INTERNATIONAL STANDARD

ISO 24014-1

Third edition
2021-01

Public transport — Interoperable fare management system —

Part 1: Architecture

Transport public — Système de gestion tarifaire interopérable —

Partie 1: Architecture

Reference number
ISO 24014-1:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 278, *Intelligent transport systems,* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This third edition cancels and replaces the second edition (ISO 24014-1:2015), which has been technically revised.

The main changes compared to the previous edition are as follows:

— in order to prepare compatibility of Interoperable Fare Management (IFM) systems with mobility platforms encompassing the entire mobility service chain, functions and roles known from IFM are expanded; and

— new roles are introduced to operate mobility platforms.

A list of all parts in the ISO 24014 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Fare management (FM) encompasses all the processes designed to manage the distribution and use of fare products in a public transport environment.

Fare management is called interoperable (IFM) when it enables the customer to use a portable electronic medium (e.g. a contact/contactless smart card or a Near Field Communications mobile device) with compatible equipment (e.g. at stops, with retail systems, at platform entry points or on board vehicles). IFM concepts can also be applied to fare management systems not using electronic media.

Potential benefits for the customer include reductions in queuing, special and combined fares, one medium for multiple applications, loyalty programmes and seamless journeys.

There are two main changes in this edition of this document compared to the previous edition. Firstly, in order to prepare compatibility of IFM systems with mobility platforms encompassing the entire mobility service chain, functions and roles known from IFM are expanded. Secondly, new roles are introduced to operate mobility platforms. These new roles should act with the roles defined in the IFM and enter into interface relations.

With the introduction of so-called mobility platforms, which can integrate various IFM systems and additional modes of transportation and deliver the travel information across these integrated domains, the customer can benefit from seamless and well-guided multi- or inter-modal travel.

Interoperability of fare management systems also provides benefits to operators and the other parties involved. However, it requires an overall system architecture that defines the system functionalities, the actors involved and their roles, the relationships and the interfaces between them.

Interoperability also requires the definition of a security scheme to protect privacy, integrity, and confidentiality between the actors to ensure fair and secure data flow within the IFM system (IFMS). The overall architecture is the subject of this document, which recognizes the need for legal and commercial agreements between members of an IFMS, but does not specify their form. The technical specifications of the component parts and, particularly, the standards for customer media (e.g. smart cards) are not included.

Note that there is not one single IFMS. Individual operators, consortia of operators, public authorities, and private companies can manage and/or participate in IFMSs. An IFMS can span country boundaries and can be combined with other IFMSs. Implementations of IFMSs require security and registration functionalities. This document allows for the distribution of these functions to enable the coordination/convergence of existing IFMSs to work together.

This document intends to provide the following benefits:

a) It defines a common definition of terms and roles that shall constitute the basis for the other parts of ISO 24014 and technical specifications and technical reports from ISO/TC 204 which address mobility platforms, fare management and interoperability between IFM and other systems.

b) It provides a framework for an interoperable fare management implementation with minimum complexity.

c) It provides guidance on how IFM Managers can benefit from external devices and services and how interoperability and appropriate security level can be established in cooperation with systems from other markets.

d) It aims to shorten the time and lower the cost of IFMS procurement as both suppliers and purchasers understand what is being purchased. Procurement against an open standard reduces cost as it avoids the need for expensive bespoke system development and provides for second sourcing.

e) It aims to simplify interoperability between IFMSs to the benefit of all stakeholders.

In Annex A, this document provides a framework for mobility platforms that integrate fare management and travel information for inter- and multimodal travel. This document also contains other informative

annexes, which elaborate on some specific subjects of the document and offer some national examples with regard to IFMS implementations (see Annex B, Annex C, Annex D and Annex E).

Public transport — Interoperable fare management system —

Part 1: Architecture

1 Scope

This document gives guidelines for the development of multi-operator/multi-service interoperable public surface (including subways) transport fare management systems (IFMSs) on a national and international level.

This document is applicable to bodies in public transport and related services which agree that their systems need to interoperate.

This document defines a conceptual framework which is independent of organizational and physical implementation. Any reference within this document to organizational or physical implementation is purely informative.

This document defines a reference functional architecture for IFMSs and establishes the requirements that are relevant for ensuring interoperability between several actors in the context of the use of electronic tickets.

The IFMS includes all the functions involved in the fare management process, such as:

— management of media,

— management of applications,

— management of products,

— security management, and

— certification, registration, and identification.

This document defines the following main elements:

— identification of the different sets of functions in relation to the overall IFMS and services and media from non-transport systems which interact with fare management systems;

— a generic model of an IFMS describing the logical and functional architecture and the interfaces within the system, with other IFMSs and with services and media from non-transport systems;

— use cases describing the interactions and data flows between the different sets of functions;

— security requirements.

In its annexes, this document provides a framework for mobility platforms that integrate fare management and travel information for inter- and multimodal travel (see Annex A). It also elaborates on specific subjects covered in document and offers some national examples with regard to IFMS implementations (see Annex B, Annex C, Annex D and Annex E).

This document does not define:

— the technical aspects of the interface between the medium and the medium access device;

— the data exchanges between the medium and the medium access device;

NOTE The data exchanges between the medium and the medium access device are proposed by other standardization committees.

— the financial aspects of fare management systems (e.g. customer payments, method of payment, settlement, apportionment, reconciliation).

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
account-based ticketing
ABT
architectural approach that stores *products* (3.30) in the *IFM* (3.19) system's back-office (i.e. the customer's personal account or a temporary account) and not in the *customer medium* (3.12)

Note 1 to entry: The customer medium carries authentication credentials and an *application* (3.7) that contains references to the account-based products in the back-office.

3.2
action list
list of items related to *IFM* (3.19) *applications* (3.7) or *products* (3.30) downloaded to *medium access devices* (3.24) (MADs) processed by the MAD if and when a specific IFM application or product referenced in the list is encountered by that MAD

3.3
actor
person, *organization* (3.25), or another (sub)system playing a coherent set of functions when interacting with the *IFM system* (3.20) within a particular *use case* (3.36)

3.4
application rules
specification of rules in the *application* (3.7) contract for the use of the application with the Customer as defined by the application owner

3.5
application specification
specification of functions, data elements, and security scheme according to the *application rules* (3.4)

3.6
application template
executable technical pattern of the *application specification* (3.5)

3.7
application
implemented and initialized *application template* (3.6)

Note 1 to entry: The application may host one or more *products* (3.30) and may support functions which identify and protect the access to these products. For ABT- and ID-based architectures, the application may reside partly in the *customer medium* (3.12) (identification and access control function) and partly in the *IFM* (3.19) back-office (products).

Note 2 to entry: The application is identified by a unique identifier.

Note 3 to entry: The application may house *products* (3.30) and other optional customer information (customer details, customer preferences).

Note 4 to entry: The application can be fully installed on customer media or distributed on the customer media and the IFM back-offices.

3.8
commercial rules
rules defining the settlement and commission within the *IFMS* (3.20)

3.9
component
any piece of hardware and/or software that performs one or more functions in the *IFMS* (3.20)

3.10
component provider
anyone who wants to bring a *component* (3.9) to the *IFMS* (3.20)

3.11
customer account
data space hosted by the *IFMS* (3.20) (typically the product retailer) that contains all information which is relevant for the business relationship between the Customer and the IFMS

Note 1 to entry: Accounts are maintained and managed by the responsible stakeholder in the IFMS. Accounts which are accessible online may also be established and managed by the Customer.

3.12
customer medium
medium (3.22) initialized with an *application* (3.7) through an application contract

3.13
derived identity
derived ID
electronic identifier generated from another *ID* (3.15) (primary ID)

Note 1 to entry: Typically, the derived ID is generated by an identity provider in such a way that the authenticity of the derived ID can be proven but there is no way to conclude from the derived ID back to the primary ID. The concept of derived ID is typically used when primary ID with high security demand (like driver licence or governmental eID) shall not be exposed to an environment that doesn't support high assurance levels.

3.14
external
object which does not follow the rules of the *IFMS* (3.20) and for which special activities are necessary to implement interoperability and security with the IFMS

3.15
identity
ID
information that describes a specific person or object in a unique and unambiguous way

Note 1 to entry: For instance, a person can be described by the attributes name, birth date, sex, address, etc. Unambiguous identification of a person typically needs, in addition, a unique identifier which is issued by the Identity Provider. An object, e.g. a ticketing machine, can be described by owner, type, and software version. A unique serial number could serve as identifier.

3.16
IFM functional model
model to define functions of *IFM roles* (3.18) and how they interact

3.17
IFM policy
commercial, technical, security, and privacy objectives of *IFM* (3.19)

3.18
IFM role
abstract object performing a set of functions in an *IFM functional model* (3.16)

3.19
interoperable fare management
IFM
all the functions involved in the fare management process such as management of *application* (3.7), *products* (3.30), security and certification, registration, and identification to enable Customers to travel with participating Service Operators using a single portable electronic *medium* (3.22)

3.20
interoperable fare management system
IFMS
all technical, commercial, security, and legal elements which enable *interoperable fare management* (3.19)

3.21
level of assurance
LoA
level of resilience of *IFMS* (3.20) *components* (3.9) and processes against a defined attack potential

Note 1 to entry: to entry; Level of assurance is typically defined by the Security Manager for all components of the IFMS and specified in the *set of rules* (3.33) for security certification.

3.22
medium
physical carrier of *applications* (3.7)

3.23
message
set of data elements transferred between two *IFM roles* (3.18)

3.24
medium access device
MAD
device with the necessary facilities (hardware and software) to communicate with a *customer medium* (3.12)

3.25
organization
legal entity covering the functions and implied responsibilities of one or more of the following operational *IFM roles* (3.18): Application Owner, Application Retailer, Product Owner, Product Retailer, Service Operator, Collection and Forwarding, etc.

3.26
pricing rule
rules defining the price and payment/billing relationships to the Customer

3.27
product rule
usage, pricing, and *commercial rules* (3.8) defined by the Product Owner

3.28
product specification
complete specification of functions, data elements, and security scheme according to the *product rules* (3.27)

3.29
product template
technical pattern of the *product specification* (3.28)

Note 1 to entry: The product template is identified by a unique identifier.

3.30
product
instance of a *product template* (3.29) stored in an *application* (3.7)

Note 1 to entry: A product defines a commercial offer to the Customer. By purchasing a product, the Customer is entitled to obtain specific services which are defined by the Product Owner.

Note 2 to entry: It is identified by a unique identifier and enables the Customer to benefit from a service provided by a Service Operator.

3.31
role
abstract object performing a set of functions

3.32
security policy
objectives of the *IFMS* (3.20) to secure the public interests and the assets within the IFMS

3.33
set of rules
regulations for achieving *IFM policies* (3.17) expressed as technical, commercial, security, and legal requirements and standards relevant only to the IFMS

3.34
trigger
event that causes the execution of a *use case* (3.36)

3.35
usage rule
rule defining the usage time, the usage area, the personal status and the type of service

3.36
use case
description of a process by defining a sequence of actions performed by one or more *actors* (3.3) and by the system itself

4 Abbreviated terms

KYC know your customer

NFC near field communication

PAYG pay-as-you-go

PT public transport

5 Requirements

The purpose of the ISO 24014 series is to achieve interoperability throughout fare management systems while making sure that participating companies in PT remain as commercially free as possible to design their own implementation in pursuing their own business strategies.

In addition, interoperability between individual IFMS, with external systems and services and also the integration of IFMS by so-called mobility platforms shall be specified.

Specific requirements of the IFMS model are as follows:

— A Customer shall be able to travel with all participating Service Operators (seamless journey) using a single medium.

— There shall be a capability to extract data appropriate to the revenue-sharing and statistical requirements of the Service Operators.

— The same medium may carry additional applications in addition to the IFM application. Conversely, external media may carry the IFM application.

— The methods associated with the application shall offer the opportunity to reduce the current time taken to enter/exit the PT system and may reduce payment handling costs significantly.

— The IFMS model shall provide the capability to accommodate new product specifications as required regardless of those already in existence.

— The IFMS model shall recognize and prevent internal or external fraud attacks.

— The IFMS model shall facilitate a balance between measures for security and fraud avoidance against the need to offer Customer convenience and performance.

— The IFMS model shall have the capability to identify the Customer while protecting their privacy as appropriate.

— The IFMS model shall ensure the integrity of exchanged data.

— The IFMS model shall enable the implementation of additional services: loyalty programmes, car sharing, park and ride, bike and ride, etc.

— The IFMS model shall provide interface definitions between identified functions within PT or other modes of transportation to enable different operator networks to interoperate.

— The IFMS model shall describe interfaces which are essential to enable data-forwarding functions between different operator networks allowing revenue-sharing agreements to be met.

— The IFMS model shall provide a framework from which commercial agreements may be developed.

— The IFMS model shall be neutral with regard to different technologies which can be deployed [e.g. contact medium, contactless medium (short range, wide range), external devices, independent of access technologies, account-, cloud- or ID-based concepts].

— The IFMS model shall be functionally neutral regarding specific transport organization structures.

— The IFMS model shall support the introduction of and migration to new technologies and architecture concepts and interoperability with media, applications and systems from other market sectors.

6 System environment for IFMS

6.1 General

Previous editions of this document have focused on interoperability between fare management systems. However, recent trends and market developments require enhancements of the IFMS architecture, interoperability with other PT systems and also interoperability with systems, customer media and applications from other market sectors. This system environment for IFMS is illustrated in Figure 1 below.

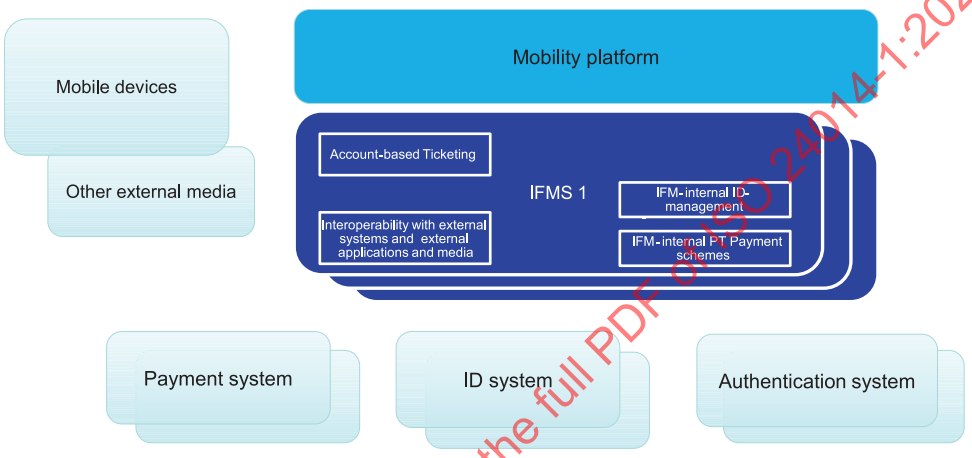


Figure 1 — System environment for IFMS

6.2 Mobility platforms

The approaches mentioned so far are primarily related to IFMS. However, advanced travel information systems and complex mobility platforms offer functionalities encompassing the entire service chain, of which fare management is only a part. For the comprehensive modelling of the roles in the context of travel information systems and their interdependencies, extensions are needed on the travel information side.

In order to integrate IFMSs in mobility platforms, functions and roles known from IFM should be expanded. In addition, new roles are required to operate mobility platforms. These new roles should act with the roles defined in the IFM and enter into interface relations.

This document defines a possible approach to mobility platforms in Annex A.

7 Conceptual framework for IFMS

7.1 General

The IFMS may be operated by a single transport undertaking, a transport authority, an association of public and private companies, or other groups.

An IFM Manager establishes and manages the IFM policies on behalf of the IFMS. These policies are embedded in the set of rules.

To manage the elements of the IFMS dealt with in this document, the IFM Manager shall appoint:

— Security Manager, and

— Registrar.

The functions and the responsibilities of the Security Manager and the Registrar can be distributed to several organizations within an IFM.

Cooperation between several IFMS requires that the IFM Managers establish a joint set of rules and synchronize the activities of the IFMS's Security Managers and Registrars. Alternatively, the roles of the Security Manager and the Registrar could be merged in order to serve all involved IFMS.

The IFM manager is also in charge if the IFMS wants to establish interoperability with external systems, components or services. In such a case, the IFM Manager and the managers of the external systems have to agree on sets of rules that establish and maintain interoperability between the IFMS and external roles, services or components.

7.2 Description of IFM roles and external roles

IFM roles are identified by capitalized initial letters of each word.

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 and specifies the application rules for the use of the application with the Customer.
Application Retailer	The Application Retailer sells and terminates applications, collects value, 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.

Within this context, 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 may 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 PT 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/herself 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 a source of trustworthy ID data.
Media Provider	The role of Media Provider: — is to provide and release the media for 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. The Media Retailer: — 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 an electronic transaction. This can be, for example, 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 chooses the one best suited for his/her purposes. This does not apply for virtual accounts which are activated by a contactless payment service. In such a case, the payment is 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 its products. **Functions of ownership:** — Specifying pricing according to pricing rules, 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: — acquisition data with no link to usage data within the reporting period; — usage data with no link to acquisition data within the reporting period; — linked aggregated product data within the reporting period. — Summary: — apportionment data and clearing report. — 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 its Customer relationship, the role of the Product Retailer may include the role of the Account Provider.

Registrar	After 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.

7.3 Basic framework of the generic IFM functional model

The links between the operational roles of the IFMS and connected external systems are illustrated in Figure 2. Roles that have been introduced in the third edition of this document are indicated in shaded boxes.

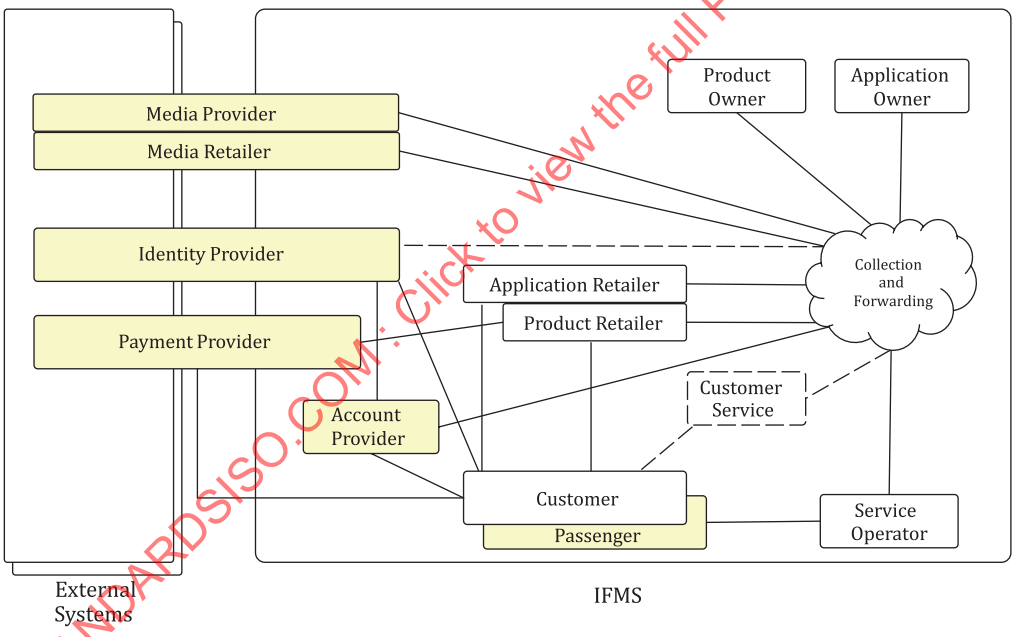


Figure 2 — Links between operational roles

These links represent information flows. Optional links and roles are drawn in dotted lines. Within an IFMS, there may be several organizations performing the functions of the IFM roles. Also, IFM roles may be aggregated by the particular IFM into own role definitions.

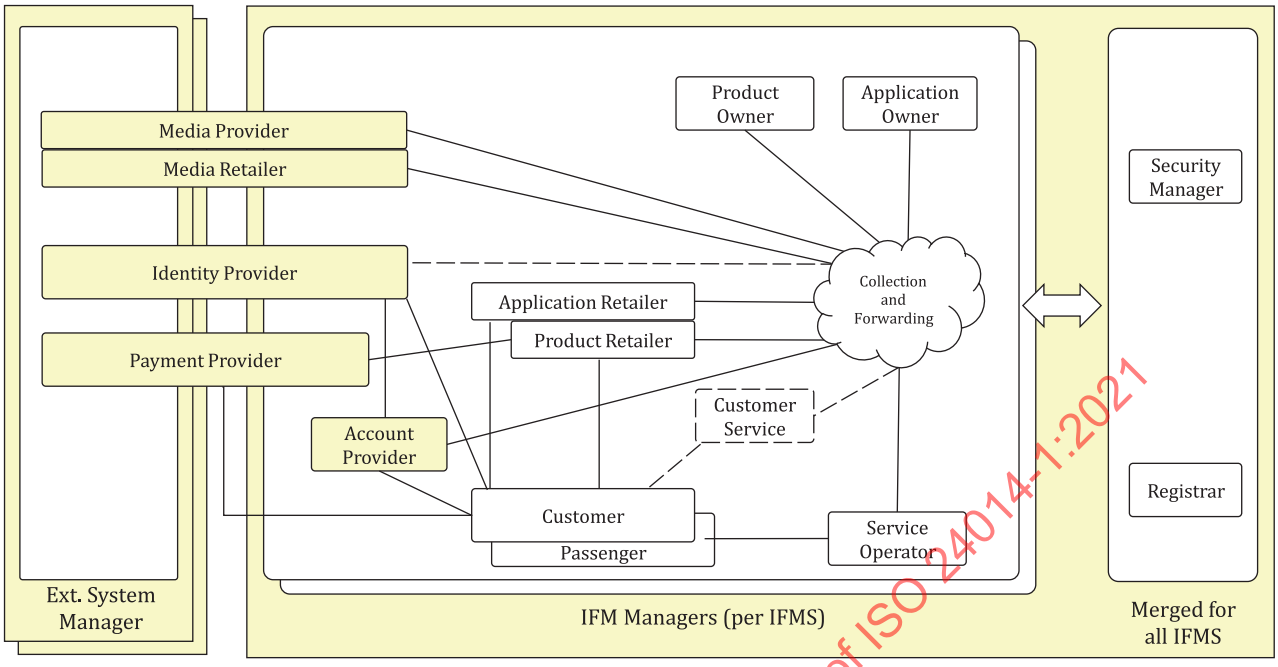


Figure 3 — Interaction of IFM domains and with external systems (operational and management roles)

Figure 3 also shows the two domains of IFM roles and the connection between them. It also shows the interaction with roles from external systems.

In addition to the IFM role model which was described in previous editions of this document, there are new roles which are indicated in shaded boxes. The IFM manager has relationships with Media Retailers. The Customer has a relationship with the issuer of the customer medium that he/she holds. Also, the Application Owner has relationships with Media Providers.

The interactions between IFM roles are described in detail in Clause 8.

8 Use case description for the IFM functional model

8.1 Description of IFM-roles and external roles

This clause describes use cases for the operation of an IFMS. The set of use cases described herein provides a toolbox for the implementation of an IFMS. Where processes described within a use case are implemented within an IFM, the use case is mandatory.

However, use cases may be adapted with modification depending on ways of management of applications and products. An application or a product can be managed either in a media centric or back-office centric way. Any variation or combination between these two approaches may be possible.

Media centric management:

> Main processes (e.g. fare calculation, billing) of management of the product are performed between a Medium and MAD.

Back-office centric management / account-based ticketing:

> Main processes of management of the product are performed in the back-office.

The following use cases describe functional aspects of the IFMS. Execution of each use case starts with a trigger, as indicated in each use case description. Contractual matters are outside the scope of this document, but are a prerequisite to implementation.

8.2 Define set of rules

8.2.1 General

Each object to be brought into the IFM should meet the IFM requirements. The proof of conformance is given by checking the object against a set of rules. This set of rules shall be defined as the first step of the onboarding process.

Within the IFM, sets of rules are required for:

— organizations,

— components with specific demands for security or interoperability,

— Customer accounts,

— media,

— ID services,

— payment services,

— application specifications and templates, and

— product specification and template.

The IFM Manager or its representatives define the sets of rules.

8.2.2 Define set of rules for Customer accounts

Use case name	**Define set of rules for Customer accounts**
Outline	Define set of rules for Customer accounts
Triggered by	IFM Manager
Actor(s)	IFM Manager Account Provider
Use case description	Definition of a set of rules for Customer accounts or service which – enforces interoperability with the components and applications of the IFMS; and – enforces an LoA as requested by the IFMS for the targeted applications and products.

8.2.3 Define set of rules for media

Use case name	**Define set of rules for media**
Outline	Define set of rules for media
Triggered by	IFM Manager
Actor(s)	IFM Manager Media Provider
Use case description	Definition of a set of rules for the media which: – enforces interoperability with the components and applications of the IFMS; and – enforces an LoA as requested by the IFMS for the targeted applications and products.

8.2.4 Define set of rules for ID services

Use case name	Define set of rules for ID services
Outline	Define set of rules for ID services
Triggered by	IFM Manager
Actor(s)	IFM Manager Identity Provider
Use case description	Definition of a set of rules for the ID application or service which: – enforces interoperability with the components and applications of the IFMS; and – enforces an LoA as requested by the IFMS for the targeted applications and products.

8.2.5 Define set of rules for payment services

Use case name	Define set of rules for payment services
Outline	Define set of rules for payment services
Triggered by	IFM Manager
Actor(s)	IFM Manager Payment Provider
Use case description	Definition of a set of rules for the payment application or service which: – enforces interoperability with the components and applications of the IFMS; and – enforces an LoA as requested by the IFMS for the targeted applications and products.

8.3 Certification

8.3.1 General

Each object to be brought into the IFM should meet the IFM requirements. The proof of conformance is given by checking the object against a set of rules. This process is called certification.

Within the IFM, the certification certifies:

— organizations,

— components with specific demands for security or interoperability,

— media,

— eID services,

— payment services,

— application specifications and templates, and

— product specifications and templates.

The IFM Manager is responsible for certifications. It may delegate security certifications to the Security Manager.

8.3.2 Certification of organizations

Use case name	Certification of organizations
Outline	Each organization which wants to participate in the IFM shall agree to abide by the set of rules.
Triggered by	Organization
Actor(s)	IFM Manager Organization
Use case description	If the IFM Manager confirms that the organization agrees to abide by the set of rules, — the organization will be certified, — else the organization will not be certified.

8.3.3 Certification of components

Use case name	Certification of components
Outline	Each component to be brought into the IFM shall meet the IFM requirements. Proof of this is given by checking this component against a set of rules.
Triggered by	Component provider
Actor(s)	IFM Manager Component provider
Use case description	The IFM Manager checks the component against the set of rules. If the component is conformant with the set of rules, — the component will be certified, — else the component will not be certified.

8.3.4 Certification of media

Use case name	Certification of media
Outline	Each medium to be brought into the IFM shall meet the IFM requirements. Proof of this is given by checking this medium against a set of rules.
Triggered by	Media Provider
Actor(s)	IFM Manager Media Provider
Use case description	The IFM Manager checks the medium against the set of rules. If the medium is conformant with the set of rules, — the medium will be certified, — else the medium will not be certified.

8.3.5 Certification of ID services

Use case name	Certification of ID services
Outline	Each ID service to be brought into the IFM shall meet the IFM requirements. Proof of this is given by checking this eID service against a set of rules.
Triggered by	Identity Provider
Actor(s)	IFM Manager Identity Provider

Use case name	Certification of ID services
Use case description	The IFM Manager checks the ID service against the set of rules. If the eID service is conformant with the set of rules, — the ID service will be certified, — else the ID service will not be certified.

8.3.6 Certification of payment services

Use case name	Certification of payment services
Outline	Each payment service to be brought into the IFM shall meet the IFM requirements. Proof of this is given by checking this payment service against a set of rules.
Triggered by	Payment Provider
Actor(s)	IFM Manager Payment Provider
Use case description	The IFM Manager checks the payment service against the set of rules. If the payment service is conformant with the set of rules, — the payment service will be certified, — else the payment service will not be certified.

8.3.7 Certification of application specifications and templates

Use case name	Certification of application specifications and templates
Outline	Each application specification and template to be brought into the IFMS shall meet the IFM requirements. Proof of this is given by checking this application specification and template against a set of rules.
Triggered by	Application Owner
Actor(s)	IFM Manager Application Owner
Use case description	The IFM Manager checks the application specification and template against the set of rules. If the application specification and template is conformant with the set of rules, — the application specification and template will be certified, — else the application specification and template will not be certified.

8.3.8 Certification of product specifications and templates

Use case name	Certification of product specifications and templates
Outline	Each product specification and template to be brought into the IFM shall meet the IFM requirements. Proof of this is given by checking this product specification and template against a set of rules.
Triggered by	Product Owner
Actor(s)	IFM Manager Product Owner
Use case description	The IFM Manager checks the product specification and template against the set of rules. If the product specification and template is conformant with the set of rules, — the product specification and template will be certified, — else the product specification and template will not be certified.

8.4 Interaction with external objects

8.4.1 General

Services, media and applications which are defined by other markets are of increasing importance for IFMSs. These objects are typically specified and certified by non-IFMS stakeholders. In such cases, IFMS internal certification is typically not an option. However, it shall be ensured that these external objects are also interoperable with the IFMS and do not infringe on the security of the IFMS. This should be ensured by a dedicated onboarding and maintenance process between the IFMS and the stakeholders which are responsible for the external object.

The alignment and the harmonization between specifications of the IFMS and those from other market sectors should be conducted by the relevant international standardization bodies. Ideally, the IFMS could reference and recognize certifications of the external object as criteria for onboarding to the IFM system.

It should be noted that terms and role definitions from non IFM system partners can not match the IFM definitions. Therefore, these roles can only be named in a generic way as “System Manager”.

8.4.2 Interaction with external media

8.4.2.1 Evaluate specifications of external media

Use case name	**Evaluate specifications of external media**
Outline	Identify potential discrepancies between external media and set of rules for IFMS internal media.
Triggered by	IFM Manager
Actor(s)	IFM Manager System Manager (of the system that specifies the external media)
Use case description	Identify potential discrepancies between external media and set of rules for IFMS internal media by: 1. reviewing specifications for the external media type and functional certification concept, 2. evaluating security concept and the security certification requirements for the external media type, and 3. comparing results with set of rules for IFMS-internal media types.

8.4.2.2 Align with the set of rules for external media

Use case name	**Align with the set of rules for external media**
Outline	Align with external System Manager on set of rules for interoperability and security of the external media type with IFMS components.
Triggered by	IFM Manager
Actor(s)	IFM Manager System Manager (of the system that specifies the external medium)

Use case name	Align with the set of rules for external media
Use case description	Agree on set of rules that includes: 1) rules for safeguarding interoperability with IFMS components (certification by ext. System Manager), 2) rules for safeguarding required assurance level (certification by ext. System Manager), 3) rules for operations (registration, black-listing, maintenance, updates), and 4) confirmation by the external System Manager that the set of rules are fulfilled by the external media.

8.4.2.3 Maintenance of the set of rules for external media

Use case name	Maintenance of the set of rules for external media
Outline	Continuous synchronization with external System Manager on set of rules for interoperability and security of external media with IFMS components. If International Standards are used for external media and the IFMS, the maintenance and harmonization work should be conducted by the responsible bodies. This is the most practical approach since the IFM Manager and the System Manager simply need to follow the evolution of the International Standards.
Triggered by	IFM Manager
Actor(s)	IFM Manager System Manager (of the system that specifies the external medium)
Use case description	Conduct continuous maintenance work that includes: 1) timely information exchange on plans for changes of specifications for the external media or the set of rules of the IFMS, and 2) timely harmonization in order to avoid discrepancies between specifications.

8.4.3 Interaction with external applications

8.4.3.1 Evaluate specifications of the external application

Use case name	Evaluate specifications of external applications
Outline	Identify potential discrepancies between the external application and set of rules for IFMS internal applications.
Triggered by	IFM Manager
Actor(s)	IFM Manager System Manager (of the system that specifies the external application)
Use case description	Identify potential discrepancies between the external application and set of rules for the IFMS-internal application by: 1) reviewing specifications for the external application and its functional certification concept, 2) evaluating security concept and the security certification requirements for the external application, and 3) comparing results with the set of rules for IFMS-internal applications.

8.4.3.2 Align with the set of rules for the external application

Use case name	Align with the set of rules for the external application
Outline	Align with external System Manager on set of rules for interoperability and security of the external application with IFMS components.
Triggered by	IFM Manager
Actor(s)	IFM Manager System Manager (of the system that specifies the external application)
Use case description	Agree on set of rules that includes: 1) rules for safeguarding interoperability with IFMS components (certification by ext. System Manager), 2) rules for safeguarding required LoA (certification by ext. System Manager), 3) rules for operations (registration, black-listing, maintenance updates), 4) confirmation by the external System Manager that the set of rules are fulfilled by the external application.

8.4.4 Interaction with external ID services

8.4.4.1 Evaluate specifications of the external ID service

Use case name	Evaluate specifications of external ID service
Outline	Identify potential discrepancies between the external ID service and set of rules for the IFMS internal ID service.
Triggered by	IFM Manager
Actor(s)	IFM Manager Identity Provider System Manager (of the system that specifies the external ID service)
Use case description	Identify potential discrepancies between the external eID service and set of rules for IFMS internal eID by: 1) reviewing specifications for the external ID service and its functional certification concept, 2) evaluating security concept and the security certification requirements for the external ID service, and 3) comparing results with the set of rules for IFMS internal ID service.

8.4.4.2 Align with the set of rules for the external ID service

Use case name	Align with the set of rules for the external ID service
Outline	Align with external System Manager on set of rules for interoperability and security of the external ID service with IFMS components.
Triggered by	IFM Manager
Actor(s)	IFM Manager Identity Provider System Manager (of the system that specifies the external ID service)

Use case name	Align with the set of rules for the external ID service
Use case description	Agree on set of rules that includes: 1) rules for safeguarding interoperability with IFMS components and IFM internal ID service (certification by ext. System Manager), 2) rules for safeguarding required assurance level (certification by ext. System Manager), 3) rules for operations (registration, black-listing, maintenance, updates), and 4) confirmation by the external System Manager that the set of rules are fulfilled by the external ID service.

8.4.5 Interaction with external payment services

8.4.5.1 Evaluate specifications of the external payment service

Use case name	Evaluate specifications of external payment services
Outline	Identify potential discrepancies between the external payment service and set of rules for IFMS internal payment services.
Triggered by	IFM Manager
Actor(s)	IFM Manager System Manager (of the system that specifies the external payment service)
Use case description	Identify potential discrepancies between the external payment service and set of rules for IFMS internal payment (if available) by: 1) reviewing specifications for the external payment service and its functional certification concept, 2) evaluating security concept and the security certification requirements for the external payment service, 3) comparing results with set of rules for IFMS internal payment (if available).

8.4.5.2 Align with the set of rules for the external payment service

Use case name	Align with the set of rules for the external payment service
Outline	Align with external System Manager on set of rules for interoperability and security of the external payment service with IFMS components.
Triggered by	IFM Manager
Actor(s)	IFM Manager System Manager (of the system that specifies the external payment service)
Use case description	Agree on set of rules that includes: 1) rules for safeguarding interoperability with IFMS components (certification by ext. System Manager), 2) rules for safeguarding required assurance level (certification by ext. System Manager), 3) rules for operations (registration, black-listing, maintenance, updates), and 4) confirmation by the external System Manager that the set of rules are fulfilled by the external payment service.

8.5 Registration

8.5.1 General

Registration is necessary to ensure that each instance of an object is unique within the IFM. This is guaranteed by a unique identifier. The process of managing these identifiers is called registration.

Objects and instances of objects within the IFM which have to be registered are:

— organizations,

— components,

— eID services,

— payment services,

— customer accounts,

— media,

— application templates and applications, and

— product templates and products.

The Registrar of the IFM is responsible for the registration process.

8.5.2 Registration of organizations

Use case name	**Registration of organizations**
Outline	A unique identification is given to each organization. This includes external organizations that provide eID or payment services, media or applications which shall be used by the IFMS.
Triggered by	Organization
Actor(s)	Registrar Organization
Use case description	The organization sends the organization certification to the Registrar. The Registrar returns a unique organization identifier to the organization.

8.5.3 Registration of components

Use case name	**Registration of components**
Outline	A unique identification is given to each component.
Triggered by	Component provider
Actor(s)	Registrar Component provider
Use case description	The component certification is sent to the Registrar. The Registrar returns a unique component identifier to the organization which requested registration.

8.5.4 Registration of ID services

Use case name	**Registration of eID services**
Outline	A unique identification is given to each ID service which has passed certification or proved conformance with the set of rules which was defined for external eID services.
Triggered by	Identity Provider or IFM Manager for external eID services

Use case name	Registration of eID services
Actor(s)	Registrar Identity Provider
Use case description	The eID service certification is sent to the Registrar. The Registrar returns a unique eID service identifier to the organization which requested registration.

8.5.5 Registration of customer accounts

8.5.5.1 General

It is assumed that a Customer can have more than one account and that pseudonymous accounts can be required. Therefore, the customer's ID as provided by the Identity Provider's IFMS-internal ID service can not always be used as account ID.

8.5.5.2 Customer applies for a personalized account

Use case name	Customer applies for a personalized account
Outline	Customer applies for registration with the Account Provider.
Triggered by	Customer
Actor(s)	Customer Account Provider Identity Provider
Use case description	Customer applies for registration with the Account Provider: – Customer completes an application form (on site or online). – Alternatively, the customer uses an ID service to apply for an account.

8.5.5.3 Customer applies for a pseudonymous account

Use case name	Enrolment of pseudonymous data
Outline	Collecting and validating pseudonymous ID and payment data
Triggered by	Customer
Actor(s)	Customer Account Provider
Use case description	Collecting and validating ID and payment data – Customer provides pseudonymous data as requested by the set of rules. – Customer establishes anonymous or pseudonymous payment method. – Customer accepts T&C. – Account Provider incorporates data and establishes account.

8.5.5.4 Activating the customer account

Use case name	Activating the customer account
Outline	Generate and register Account ID, activate customer account
Triggered by	Account Provider

Use case name	Activating the customer account
Actor(s)	Account Provider Registrar Customer
Use case description	The Account Provider conducts the following activities: – Generate and register Account ID. – In case of an Online customer account, the Account provider sends the login-data to the Customer.

8.5.6 Registration of payment services

Use case name	Registration of payment services
Outline	A unique identification is given to each payment service which has passed certification or proved conformance with the set of rules which was defined for external payment services.
Triggered by	Identity Provider or IFM Manager for external payment services
Actor(s)	Registrar Payment Provider
Use case description	The payment service certification or proof of conformance is sent to the Registrar. The Registrar returns a unique payment service identifier to the organization which requested registration.

8.5.7 Registration of media

Use case name	Registration of media
Outline	A unique identification is given to each media type which passed certification or proved conformance with the set of rules which was defined for external media.
Triggered by	Media Provider or IFM Manager for external media
Actor(s)	Registrar Media Provider
Use case description	The media certification or proof of conformance is sent to the Registrar. The Registrar returns a unique media identifier to the organization which requested registration.

8.5.8 Registration of customer media

Use case name	Registration of customer media
Outline	A unique identification is given to each customer medium after an application template has been installed and personalized. This registration is typically only performed if the installation of the application will result in substantial changes to the medium's setup.
Triggered by	Application Retailer
Actor(s)	Registrar Application Retailer
Use case description	Notice about installation of the application onto the customer medium is sent to the Registrar. The Registrar returns a unique customer medium identifier to the organization which requested registration.

8.5.9 Registration of application templates

Use case name	Registration of application templates
Outline	A unique identification is given to each application template.
Triggered by	Application Owner
Actor(s)	Registrar Application Owner
Use case description	The Application Owner sends the application template certification to the Registrar. The Registrar returns a unique application template identifier to the Application Owner.

8.5.10 Registration of applications

Use case name	Registration of applications
Outline	A unique identification is given to each instance of an application.
Triggered by	Application Retailer
Actor(s)	Registrar Application Retailer
Use case description	a) The Application Owner sends the application template identification to the Registrar and requests an application identification. The Registrar sends a unique application identifier to the Application Owner. This can be performed for a single identifier as well as for a batch of identifiers. b) The Application Retailer sends the application template identification to the Application Owner through the Collection and Forwarding and requests an application identification. The Application Owner sends the unique application identifier through the Collection and Forwarding to the Application Retailer. The The processes described in a) and b) could happen at any time in any order.

8.5.11 Registration of product templates

Use case name	Registration of product templates
Outline	A unique identification is given to each product template.
Triggered by	Product Owner
Actor(s)	Registrar Product Owner
Use case description	The Product Owner sends the product specification certification to the Registrar. The Registrar returns a unique product template identifier to the Product Owner.

8.5.12 Registration of products

Use case name	Registration of products
Outline	A unique identification is given to each instance of a product.
Triggered by	Product Retailer
Actor(s)	Registrar Product Retailer

Use case name	Registration of products
Use case description	a) The Product Owner sends the product template identification to the Registrar and requests a product identification. The Registrar sends a unique product identifier to the Product Owner. This can be done for a single identifier as well as for a batch of identifiers. b) The Product Retailer sends the product template identification to the Product Owner through the Collection and Forwarding and requests a product identification. The Product Owner sends the unique product identifier through the Collection and Forwarding to the Product Retailer. The processes described in a) and b) could happen at any time in any order.

8.6 Managing ID services

8.6.1 General

The use case "Managing ID services" comprises:

— enrolment and update of Customer ID data via an application form;

— enrolment and update of Customer ID data via an external ID service;

— update of Customer ID data via an online account;

— re-use of incumbent Customer ID data;

— management and maintenance of ID data;

— providing the ID service to IFMS-internal and external organizations.

8.6.2 Enrolment and update of Customer ID data via an application form

Use case name	Enrolment and update of Customer ID data via an application form
Outline	Collecting and validating ID data via application form.
Triggered by	Customer
Actor(s)	Customer Identity Provider
Use case description	Collecting and validating Customer's ID attributes via application form: – Customer opts in. – Customer provides ID data as requested by the set of rules of a form. – Customer can provide payment information (personalized or anonymously). – Customer accepts terms and conditions. – Identity Provider conducts validation of ID data. If successful, the Identity Provider releases the Customer eID, the derived eID and incorporates ID data into the IFMS internal eID service. – If applicable, the Identity Provider checks the Customer's creditworthiness, validity of driver licence, etc.

8.6.3 Enrolment and update of Customer ID data via an external ID service

Use case name	Enrolment of ID data via an external ID service
Outline	Collecting and validating ID attributes via an external ID service.
Triggered by	Customer
Actor(s)	Customer Identity Provider
Use case description	Collecting and validating Customer's ID and payment data via trustworthy ID service: – Customer opts in. – Identity Provider checks if the LoA of the ID service is equal or higher than the LoA required for the IFMS internal ID service. – Customer provides ID data as requested by the set of rules (ID data, optional payment information, driver licence, etc.). – Customer accepts terms and conditions. – Identity Provider generates Customer ID, derived ID and incorporates ID data into the IFMS internal ID service. – If applicable, the Identity Provider checks the Customer's creditworthiness, validity of driver licence etc.

8.6.4 Update of Customer ID data via an online account

Use case name	Update of Customer ID data via an online account
Outline	After secure login to the online account, the Customer may modify his/her Customer-related ID data. The implementation of the eID service's customer account makes sure that Customer-related ID data that have a certain LoA may not be updated by a method which has a lower LoA. EXAMPLE To keep a high LoA, Customer-related ID data which have been obtained from a trustworthy eID service can not be changed manually by the Customer. Any change shall use data from a source that provides the required trust level.
Triggered by	Customer
Actor(s)	Customer Identity Provider

Use case name	Update of Customer ID data via an online account
Use case description	The Customer may change his/her Customer-related ID data in his/her online account with the eID service. Alternatively, also another online account in the IFMS may be used for this purpose. The rights for changing the Customer-related ID data depend on the LoA requirements of the existing ID data and the LoA which is provided by the login method and the method for updating the Customer-related ID data. – Customer login to his/her online account. – Identity Provider confirms validity of Customer's login credentials – Identity Provider grants access/rejects access according to the LoA which was presented during login. – Identity Provider allows modification of Customer-related ID data according to the LoA of the login method. – Depending on the required LoA for the Customer-related ID data, the Identity Provider allows manual change or requests use of an external ID service with the appropriate LoA for update of the Customer-related ID data. – Customer updates Customer-related ID data.

8.6.5 Re-use of incumbent Customer ID data

Use case name	Re-use of incumbent Customer ID data
Outline	The IFMS may own a customer data base. The goal is to make this ID data available for the ID service. This requires a validation and potentially a consolidation and enhancement of the available data.
Triggered by	Identity Provider
Actor(s)	Customer Identity Provider
Use case description	The re-use of incumbent Customer ID data requires the support for following functions: – Identity Provider requests agreement from the Customer. – Identity Provider incorporates the incumbent ID data. – Identity Provider conducts validation of ID data. If successful, the Identity Provider releases the Customer ID and derived ID and incorporates the ID into the IFMS internal ID service. – If required, the Customer is requested to provide updates or corrections.

8.6.6 Management and maintenance of Customer ID data

Use case name	Management and maintenance of Customer ID data
Outline	The Identity Provider shall manage the life cycle of the Customer ID data which is available via this ID service and shall make sure that the data is accurate and up to date. This applies in particular for ID attributes that can change on short notice (e.g. possession of a valid driver licence, creditworthiness). The identity Provider shall implement processes that identify issues with the ID data and support updates and corrections.
Triggered by	Identity Provider Customer Organizations that use the ID service

Use case name	Management and maintenance of Customer ID data
Actor(s)	Identity Provider Customer Organizations that use the ID service
Use case description	The management and maintenance of Customer ID data requires support for following functions: – Implementation of an information security management system for the ID service in order to ensure the targeted assurance level. – Implementation of interfaces to Customers and organizations that use the ID. services in order to obtain requests for updates or problem reports. – Update of ID data by the Customer. – Deletion of ID data and ID account. – ID data validation. – Revocation and re-issuing of ID.

8.6.7 Providing the ID service to IFMS internal and external organizations

Use case name	Providing the ID service to IFMS internal and external organizations
Outline	The purpose of the ID service is to provide trustworthy ID information and login credentials to IFMS internal and external organizations. This requires that the required processes and interfaces to these organizations be implemented.
Triggered by	Identity Provider Organizations that use the ID service
Actor(s)	Identity Provider Customer Organizations that use the ID service
Use case description	Providing the ID service to IFMS internal and external organizations requires support for the following functions: – Establishing commercial and legal agreements. – Provisioning of login tools and login credentials for organizations that use the ID service. – Interfaces for supply of ID information. – Interfaces for order, status and error management.

8.7 Management of customer accounts

8.7.1 General

The Management of customer accounts comprises:

— secure login to customer accounts;

— update of customer account data;

— connect system generated account with customer account;

— connect/disconnect customer medium to/from the customer account;

— transfer of products between customer medium which are registered to the customer account; and

— termination of customer account.

8.7.2 Secure login to customer online accounts

Use case name	Secure login to customer online accounts
Outline	Secure sign-on to the customer online account by using an identification or authentication method with appropriate LoA provided by the Identity Provider.
Triggered by	Customer
Actor(s)	Customer Account Provider Identity Provider
Use case description	Secure sign-on to the customer online account by using an identification or authentication method with appropriate LoA provided by the Identity Provider: – Customer uses the eID service provided by the Identity Provider for secure login to his/her online account. – Identity Provider confirms validity of the Customer's login credentials – Account Provider grants access according to the assurance level which was presented by the ID service or rejects access.

8.7.3 Connect/disconnect customer media to/from the customer online account

Use case name	Connect/disconnect customer media to/from the customer online account
Outline	The Customer may connect/disconnect existing customer media to/from his/her customer online account. This means that the Customer shall be in a position to upload or manage products to existing own customer media or to customer media of family members, for example. A company may do the same for customer media of employees. Connecting/disconnecting an existing customer media to a customer online account shall require that the customer media be physically available to the Customer and that the validity of the customer media may be checked via an electronic interface. If the Customer orders a new customer media via the customer online account, the customer media shall by default be connected to the customer account.
Triggered by	Customer
Actor(s)	Customer Account Provider Identity Provider Registrar

Use case name	Connect/disconnect customer media to/from the customer online account
Use case description	– The Customer connects/disconnects existing customer media to/from his/her customer online account. – Customer conducts login to his/her customer online account with appropriate LoA. – Customer starts the process for connecting/disconnecting the customer media from the customer online account. – Customer connects the customer media via an electronic interface (e.g. online, NFC, Bluetooth). – If the customer media to be connected/disconnected is registered for a person/organization, this person/organization shall provide its consent during the process (e. g. by a PIN). – The Registrar checks the validity of the customer media via the electronic interface. – If successful, the customer media will be connected/disconnected to/from the customer account.

8.7.4 Transfer of products between connected customer media

Use case name	Transfer of products between connected customer media
Outline	The Customer may transfer products between customer media which are connected to his/her online account. Transfer of products between connected customer media to a customer online account shall require that both customer media are physically available to the Customer and that both customer media are connected to the customer online account via an electronic interface.
Triggered by	Customer
Actor(s)	Customer Account Provider Identity Provider Registrar
Use case description	– The Customer connects/disconnects existing customer media to/from his/her online account. – Customer conducts login to his/her online account with appropriate LoA. – Customer starts the process for transferring products from the customer online account and selects customer medium A (source) and customer medium B (target). – Customer connects both customer media via an electronic interface (e.g. Online, NFC, Bluetooth) to the customer online account. – If the involved customer media are registered for a person/organization, this person/organization shall provide its consent during the process (e. g. by a PIN). – The Registrar checks the validity of both customer media via the electronic interface. – If successful, the product is deleted from customer medium A and is uploaded to customer medium B.

8.7.5 Connect system generated account with a customer account

Use case name	Connect system generated account with a customer account
Outline	Based on the set of rules for certain applications, the system may automatically generate accounts in order to collect data from, for example, interactions with contactless payment cards for usage-based products. The use case supports connecting these automatically generated accounts to the customer's online account. Before this use case can be conducted, the Customer shall connect the customer medium which holds the application to his/her online account.
Triggered by	Customer
Actor(s)	Customer Account Provider Identity Provider Registrar
Use case description	– Customer connects/disconnects existing customer media to/from his/her online account. – Customer conducts login to his/her online account with appropriate LoA. – Customer starts the process for connecting automatically generated accounts and selects the related customer media. – Customer connects the customer media via an electronic interface (e.g. Online, NFC, Bluetooth) to the online account. – If the involved customer media are registered for a person/organization, this person/organization shall provide its consent during the process (e. g. by a PIN). – The Registrar checks the validity of the customer media via the electronic interface. – If successful, the automatically generated account will be connected to the customer account.

8.7.6 Termination of customer accounts

8.7.6.1 General

The use case "Termination of customer accounts" comprises the following:

— regular termination of customer account;

— forced termination of a customer account.

8.7.6.2 Regular termination of customer accounts

Use case name	Regular termination of customer accounts
Outline	A customer account is terminated in the IFM by request of the Customer.
Triggered by	Customer
Actor(s)	Customer Collection and Forwarding Account Provider Registrar

Use case name	Regular termination of customer accounts
Use case description	The Customer wants to terminate the customer account. This comprises: — distribution of the termination of a registered customer account to the Account Provider; — distribution of the termination of a registered customer account via Collection and Forwarding to the Registrar.

8.7.6.3 Forced termination of customer accounts

Use case name	Forced termination of customer accounts
Outline	Termination of customer accounts by request of the IFM Manager.
Triggered by	IFM Manager
Actor(s)	Account Provider
Use case description	The IFM Manager sends the request for termination of a customer account to the Account Provider.

8.8 Management of customer media

8.8.1 General

The management of customer media comprises:

— provisioning of media,

— termination of customer media.

8.8.2 Provisioning of media

8.8.2.1 General

The use case “Provisioning of customer media” comprises the following alternatives:

— provisioning of IFMS-owned media;

— provisioning of a Customer-owned media,

8.8.2.2 Provisioning of IFMS-owned media

Use case name	Provisioning of IFMS-owned media
Outline	A medium which is owned by an IFMS stakeholder (e.g. the Application Retailer) is provisioned with the application template.
Triggered by	Application Retailer
Actor(s)	Application Retailer Media Retailer Collection and Forwarding Registrar

Use case name	Provisioning of IFMS-owned media
Use case description	The Application Retailer wants the application template to be uploaded to the medium. This comprises: — dissemination of the application template to the Media Retailer; — provisioning of the medium with the application template by the Media Retailer; — Media Retailer requests registration as customer medium by the Registrar; — delivery of the unpersonalized customer medium to the Application Retailer.

8.8.2.3 Provisioning of customer-owned media

Use case name	Provisioning of customer-owned media
Outline	A media which is owned by the Customer (e.g. a smartphone) is provisioned with an application template. This requires that the media be registered by the Registrar.
Triggered by	Customer
Actor(s)	Application Retailer Media Retailer Collection and Forwarding Registrar
Use case description	The Customer wants to use his/her medium as customer medium. This comprises: — dissemination of the application template to the Media Retailer; — provisioning of the media with the application template by the Media Retailer; — Media Retailer requests registration as customer media by the Registrar; — handover of access rights to the application template for personalization from the Media Retailer to the Application Retailer.

8.8.3 Termination of customer media

8.8.3.1 General

The use case “Termination of customer media” comprises the following:

— regular termination of customer media;

— forced termination of customer media,

8.8.3.2 Regular termination of customer media

Use case name	Regular termination of customer media
Outline	A customer medium is terminated in the IFM by request of the Customer.
Triggered by	Customer
Actor(s)	Collection and Forwarding Registrar Account Provider Media Retailer

Use case name	Regular termination of customer media
Use case description	The Customer wants to terminate the customer medium. This comprises: — execution of the use case “Regular termination of application”; — the Customer notifies the Media Retailer; — distribution of termination of the registered customer medium to the Registrar through the Collection and Forwarding; and — distribution of termination of the registered customer medium to the Account Provider through the Collection and Forwarding.

8.8.3.3 Forced termination of customer media

Use case name	Forced termination of customer media
Outline	Termination of customer media by request of the IFM Manager.
Triggered by	Media Retailer
Actor(s)	Security Manager
Use case description	The Media Retailer sends the request for termination of a customer medium to the Security Manager. The Security Manager notifies the Media Retailer and the Account Provider.

8.9 Management of applications

8.9.1 General

The management of applications comprises:

— dissemination of application templates,

— acquisition of applications,

— termination of application templates, and

— termination of applications.

Only certified and registered application templates shall be disseminated.

Updating of application consists of terminating an application and acquiring a new application.

8.9.2 Dissemination of application templates

Use case name	Dissemination of an application template
Outline	Dissemination of an application template enables the authorized Application Retailer to sell an application and an authorized Service Operator to access this application.
Triggered by	Application Owner
Actor(s)	Application Retailer Collection and Forwarding Service Operator Application Owner
Use case description	Dissemination of an application template comprises: — distribution of registered application template by an Application Owner to the Application Retailer through the Collection and Forwarding, and — distribution of registered application template by Application Owner to the Service Operator through the Collection and Forwarding.

8.9.3 Acquisition of applications

Use case name	Acquisition of applications
Outline	An application is loaded on the medium.
Triggered by	Customer
Actor(s)	Application Retailer Application Owner Collection and Forwarding Customer Media Retailer
Use case description	The authorized Application Retailer initiates the installation of an instance of a registered application template on a medium. The Application Retailer: — initiates the installation of the instance of the registered application template by the Media Retailer, — initializes and personalizes the application template, and — performs distribution of the application identifier and the application acquisition data to the Application Owner through the Collection and Forwarding.

8.9.4 Termination of application templates

8.9.4.1 General

The use case “Termination of application templates” comprises the following:

— regular termination of application templates; and

— forced termination of application templates.

8.9.4.2 Regular termination of application templates

Use case name	Regular termination of application templates
Outline	An application template is terminated in the IFM by request of the Application Owner.
Triggered by	Application Owner
Actor(s)	Application Retailer Collection and Forwarding Service Operator Product Retailer Security Manager Registrar Application Owner Media Retailer

Use case name	Regular termination of application templates
Use case description	The Application Owner wants to terminate the application template. This comprises: — distribution of termination of registered application template to the Media Retailer through the Collection and Forwarding; — distribution of termination of registered application template to the Service Operator through the Collection and Forwarding; — distribution of termination of registered application template to the Product Retailer through the Collection and Forwarding; — distribution of termination of registered application template to the Security Manager; — distribution of termination of registered application template to the Registrar; — (optional) distribution of termination of registered application template to the customer service through the Collection and Forwarding; and — (optional) the MAD reports the application template identifier and application template termination data to the Application Owner and Security Manager through the Collection and Forwarding.

8.9.4.3 Forced termination of application templates

Use case name	Forced termination of application templates
Outline	Termination of an application template by request of the IFM Manager.
Triggered by	IFM Manager
Actor(s)	Security Manager
Use case description	The IFM Manager sends the request for termination of an application template to the Security Manager.

8.9.5 Termination of applications

The use case “Termination of applications” comprises the following:

— regular termination of applications; and

— forced termination of applications.

8.9.5.1 Regular termination of applications

Use case name	Regular termination of applications
Outline	An application is terminated on the Customer Medium.
Triggered by	Customer
Actor(s)	Application Retailer Application Owner Collection and Forwarding Registrar Customer

Use case name	Regular termination of applications
Use case description	The Customer wants to terminate the application. The Application Retailer; — de-installs the application on the Customer Medium; — sends the de-installed application identifier to the Application Owner through the Collection and Forwarding. The Application Owner sends application identifier to the Registrar.

8.9.5.2 Forced termination of applications

Use case name	Forced termination of applications
Outline	Application is put on a security list by request of the Application Owner.
Triggered by	Application Owner
Actor(s)	Application Owner Collection and Forwarding Security Manager
Use case description	The Application Owner wants to terminate an application and sends the application identifier to the Security Manager through the Collection and Forwarding.

8.10 Management of products

The management of products comprises the following:

— dissemination of product templates;

— termination of product templates;

— management of action lists;

— acquisition of products;

— modification of product parameters;

— termination of products;

— use and inspection of products;

— collection of data;

— forwarding data; and

— generation and distribution of clearing reports.

8.10.1 Dissemination of product templates

Use case name	Dissemination of product templates
Outline	Dissemination of registered product template enabling authorized actors to handle the product.
Triggered by	Product Owner
Actor(s)	Collection and Forwarding Product Retailer Service Operator Product Owner

Use case name	Dissemination of product templates
Use case description	Dissemination of product templates comprises the following: — distribution of product templates by Product Owner to Collection and Forwarding; — distribution of product templates by Collection and Forwarding to authorized Product Retailers; — distribution of product templates by Collection and Forwarding to authorized Service Operators.

8.10.2 Termination of product templates

8.10.2.1 General

The use case “Termination of product templates” comprises the following:

— regular termination of product templates,

— forced termination of product templates.

8.10.2.2 Regular termination of product templates

Use case name	Regular termination of product templates
Outline	Termination of product templates on decision of the Product Owner.
Triggered by	Product Owner
Actor(s)	Collection and Forwarding Product Retailer Service Operator Product Owner
Use case description	Termination of product templates comprises the following: — distribution of request for termination of product templates by a Product Owner to Collection and Forwarding; — distribution of request for termination of product templates by Collection and Forwarding to authorized Product Retailers; — distribution of request for termination of product templates by Collection and Forwarding to authorized Service Operators; — sending of the request for termination of product templates by a Product Owner to the Security Manager; and — (optional) sending of the identifier of the terminated product template by the Product Owner to the Registrar.

8.10.2.3 Forced termination of product templates

Use case name	Forced termination of product templates
Outline	Termination of product templates on decision of the IFM Manager.
Triggered by	IFM Manager
Actor(s)	Security Manager
Use case description	The IFM Manager sends the request for termination of a product template to the Security Manager.

8.10.3 Management of action lists

Use case name	Management of action lists
Outline	Management of an action list enables actions related to products or applications.
Triggered by	Application Retailer or Product Retailer or Customer
Actor(s)	Application Retailer Product Retailer Collection and Forwarding Customer
Use case description	Management of action lists consists of — adding an item to the action list, which will result in the one-time addition of a product or application to the Customer Medium; — adding an item to the action list, which will result in the one-time removal of a product or application from the Customer Medium; — removing an item from the action list; — aggregation of action list data; and — distribution of action list to any MAD, which is able to update products or applications into the Customer Medium through the Collection and Forwarding. After a Customer Medium is updated, the MAD sends information back to the action list.

8.10.4 Acquisition of products

Use case name	Acquisition of products
Outline	Acquisition of products; enabling Customer to benefit from a transport service.
Triggered by	Customer
Actor(s)	Product Retailer Collection and Forwarding Product Owner Customer
Use case description	The authorized Product Retailer installs an instance of a registered product template on a registered Application. The Product Retailer performs the following: — detection and verification of registered application; — verification of application according to security policies; — installation of the instance of the registered product template; and — distribution of product identifier and product acquisition data to the Product Owner through the Collection and Forwarding.

8.10.5 Modification of product parameters

Use case name	Modification of product parameters
Outline	Modifying changeable product parameters for an existing product.
Triggered by	Customer
Actor(s)	Product Retailer Collection and Forwarding Product Owner Customer

Use case name	Modification of product parameters
Use case description	The authorized Product Retailer modifies changeable product parameters of an existing product. The Product Retailer distributes the product identifier and product modification data to the Product Owner through the Collection and Forwarding.

8.10.6 Termination of products

8.10.6.1 General

A product which can be extended or recharged is covered by 8.10.5. Once a product has been terminated, it shall not be extended or recharged.

When a product is terminated, it is always for a valid reason. For example, payment was not honoured or the product was sold in error in the first place. To reactivate such a product would be to run the risk that a security-related issue that may no longer be on record might be disregarded enabling fraudulent use. Best practice requires that terminated products cannot therefore be reactivated. Similar products may, of course, replace them.

The use case "Termination of product" comprises:

— regular termination of product, and

— forced termination of product.

8.10.6.2 Regular termination of products

Use case name	Regular termination of products
Outline	Termination of products by request of the Customer.
Triggered by	Customer
Actor(s)	Customer Product Retailer Collection and Forwarding Product Owner
Use case description	The authorized Product Retailer de-installs/terminates a product. The Product Retailer distributes the product identifier and product termination data to the Product Owner through the Collection and Forwarding.

8.10.6.3 Forced termination of products

Use case name	Forced termination of products
Outline	The product is put on a security list by request of the Product Owner.
Triggered by	Product Owner
Actor(s)	Product Owner Security Manager Collection and Forwarding
Use case description	The Product Owner wants to terminate a product and sends the product identifier to the Security Manager through the Collection and Forwarding.

8.10.7 Use and inspection of products

Use case name	Use and inspection of products
Outline	The Service Operator checks and collects the data of a Customer Medium using the PT service.

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

8.10.8 Collection of data

Use case name	Collection of data
Outline	The Collection and Forwarding receives data and checks the completeness and integrity of the data.
Triggered by	Application Owner Product Owner Application Retailer Product Retailer Service Operator other Collection and Forwarding Security Manager Registrar
Actor(s)	Collection and Forwarding Application Owner Product Owner Application Retailer Product Retailer Service Operator other Collection and Forwarding Security Manager Registrar

Use case name	Collection of data
Use case description	The received data consist of administrative data and transaction data: — receiving application template from Application Owner; — receiving product templates from Product Owners; — receiving data from Service Operators; — receiving data from Product Retailer; — receiving data from Application Retailer; — receiving data from other Collection and Forwarding; — receiving security list data from Security Manager; — receiving clearing reports from Product Owner; — completeness and integrity check of the data collected on a technical level and the acknowledgement of receipt to the sender; and — receiving address list of all IFM roles in the IFM from the Registrar.

8.10.9 Forwarding data

Use case name	Forwarding data
Outline	The Collection and Forwarding forwards data.
Triggered by	Collection and Forwarding
Actor(s)	Application Owner Product Owner Application Retailer Product Retailer Service Operator Collection and Forwarding other Collection and Forwarding Security Manager
Use case description	The forwarding of data consists of the following: — forwarding “Not On Us” data to other Collection and Forwarding; — forwarding “On Us” data to the Application Owner; — 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; and — forwarding forced termination requests to the Security Manager.

8.10.10 Generation and distribution of clearing reports

Use case name	Generation and distribution of clearing reports
Outline	The Product Owner performs the clearing procedure and distributes the results to relevant IFM roles.
Triggered by	Product Owner
Actor(s)	Product Retailer Service Operator Collection and Forwarding Product Owner

Use case name	Generation and distribution of clearing reports
Use case description	The generation and distribution of clearing reports consist of the following: — clearing of the Product data (acquisition and usage data) and generating reports for the Product Retailer and Service Operator by the Product Owner; — distribution of the clearing report to the Product Retailer through the Collection and Forwarding; and — distribution of the clearing report to the Service Operator through the Collection and Forwarding. The distribution of clearing reports can also be performed by direct transmission from the Product Owner.

8.11 Security management

8.11.1 General

The security policy secures the assets in the IFMS, the privacy of the Customers, and the integrity and non-repudiation of the transaction data.

Conformance with the security policy is based on adherence to the set of rules, in particular the security rules, by the IFM members.

The Security Manager is responsible for the operation of the security of the IFMS.

The functions of Security Manager are performed by a central body in the IFM and, possibly and by delegation of this body, by other trusted organizations.

The Security Manager will be responsible for the implementation of the security policy by all actors concerned. The responsibility commences at the start of the IFMS.

Whenever a new actor joins the IFMS, he/she shall accept and implement the IFM security policy.

Security management consists of:

— monitoring processes,

— managing security keys, and

— managing security lists.

8.11.2 Monitoring of IFM processes and IFM data life cycle

Use case name	Monitor IFM processes and IFM data life cycle
Outline	The monitoring of the processes and data life cycle (generation of data, movement of data, storage of data, use of data, changes of data, and deletion of data) shall guarantee the secure operation of the IFMS, providing the required trust by the Customers and Service Operators concerning handling and protection of assets and sensitive information.
Triggered by	Security Manager
Actors	All
Use case description	The Security Manager participates in the collection of information regarding the general security level from all organizations and audits both the processes and the IFMS components from which the data are generated until they are deleted. The Security Manager may collect targeted information from all the use cases and may monitor both the processes as well as the life cycle of the IFM data.

8.11.3 Management of IFM security keys

Use case name	Management of IFM security keys
Outline	The generation, distribution, storage, and termination of IFM security keys.
Triggered by	Security Manager
Actor(s)	Security Manager Organizations using IFM security keys
Use case description	Security keys management covers the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation, and destruction of public or secret keying material in accordance with the IFM security policy at the general security level. The use case is triggered by any organization that will receive, install, store, and use IFM security keys or by the Security Manager as part of his/her security implementation tasks. The possibility of attacks shall be taken into consideration.

8.11.4 Management of security lists

8.11.4.1 Provision of security lists

Use case name	Provision of security lists
Outline	Provision of a security list by the Security Manager.
Triggered by	Security Manager
Actors	Security Manager Application Owner Product Owner Application Retailer Product Retailer Service Operator Customer
Use case description	The Security Manager provides a new security list to: — Application Owner, — Product Owner, — Application Retailer, — Product Retailer, — Service Operator, — Registrar, and — (optional) Customer Service through the Collection and Forwarding.

8.11.4.2 Updating security list data

Use case name	Updating security list data
Outline	Aggregation of security list data concerning components, customer medium, installed products and installed applications.

Use case name	Updating security list data
Triggered by	Security Manager Organization Application Owner Product Owner Application Retailer Product Retailer Service Operator Customer
Actors	Security Manager Organization Application Owner Product Owner Application Retailer Product Retailer Service Operator Customer
Use case description	The use case covers the activities of the Security Manager concerning the generation and maintenance of security lists.

8.11.4.3 Add or remove a component to/from a security list

Use case name	Add or remove a component to/from a security list
Outline	The adding of a component to, or removing of a component from, a security list.
Triggered by	Security Manager Organization Application Owner Product Owner Application Retailer Product Retailer Service Operator Customer
Actors	Security Manager Organization Application Owner Product Owner Application Retailer Product Retailer Service Operator Customer
Use case description	An organization may request that a component be added to or removed from the security list, e.g. a stolen card-issuing machine or a ticketing machine.

8.11.4.4 Add or remove a customer medium to/from a security list

Use case name	Add or remove a customer medium to/from a security list
Outline	The adding of a customer medium to or removing of a customer medium from a security list.
Triggered by	Media Retailer
Actors	Security Manager
Use case description	A Media Retailer requests the addition/removal of the customer medium to/from a security list.

8.11.4.5 Add or remove an application template to/from a security list

Use case name	Add or remove an application template to/from security list
Outline	The adding of an application template to or removing of an application template from a security list.
Triggered by	Security Manager
Actors	Security Manager
Use case description	The Security Manager requests the addition/removal of an application template to/from a security list. NOTE In the case of a prohibition list, the IFM Manager later receives from the Security Manager an acknowledgement of the termination.

8.11.4.6 Add or remove an application to/from a security list

Use case name	Add or remove an application to/from a security list
Outline	The adding of an Application to or removing of an Application from a security list.
Triggered by	Application Owner
Actors	Security Manager Application Owner
Use case description	An Application Owner requests the addition/removal of the installed Application to/from a security list. NOTE In the case of a prohibition list, the Application Owner later receives through Collection and Forwarding an acknowledgement of the termination by an Application Retailer.

8.11.4.7 Add or remove a product template to/from a security list

Use case name	Add or remove a product template to/from a security list
Outline	The adding of a product template to or removing of a product template from a security list.
Triggered by	Security Manager
Actors	Security Manager
Use case description	A Security Manager requests the addition/removal of a product template to/from a security list. NOTE In the case of a prohibition list, the Product Owner later receives through Collection and Forwarding an acknowledgement of the termination.

8.11.4.8 Add or remove a product to/from a security list

Use case name	Add or remove a product to/from a security list
Outline	The adding of a product to or removing of a product from a security list.
Triggered by	Product Owner or Product Retailer
Actors	Product Owner Product Retailer Security Manager
Use case description	A Product Owner or a Product Retailer requests the addition/removal of a product to/from a security list. NOTE In the case of a prohibition list, the Product Owner or the Product Retailer later receives through Collection and Forwarding an acknowledgement of the termination.

8.12 Customer Service management (optional)

Use case name	Customer Service management (optional)
Outline	Customer Service provides a “helpline” and any similar facilities.
Triggered by	Customer
Actor(s)	Customer Customer Service Collection and Forwarding
Use case description	Customer Service receives a request from a Customer. The Customer Service forwards the request to the relevant IFM roles through the Collection and Forwarding and receives the reply. Customer Service answers the request.

9 System interface identification

The interfaces with the Customer medium are out of the scope of this document.

10 Identification

10.1 General

By identification is meant a set of attributes that describe a specific person or object in a unique and unambiguous way. For instance, a person can be described by the attributes name, birth date, sex, address, etc. to be uniquely identified. An object, for example a ticketing machine, can be identified by owner, type and serial number. The term eID is used if identity and attributes are available as electronic data.

Identification is important in an IFMS for the following main reasons:

— Security — Identification of IFM roles, objects, applications, products, etc. enables the use of security lists, for example to record stolen components. The identification can also be used in an authentication procedure by including a unique ID.

— Communication — In an IFM network, there are many entities like organizations, companies, and components which act as a sender and/or a receiver of information. A unique identification is needed for addressing the different entities in a communication network.

— Auditing — It is necessary to be able to audit any transaction and any piece of information in an IFMS, for example following a usage transaction from creation by the Service Operator until it is cleared and refunded by the Product Owner. If something goes wrong or any information is changed during its lifetime, it is important to be able to investigate what happened and where in the IFMS it occurred.

Electronic identities, identity attributes and data which may be related to persons have to be protected against misuse and handled according to privacy and data protection laws.

10.2 Numbering scheme

As a minimum, the following objects shall have a unique identity in an IFMS:

— all actors (organizations) involved in the IFMS, e.g. all Product and Application Owners, Retailers, and Service Operators;

— all application templates;

— all applications (instances of implemented and initialized application templates);

— all product templates;

— all products (instances of product templates);

— all customer media;

— all media which have been issued within the IFMS;

— all components.

10.3 Prerequisites

10.3.1 There is one Registrar within the IFMS.

10.3.2 All objects, e.g. templates and components, have an owner who is one of the actors in the IFMS.

10.3.3 The identification of the application and product shall be as short and compact as possible due to the minimization of the transaction time between the customer medium and the MAD.

11 Security in IFMSs

11.1 General

IFMSs are subject to fraud by Customers and Service Operators, but also by people outside the IFMS. The security policy for an IFMS shall enable the protection of the public interests and the assets in the system.

It is recommended that the IFMS implements an Information Security Management System as defined in the ISO/IEC 27000 series.

The following subclauses provide examples of points which should be considered by the IFMS.

11.2 Protection of the interests of the public

The public interests are founded not only on quantifiable financial aspects, but also on human/cultural values. Some overall principles of public interests are formulated below.

— Quality of service — The IFMS shall be used as an instrument to ensure that national/local PT service strategic goals are met.

— Fairness of payment — Customers shall be convinced that everyone is paying the correct amount according to valid tariff principles.

— Public trust — Customers shall be convinced that they are paying the correct amount for the desired service.

— Public moral — Deliberate sabotage and fraud should be discouraged and considered illegal. This is related to the principles of fairness and public trust.

— Privacy — Information generated by the IFMS shall be protected, taking into consideration applicable laws.

These principles are of a general nature and are not further specified in this document, but should nevertheless be accounted for and followed within any organization responsible for PT services.

Regarding privacy, international and European regulations impose restrictions on the collection, storage, processing and dissemination of data relating to individuals and their behaviour. Some countries require a fully anonymous system. For that reason, the IFMS shall safeguard users' privacy. To achieve this, at least the following rules apply:

— only relevant personal data needed for the operation of the IFMS shall be requested from the Customer and stored, taking into consideration any requirements of local/regional privacy directives;

— the itemized disclosure of service consumption on an invoice shall be an option that can be chosen by the Customer;

— an IFM actor shall not disclose Customer-related information to third parties without specific authorization from the Customer;

— within the IFMS, the Customer-specific data shall be handled only in connection with the identification number of the contract (implicit or explicit) between the Customer and Product Owner. A link between the contract number and the name of the Customer can only be achieved by the contractual partner at the request of the Customer.

11.3 Assets to be protected

The security architecture for an IFMS shall protect the assets in the IFMS. The assets can be categorized as follows:

— Physical assets — Computers, servers, communication systems, storage media, customer media, ticketing machines, validators, etc.;

— Software assets — All software in the IFMS, including software on the customer media;

— Information assets — Information in databases, customer media, ticketing machines, validators, system documentation, user manuals, procedures for operation, plans, etc.

The information assets can be further divided into the following categories:

— public information, i.e. any information as regards the IFMS that is publicly known;

— private information, i.e. information that is subject to data protection in line with laws and regulations for privacy;

— commercial information, e.g. information related to the operation of the system, Commercial Rules, clearing, and apportionment and financial transactions;

— sensitive information, e.g. information related to security procedures and travel information for special persons;

— very sensitive information, e.g. security keys.

11.4 General IFM security requirements

An IFMS shall fulfil the following general security requirements:

a) provide the assurance that information is not made available or disclosed to unauthorized individuals, entities, or processes (confidentiality);

b) provide the confidence that information has not been altered or destroyed in an unauthorized manner (information integrity);

c) provide the confidence which ensures that the identity of a subject or resource is the one claimed (authenticity). Authenticity applies to entities such as users, processes, systems, and information;

d) provide the confidence of protection against an entity's false denial of having created the content of a message (non-repudiation of creation), e.g. a Customer claiming that he has not benefited from a transport service at a specific location and time;

e) provide the confidence of protection against a recipient's false denial of having received the message and recognized the content of the message (non-repudiation of delivery);

f) provide the confidence that each message is unique, e.g. a transaction describing the use of a product;

g) manage security keys, including the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation, and destruction of public or secret keying material in accordance with the IFM security policy at the general security level;

h) manage security lists including, but not limited to:

   1) add or remove component to/from security list,

   2) add or remove customer medium to/from security list,

   3) add or remove installed product to/from security list, and

   4) add or remove installed application to/from security list.

Annex A
(informative)

Mobility Platform – German example

A.1 Conceptual framework for mobility platforms

All stages of the holistic mobility service should be supported by a mobility platform (see Figure A.1). IFM for PT plays a key role in the mobility service offer. It is therefore important to place the IFM role model in relation to the emerging mobility platforms and to identify and define the necessary new roles or the resulting extended requirements for the roles of the IFM.

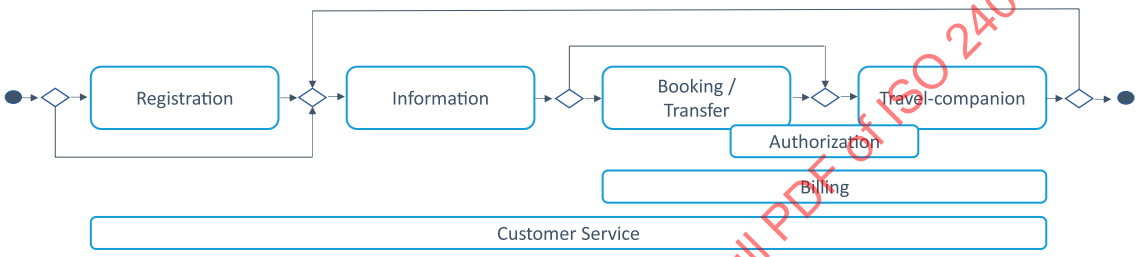


Figure A.1 — Holistic mobility service

A.2 Description of MP roles

On the basis of the role model presented in this document, an extended role-relationship model shows responsibilities and tasks in the field of offering mobility services. This role model forms the basis for the design of possible cooperation scenarios between mobility service providers and distinctive platform variants.

The approaches mentioned are primarily related to an IFMS. However, advanced travel information systems and complex mobility platforms offer functionalities encompassing the entire service chain, of which fare management is only a part. For the comprehensive modelling of the roles in the context of travel information systems and their interdependencies, extensions are required regarding travel information.

New identified roles are:

— Subdivision of the Customer role,

— Mediator,

— Information Service Manager (responsible for information),

— Trip Information Provider,

— Customer Contract Partner (merging the roles of Product Retailer and Account Provider for mobility services),

— Service Provider (Extension of the role of the PT Service Operator), and

— Expansion of the role Payment Provider.

In the subsequent subclauses, the newly defined roles are described in more detail and the extensions to the relationship diagram of IFM roles are presented.

A.2.1 Customer

A.2.1.1 General

Considering the topic of mobility platforms, the Customer role is split into three roles:

— Booker,

— Payer and

— Mobility Service User.

All of these three roles can be assumed by a single Customer, but also by different Customers. A typical example for the latter case would be the travel department in a company: a person chooses the journey and performs the booking, a different person from the finance department is responsible for the payment and a third person from the customer service department finally goes on the journey as the mobility service user.

A.2.1.2 Booker

The Booker is informed about the possibilities for using the mobility services through participation in the mobility platform. It is possible that this contract is mediated by the Mediator.

Here, the Customer as a Booker primarily represents a contracting partner of usage contracts for mobility services based on products.

A.2.1.3 Payer

The Customer is, as the Payer, responsible for the settlement of claims arising from usage contracts. The Booker thus transfers the obligation to pay to the Payer.

A.2.1.4 Mobility Service User

As the Mobility Service User, the Customer may use the purchased services, which are provided by the Service Provider. During usage, usage data can arise (such as driven mileage or usage duration), which are gathered by the Service Provider and transferred to the Product Retailer for accounting purposes based on defined products of a Product Owner. The mobility platform supports the Mobility Service User during their journey with relevant services with respect to travel assistance and provides up-to-date information.

In this subrole, the Mobility Service User acts in the role of the Passenger as defined in the IFM role model.

A.2.2 Mediator

The Mediator provides contracts to Bookers. At this point, information about the Payer and invoice data to the Payment Provider will be transferred.

The organization that acts as a Mediator can additionally act as an Information Service Manager and/or Customer Contract Partner or operate independently.

The mediation can occur across electronic channels or via stationary devices (e.g. ticketing machine, branch office).

A.2.3 Information Service Manager

The Information Service Manager provides trip information to the Customer/Mobility Service User using intermodal travel options. For this purpose, today's technological systems are interacting with the Customer/Mobility Service User. The systems request the starting point and destination of the trip, as well as further options and requirements of the Mobility Service User. These interactions can be performed in browser-based applications, mobile applications, voice-controlled systems or in any

other possible interaction system. Sensor data, which automatically record the context situation of the Mobility Service User, are increasingly being used.

The services offered by the Information Service Manager include the connection search from a starting point to a destination point, the price information or price estimate, the indication of current departure times/arrivals at stops and stations, the locations of sharing vehicles and their availability, the locations of parking objects and charging stations and their availability, the representation of routes on maps for navigation on roads and in buildings during interchanges and many more.

The Information Service Manager offers the following services: trip calculation from start to destination point, fare calculation or fare estimation, current departures/arrivals at stops/stations, locations and availabilities of shared vehicles, locations and availabilities of parking spaces and charging stations, display of routes on maps for routing and indoor routing (interchanges) and others.

The data required by the Information Service Manager for providing his services, are sourced from the Information Manager and other (remote) Information Dealers. Using real-time data is a typical example for this case. The real-time data are not presented to the Information Service Manager him/herself, but provided by another Information Dealer.

For trip calculation, the Information Service Manager tries to optimize the result, which has to fulfil the criteria of the Customer (or a combination of several criteria) in all of his/her roles. Typical criteria of optimization are: fastest connection, shortest distance, cheapest connection, shortest footpath, fewest interchanges etc. Especially for persons with reduced mobility (e.g. wheelchair users, baby carriage) further criteria can be taken into account (e.g. floor-level access, avoidance of stairs, availability of lifts, etc.).

During the trip, the Information Service Manager provides information (relevant for the trip) to the Mobility Service User using the trip guidance service. This can be navigation assistance or disruptions which might concern/influence the trip. If necessary, the Information Service Manager provides an alternative trip, which helps the Mobility Service User to bypass the disruption.

A.2.4 Trip Information Provider

The Trip Information Provider collects all data which are necessary for a comprehensive, integrated, intermodal trip- and fare calculation. This includes timetables and real-time information on locations of stops, parking spaces, sharing stations, vehicles, charging stations, product definitions and fare data, maps, etc.

These data are provided by the respective Service Providers or, in the case of tariff and product data, by the Product Owner.

The Trip Information Provider monitors the data with regard to immediacy, correctness/plausibility, completeness and consistence. The data collecting Service Providers or Product Owner receive feedback for quality improvement purposes.

After receiving the data deliveries, the Trip Information Provider harmonizes the data and forwards this integrated database to the Information Service Manager. The Trip Information Provider also checks if the data is unique and eliminates double deliveries, for example, data on stops which are served and used by several transport authorities and therefore where several Service Providers provide the data (which might be inconsistent) to the Trip Information Provider. In Germany, for the area of PT data this task is performed by the DELFI-data pool in connection with a central tariff station register.

A.2.5 Customer Contract Partner

The Customer Contract Partner regulates the Customer's sales, taking into account the contractual dependencies towards the Application Owner and the Product Owner of a different mobility service.

In particular, the Customer Contract Partner is responsible for the accounting, ticketing and billing of different mobility services to the Customer. This actor therefore takes on the role of the Product

Retailer and Account Provider. As Account Provider, this actor uses the services of Payment Providers of their choice with whom they are contractually bound.

In a basic sense, the Customer Contract Partner serves as an authority to conclude a mobility contract with the Customer. In addition, they offer a Customer Service for matters relating to the conclusion of the contract.

The Customer Contract Partner bundles the offered services under a customer identity and also assumes the role of Identity Provider or commissions an external partner with the task.

A.2.6 Product Owner

The Product Owner defines the products which are intended to be issued/sold as entitlement/tickets and provides them to the Customer Contract Partner in the form of product definitions and templates to be sold. The products can be composed of several heterogeneous service types.

Furthermore, the Product Owner is responsible for mapping and managing the effective costs after the execution of a travel chain (clearing).

A.2.7 Service Provider

Within the mobility service, the PT Service Operator becomes a Service Provider.

The Service Provider delivers mobility services in both a narrow and a broader sense. Mobility services in a narrow sense are transportation services, e.g. public transportation or vehicle sharing. Examples for mobility services in a broader sense are provision of parking spaces or insurance services.

In the area of public transportation services, a transportation contract is created between a Service Provider and a Mobility Service User by entering the public transit. In case of vehicle sharing, a permission for use contract is used. The configuration and formation of a contract can vary concerning other services.

Its task "collection of usage data" is enhanced by the task "acquisition of real-time data". The task "gathering of real-time data" refers to the acquisition of all real-time data of the provided service, e.g. timetable information in PT, current availability of common use of vehicles, current availability of parking/status interruption of escalators and elevators. This real-time data is needed by the Information Service Manager to generate travel information and travel assistance.

A.2.8 Payment Provider

The Payment Provider organizes the settlement for the use of different mobility services between the Payer and the Customer Contract Partner or an Account Provider, who is integrated as an external partner of the Customer Contract Partner.

The Payment Provider offers secure and straightforward cashless payment processing for the mobility services applications with all current payment systems and optimized multi-device solutions for Customer/Payer end devices.

The Payment Provider is also responsible for receivables management, including dunning. An exchange of information with the Booker is possible via the Mediator.

The Payment Provider also offers a customer service around the payment processing.

A.3 Basic framework of the generic mobility platform functional model

The links between the operational mobility platform roles are illustrated in Figure A.2. These links represent information flows.

It is assumed that the Customer already has a medium with a mobility application or is provided with one by the Customer Contract Partner. Within the mobility platform, there may be several organizations performing the functions of the mobility platform roles.

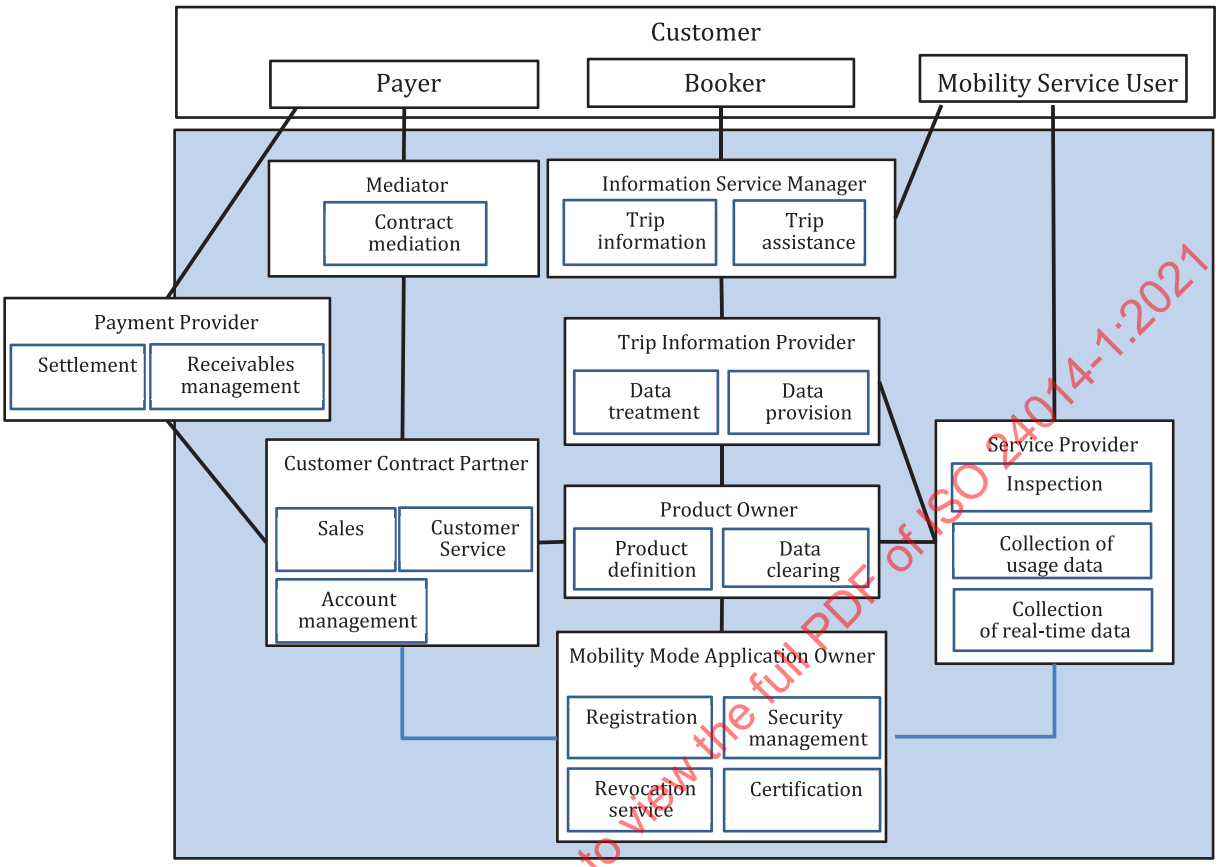


Figure A.2 — Interaction of actors within a mobility platform (operational and management mobility platform roles)

The Mediator establishes and manages the policies on behalf of the mobility platform. These policies are embedded in the set of rules.

Annex B
(informative)

Pay-As-You-Go (PAYG) roles and relationships in an IFMS

B.1 Introduction

This annex is for informative purposes only. Its purpose is to identify roles and relationships which could be appropriate if the main body of this document were to be extended in a later edition to include usage-based tariffs, such as PAYG.

In conventional ticketing, the role of Payment Provider is simply to enable customers to have access to funds to buy transport products. In PAYG, the role of the Payment Provider is to provide access to funds so that after a passenger has travelled, the Product Owner can claim and receive payment. There are two PAYG methods currently used in fare management systems: the first is where a transport smartcard issuer (e.g. a transport operator or transport authority) holds the passenger's PAYG funds, and the second is where a bankcard issuer holds the passenger's debit or credit account, from which PAYG charges are deducted.

The following subclauses describe the roles for conventional retail ticketing (where a product is bought before travel), PAYG with a transport smartcard issuer (where the operator or authority issues a PAYG smartcard and holds the PAYG balance) and finally PAYG with a bankcard issuer (where the bank issues the contactless bank card and where there is no specific PAYG balance).

Some additional roles are introduced, building on those described in main body of this document. These are Product Fulfiller, Merchant Acquirer, Bank Card Issuer and PAYG Balance Holder.

The role of the Product Fulfiller is to:

— implement the scheme security methods on its media readers, and

— load products onto the Passenger media as instructed by the Product Retailer.

The role of the Merchant Acquirer is to:

— contract with the Product Retailer/Owner to pay authorized payment requests,

— impose card scheme commercial rules on the Product Retailer/Owner, and

— certify that the merchant system meets card scheme and PCI-DSS technical rules.

NOTE PCI-DSS is the worldwide Payment Card Industry Data Security Standard that was set up to make sure that businesses process card payments securely in order to reduce card fraud. This is achieved through enforcing tight controls surrounding the storage, transmission and processing of cardholder data that businesses handle.

The role of the Bank Card Issuer is to:

— issue bank card to Passenger, including Know Your Customer (KYC) checks

— agree with other issuing banks the card scheme commercial rules under which bankcard PAYG takes place – in this case the Bank Card Issuer is the IFMS Media Provider

— impose card scheme commercial rules on Passenger

— charge Passenger for authorized payment requests from Product Retailer/Owner

The role of the PAYG Balance Holder is to:

— meet appropriate regulatory requirements for PAYG balance deposit taking

— maintain an account system for Passenger payments and receipts

— carry out KYC checks if needed by regulation

— receive funds from PAYG Top-up Retailers

— contract with PAYG Product Owner to pay authorised payment requests

The reason for adding these roles is to demonstrate the significant difference in roles between PAYG with a transport smartcard issuer or PAYG with a bankcard issuer when compared against conventional retail ticketing. With conventional retail ticketing and PAYG with a bankcard issuer the IFMS Payment Provider is an external role, whereas with PAYG with a transport smartcard issuer the IFMS Payment Provider is an internal IFMS role. An internal IFMS Payment Provider can set its own commercial rules, technology and governance, none of which are possible with an external IFMS Payment Provider.

B.2 Conventional retail ticketing

Figure B.1 shows the roles involved in the conventional retail ticketing model.

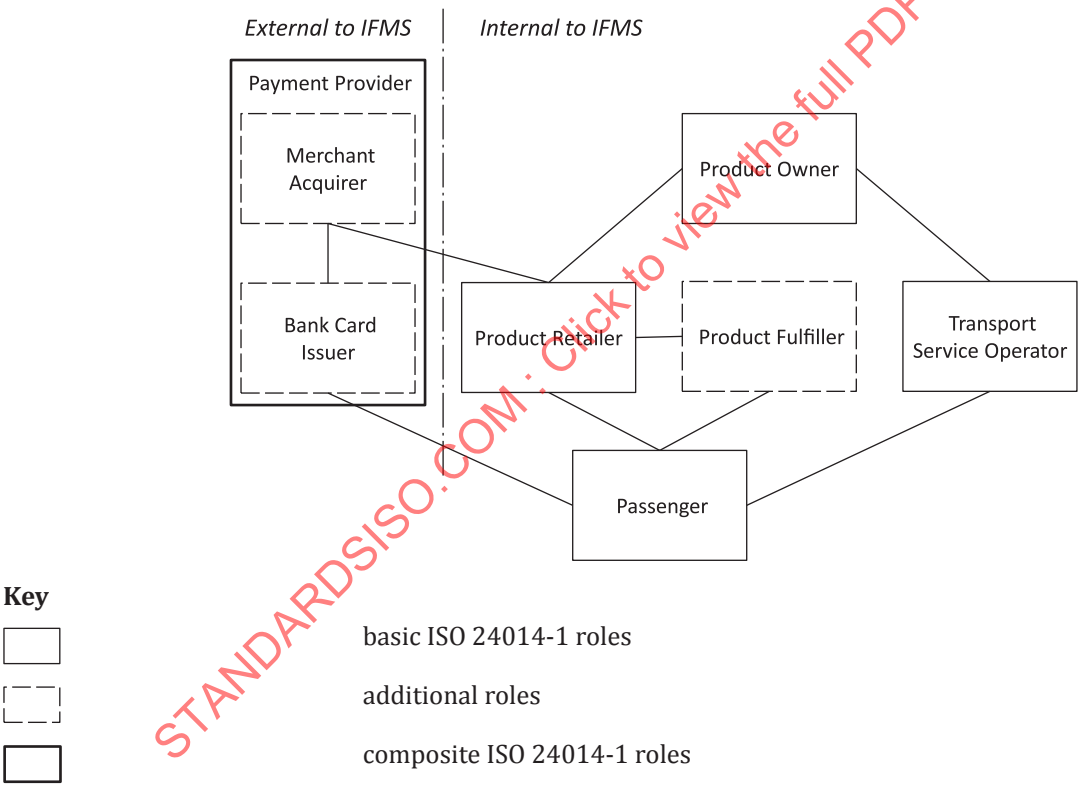


Figure B.1 — Conventional retail ticketing

The main business flows for this model are as follows:

1) The Product Owner agrees with the Transport Service Operator what retail transport products can be created and sold.

2) The Product Retailer agrees with the Product Owner what products it can sell.

3) The Passenger buys a product – a defined entitlement to travel

4) The product is loaded on to the media by either the Product Retailer or remotely by the Product Fulfiller (who is usually but not always a Transport Service Operator).

5) Where a payment card is used the Product Retailer claims payment from the Merchant Acquirer and settles with the Product Owner.

6) The Merchant Acquirer claims payment from the Card Issuer, who claims payment from the Passenger.

7) The Passenger uses the product to travel on the Transport Service Operator.

In this model the source of funds for travel is the Bank Card Issuer (unless cash or other forms of payment are being used) and the Bank Card Issuer together with the Merchant Acquirer is the Payment Provider.

a) The Payment Provider can be regarded as being external to the IFMS.

b) The IFMS Manager has no part in the governance of the Payment Provider.

c) The IFMS Manager integrates the external media and the payment service provided by the Payment Provider as described subclauses 7.3 and 7.4.

B.3 PAYG with a transport smartcard issuer

Figure B.2 shows the roles involved in the PAYG with a transport smartcard issuer model.

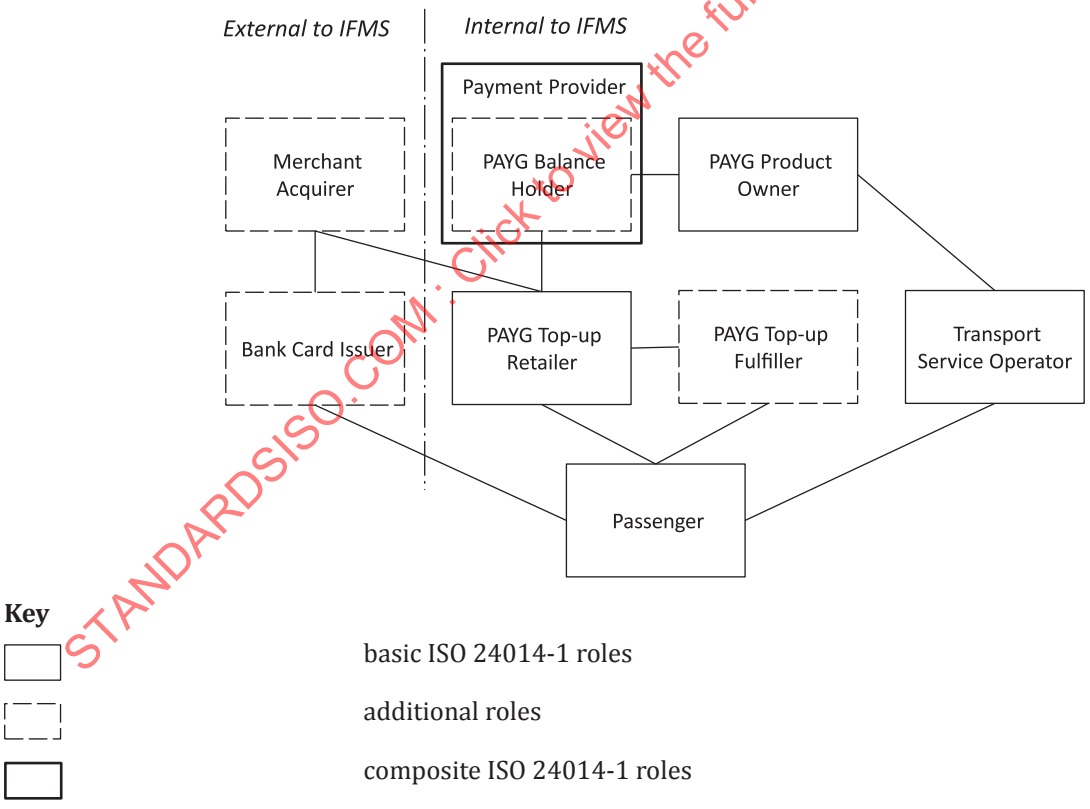


Figure B.2 — PAYG with a transport smartcard issuer

The main business flows for this model are as follows:

1) The PAYG Product Owner agrees the PAYG rules and prices with the Transport Service Operator.

2) There is no Product Retailer role for PAYG although both the Payment Provider and the PAYG Product Owner are each obliged to perform an Account Provider role. The former is in respect of transactions on the Passenger's financial account and the latter in respect of the journeys made by the Passenger.

3) The PAYG Balance Holder (usually a transport operator or a transport authority) agrees that the PAYG Product Owner can use the Passenger's PAYG balance (the Balance Holder and the Product Owner are usually the same entity but do not need to be). The PAYG Product Owner can agree to contract with several PAYG Balance Holders to allow the use of their funds for PAYG travel, essentially providing PAYG roaming.

4) The PAYG Top-up Retailer agrees with the PAYG Balance Holder that it may sell PAYG top-ups.

5) The Passenger buys a PAYG top-up. In doing so, the Passenger explicitly contracts to pay the fare once travel is completed. Such a contract is subject to the Product Owner's PAYG terms and conditions.

6) The value is loaded onto the media by either the PAYG Top-up Retailer or remotely by the PAYG Top-up Fulfiller, unless it is a server-based system, in which case no physical loading takes place.

7) Where a payment card is used for top-up, the PAYG Top-up Retailer claims payment from the Merchant Acquirer.

8) The Merchant Acquirer claims payment from the Card Issuer, who claims payment from the Passenger.

9) The Passenger uses their PAYG balance to travel on the Transport Service Operator.

10) The PAYG Product Owner may from time to time check with the PAYG Balance Holder that the Passenger has sufficient PAYG balance to travel.

11) The Transport Service Operator reports usage to the PAYG Product Owner.

12) The PAYG Product Owner calculates the price of travel, claims payment from the PAYG Balance Holder and pays the Transport Service Operator for the travel undertaken.

In this model, the source of funds for travel is the PAYG Balance Holder (even if cash is being used to top-up the balance) and the PAYG Balance Holder is the Payment Provider.

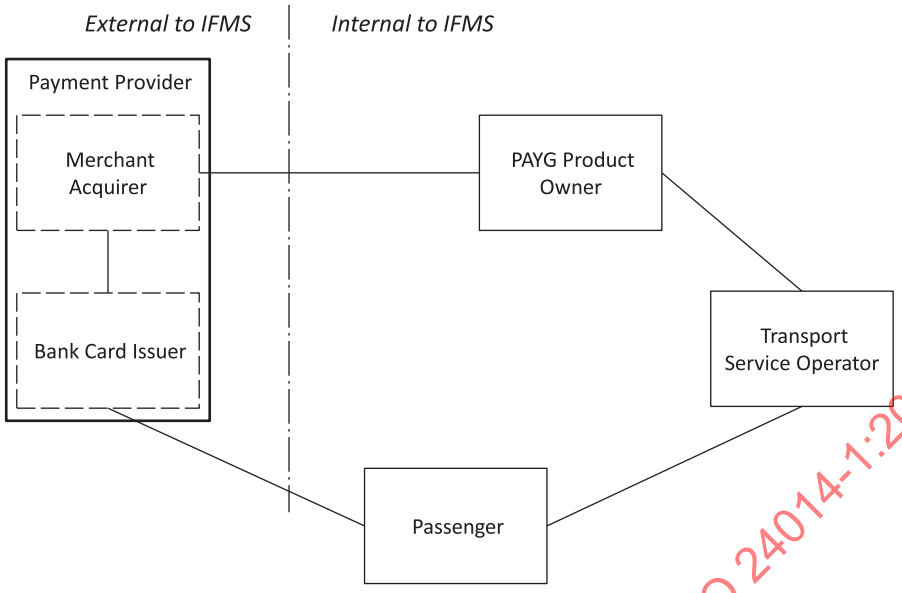
a) The Payment Provider can be regarded as being internal to the IFMS.

b) The IFMS Manager normally participates in the governance of the Payment Provider, even if it is a Common Transport Service Account as defined in ISO/TR 21724-1.

c) The IFMS Manager integrates the Merchant Acquirer as described in subclauses 8.4 and 8.5.

B.4 PAYG with a bankcard issuer

Figure B.3 shows the roles involved in the PAYG with a bankcard issuer model.



Key

basic ISO 24014-1 roles

additional roles

composite ISO 24014-1 roles

Figure B.3 — PAYG with a bankcard issuer

The main business flows for this model are as follows:

1) The PAYG Product Owner agrees with the Transport Service Operator the PAYG rules and prices.

2) There is no Product Retailer role for PAYG although both the Payment Provider and the PAYG Product Owner are each obliged to perform an Account Provider role. The former is in respect of transactions on the Passenger's financial account and the latter in respect of the journeys made by the Passenger.

3) The Merchant Acquirer agrees that the PAYG Product Owner can take the Passenger's money from the Bank Card Issuer for PAYG travel. This agreement is included in the Product Owner's acquiring contract with the Merchant Acquirer and it reflects the Transit Model rules of each bank card scheme used by the Bank Card Issuer.

4) The Passenger uses the Bank Card to travel on the Transport Service Operator. In doing so, the Passenger implicitly contracts to pay the fare once travel is completed. Such a contract is subject to the Product Owner's PAYG terms and conditions.

5) The PAYG Product Owner may from time to time check with the Merchant Acquirer that the Passenger has sufficient funds to travel.

6) The Transport Service Operator reports usage to the PAYG Product Owner.

7) The PAYG Product Owner calculates the price of travel, claims payment from the Merchant Acquirer and pays the Transport Service Operator for the travel undertaken.

8) The Merchant Acquirer claims payment from the Card Issuer who claims payment from the Passenger.

In this model, the source of funds for travel is always the Bank Card Issuer (cash is never used in this model). The Bank Card Issuer together with the Merchant Acquirer is the Payment Provider.

a) The Payment Provider can be regarded as being external to the IFMS.

b) The IFMS Manager has no part in the governance of the Payment Provider.

c) The IFMS Manager integrates the external media and the payment service provided by the Payment Provider as described in subclauses 8.4 and 8.5.

Annex C
(informative)

Mobility ID service example

C.1 Introduction

This annex provides an example on how identities that represent Customers and customer media can be made available, managed, maintained and provided for purposes of the IFMS and its external mobility partners by using the definitions, functions and use cases which are documented in the main body of this document.

This example addresses the following scenarios:

1) The IFMS possesses a significant inventory of customer data and an internal Identity Provider wants to use this data as a basis for its own, transport-specific ID service.

2) The available customer data potentially have to be completed and consolidated in order to support a defined LoA. This can require a cooperation with external eID services and data exchanges with external eID media.

3) The IFMS-internal Identity Provider plans to offer the ID service not only for internal purposes but also to external partners of the IFMS.

4) The IFMS has issued media to its Customers which shall be used for ID-based mobility services of the IFMS and its external service partners.

5) Defined levels of trust for identity information and a scalable approach to assurance and security shall be implemented.

C.2 Definitions relevant for this example

The ISO/IEC 24760 series provides a framework for identity management. This example uses ISO/IEC 24760-1 as a point of reference for terms and definitions concerning identities and identity management in transport and mobility.

For the purpose of this example, the following terms and definitions apply:

entity — item (person, organization, device etc.) that has recognizably distinct existence and may be identified

identity — set of attributes related to an entity

identity information — set of values of attributes optionally associated with any metadata in an identity

NOTE In an IT system, an identity is present as identity information.

identifier — unique identity information that unambiguously distinguishes one entity from another

attribute — characteristic or property of an entity that can be used to describe its state, appearance, or other aspects (e.g. entity type, address information, telephone number)

eID	electronic identity card or service NOTE This is typically issued by governments or their representatives. It typically provides a defined level of trust and can serve as a trustworthy source of attribute values for identities, e.g. in the mobility domain.
IDc	customer identity which is defined and managed by the Identity Provider
IDx	identity of customer media or applications issued by the Media or Application Retailer NOTE Any customer media or applications identity shall be uniquely identified by an identifier and may have a set of additional attributes.
derived eID	ID attributes which are derived by the Identity Provider from governmental or other external eID by using. for example, a unidirectional algorithm NOTE They represent these external eID for the purposes of the Identity provider's service.

ISO/IEC 24760-1 supports the definition of identities not only per entity but also per market domain. This means that a specific person may have different ID with a different selection of attributes, e.g. for payment, for governmental purposes and for mobility and transport services.

In this example, the role "Identity Provider" includes the ISO/IEC 24760-1 roles "Identify information provider" and also "Identify information authority" for the mobility and transport domain.

The customer identity, IDc, is specifically designed by the IFMS for the mobility and transport domain. It is generated and maintained by the Identity Provider and includes attributes which are required for the mobility services of the IFMS and its external service partners. These attributes include the name, address and payment data, as in most other application areas. In addition, there may be attributes that are specific to transport: it may be useful to include an attribute that notifies if the customer is eligible for special fare discounts or needs assistance when travelling is specific to mobility. For mobility services, it would be instrumental to include an attribute that provides trustworthy information if the Customer has a valid driver licence. In both examples, the attributes may not be managed by the Customer for security reasons. Instead, there needs to be a trustworthy external source of information and a frequent synchronization with these sources.

Figure C.1 provides an example for a customer identity, IDc, which is specifically designed for the mobility market.