Module 21: Mobile Fare Ticketing/Payment Apps

Table of Contents

1. Module Description

The Mobile Fare Payment module provides an overview of Mobile Fare Payment apps for transit and the ways in which they are deployed.

2. Introduction/Purpose

The Mobile Fare Payment module will focus on stakeholders and their roles, business models, and open architecture specifications including open Application Programming Interfaces (API) and integration with multimodal mobility services. Previous modules, Modules 10 and 12, covered banking and media standards associated with electronic fare payment including contactless cards, mobile banking, and account-based systems. These concepts will be incorporated in this module with respect to their application to mobile ticketing/payment systems.

3. Samples/Examples

The Module describes the Interoperable Fare Management System (IFMS) architecture and TCRP Synthesis 148 Mobile Fare Payment App business models. More detailed descriptions of these models are included in this section.

3.1. IFMS Architecture and Use Cases

3.1.1. IFMS Role-Based Architecture and Definitions

The IFMS role-based architecture, adapted from ISO/DIS 24014-1 version 3 and described in slide 34, is shown in Figure 1. The shapes in the concept model are described in Table 1.

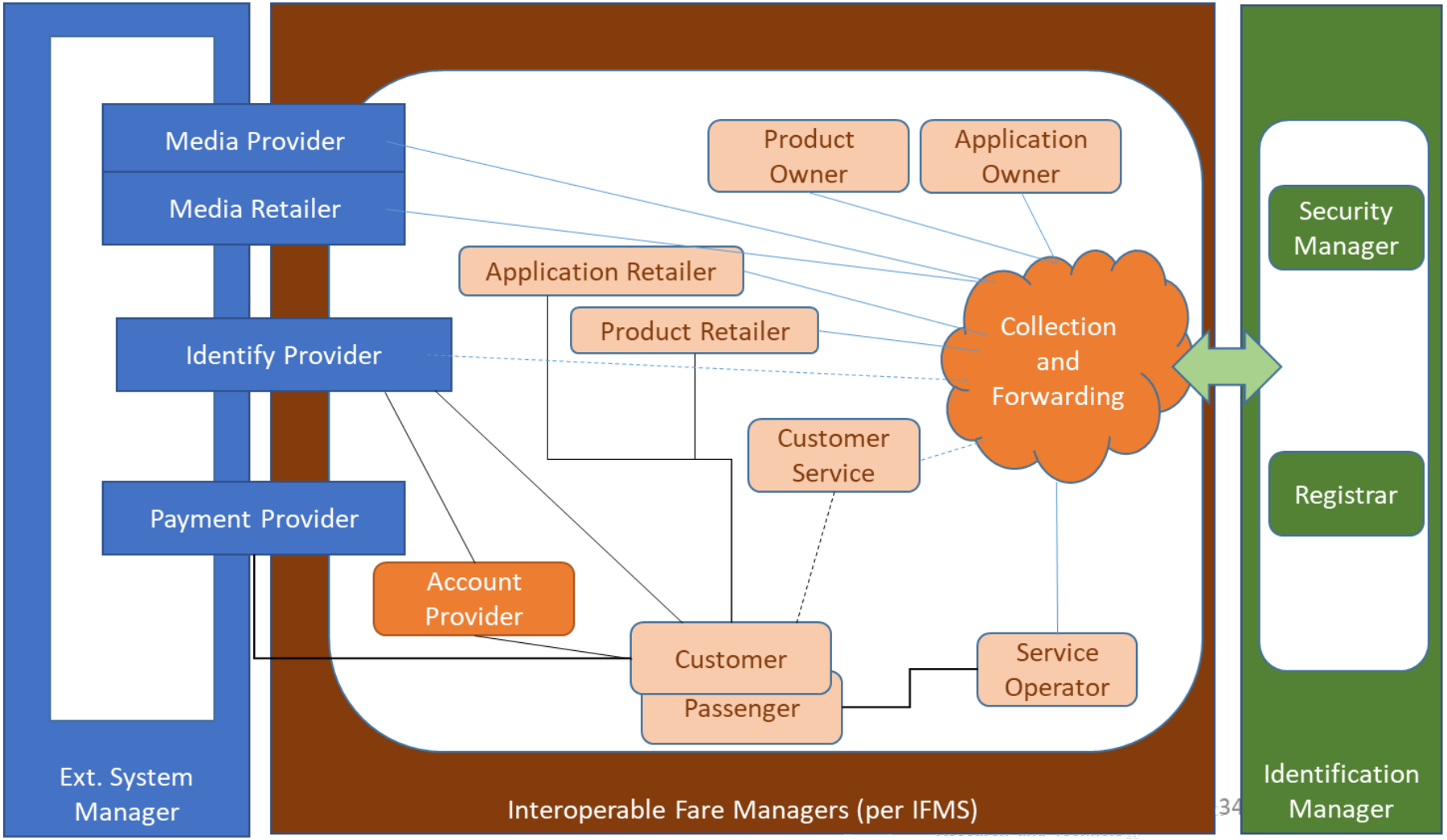


Figure 1: IFMS Concept Model

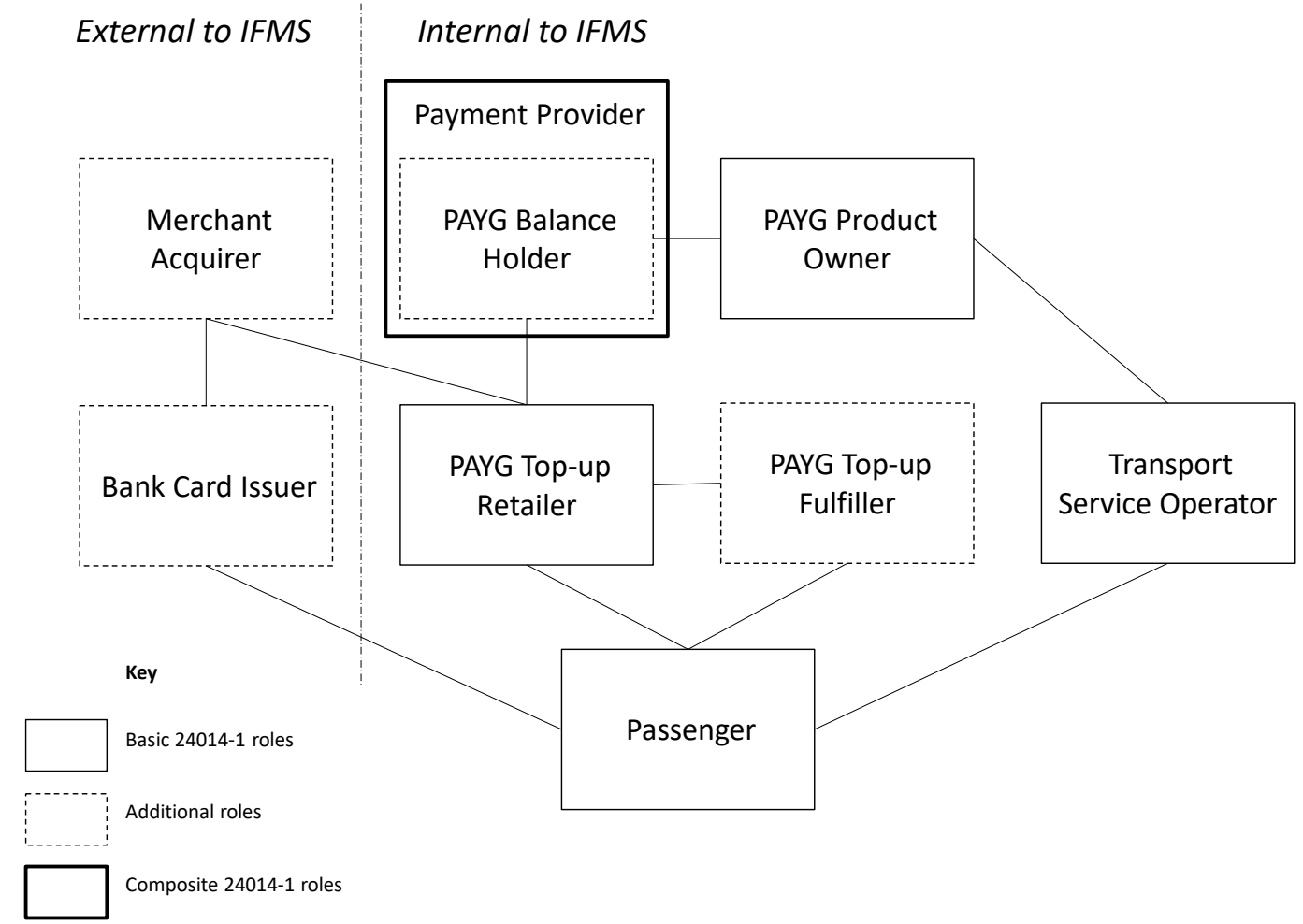


Figure 2: IFMS Architecture applied to an Open Payment Model with Transit Wallet (source: IFMS-1 v3, Appendix B)

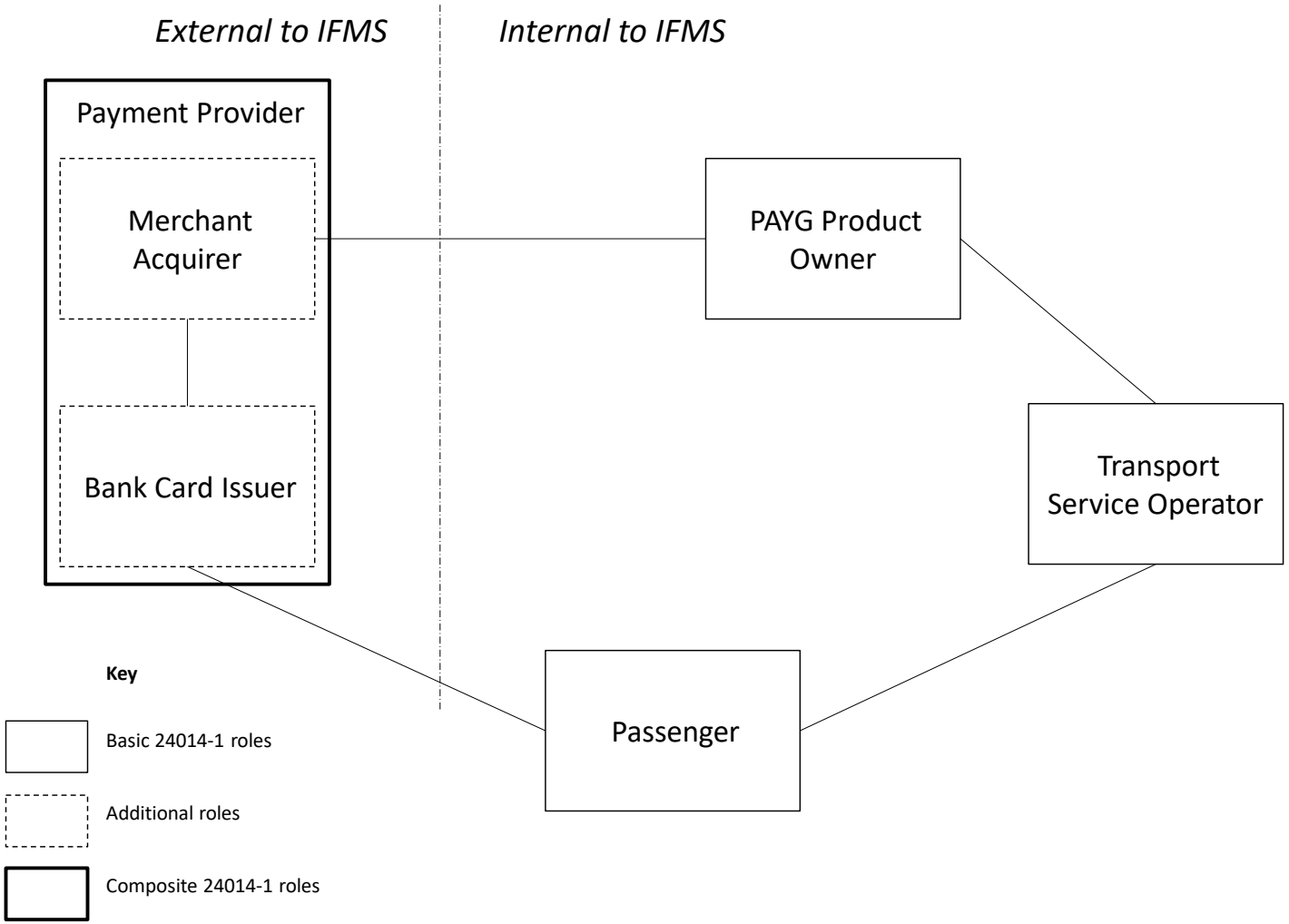


Figure 3: IFMS Architecture applied to an Open Payment with Virtual Bankcard (source: IFMS-1 v3, Appendix B)

Table 1: IFMS Roles and Responsibilities

Role	Responsibilities
Account Provider	The Account Provider supports the following functions: – provisioning and hosting of customer accounts – creates and validates Customer login credentials for access to a customer online account
Application Owner	The Application Owner holds the application contract for the use of the application with the Customer.
Application Retailer	The Application Retailer sells and terminates applications, collects, and refunds value to a Customer as authorized by an Application Owner. The Application Retailer is the only financial interface between the Customer and the IFMS related to applications.
Collection and Forwarding (set of functions)	The IFM-role of Collection and Forwarding is the facilitation of data interchanges of the IFMS. The general functions are data collection and forwarding. They contain at least the following functions: Functions of collecting – Receiving application template from Application Owner. – Receiving product template from Product Owner. – Receiving data from Service Operators. – Receiving data from Product Retailer. – Receiving data from Application Retailer. – Receiving data from Media Retailer. – Receiving data from other collection and forwarding functions. – Receiving security list data from Security Manager. – Receiving clearing reports from Product Owner. – Consistency and completeness check of the data collected on a technical level. – Receiving the address list of all IFM-roles in the IFM from the Registrar. Functions of forwarding – Forwarding “Not on Us” data to other collection and forwarding functions. – Recording “Not on Us” data. – Forwarding data with a corrupt destination address to the Security Manager. – Forwarding “On Us” data to the Product Owner for clearing and reporting. – Forwarding clearing reports, application template, product template, and security list data to the Product Retailer and Service Operator. – Forwarding application templates and security list data to the Application Retailer and Service Operator. Note 1 to entry: The concept of this connectivity functionality is as follows. – A specific Collection and Forwarding function is to collect data from one IFM-role and forward it to other IFM-roles. – Logically, there may be several Collection and Forwarding functions within the IFM. – IFM-roles may be linked to different Collection and Forwarding functions, but each IFM-role can only be linked to one. – The concept of “ON US and NOT ON US” addresses this connectivity functionality:

	– Data collected by a specific Collection and Forwarding function addressed to IFM-roles directly linked to this Collection and Forwarding function is termed “ON US” data. – Data collected by a specific Collection and Forwarding function addressed to IFM-roles not linked to this Collection and Forwarding function is termed “NOT ON US” data. – Data held by a specific Collection and Forwarding function is either “ON US” or “NOT ON US” data.
Customer	The Customer holds a customer medium with an application and acquires products in order to use the public transport services. In many cases, the Customer is also a Passenger. The Customer may also hold a personal account and external media or applications which may be used for purposes of the IFMS. The Customer may acquire customer media, applications and products for himself or other Passengers. Examples: – Parents may act as Customers and purchase products for their children. – Enterprises may act as Customers while the employees take the role of Passengers.
Customer Service	Subject to commercial agreements, Customer Service may provide “helpline” and any similar facilities including replacement of stolen and damaged customer medium and consequent product reinstalling.
Identity Provider	The Identity Provider is an IFM-role which – establishes a trustworthy scheme for creating, managing and providing customer and media ID and related attributes – ensures consistency of customer ID across the IFMS according to the set of rules – is responsible for the enrolment of customer data and the creation of derived customer ID (which may be used for customer media or applications) according to an assurance level as specified by the specific set of identity rules – provides authentication or identification mechanisms for use in the mobility platform and the IFMS according to the required assurance level. – may use external ID services as sources of trustworthy customer identities or authentication or identification mechanisms External Identity Providers may offer external ID services which are used by the IFM-internal Identity Provider as source of trustworthy ID data.
Media Provider	The role of Media Provider: is to provide and release the media for the use with one or more applications.
Media Retailer	The role of the Media Retailer is required if the application requests special provisions like a – secure element that shall be supported by the medium. – holds the contract with the Application Retailer for the use of the medium by the Application template and the application, – holds the contract and related customer service in relation to the secure element community – loads the application template onto the medium or terminates the application template.
Passenger	The Passenger uses a product to obtain the service provided by the service operator.
Payment Provider	A Payment Provider is the party that provides the function to pay for travel products with electronic transaction. This can for example be a bank account accessed by direct debit or credit transfer, a payment card account accessed through an acquirer, a transport purse held by a Product Owner, or a mobile network operator.

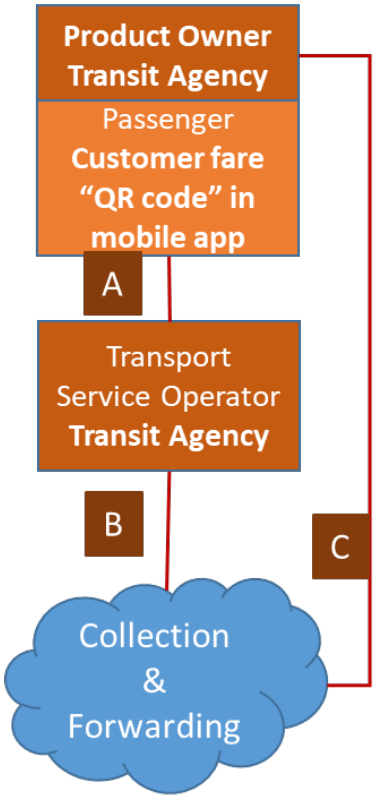
	One or more Payment Provider may be proposed to the Customer by the Product Retailer and the Customer will choose the one best suited for her/his purposes. This does not apply for virtual accounts which are activated by contactless payment service. In such case, the payment will be conducted via the Payment Provider who is referenced by the contactless payment service. The Account Provider makes payment requests to the Payment Provider on the basis of the travel consumed by the Passenger.
Product Owner	The Product Owner is responsible for his products. Functions of ownership: – Specifying pricing, usage rules, and commercial rules. Functions of clearing: – Trip reconstruction – Product aggregation based on received usage data using product definition rules (e.g. for usage-based products); – Linking of aggregated usage data with acquisition data; – Preparation of apportionment data based on product specification. Functions of reporting: – Detailed: o acquisition data with no link to usage data within the reporting period; o usage data with no link to acquisition data within the reporting period; o linked aggregated product data within the reporting period. – Summary: o apportionment data and clearing report. o Total acquisition data.
Product Retailer	The Product Retailer sells and terminates products, collects, and refunds value to a Customer as authorized by a Product Owner. The Product Retailer is the only financial interface between the Customer and the IFMS related to products. Based on his Customer relationship, the role of the Product Retailer may include the role of the Account Provider.
Registrar	After the certification, the Registrar issues unique registration codes for organizations, components, application templates, and product templates. The Registrar function also issues unique identifiers or rules for generating unique identifiers for the applications, products, and messages.
Security Manager	The Security Manager is responsible for establishing and coordinating the security policy and for – certification of organizations, application templates, components and product templates, – auditing of organizations, application templates/applications, components, and product templates/products, – monitoring the system, and – operation of the security of the IFMS, e.g. key management.
Service Operator	The Service Operator provides a service to the Customer against the use of a product.

3.1.2. IFMS Use Case Examples

This section contains the example of IFMS Use Case and Information Flow between Roles (slides 49 and 50). The use case describes the *Use and inspection of products.*

Example 1: Product owner is the transit agency, the product may be a ticket, period pass or other product issued and tracked by the transit agency.

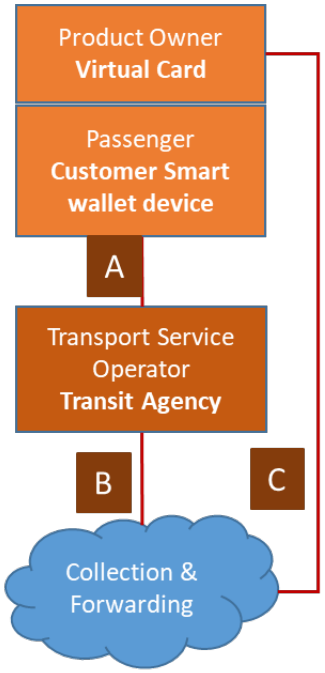
Example 2: Product owner is the customer using a virtual card that they store in their mobile app wallet.



Example using a white label with hardware model

Use case name	Use and inspection of products
Outline	The Service Operator checks and collects the data of a Customer Medium using the public transport service.
Triggered by	Service Operator
Actor(s)	Customer Service Operator Collection and Forwarding Product Owner
Use case description	A Customer who uses a product on public transport. The use case consists of several processes performed by the A Service Operator: — detection and verification of application; — detection, selection and verification of product; — verification of application and product according to security policies; B — processing of product data; — communication between customer medium and Back Office; — computation of product rules; — collection of the product usage and inspection data; C — distribution of product usage and inspection data to the Product Owner through the Collection and Forwarding. B Inspection consists of — simple detection, — detection and verification, or — detection, verification and further processing.

Figure 4: Use Case Example 1 – Transit Agency is Product Owner



Same use case but using an open payment with bank card model

Use case name	Use and inspection of products
Outline	The Service Operator checks and collects the data of a Customer Medium using the public transport service.
Triggered by	Service Operator
Actor(s)	Customer Service Operator Collection and Forwarding Product Owner
Use case description	A Customer who uses a product on public transport. The use case consists of several processes performed by the A Service Operator: — detection and verification of application; — detection, selection and verification of product; — verification of application and product according to security policies; B — processing of product data; — communication between customer medium and Back Office; — computation of product rules; — collection of the product usage and inspection data; C — distribution of product usage and inspection data to the Product Owner through the Collection and Forwarding. B Inspection consists of — simple detection, — detection and verification, or — detection, verification and further processing.

Figure 5: Use Case Example 2 -- Product Owner is Customer using Virtual Bankcard

3.2. TCRP 148 Business Model Description

This section includes descriptions of the 5 business models from the TCRP Synthesis 148 (see page 41 on the slides). The descriptions from the research are extracted and listed in Table 2.

Figure 6: 5 Fare App Business Models Described by TCRP Synthesis 148

Table 2: TCRP Synthesis 148 Business Model Description (source: TCRP Synthesis 148)

Business Model Name	Description
Shared App	In a "shared app" model, multiple transit agencies in different regions use the same mobile fare payment app provided by a single vendor. This model is quick to implement and low in cost; a shared app can be configured in a few days to add specific fare types and some limited agency branding. However, this model typically does not include integration with preexisting fare payment systems, and validation of fares is typically done only by visual inspection. The case example for this model is the City of Santa Monica's Big Blue Bus.
White Label App	This model is referred to as "white label" because the app is developed by a vendor but rebranded to look as if it were made by the transit agency. A white label app is relatively quick to deploy, comparatively low cost, and allows for configuration including specific fare types and some agency branding. When offered as a stand-alone system, white label apps are usually not integrated with preexisting fare payment systems, and they typically rely only on visual inspection for fare validation. Denver's Regional Transportation District is the case example of this model.
White Label App with Validation Hardware	This model is similar to the previous one, except it also includes hardware for validation, such as readers installed on transit vehicles. An additional vendor is typically part of the contractual process to facilitate hardware installation and integration. The costs are usually higher, and the

	deployment time may be longer. The case example for this model is Austin's Capital Metropolitan Transportation Authority.
Open Payment App	This model applies to fare payment systems that are both standards based (commonly called open payment) and account-based. Riders download the transit agency's mobile fare payment app, which can be used to manage transit accounts by reloading value or purchasing passes. Transit accounts can be loaded into mobile wallets (e.g., Apple Pay, Google Pay) using virtual cards. Fare products can be validated in different ways, such as tapping Near Field Communication (NFC) on the user's phone at readers. Because this is still an emerging model and is usually part of a fully integrated system, costs are currently high; however, this could change in the future if other agencies adopt this model. The Chicago Transit Authority is the case example.
SDK Only	The last model is an "SDK only" approach in which only a Software Development Kit (or SDK) is procured from a mobile fare payment app vendor. Then, the SDK can be integrated into other smartphone apps, such as real-time information or ridesourcing apps. This model appears to have relatively low costs (both upfront and ongoing). Validation is done visually by drivers, and there is typically limited integration with the transit agency's preexisting fare payment system. St. Catharine's Transit Commission is the case example of this model.

3.3. IFMS Architecture Applied to TCRP Business Model Descriptions

3.3.1. Shared App Model

Characteristics:

- ✓ Multiple agencies on same mobile app
- ✓ Agencies share common platform
- ✓ No hardware needed
- ✓ Validation methods
- ✓ Visual verification
- ✓ No integration with fare system
- ✓ Turnkey / service subscription

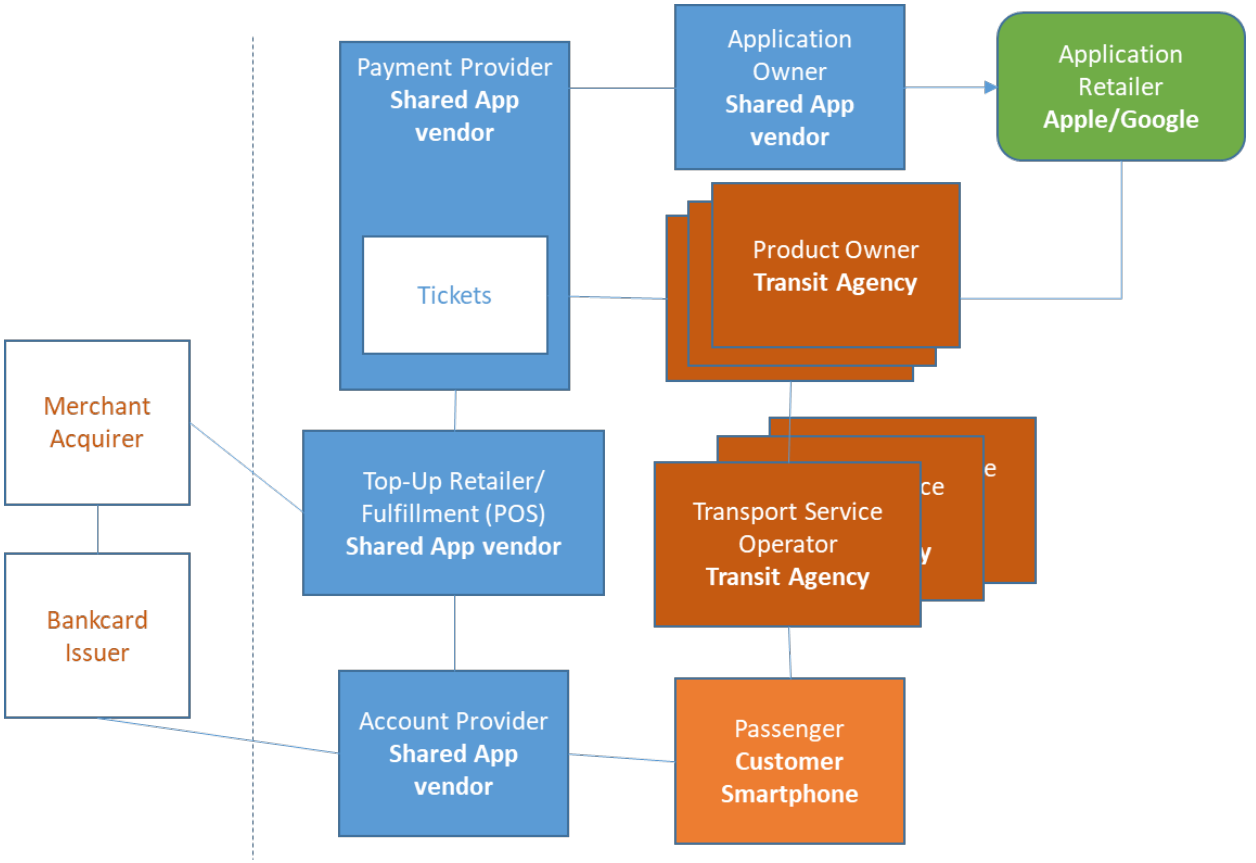


Figure 7: Shared App model using IFMS Architecture Roles

3.3.2. White Label App Model

White Label App Characteristics

- ✓ Single agency mobile app
- ✓ No hardware needed
- ✓ Validation Methods
- ✓ Visual verifiable
- ✓ QR code method
- ✓ Limited integration with fare system
- ✓ Turnkey / service subscription

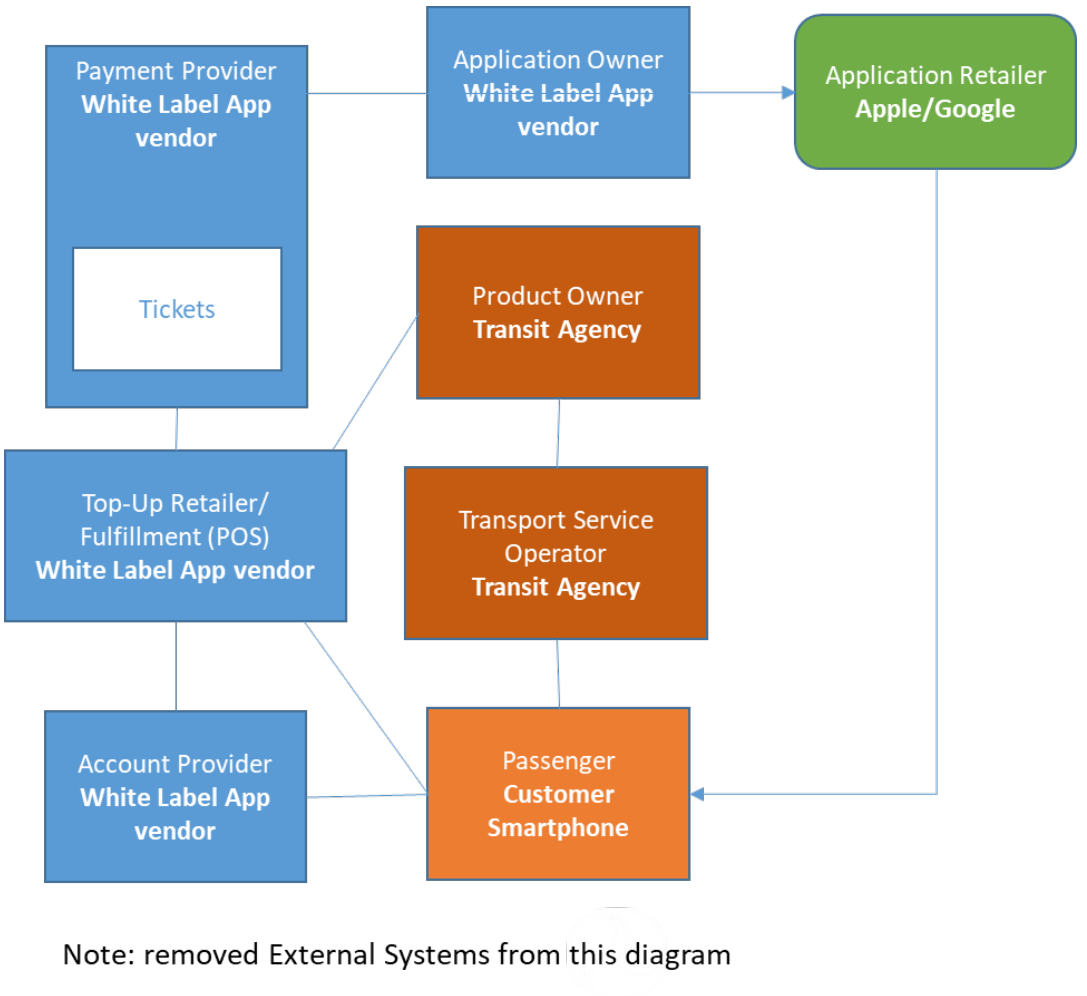


Figure 8: White Label App Model using IFMS Roles

3.3.3. White Label App with Hardware Model

White Label App with Hardware Characteristics

- ✓ Single/regional agency mobile app
- ✓ Hardware reader / validation
- ✓ Validation Methods
- ✓ QR code method
- ✓ NFC – Transit Wallet
- ✓ Limited integration with fare system
- ✓ Turnkey / service subscription

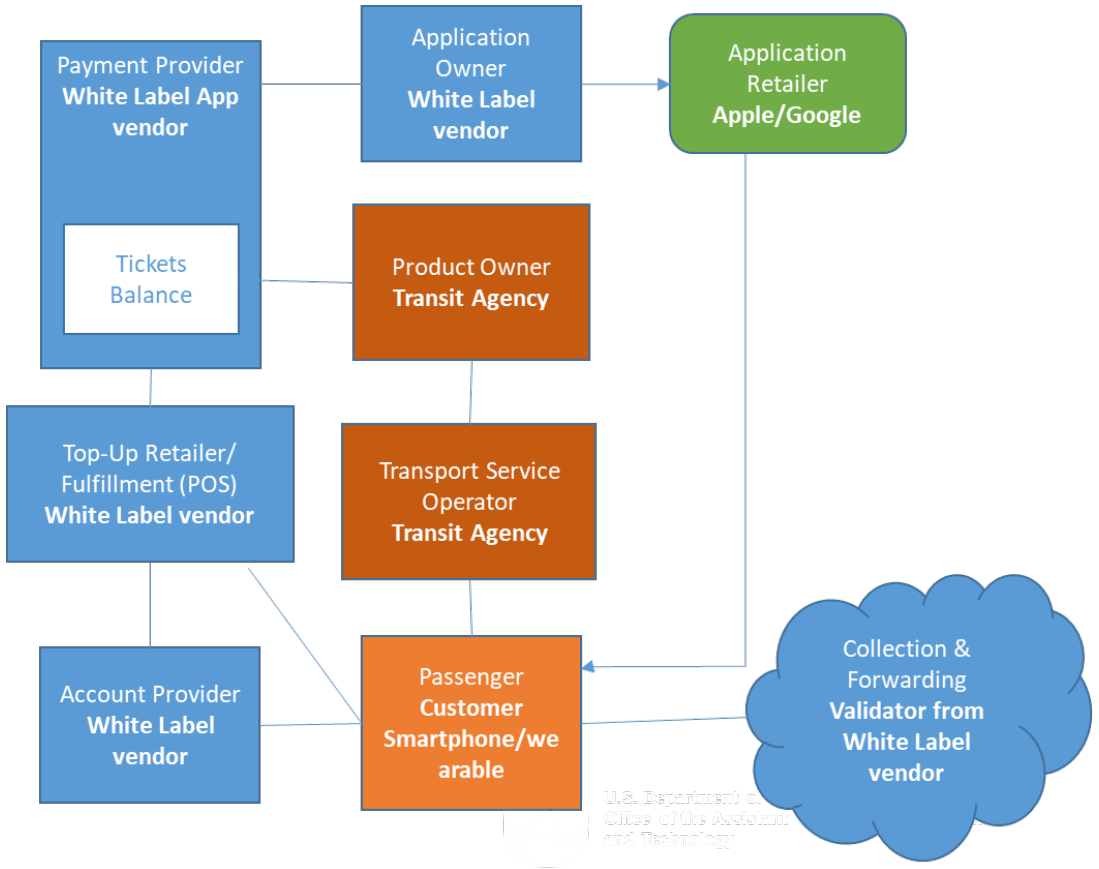


Figure 9: White Label App with Hardware Model using IFMS Roles

3.3.4. Open Payment using Bankcard Model

Open Payment using Bankcard Characteristics

- ✓ Transit's role is as a merchant
- ✓ Hardware validation using NFC
- ✓ Requires external identify and financial authentication of payment

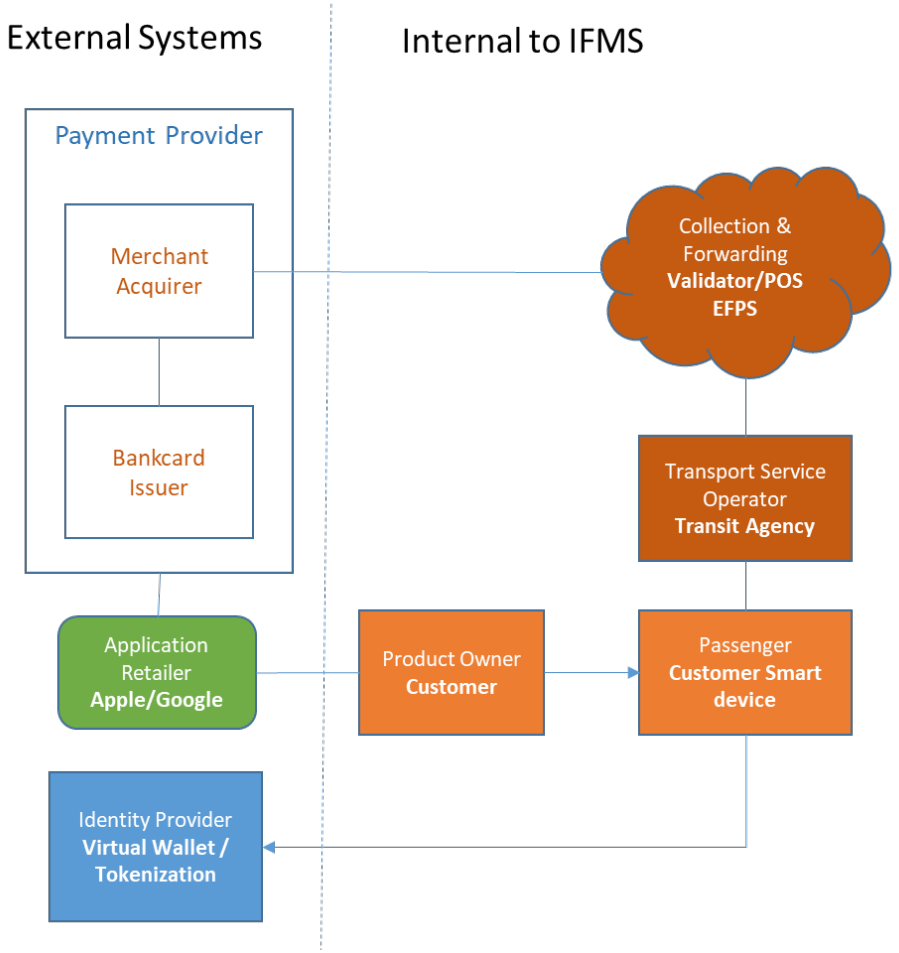


Figure 10: Open Payment using Bankcard Model using IFMS Roles

3.3.5. Open Payment using Transit Wallet Model

Open Payment using Transit Wallet Characteristics

- ✓ Multimodal mobility and event product integration
- ✓ Hardware validation using NFC
- ✓ Requires external identity and financial authentication of payment

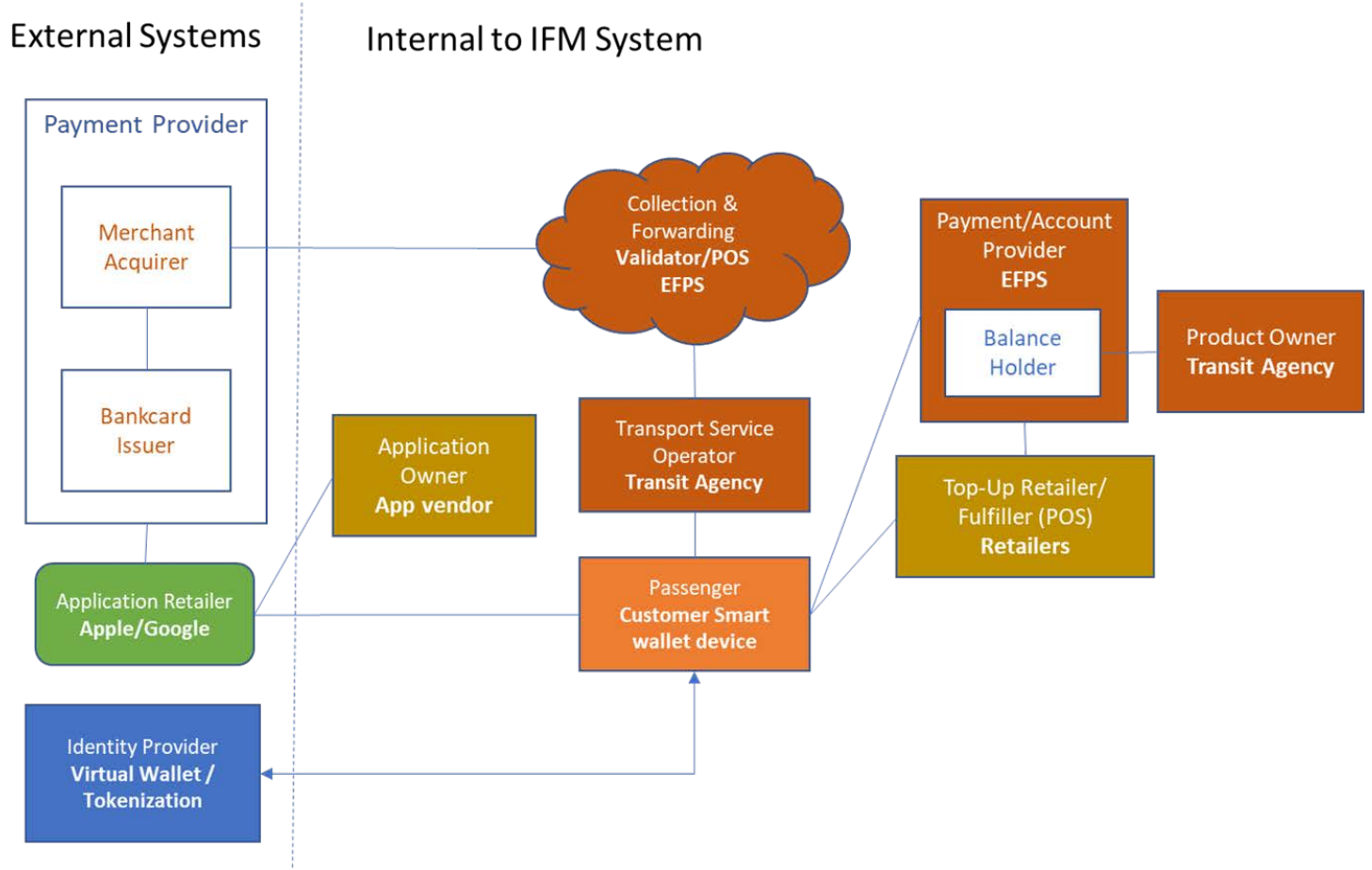


Figure 11: Open Payment using Transit Wallet Model using IFMS Roles

3.3.6. Software Development Kit Model

Software Development Kit Characteristics

- ✓ Multimodal mobility and event product integration
- ✓ Hardware validation using either QR or NFC
- ✓ Centralized payment model

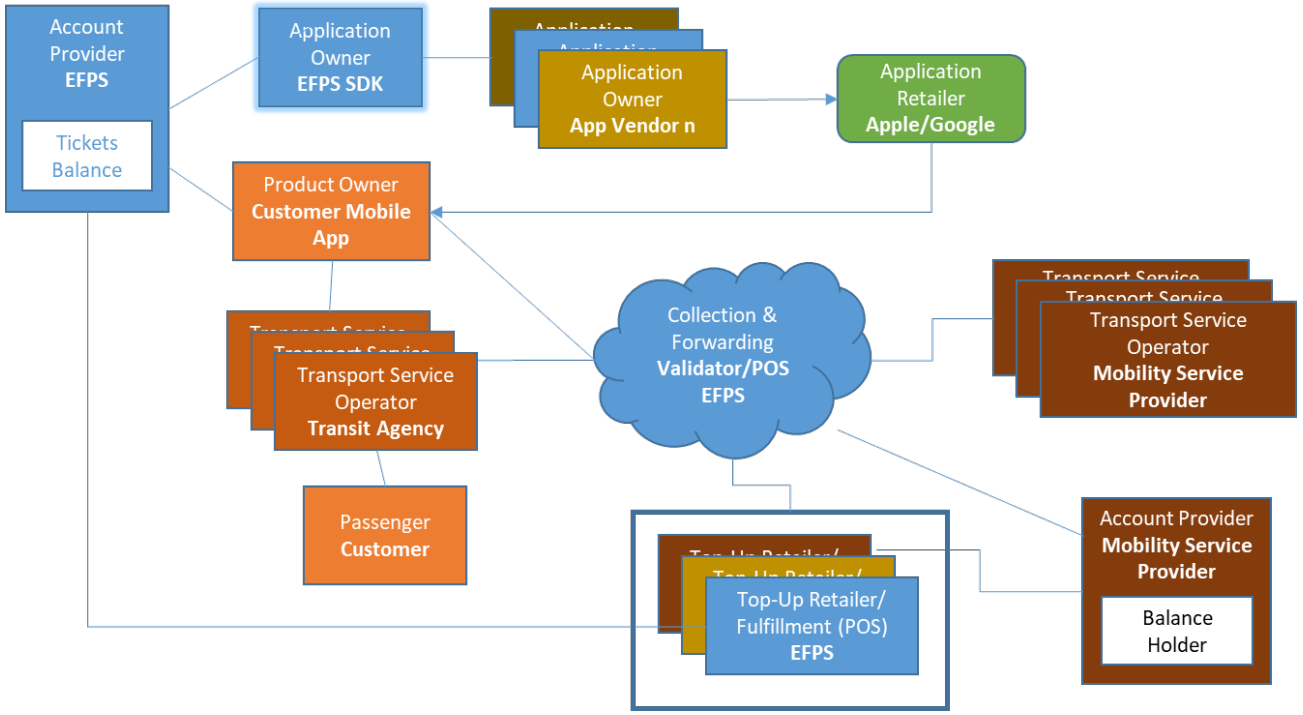


Figure **12**: Software Development Kit Model using IFMS Roles

4. Reference to Other Standards

Several standards enable mobile fare apps. The ones included in the module are listed below:

ISO/DIS 24014-1 Public transport — Interoperable fare management system — Part 1: Architecture

ISO/IEC 18004:2015 *Information – Automatic identification and data capture techniques – QR Code barcode symbology specification*

ISO/IEC 14443-2:2016 Part 2: Radio frequency power and signal interface

SO/IEC 18092 / ECMA-340—Near Field Communication Interface and Protocol-1 (NFCIP-1)

ISO/IEC 21481 / ECMA-352—Near Field Communication Interface and Protocol-2 (NFCIP-2)

5. Case Studies

5.1. Selected Case Studies from Conference Proceedings

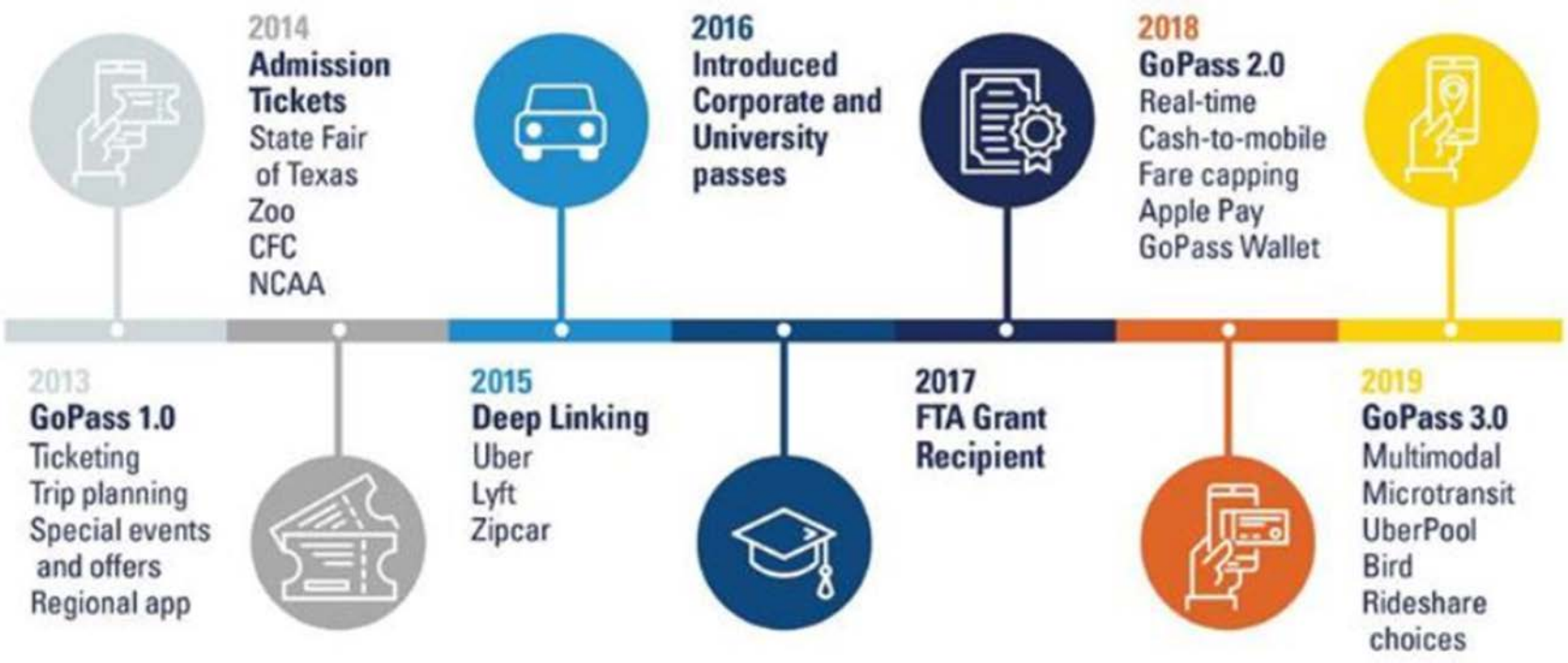
The American Public Transportation Association holds APTATech. There are many case studies and presentations from agencies, regions and vendors on lessons learned, emerging trends and challenges for mobile fare payment systems. See https://www.apta.com/conferences-events/aptatech/

The Secure Technology Alliance (SCT) includes a transportation group that publishes resources, white papers and reports on state of the practice multimodal payment systems. See https://www.securetechalliance.org/applications-transportation/ for a link to their reports and to their Knowledge Center or transportation payment.

5.2. Dallas Area Rapid Transit GoPass Case Study Presentation

Courtesy of Tina Mörch-Pierre, DART

The GoPass Journey



GoPass Mobility As A Service (MaaS) App Platform

Robust Trip Planning, Ticketing & Payment platform

Mature Multi-Agency Platform

- ✓ GoPass supports multiple Agencies across DFW region
- ✓ In operation since 2013, frequent feature additions
- ✓ Currently scaling to different regional partners
- ✓ White-label platform version also available

Multi-Modal Trip Planning

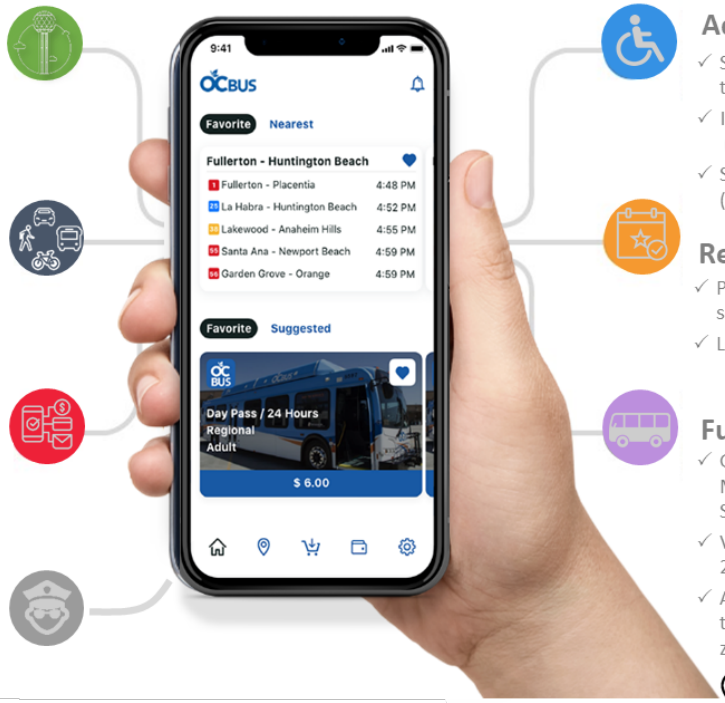
- ✓ Seamless end-to-end directions for Point A – B – C
- ✓ Real-time vehicle status updates
- ✓ Map interface displaying DART vehicles in motion
- ✓ Additional options for TNCs & Micro-Mobility (Uber, Bird)

Digital Payments & Cash to Mobile

- ✓ Cash-to-Mobile supporting unbanked riders (7-Eleven, Tom Thumb, Ace Cash Express & More)
- ✓ Google Pay, Apple Pay, All Major Credit Cards
- ✓ Digital Wallet solution for loading and storing value

Rider and Operator Safety & Security

- ✓ DART See Something-Say Something integration alerts authorities to incidents and protect rider safety
- ✓ Rider Alerts from Agency presented to flag issues to riders



Additional Rider Support

- ✓ Support to service riders in transit deserts through on-demand services
- ✓ Integrated Concessions for eligible riders (Low income programs, minors, seniors)
- ✓ Support for riders with additional needs (wheelchair, service animal)

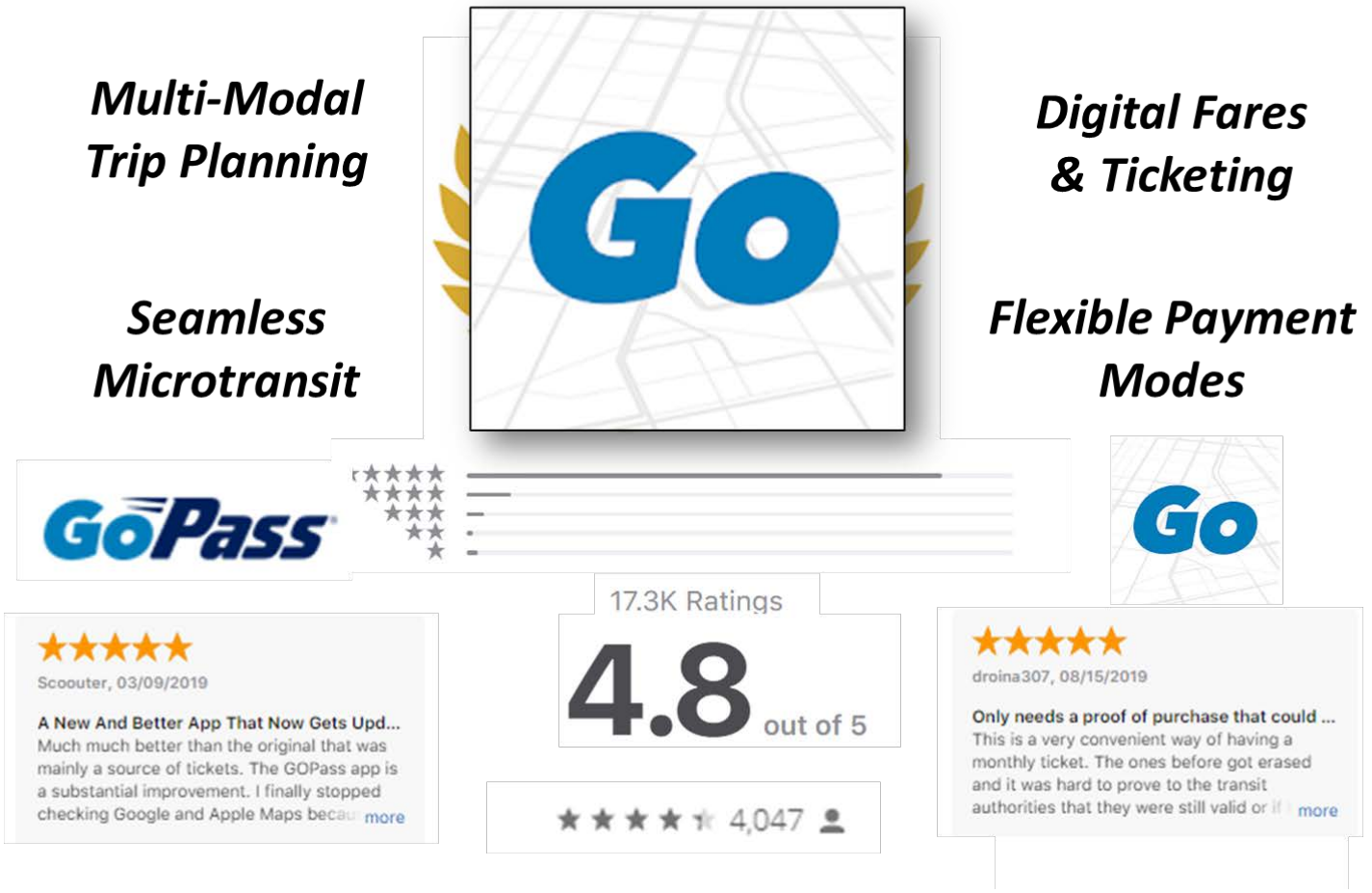
Regional Events & Wayfinding

- ✓ Presents and sell tickets to key regional events such as State Fair and NCAA events
- ✓ Local events promotion and listings through App

Fully Integrated Microtransit

- ✓ GoPass includes full integration of GoLink™ Microtransit booking and payments, powered by Spare
- ✓ VIA Microtransit integration is planned for Q3 2020
- ✓ App intelligently offers Microtransit options for trips with origin or destination within defined zones, linking to transit hubs

GoPass – Transit's Best Mobile Solution



6. Glossary

To include additional **descriptions/acronyms** used primarily in the module. Listed in alphabetical order.

Term	Definition
Activation	"The process of making a mobile fare product valid for a given period of time". [TCRP Synthesis 148]
Application Programming Interface (API)	Set of communication protocols for exchanging information between one or more applications. Payment application owners sometimes provide open APIs.
Cryptocurrency Apps and Wallets	Mobile apps to manage and pay for services. ▫ Examples of different crypto currency apps are: Coinbase, Blockchain.
Customer service for riders	Technical support for app; sale support for sales and refunds, other commendations and complaints. [TCRP Synthesis 148]
Deep Link	Relationship between multiple applications in which one app redirects users to another app
Fare Capping	a fare policy that fixes the maximum amount a customer pays for rides over a specified time period such as a day, week, or month by tracking the amount spent by registered fare media such as a smart card or mobile fare app. The policy typically replaces period passes.
Host-based Card Emulation (HCE)	A chip used as a secure element in a smartphone to secure the PII by using a unique alias or token in place of the sensitive information.
Hosting the app	The software that implements the back-office functionality including account and user management, fare product, sales/refunds, reporting, etc. [TCRP Synthesis 148]
Marketing the app to riders	Outreach and training materials to travelers and potential customers. This may include advertising and promotion of special services. [TCRP Synthesis 148]
Payment App	Mobile app that provides sales, customer services and account management support to customers.
Payment processing	Manages the financial transactions for sale transactions, validation, authentication, and tokenization.

Term	Definition
	[TCRP Synthesis 148]
PCI Compliance	Payment Card Industry security standards certification to protect device, data and functions of the system. Credit card companies and banks require annual PCI testing to ensure compliance. [TCRP Synthesis 148]
Peer-to-peer payment apps	Mobile app that enables the electronic transfer of money between two bank accounts. Examples of peer to peer payment apps include Venmo, Paypal.Me, clearXchange
Point of Sales	Sales channel where customers purchase fare media and products.
Proof of payment	Validates a fare product when proof of payment is required. Fare products include period pass or ticket was bought and activated
Software Development Kit (SDK)	Set of libraries, documentation or tools which may also include APIs that can be tailored by an app.
Tokenization	Is the process used to generate a token for the information, storing the token in an HCE, and storing the PII in a more secure environment (https://searchsecurity.techtarget.com/definition/tokenization).
Validation	In transit fare payment systems, this refers to the process or method used to assure that fare products are not fraudulent or expired [and have sufficient funds to pay the fare]. [TCRP SA-46]
Virtual card	An electronic replica of a physical card and it usually contains a randomly generated credit card number that change every time your credit card is used for a purchase. [https://creditcards.usnews.com/articles/virtual-credit-cards-explained] extracted Jan 23, 2020.
Virtual wallet	Store virtual cards that emulate contactless bankcards (support ISO 14443 and NFC) stored in a mobile operating system "wallet". ▫ Bank cards such as PNC ▫ Ventra Apple wallet (Ventra is the Chicago area multiagency fare system) ▫ OMNY Google wallet
Walled Garden	Closed ecosystem in which all operations are controlled by the ecosystem operator.

7. References

Brakewood, C. (2020). Mobile Fare APPs Business Models. TCRP, Synthesis 148 (from TCRP Synthesis J-07/Topic SA-46 Mobile Fare APPs Business Models). Washington, DC: The National Academies Press.

Kok, J., & Lipták, R. (2020). Multimodal Fare Payment Integration. TCRP, Synthesis 144, pp.86. Washington, DC: The National Academies Press.

Okunieff, P. (2017). Multiagency Electronic Fare Payment Systems. TCRP, Synthesis 125, pp.131. Washington, DC: The National Academies Press.

8. Study Questions

To include the quiz/poll questions and answer choices as presented in the PowerPoint slide to allow students to either follow along with the recording or refer to the quiz at a later date in the supplement.

1. Who does the primary marketing of an agency's fare app to riders?
    a) Vendor
    b) Social Media
    c) Agency
    d) App Store

2. What payment access method is most proprietary?
    a) SDK
    b) API
    c) Walled Garden
    d) Deep Link

3. What is a Software Development Kit?
    a) A stand-alone application can be installed on a workstation
    b) A first aid kit for your computer
    c) A set of interfaces that can be used to exchange information between two applications
    d) A software library for building applications, interfaces, and user interfaces

4. Which of the following is an incorrect statement related to the RTD Mobile App?
    a) The RTD mobile fare app is implemented as a SaaS
    b) RTD manages the interface with Uber
    c) RTD uses visual verifiable validation of mobile fare products
    d) All fare products offered on RTD's mobile fare app are also offered on the Uber app

9. Icon Guide

The following icons are used throughout the module to visually indicate the corresponding learning concept listed out below, and/or to highlight a specific point in the training material.

1) **Background information:** General knowledge that is available elsewhere and is outside the module being presented. This will be used primarily in the beginning of slide set when reviewing information readers are expected to already know.

2) **Tools/Applications:** An industry-specific item a person would use to accomplish a specific task, and applying that tool to fit your need.

3) **Remember:** Used when referencing something already discussed in the module that is necessary to recount.

4) **Refer to Student Supplement:** Items or information that are further explained/detailed in the Student Supplement.

5) **Example:** Can be real-world (case study), hypothetical, a sample of a table, etc.

6) **Checklist:** Use to indicate a process that is being laid out sequentially.