customer. The network operator can also view the transaction history for each point of sale, including Aggregate or specific analyses of the consumption of each client company can be carried out. This information is not used for automatic profiling activities. At the end of the period agreed with each client company, the network operator issues an invoice, from which personal data and sales volumes per period can be accessed. The network operator can also send invoices to the client company via email or fax. The client company can also access the portal to view the invoices issued. The client company can also send invoices to the network operator via email or fax. The network operator can also send invoices to the client company via email or fax.

- **Phase 6**. The client company typically makes the payment via credit institution platforms and communicates the outcome to the network operator. The network operator records this payment within the Fuel Card management platform, either manually or automatically, and this operation restores the credit limit available to the client company. The data transferred at this stage is therefore administrative in nature. The client company can then use the Fuel Card to make payments at the network operator's

Loyalty Cards A typical operational flow concerning loyalty cards is described below.

- **Phase 1**. The personal details of the individual applicant are sent for correct identification. Optionally, the user may provide additional information, such as details of the vehicle associated with the card and the mileage travelled during the course of a year.
- **Phase 2**. Loyalty Cards are not subject to an approval phase; they are automatically issued and delivered to the customer in both physical and virtual form.
- **Phase 3**. Loyalty Cards can be either 'physical' (plastic cards with a magnetic strip and NFC tag) or 'virtual' (usable only via a mobile app). In both cases, when the cards are used, their identification codes are transmitted to various systems. However, this data is anonymised, as the personal data of individuals is never transmitted, except when a new card is issued directly at a service station via the EFT-POS terminal.
- **Phase 4**. Through a dedicated web portal or mobile app, Loyalty Card holders can view a detailed report of all purchases made, check their points balance and whether they have reached the thresholds set by the promotional scheme, block their card in the event of theft or loss, etc. The data managed at this stage includes all the details of individual purchases or points redemption requests. When using the mobile app to receive points via virtual cards, the holder may, at their discretion, share their geographical location. The data processed in this phase is the geographical location of the cardholder.
- **Phase 5**. Through a dedicated web portal, the network operator or a representative can analyse all purchase transactions recorded in real time at their points of sale at any time. Aggregate or specific analyses of each customer's consumption can be carried out. This information is not used for automatic profiling activities. The network operator, or a representative, can analyse all purchase transactions recorded in real time at their points of sale at any time. Aggregate or specific analyses of each customer's consumption can be carried out. This information is not used for automatic profiling activities.
- **Phase 6**. Suppose the promotional mechanism provides for one or more point thresholds for obtaining a reward. In that case, the customer can decide which threshold to reach and request the collection of the corresponding reward. The process of purchasing, storing and delivering the reward to the customer, unless it is a fuel voucher, is managed by the network operator using electronic systems or other means.

4 Case studies

This Deliverable continues to delve into the details of the use of fuel cards and loyalty cards. What follows below are four case studies describing in detail specific uses of the two cards.

For each case study, we describe actors and operations involved with MSC diagrams, a cybersecurity and privacy analysis.

- **Case 1.** Fuel Cards as a payment and loyalty tool – Physical Cards
- **Case 2.** Fuel Cards as a payment and loyalty tool – Virtual Cards in App
- **Case 3.** Loyalty Cards as a marketing and loyalty tool – Physical Cards
- **Case 4.** Loyalty Cards as a marketing and loyalty tool – Virtual Cards in App

4.1 Case 1: Fuel Cards as a payment and loyalty tool – Physical Cards

4.1.1 Sub-case: Self-Service

This sub-case is depicted in Figure 1.

Actors

- **Fuel Pump** (dispenser controller).
- **Customer** (cardholder operating the island).
- **OPT (Outdoor Payment Terminal, secure card/PIN entry and user I/O)**.
- **Card Processing System** (CPS; payment/acquirer gateway for transaction orchestration).
- **Authorisation System** (issuer/authoriser or network service providing approval/decline).

Step-by-step

1. **Customer → OPT: *Insert fuel card and enter PIN.*** The Customer inserts a physical fuel/payment card into the OPT and enters the personal identification number. The OPT acquires the card data via a secure reader and collects the PIN through a PCI-compliant keypad. A local activation begins on the OPT to process the input and initialise a transaction context.

2. **OPT → Card Processing System: *Reading Card Data.*** The OPT forwards the card metadata and transaction preamble to the CPS. PIN values are not sent in clear; they are handled in accordance with the secure PIN entry path. The CPS opens a request scope to validate the card format and route the authorisation.

3. **Card Processing System → Authorisation System: *Request Authorisation (Card + PIN Encrypted).*** The CPS constructs an authorisation request containing the card token/track data and the encrypted PIN block (plus terminal capabilities, merchant identifiers, and preliminary product constraints if applicable). The message is synchronous and awaits the issuer/network decision.

4. **Authorisation System → Card Processing System: *Approval/Decline — product and amount check.*** The Authorisation System evaluates PAN (Primary Account Number, the credit card number) status, risk rules, and any product/amount restrictions associated with the card. It returns an *approval* or *decline* code to the CPS.

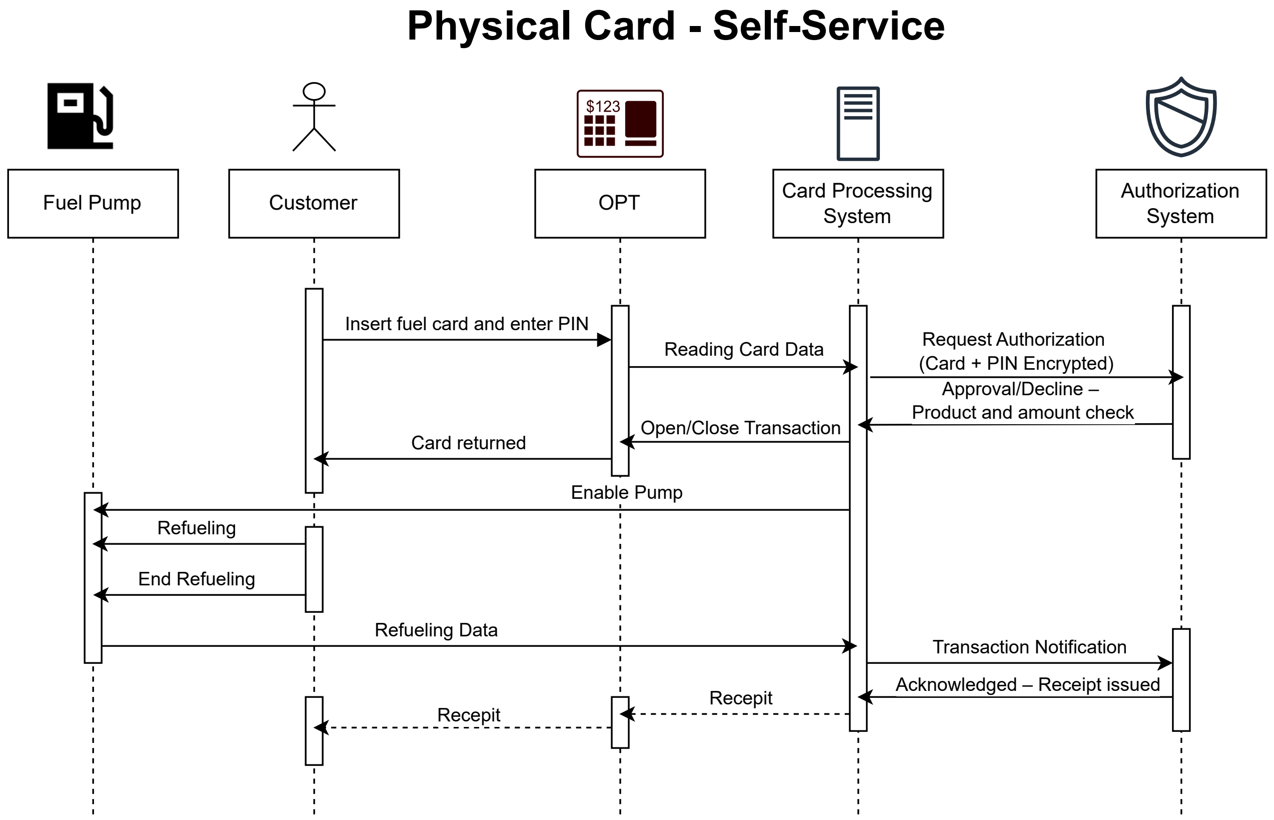

Figure 1: Sub-case fuel physical card with self-service

5. **Card Processing System → OPT:** ***Open/Close Transaction.*** On *approval*, the CPS instructs the OPT to *open* a forecourt transaction and to prepare for product delivery accounting. (If the response had been a decline, the OPT would present the refusal to the Customer and no forecourt enable would occur; that alternative is implicit in the MSC.)

6. **OPT → Customer:** ***Card returned.*** The OPT ejects and returns the physical card to the Customer, signalling that payment preauthorisation has completed and the fueling position can be enabled. User interaction continues without the card retained.

7. **OPT → Fuel Pump:** ***Enable Pump.*** The OPT sends a control command to the dispenser controller to enable fueling for the authorised grade(s) and with the configured preauthorisation limit. The pump transitions to an enabled state; the Fuel Pump lifeline enters an active segment.

8. **Customer ↔ Fuel Pump:** ***refuelling.*** The Customer lifts the nozzle and initiates dispensing. The Fuel Pump meters the delivered product and continuously updates local totals (volume, amount, product code). In the MSC this is shown as ongoing *refuelling* activity on both lifelines.

9. **Customer → Fuel Pump:** ***End refuelling.*** The Customer completes fueling (nozzle replaced or stop command issued). The dispenser finalizes metering, computes the sale totals, and closes the physical delivery session.

10. **Fuel Pump → Card Processing System:** ***refuelling Data.*** The dispenser (often via the OPT/forecourt controller) transmits the transaction data set to the CPS: product type(s), unit price, volume, amount, pump position, time stamps, and any loyalty or constraints applied. This message closes the loop between the preauthorisation and the actual delivery.

11. **Card Processing System → Authorisation System:** ***Transaction Notification.*** The CPS notifies the Authorisation System of the completed sale for capture/clearing. Depending on the model, this can be a completion message that references the prior approval code and adjusts the authorised amount to the final ticket (completion or advice).

12. **Authorisation System → Card Processing System:** ***Acknowledged — Receipt issued.*** The Authorisation System acknowledges receipt and acceptance of the completion/notification. This acknowledgement confirms that settlement processing can proceed. The MSC annotates this return with “Receipt issued” to indicate that the customer receipt may now be produced.

13. **Card Processing System → OPT:** ***Receipt.*** The CPS sends the receipt payload (merchant, pump, products, totals, masked PAN, authorisation code). The OPT renders/prints the customer copy in accordance with card scheme and privacy rules.

14. **OPT → Customer:** ***Receipt.*** The OPT provides the receipt to the Customer (depicted as a dashed arrow for a local/physical handover). The transaction lifecycle on all lifelines ends.

4.1.2 Sub-case: Assisted by Station Attendant

This sub-case is depicted in Figure 2.

Actors

- **Fuel Pump** (dispenser controller).
- **Station Operator** (attendant managing the fueling position).

- **Customer** (cardholder operating the island).
- **POS/Pinpad** (point-of-sale terminal with secure PIN entry).
- **Authorisation System** (issuer/authoriser or network service providing approval/decline).

Step-by-step

1. **Customer → Station Operator: *Request refuelling.*** The Customer requests service from the attendant, indicating the desired product and—if applicable—a target amount or "fill" instruction. The Station Operator opens a service context for the selected pump position.
2. **Station Operator → Fuel Pump: *refuelling.*** The attendant enables the dispenser and selects the product grade according to the Customer's request. The Fuel Pump transitions to the *enabled* state and allows dispensing.
3. **(Local activity) Customer ↔ Fuel Pump: *Dispensing.*** The Customer lifts the nozzle and fuel is delivered. The dispenser meters volume and computes monetary totals in real time. This continuous action is implied by the "refuelling" segment on the pump lifeline.
4. **Fuel Pump → Station Operator: *Refuel Amount & Product.*** When dispensing ends (nozzle replaced or stop command), the pump finalizes metering and reports the sale details—product, unit price, volume, and amount—to the attendant's console.
5. **Station Operator → POS/Pinpad: *Amount & Product.*** The attendant forwards the sale data to the POS. This binds the forecourt transaction (physical delivery) to a payment transaction context on the POS.
6. **Customer → POS/Pinpad: *Insert fuel card and enter PIN.*** The Customer inserts a physical card and enters the PIN on a PCI-compliant keypad. The POS/Pinpad captures card data via the secure reader and forms an authorisation request. The PIN is *never* available in clear to the merchant system; it is processed as an encrypted PIN block.
7. **POS/Pinpad → Authorisation System: *Request Authorisation (Card + PIN Encrypted).*** The POS submits a synchronous authorisation request that includes card token/track data, the encrypted PIN block, terminal and merchant identifiers, and the sale totals (product/amount) obtained from the forecourt. The Authorisation System opens an evaluation context.
8. **Authorisation System → POS/Pinpad: *Approval/Decline + Receipt data.*** The Authorisation System applies issuer/network rules (card status, risk scoring, offline limits, product restrictions). It returns either an *approval* with an authorisation code and receipt fields, or a *decline* with a reason code.[1]
9. **POS/Pinpad → Customer: *Card returned.*** Upon receipt of a terminal outcome, the POS/Pinpad ejects and returns the card to the Customer. For an approval, the payment transaction is considered authorised; for a decline, alternative tender handling is invoked (see remarks).
10. **POS/Pinpad → Customer: *Receipt.*** The POS prints or displays the receipt, including merchant information, pump position, product, totals, masked PAN, and the authorisation code when applicable. The dashed arrow denotes a local/physical handover to the Customer. The service context is closed on all lifelines.

[1] In card-scheme terms, this exchange typically corresponds to an ISO 8583 authorisation request/response.

4.1.3 Cybersecurity and privacy analysis

Table 1 presents the cybersecurity properties associated with the different steps presented within Case 1. Each row lists a communication flow (Step), the associated security protocols, and the cybersecurity properties they aim to guarantee. As described, the granted properties are confidentiality, integrity, authentication, and Non-repudiation.

The first row describes the communication from the OPT (Outdoor Payment Terminal) directly to the cloud, using the IFSF POS to FEP protocol with HMAC, ensuring confidentiality, integrity, and authentication. The second row shows a more layered architecture where the OPT communicates through an H2H (Host-to-Host) system to the cloud via VPN and IFSF H2H protocol; the same properties are granted, although the OPT → H2H segment's security may depend on the manufacturer's implementation. The third row highlights the POS-to-cloud communication, secured with mutual TLS and AES/3DES encryption, ensuring not only confidentiality, integrity, and authentication but also non-repudiation. Finally, the mobile application communicates with the cloud API via TLS 1.2 and uses JWT (JSON Web Tokens) for secure authentication and data integrity, ensuring C, I, and A.

Table 2 provides an overview of the key data types processed within the system, along with their purposes and corresponding legal bases under the GDPR (General Data Protection Regulation). Each row details a specific category of data, its classification, the reason for its collection or use, and the legal foundation that justifies its processing.

The Vehicle Plate Number is categorized as personal data and is used primarily for vehicle identification, with the legal basis being contractual necessity as per Article 6.1.b of the GDPR. The GPS Position obtained via the mobile application is considered sensitive data and is processed to provide location-based services; this requires explicit user consent in accordance with Article 6.1.a. The Fuel Card Code, which functions similarly to a Primary Account Number (PAN), is pseudonymised data used for authentication and authorisation, justified under contractual obligations. Finally, the PIN, also classified as sensitive data, is used to secure transactions and is processed based on both contractual necessity and security-related justifications.

4.2 Case 2: Fuel Cards as a payment and loyalty tool – Virtual Cards in App

This sub-case is depicted in Figure 3.

4.2.1 Sub-case: Self-Service

Actors

- **Fuel Pump** (dispenser controller).
- **Customer** (cardholder operating the island).
- **Mobile App** (system for payment).
- **Card Processing System** (CPS; payment/acquirer gateway for transaction orchestration).
- **Authorisation System** (issuer/authoriser or network service providing approval/decline).

Step-by-step

- **Customer → Mobile App: *Login.*** Customer accesses the mobile payment app.
- **Customer → Mobile App: *Select Card, Amount, PIN, Pump Number.*** Inputs payment details and selects pump.

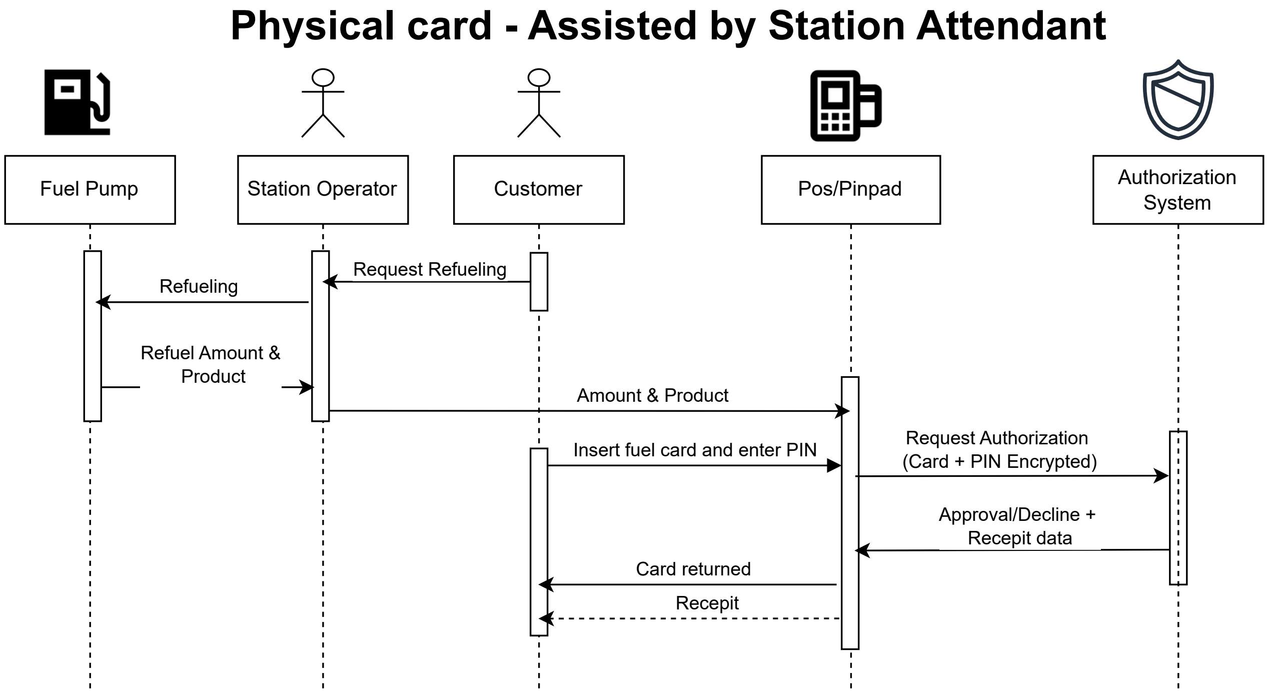
Physical card - Assisted by Station Attendant
Fuel Pump
Station Operator
Customer
Pos/Pinpad
Authorization System
Request Refueling
Refueling
Refuel Amount & Product
Amount & Product
Insert fuel card and enter PIN
Request Authorization (Card + PIN Encrypted)
Approval/Decline + Recepit data
Card returned
Recepit

Figure 2: Sub-case fuel physical card assisted by station attendant

Table 1: Cybersecurity properties Case 1

Step	Protocols	Granted Properties
OPT → Cloud (direct)	IFSF POS to FEP + HMAC	C, I, A
OPT → H2H → Cloud	VPN + IFSF H2H	C, I, A (OPT → H2H depending on manufacturer)
POS → Cloud (direct)	TLS mutual + AES/3DES	C, I, A, NR
APP mobile → API cloud	TLS 1.2 + JWT	C, I, A

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)
Fuel Card Code (PAN-like)	Pseudonymised Data	Authentication and authorisation	Contractual
PIN	Sensitive Data	Transaction security	Contractual + Security

- **Mobile App → Card Processing System:** ***Request Authorisation (Card + PIN Encrypted).*** Sends secure payment request.
- **Card Processing System → Authorisation System:** ***Request Authorisation.*** Forwards authorisation to auth system.
- **Authorisation System → Card Processing System:** ***Approval/Decline.*** Auth system responds with transaction result.
- **Card Processing System → Fuel Pump:** ***Enable Pump Request - Max Amount.*** Enables pump with approved max value.
- **Fuel Pump → Customer:** ***OK/KO.*** Confirmation sent to user if pump is ready or not.
- **Customer → Fuel Pump:** ***refuelling.*** Customer begins fueling the vehicle.
- **Fuel Pump → Customer:** ***End refuelling.*** Refuelling session ends.
- **Fuel Pump → Mobile App:** ***refuelling Data.*** Pump sends refuelling data to app.
- **Mobile App → Card Processing System:** ***Digital Receipt.*** App sends receipt data to processor.
- **Card Processing System → Authorisation System:** ***Transaction Notification.*** Notifies auth system of transaction.
- **Authorisation System → Card Processing System:** ***Acknowledged – Receipt issued.*** Confirms receipt issuance.
- **Mobile App → Customer:** ***Receipt – Push Notification.*** Customer receives digital receipt on mobile.

4.2.2 Sub-case: Assisted by Station Attendant

This sub-case is depicted in Figure 4.

Actors

- **Fuel Pump** (dispenser controller).
- **Customer** (cardholder operating the island).
- **Station Operator** (attendant managing the fueling position).
- **Mobile App** (system for payment).
- **Mobile Payments Gateway** (payment/acquirer gateway for transaction orchestration).
- **Authorisation System** (issuer/authoriser or network service providing approval/decline).

Step-by-step

1. **Customer → Station Operator:** ***Request Refuelling***. Customer asks attendant to initiate refuelling.
2. **Station Operator → Fuel Pump:** ***Refuelling.*** The attendant activates the fuel pump.
3. **Fuel Pump → Station Operator:** ***Refuel Amount & Product***. Pump sends refuel data (amount, product type).
4. **Station Operator → Customer:** ***Transactions List***. Attendant shows list of pending transactions to customer.
5. **Customer → Mobile App:** ***Login.*** Customer logs into the mobile app.
6. **Customer → Mobile App:** ***Select Card and Pump number***. Customer selects payment card and pump.
7. **Customer → Mobile App:** ***Select Transaction and PIN***. Customer chooses transaction and enters secure PIN.
8. **Mobile App → Mobile Payments Gateway:** ***Request Pump Transactions.*** App requests transaction info from gateway.
9. **Mobile Payments Gateway → Mobile App:** ***Transactions List***. Gateway responds with transaction options.
10. **Mobile App → Mobile Payments Gateway:** ***Request Authorisation (Card + PIN Encrypted).*** Sends encrypted payment request.
11. **Mobile Payments Gateway → Authorisation System:** ***Request Authorisation.*** Gateway forwards for approval.
12. **Authorisation System → Mobile Payments Gateway:** ***Approval/Decline + Digital Receipt.*** Auth system replies with result.
13. **Mobile Payments Gateway → Mobile App:** ***Transaction Notification.*** Gateway informs app of approval/decline.
14. **Mobile App → Customer:** ***Receipt Push Notification.*** Customer receives digital receipt via app.

4.2.3 Cybersecurity and privacy analysis

Table 3: Cybersecurity properties of Case 2

Step	**Protocols**	**Granted Properties**
API cloud → Mobile Automation Payment	VPN + private protocol	I, A, NR
POS → Cloud (direct)	TLS mutual + AES/3DES	C, I, A, NR
APP mobile → API cloud	TLS 1.2 + JWT	C, I, A

Table 3 outlines the cybersecurity mechanisms employed in Case 2 by listing key communication steps, the protocols involved, and the security properties they ensure. The goal is to demonstrate how integrity, confidentiality, availability, and non-repudiation are supported across different interactions in the system.

The first step, from the API cloud to the Mobile Automation Payment module, utilises a VPN combined with a private protocol. This setup guarantees integrity (I), availability (A), and non-repudiation (NR). The second communication path, from **POS to Cloud (direct)**, uses mutual TLS along with symmetric encryption (AES/3DES), ensuring confidentiality (C), integrity (I), availability (A), and non-repudiation (NR). Lastly, the connection from the **mobile app to the API cloud** is secured using TLS 1.2 and JWT (JSON Web Tokens), offering confidentiality, integrity, and availability.

Table 4: 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)
Fuel Card Code (PAN-like)	Pseudonymised Data	Authentication and authorisation	Contractual
PIN	Sensitive Data	Transaction security	Contractual + Security

Table 4 presents a summary of the main types of data processed in Case 2, along with their intended purposes and the corresponding legal bases under the General Data Protection Regulation (GDPR). This overview supports the analysis of privacy compliance by associating each data item with its classification and justification for processing.

The Vehicle Plate Number is classified as personal data and is used for vehicle identification, with its processing grounded in a contractual necessity, as outlined in Article 6.1.b of the GDPR. The GPS Position, collected through the mobile application, is considered sensitive data and is processed for providing location-based services. This processing is based on the user's explicit consent, in accordance with Article 6.1.a. The Fuel Card Code, which behaves similarly to a Primary Account Number (PAN), is treated as pseudonymised data and is used for authentication and authorisation, under a contractual legal basis. Lastly, the PIN is also sensitive data and is required for transaction security; its processing is justified through both contractual necessity and security requirements.

The same considerations described in the first case apply.

4.3 Case 3: Loyalty Cards as a marketing and loyalty tool – Physical Cards

4.3.1 Sub case: Self-service

This sub-case is depicted in Figure 5.

Actors

- **Fuel Pump** (dispenser controller).
- **Customer** (cardholder operating the island).
- **OPT (Outdoor Payment Terminal, secure card/PIN entry and user I/O)**.
- **Card Processing System** (CPS; payment/acquirer gateway for transaction orchestration).
- **Authorisation System** (issuer/authoriser or network service providing approval/decline).

Step-by-Step

1. **Customer → OPT:** ***Insert Payment card and enter PIN or cash.*** Customer inserts a payment card and enters a PIN or cash, initiating the payment process.

2. **OPT → Customer:** ***Card returned.***

3. The OPT returns the payment card to the Customer after reading the card and validating the entered PIN or cash.

4. **Customer → OPT:** ***Insert Loyalty card.*** The Customer inserts a physical loyalty card to receive benefits or rewards from the loyalty program.

5. **OPT → Customer:** ***Card returned.*** The OPT reads the loyalty card and returns it to the Customer.

6. **OPT → Fuel Pump:** ***Enable Pump.*** After the payment and loyalty card validation, the OPT sends a signal to the Fuel Pump to enable the refuelling process.

7. **Fuel Pump → Fuel Pump:** ***Refueling.*** The Fuel Pump starts the refueling process, based on the customer's selection and card validation.

8. **Fuel Pump → OPT:** ***End Refueling.*** The Fuel Pump notifies the OPT that the refuelling process has ended.

9. **Fuel Pump → Card Processing System:** ***Refueling Data.*** The Fuel Pump sends refueling data (e.g., amount of fuel, cost) to the Card Processing System.

10. **Card Processing System → Card Processing System:** ***Reading Card Data.*** The Card Processing System reads data from the card (either payment or loyalty card) for transaction verification.

11. **Card Processing System → Card Processing System:** ***Open/Close Transaction.*** The Card Processing System opens and closes the transaction, ensuring that the payment amount is accurately recorded.

12. **Card Processing System → authorisation System:** ***Card auth. server.*** The Card Processing System sends the authentication request to the authorisation System, which communicates with the card's authorisation server.

13. **authorisation System → Card Processing System:** ***Transaction Notification.*** The authorisation System sends a transaction notification back to the Card Processing System, confirming the approval of the transaction.

14. **Card Processing System → Customer:** ***Acknowledged - Receipt issued.*** The Card Processing System acknowledges the transaction and issues a receipt to the Customer, marking the transaction completion.

4.3.2 Sub case: Assisted by Station Attendant

This sub-case is depicted in Figure 6.

Actors

- **Fuel Pump** (dispenser controller).
- **Customer** (cardholder operating the island).
- **Station Operator** (attendant managing the fueling position).
- **Mobile App** (system for payment).
- **Mobile Payments Gateway** (payment/acquirer gateway for transaction orchestration).
- **Authorisation System** (issuer/authoriser or network service providing approval/decline).

Step-by-step

- **Customer → Station Operator:** ***Request refuelling.*** Customer asks the station operator to begin refuelling.
- **Station Operator → Fuel Pump:** ***refuelling.*** Operator activates the pump to start the refuelling process.
- **Fuel Pump → Station Operator:** ***Refuel Amount & Product.*** Pump returns information on amount and product refueled.
- **Station Operator → Customer:** ***Amount & Product.*** Operator communicates the transaction details to the customer.
- **Customer → Pos/Pinpad:** ***Insert payment card and enter PIN or cash.*** Customer initiates payment by inserting a physical card or using cash.
- **Pos/Pinpad → Authorisation System:** ***Card auth. server.*** POS system connects to the card authorisation server.
- **Pos/Pinpad → Authorisation System:** ***Request Authorisation.*** Transaction authorisation is requested from the system.
- **Authorisation System → Pos/Pinpad:** ***Acknowledged – Receipt issued.*** Authorisation result is received and receipt is prepared.
- **Pos/Pinpad → Customer:** ***Card returned.*** Customer's payment card is returned.

  Customer → Pos/Pinpad: ***Insert Loyalty card.*** Customer inserts the loyalty card to collect points or rewards.
- **Pos/Pinpad → Customer:** ***Card returned.*** Loyalty card is returned to the customer.
- **Pos/Pinpad → Customer:** ***Receipt.*** Final printed or digital receipt is delivered to the customer.

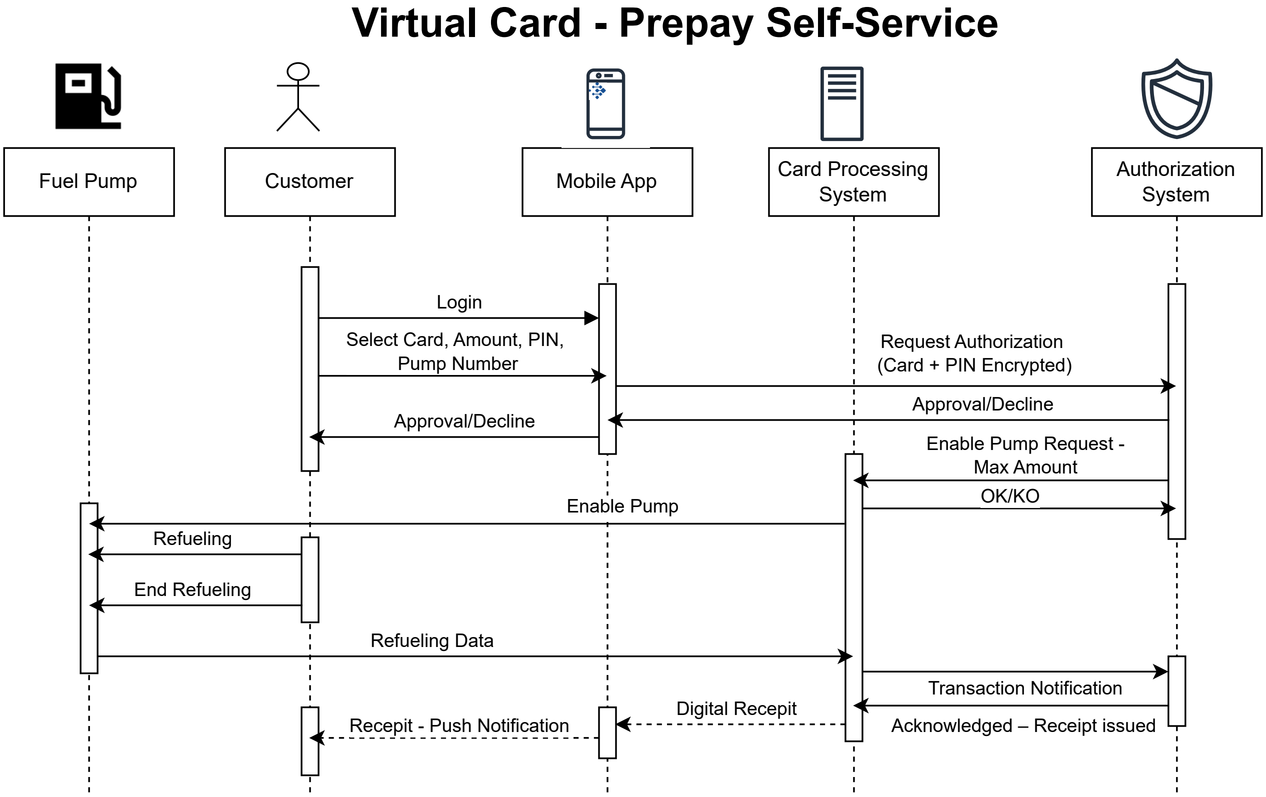
Virtual Card - Prepay Self-Service
Fuel Pump
Customer
Mobile App
Card Processing System
Authorization System
Login
Select Card, Amount, PIN, Pump Number
Request Authorization (Card + PIN Encrypted)
Approval/Decline
Approval/Decline
Enable Pump Request - Max Amount
OK/KO
Enable Pump
Refueling
End Refueling
Refueling Data
Transaction Notification
Digital Recepit
Acknowledged – Receipt issued
Recepit - Push Notification

Figure 3: Sub-case fuel virtual card with self-service

Table 5: Communication Steps, Protocols, and Security Guarantees

Step	Protocol	Guaranteed Properties
OPT → Cloud (direct)	IFSF POS to FEP + HMAC	C, I, A
OPT → H2H → Cloud	VPN + IFSF H2H	C, I, A (OPT → H2H depends on manufacturer)
POS → Cloud (direct)	TLS mutual + AES/3DES	C, I, A, NR
APP mobile → API cloud	TLS 1.2 + JWT	C, A, I

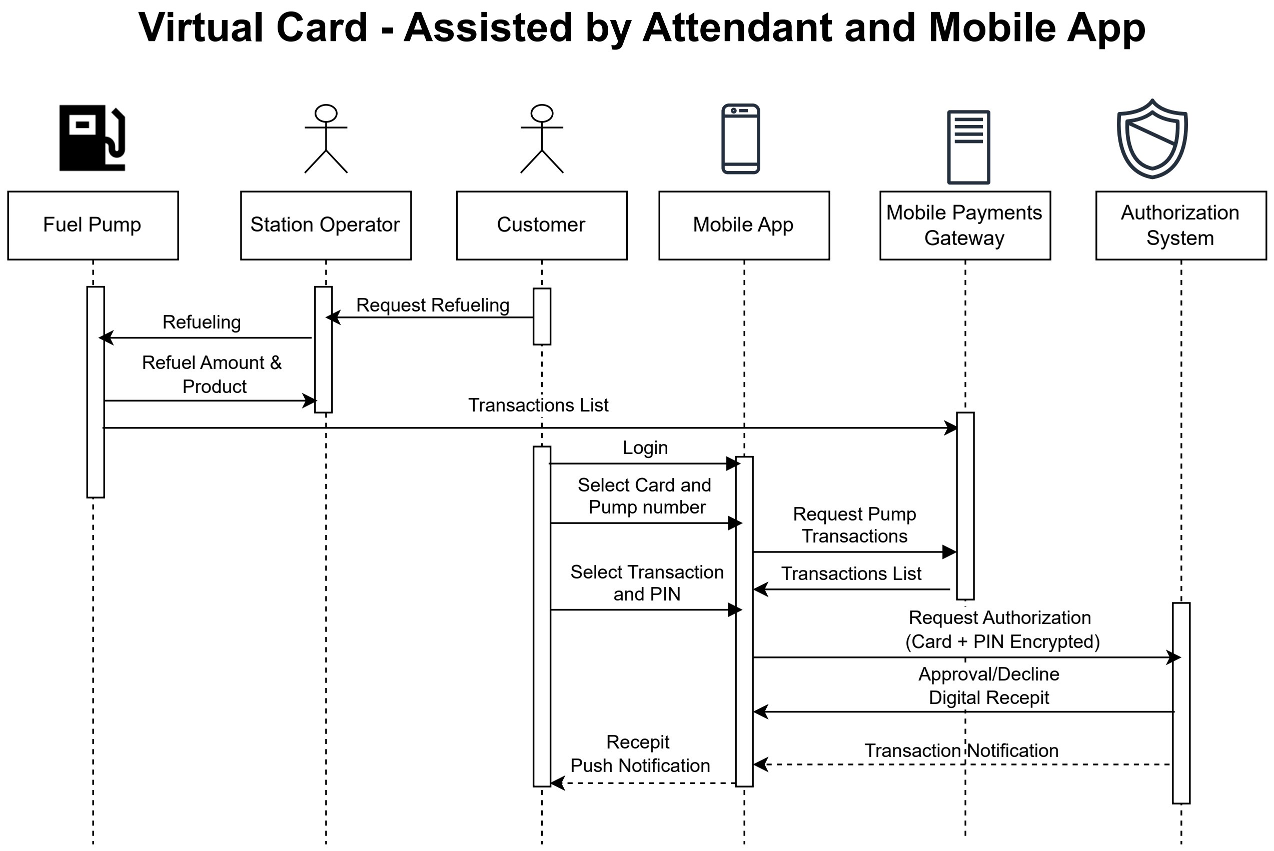
Virtual Card - Assisted by Attendant and Mobile App
Fuel Pump
Station Operator
Customer
Mobile App
Mobile Payments Gateway
Authorization System
Request Refueling
Refueling
Refuel Amount & Product
Transactions List
Login
Select Card and Pump number
Request Pump Transactions
Transactions List
Select Transaction and PIN
Request Authorization (Card + PIN Encrypted)
Approval/Decline Digital Recepit
Transaction Notification
Recepit Push Notification

Figure 4: Sub-case fuel virtual card assisted by station attendant

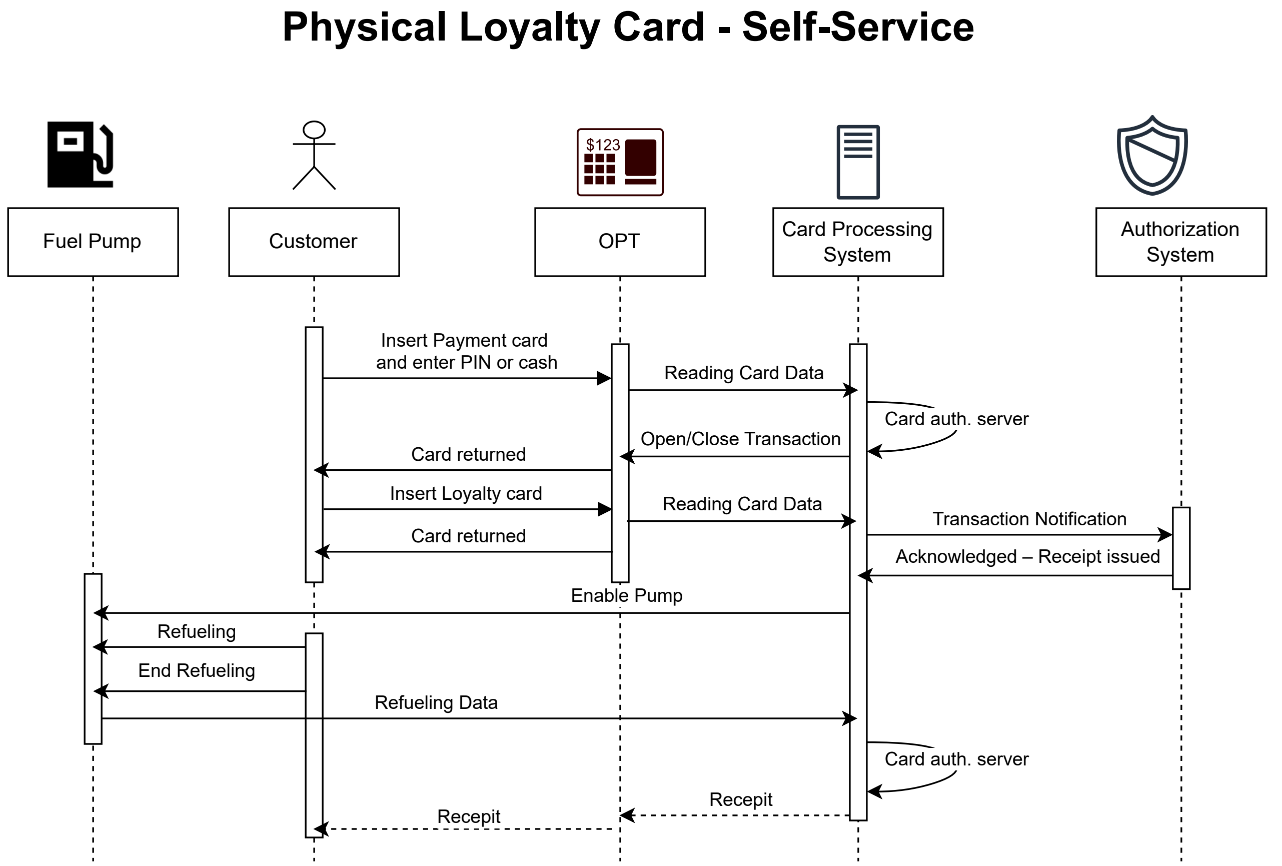

Figure 5: Sub-case physical loyalty card with self-service

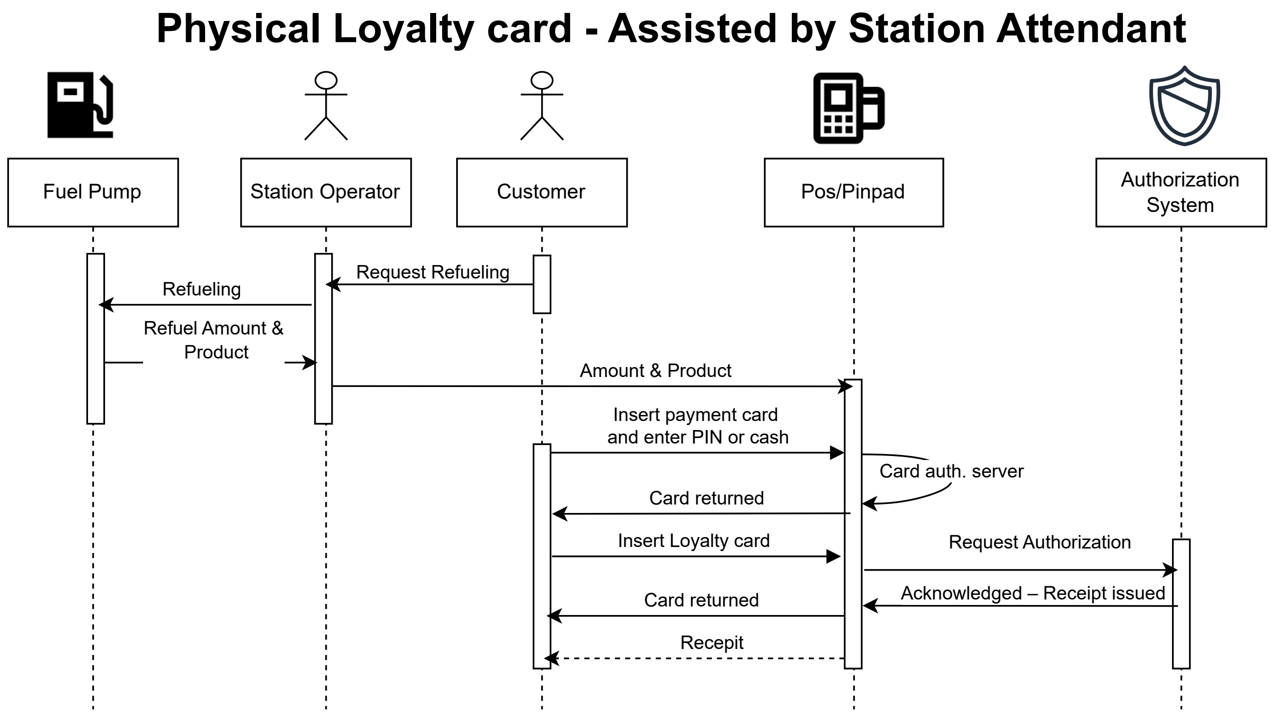

Figure 6: Sub-case virtual loyalty card assisted by station attendant

4.3.3 Cybersecurity and privacy analysis

Table 5 summarises the key communication flows within the system, along with the security protocols employed and the cybersecurity guarantees provided. The table highlights how different technologies contribute to achieving core security properties: C for Confidentiality, I for Integrity, A for Authentication, and NR for Non-repudiation.

The first row describes the direct communication from the Outdoor Payment Terminal (OPT) to the Cloud, protected via the IFSF POS to FEP protocol along with HMAC. This ensures confidentiality, integrity, and authentication. The second scenario involves communication from the OPT to the Cloud via a Host-to-Host (H2H) layer, secured using a VPN and IFSF H2H protocol. The same properties are guaranteed, although the level of security between OPT and H2H may vary depending on the manufacturer. The third row shows the POS to Cloud connection, which employs mutual TLS and encryption algorithms such as AES or 3DES, guaranteeing all four core security properties, including non-repudiation. Lastly, the Mobile App to Cloud API communication uses TLS 1.2 with JWT tokens to ensure confidentiality, integrity, and authentication.

Table 6: 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)
Fuel Card Code (PAN-like)	Pseudonymised Data	Authentication and authorisation	Contractual
PIN	Sensitive Data	Transaction security	Contractual + Security

Table 6 outlines the various types of data processed within the system, their intended purposes, and the legal bases justifying their collection and use under the General Data Protection Regulation (GDPR). Each entry connects a specific data item with its classification and lawful processing condition.

The Vehicle Plate Number is treated as personal data, used for identifying vehicles during operations, and its processing is based on contractual necessity in accordance with Article 6.1.b of the GDPR. The GPS Position gathered by the mobile application is considered sensitive data and supports the provision of location-based services; its processing requires explicit user consent under Article 6.1.a. The Fuel Card Code, which functions similarly to a Primary Account Number (PAN), is pseudonymised data used for authentication and authorisation, with the legal basis being contractual necessity. Finally, the PIN is sensitive data used to secure transactions, and its processing is justified by both contractual and security requirements.

4.4 Case 4: Loyalty Cards as a marketing and loyalty tool – Virtual Cards in App

4.4.1 Sub case: Self-service

Actors

- **Fuel Pump** (dispenser controller).
- **Customer** (cardholder operating the island).
- **Mobile App** (system for payment).
- **OPT (Outdoor Payment Terminal, secure card/PIN entry and user I/O)**.

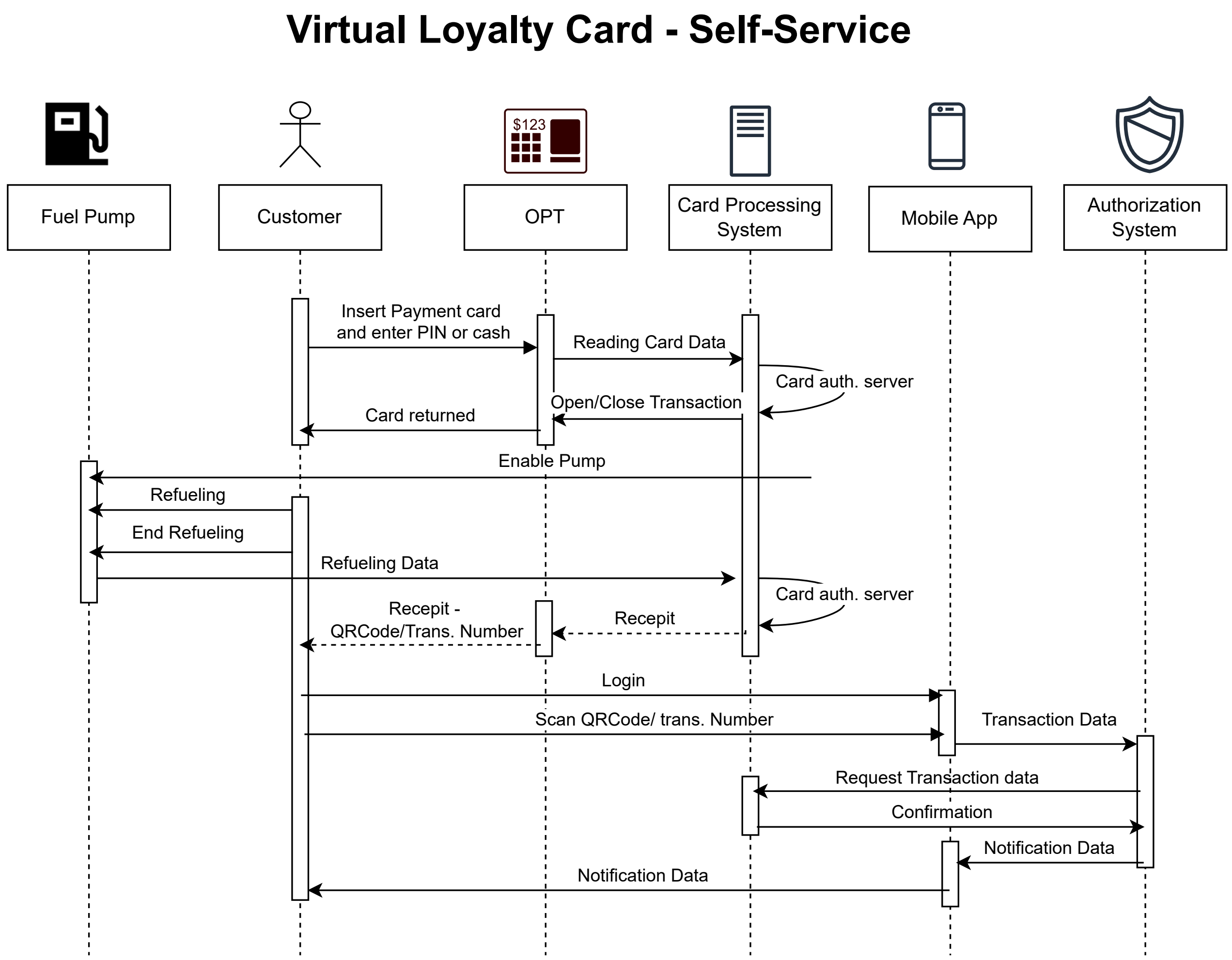

Figure 7: Sub-case virtual loyalty card with self-service

- **Card Processing System** (CPS; payment/acquirer gateway for transaction orchestration).
- **Authorisation System** (issuer/authoriser or network service providing approval/decline).

Step-by-step

- **Customer → OPT:** ***Insert Payment card and enter PIN or cash.*** Customer initiates payment using card or cash at the Outdoor Payment Terminal (OPT).
- **OPT → Card Processing System:** ***Reading Card Data.*** OPT reads payment card information.
- **Card Processing System → authorisation System:** ***Card auth. server.*** authorisation is requested for the payment.
- **Card Processing System → OPT:** ***Open/Close Transaction.*** Transaction is opened after authorisation is successful.
- **OPT → Customer:** ***Card returned.*** Customer's card is returned by the OPT.
- **OPT → Fuel Pump:** ***Enable Pump.*** Pump is enabled for fuel dispensing.
- **Customer → Fuel Pump:** ***Refueling.*** Customer performs the refueling.
- **Fuel Pump → Customer:** ***End Refueling.*** Refueling is completed.
- **Fuel Pump → OPT:** ***Refueling Data.*** Pump sends fuel volume and product info to the terminal.
- **OPT → Card Processing System:** ***Receipt.*** Transaction data is sent to the backend for receipt generation.
- **Card Processing System → authorisation System:** ***Card auth. server.*** System logs transaction status.
- **Card Processing System → OPT:** ***Receipt.*** Printed receipt with QR code and transaction number is issued.
- **OPT → Customer:** ***Receipt – QRCode/Trans. Number.*** Customer receives receipt for loyalty transaction.
- **Customer → Mobile App:** ***Login.*** Customer opens loyalty app.
- **Customer → Mobile App:** ***Scan QRCode/trans. Number.*** QR code or transaction number is scanned to retrieve loyalty info.
- **Mobile App → Card Processing System:** ***Transaction Data.*** Mobile app requests loyalty transaction data.
- **Card Processing System → authorisation System:** ***Request Transaction data.*** authorisation system validates or processes the loyalty data.
- **authorisation System → Card Processing System:** ***Confirmation.*** Transaction confirmation is sent back.
- **Card Processing System → Mobile App:** ***Notification Data.*** Loyalty information and rewards are pushed to the app.
- **Mobile App → Customer:** ***Notification Data.*** Customer receives confirmation or reward from loyalty system.

4.4.2 Sub case: Assisted by station attendant

Actors

- **Fuel Pump** (dispenser controller).
- **Customer** (cardholder operating the island).
- **Station Operator** (attendant managing the fueling position).
- **Mobile App** (system for payment).
- **Card Processing System** (CPS; payment/acquirer gateway for transaction orchestration).
- **Authorisation System** (issuer/authoriser or network service providing approval/decline).

Step-by-step

- **Customer → Station Operator:** ***Request Refueling.*** Customer asks the attendant to start refueling.
- **Station Operator → Fuel Pump:** ***Refueling.*** Operator activates the pump.
- **Fuel Pump → Station Operator:** ***Refuel Amount & Product.*** Pump returns the amount of fuel and type of product dispensed.
- **Station Operator → Customer:** ***Transaction Receipt QRCode/Trans Number.*** Customer receives receipt with transaction number or QR code.
- **Customer → Mobile App:** ***Login.*** Customer logs into the mobile app.
- **Customer → Mobile App:** ***Scan QRCode/Trans. Number.*** Customer scans the receipt to fetch transaction data.
- **Mobile App → Card Processing System:** ***Transaction Data.*** App sends request to retrieve transaction details.
- **Card Processing System → authorisation System:** ***Request Transaction data.*** System requests authorisation or validation from the server.
- **authorisation System → Card Processing System:** ***Confirmation.*** authorisation system confirms the transaction.
- **Card Processing System → Mobile App:** ***Notification Data.*** Transaction confirmation and rewards are sent back to the mobile app.
- **Mobile App → Customer:** ***Notification Data.*** Customer receives a digital confirmation or reward notification.

4.4.3 Cybersecurity and privacy analysis

Table 7 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

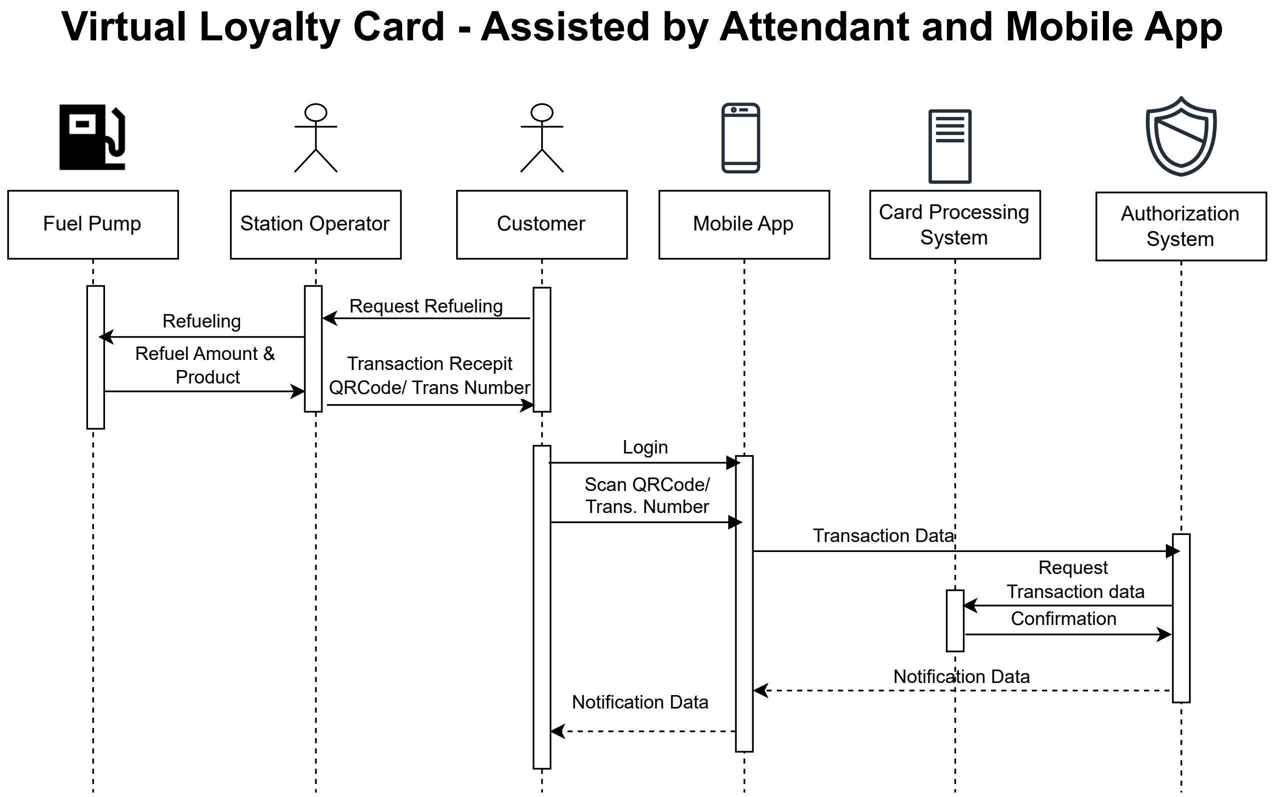

Figure 8: Sub-case virtual loyalty card assisted by station attendant

Table 7: 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

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 8 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 fuel card code, 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.

Table 8: 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)
Fuel Card Code (PAN-like)	Pseudonymised Data	Authentication and authorisation	Contractual
PIN	Sensitive Data	Transaction security	Contractual + Security

5 Augmenting Identity-Based Authentication with Zero-Knowledge Proof of Knowledge

In a typical fuel card 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. This approach can be enhanced by adopting a zero-knowledge (ZK) perspective in a broad security context, where pseudonymous identifiers or attribute-only tokens enable the system to authenticate users without revealing their actual identities. Static policies, such as fuel type restrictions or authorised vehicle access, provide a fixed, consistent set of rules that complement IBA by ensuring basic operational compliance, even in a pseudonymous authentication model.

More precisely, we advance the application of Zero-Knowledge Proofs (ZKPs) to enable users to prove the genuineness of their credentials—including identity and sensitive attributes such as the card number (PAN), PIN – during authentication and authorisation processes, without revealing the underlying information. In this approach, each user is issued a credential by a trusted issuer, which contains cryptographically signed attributes and static policies, such as maximum transaction amount, fuel type, or user role. These policies are embedded at the time of issuance and remain immutable throughout the credential's lifetime, contributing to its verifiable authenticity.

The overarching idea is that, during a transaction, the user generates a zero-knowledge proof that attests to the genuine and policy-compliant nature of the credential, without exposing the actual attribute values. For numerical constraints (e.g., amount $\leq$ 100), range proofs are employed, while categorical or string-based constraints (e.g., fuel type "diesel") are verified using equality proofs or set membership proofs. Through this mechanism, the verifier can confidently assess the genuineness and validity of the credential and its compliance with predefined policies, while remaining blind to the sensitive details. This ensures both correctness and privacy in a decentralised, non-interactive, and secure manner.

We therefore apply the ZKP measure to both the phyisical and virtual fuel card case studies seen above. The outcomes are respectively in Figure 9 and Figure 10. It can be seen that, in both cases, the following steps (highlighted in red in the figures) are added to the steps already described.

- **OPT → CardProcessingSystem:** ***Build ZKP input (PAN, PIN).*** The OPT prepares the required input to generate a Zero-Knowledge Proof, using the PAN and encrypted PIN.
- **CardProcessingSystem → OPT:** ***Generate ZKP.*** The Card Processing System generates the ZKP based on the received input.
- **OPT → AuthorisationSystem:** ***Send ZKP, PAN, amount.*** The OPT sends the Zero-Knowledge Proof, card PAN, and transaction amount to the Authorisation System.
- **AuthorisationSystem → AuthorisationSystem:** ***Retrieve commitment for PAN.*** The system retrieves the stored commitment (reference data) for the provided PAN to validate the ZKP.
- **AuthorisationSystem → AuthorisationSystem:** ***Verify ZKP (PIN correct, amount authorised).*** The system verifies that the PIN is correct and the requested amount is within authorised limits.
- **AuthorisationSystem → OPT:** ***Send authorisation response (approved/denied).*** The Authorisation System sends the result of the ZKP verification and payment authorisation back to the OPT.

Our attempts confirm that ZKPs can be applied as a tool that seamlessly integrate with previous MSC designs much the way the red, new MSC portions were introduced above. Therefore, we consider the expected integration accomplished in general, across all our target use cases.

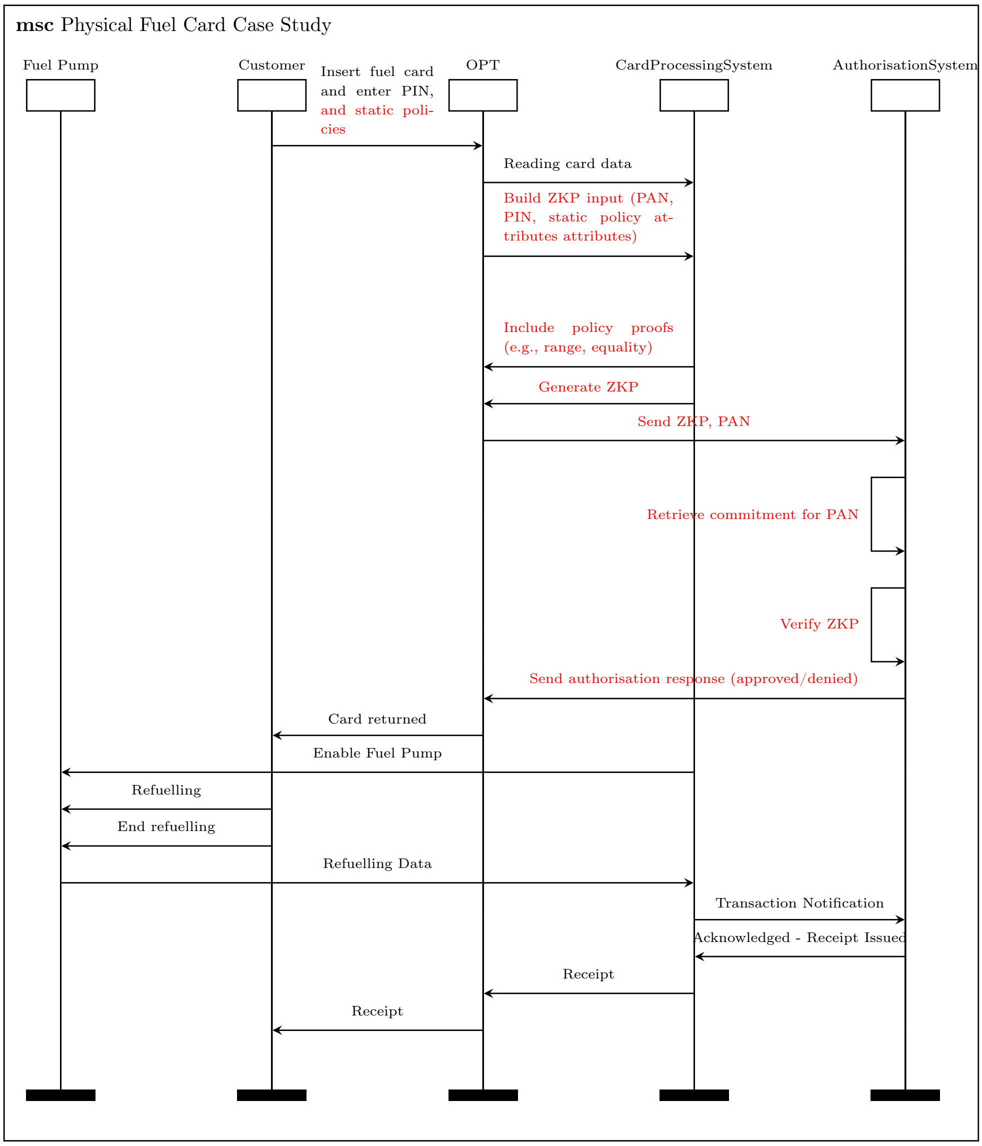
msc Physical Fuel Card Case Study
Fuel Pump
Customer
OPT
CardProcessingSystem
AuthorisationSystem
Insert fuel card and enter PIN, and static policies
Reading card data
Build ZKP input (PAN, PIN, static policy attributes attributes)
Include policy proofs (e.g., range, equality)
Generate ZKP
Send ZKP, PAN
Retrieve commitment for PAN
Verify ZKP
Send authorisation response (approved/denied)
Card returned
Enable Fuel Pump
Refuelling
End refuelling
Refuelling Data
Transaction Notification
Acknowledged - Receipt Issued
Receipt
Receipt

Figure 9: The Physical Fuel Card case study augmented with a ZKP

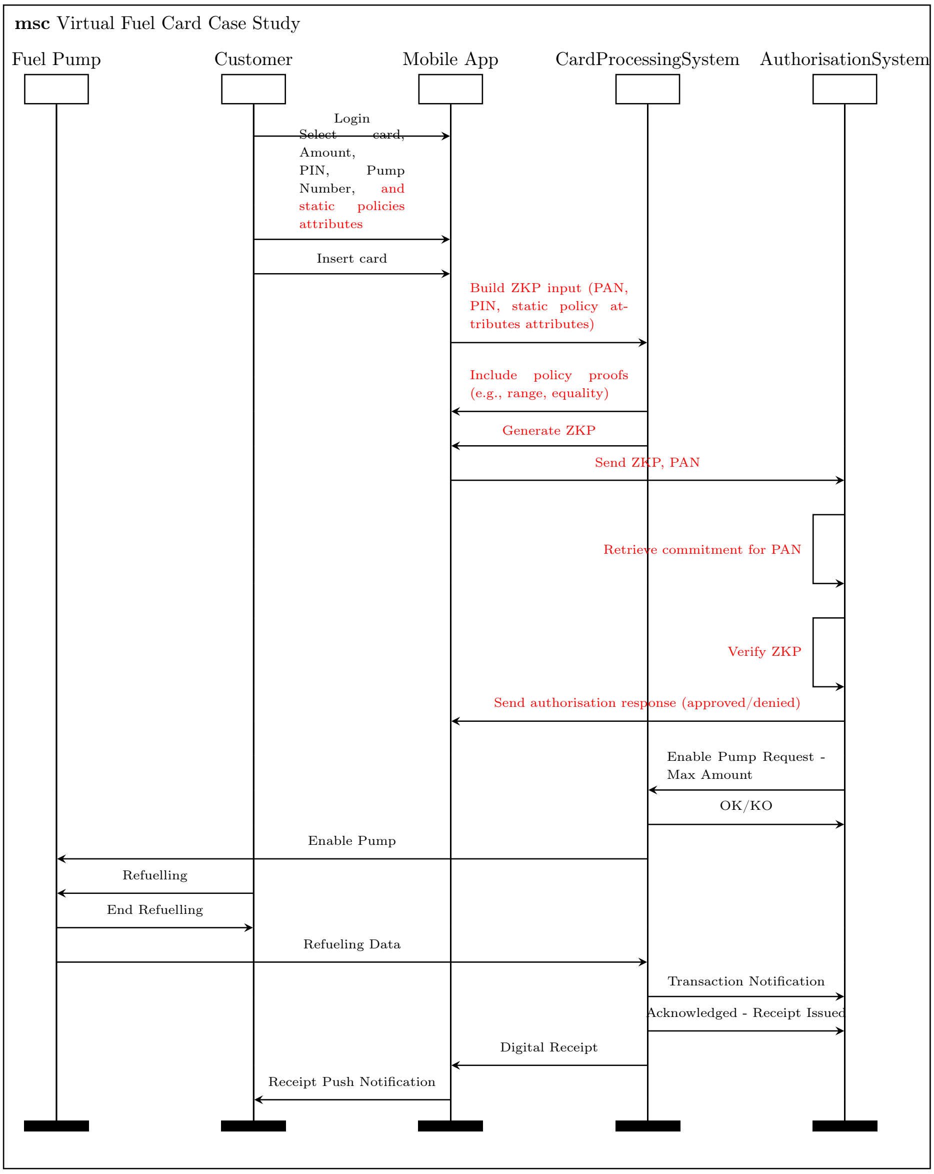
msc Virtual Fuel Card Case Study
Fuel Pump
Customer
Mobile App
CardProcessingSystem
AuthorisationSystem
Login
Select card, Amount, PIN, Pump Number, and static policies attributes
Insert card
Build ZKP input (PAN, PIN, static policy attributes attributes)
Include policy proofs (e.g., range, equality)
Generate ZKP
Send ZKP, PAN
Retrieve commitment for PAN
Verify ZKP
Send authorisation response (approved/denied)
Enable Pump Request - Max Amount
OK/KO
Enable Pump
Refuelling
End Refuelling
Refueling Data
Transaction Notification
Acknowledged - Receipt Issued
Digital Receipt
Receipt Push Notification

Figure 10: The Virtual Fuel Card case study augmented with a ZKP

6 Conclusions

In this deliverable, we completed a systematic assessment of Identity-Based Authentication (IBA) across four real-world automotive use cases involving payment and loyalty cards. Drawing on external domain consultancy, we captured the operational context of each case, identified actors and trust anchors (vehicle, mobile app, forecourt POS/terminal, acquirer/issuer), and analysed authentication flows under typical conditions. As an outcome, the project consolidated a set of IBA designs that consistently support card and loyalty scenarios.

Furthermore, we investigated and specified the application of Zero-Knowledge Proofs (ZKPs) to these flows, enabling a prover to demonstrate possession and validity of required items without disclosing extraneous information. Concretely, we defined the verifier–prover interaction so that the Customer (card holder) can prove the genuineness of the card to the Authorisation System by attesting, in zero knowledge, to issuer-signed credentials and policy predicates, while withholding raw identifiers (e.g., PAN, PIN) and binding each proof to existing commitments. The resulting construction preserves authorisation semantics — accept/reject based on validated predicates — while minimising data exposure.

References

[1] C.H. Robinson. New ebol for ltl shipments, 2024. Press release; NMFTA Digital LTL Council eBOL API adoption.

[2] Cybersecurity and Infrastructure Security Agency (CISA). Cisa released security advisory on micodus mv720 global positioning system (gps) tracker, 07 2022. Advisory on vulnerabilities including potential fuel cut-off commands.

[3] European Commission. Nis2 directive: securing network and information systems, 2023. EU policy page on NIS2 obligations for essential and important entities.

[4] 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.

[5] 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.

[6] Information Commissioner's Office (ICO). Ico publishes guidance to ensure lawful monitoring in the workplace, 10 2023. Guidance on necessity, transparency, DPIAs for worker monitoring.

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

[8] 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.

[9] Reuters. Shell re-routes oil supplies after cyberattack on german firm, 02 2022. Oiltanking/Mabanaft incident in Germany.

[10] Reuters. Iran petrol stations hit by cyberattack, oil minister says, 12 2023. Nationwide disruption of petrol stations in Iran.

[11] S&P Global Commodity Insights. German oil terminals, tank farms operating at 'limited capacity' after cyber attack, 02 2022. Context and impacts around German terminal disruption.