

DIN EN ISO 24014-1

ICS 03.220.01; 35.240.60

Ersatz für
DIN EN ISO 24014-1:2016-04**Öffentlicher Verkehr –
Interoperables Fahrgeldmanagement System –
Teil 1: Architektur (ISO 24014-1:2021);
Englische Fassung EN ISO 24014-1:2021**

Public transport –
Interoperable fare management system –
Part 1: Architecture (ISO 24014-1:2021);
English version EN ISO 24014-1:2021

Transport public –
Système de gestion tarifaire interopérable –
Partie 1: Architecture (ISO 24014-1:2021);
Version anglaise EN ISO 24014-1:2021

Gesamtumfang 97 Seiten

DIN-Normenausschuss Automobiltechnik (NAAutomobil)
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

Dieses Dokument (EN ISO 24014-1:2021) wurde vom Technischen Komitee ISO/TC 204 „Intelligent Transport Systems“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 278 „Intelligente Verkehrssysteme“, dessen Sekretariat von NEN (Niederlande) gehalten wird, erarbeitet.

Das zuständige deutsche Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 052-02-71 GA „Intelligente Verkehrssysteme“ des DIN-Normenausschusses Automobiltechnik (NAAutomobil).

Das Präsidium des DIN hat mit seinem Beschluss 1/2004 festgelegt, dass von dem in den Regeln der europäischen Normungsarbeit von CEN/CENELEC verankerten Grundsatz, wonach Europäische Normen in den drei offiziellen Sprachen Deutsch, Englisch und Französisch veröffentlicht werden, in begründeten Ausnahmefällen abgewichen und auf die deutsche Sprachfassung verzichtet werden kann.

Die Genehmigung dafür hat die DIN-Geschäftsleitung entsprechend ihren in Anlage 1 zu dem DIN-Rundschreiben A 5/2004 festgelegten Kriterien für die vorliegende Norm auf Antrag des NA 052 NAAutomobil als Ergebnis einer Einzelfallentscheidung erteilt, zumal bereits dieser Norm zugrunde liegende Papiere überwiegend in englischer Sprache auch von den deutschen Marktteilnehmern angewendet werden.

Fahrgeldmanagement Systeme umfassen alle Prozesse zur Verteilung und Nutzung von Fahrkostenprodukten im Umfeld des öffentlichen Verkehrs.

Fahrgeldmanagement Systeme werden dann als „interoperabel“ bezeichnet, wenn Sie dem Kunden ermöglicht, ein tragbares elektronisches Medium (z. B. Smartcard) im Zusammenspiel mit kompatiblen Einrichtungen (z. B. an Haltestellen) zu verwenden.

Interoperabilität von Fahrgeldmanagement Systeme erfordert eine übergeordnete Systemarchitektur, welche die Funktionalität, die betroffenen Akteure und deren Rollen, sowie die Beziehungen und Schnittstellen beschreibt und in dieser Norm berücksichtigt werden. Dazu gehört außerdem ein Sicherheitsschema zum Schutz der Privatsphäre, Integrität sowie Diskretion zwischen den Akteuren.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Änderungen

Gegenüber DIN EN ISO 24014-1:2016-04 wurden folgende Änderungen vorgenommen:

- a) Abschnitt 2 „Normative Verweisungen“ hinzugefügt;
- b) Erweiterungen durchgeführt, welche neu Trends im öffentlichen Verkehr reflektieren;
- c) Erweiterungen durchgeführt, welche die Kollaboration mit anderen marktrelevanten Systemen und Anwendungen berücksichtigen;
- d) redaktionelle Korrekturen.

Frühere Ausgaben

DIN EN ISO 24014-1: 2008-09, 2016-04

Nationaler Anhang NA (informativ)

Begriffe

Die Benummerung der folgenden Begriffe und Abkürzungen ist identisch mit der Benummerung in der englischen Fassung.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

3.1

kontobasierter Fahrkartenverkauf

ABT, en: account based ticketing

architekturbasierter Ansatz, der *Produkte* (3.30) im *interoperablen Fahrgeldmanagement-System Backoffice* (en: interoperable fare management, IFM) (3.19) speichert (d. h. den persönlichen Kundenzugang oder einen temporären Zugang) und nicht im *Kundenmedium* (3.12)

Anmerkung 1 zum Begriff: Das Kundenmedium führt Authentifizierungsberechtigungen mit sich sowie eine *Anwendung* (3.7), die Referenzen zu kontobasierten Produkten im Backoffice beinhaltet.

3.2

Aktionsliste

(en: action list)

Objektliste bezogen auf *IFM-Anwendungen* (3.19, 3.7) oder *-produkte* (3.30), die auf *Zugriffsgeräte* (en: medium access devices, MAD, 3.24) heruntergeladen und verarbeitet wird, wenn es eine spezifische IFM-Anwendung oder ein IFM-Produkt betrifft, das in der Liste im Zugriffsgerät referenziert wird

3.3

Akteur

(en: actor)

Person, *Organisation* (3.25) oder anderes (Unter)System, welche(s) eine kohärente Menge an Funktionen im *IFM-System* (3.20) für einen bestimmten *Anwendungsfall* (3.36) bedient

3.4

Anwendungsregeln

(en: application rules)

Spezifikation von Regeln im *Anwendungsvertrag* (3.7) zur Verwendung der Anwendung mit dem Kunden, wie vom Anwendungseigner festgelegt

3.5

Anwendungsbeschreibung

(en: application specification)

Funktionsspezifikation, Datenelemente und Sicherheitsschemata nach den *Anwendungsregeln* (3.4)

3.6

Anwendungsvorlage

(en: application template)

ausführbare technische Vorlage der *Anwendungsbeschreibung* (3.5)

3.7

Anwendung

(en: application)

implementierte und initialisierte *Anwendungsvorlage* (3.6)

Anmerkung 1 zum Begriff: Die Anwendung kann eine oder mehrere *Produkte* (3.30) beherbergen und kann Funktionen unterstützen, welche die Identifizierung und den Schutz dieser Produkte unterstützen. Für ABT- und ID-basierenden Architekturen, kann die Anwendung sich teilweise im *Kundenmedium* (3.12) (Identifikation und Zugriffssteuerungsfunktion) und teilweise sich im *IFM-Backoffice* (3.19) befinden (Produkte).

Anmerkung 2 zum Begriff: Die Anwendung ist durch einen eindeutigen Bezeichner gekennzeichnet.

Anmerkung 3 zum Begriff: Die Anwendung kann *Produkte* (3.30) und andere optionale Kundeninformationen (Details zum Kunden, Kundenpräferenzen) beinhalten.

Anmerkung 4 zum Begriff: Die Anwendung kann vollständig auf Kundenmedien installiert werden oder auf dem Kundenmedium und dem IFM-Backoffice verteilt werden.

3.8

kommerzielle Regeln

(en: commercial rules)

Regeln, die das Abkommen und die Vergütung in einem *IFMS* (3.20) festlegen

3.9

Komponente

(en: component)

beliebiger Anteil der Hardware und/oder Software, der eine oder mehrere Funktionen in einem *IFMS* (3.20) ausführt

3.10

Komponentenlieferant

(en: component provider)

jeder Beliebige, der eine *Komponente* (3.9) in ein *IFMS* (3.20) einbringen möchte

3.11

Kundenkonto

(en: customer account)

Datenbereich, der von einem *IFMS* (3.20) ausgerichtet wird (typischerweise der Produkthändler), welcher alle Informationen beinhaltet, die für die Geschäftsbeziehung zwischen dem Kunden und dem IFMS relevant sind

Anmerkung 1 zum Begriff: Konten werden vom betroffenen Interessensvertreter im IFMS gepflegt und betrieben. Konten, auf die online zugegriffen werden kann, können vom Kunden aufgesetzt und betrieben werden.

3.12

Kundenmedium

(en: customer medium)

Medium (3.22), welches von einer *Anwendung* (3.7) über einen Anwendungsvertrag initialisiert wird

3.13**abgeleitete Identität**

(en: derived identity)

abgeleitete ID

(en: derived ID)

elektronischer Bezeichner, der von einer anderen *ID* (3.15) generiert wurde (primärer ID)

Anmerkung 1 zum Begriff: Typischerweise wird die abgeleitete ID von einem Identitätsanbieter in der Art und Weise generiert, dass die Authentizität nachgewiesen werden kann, es gibt aber keine Möglichkeit, von der abgeleiteten ID zurück auf die ursprüngliche ID zu schließen. Das Konzept einer abgeleiteten ID wird typischerweise dann verwendet, wenn die ursprüngliche ID mit hoher Sicherheitsanforderung (ähnlich einer Fahrerlaubnis oder behördliche eID) nicht in einer Umgebung offengelegt werden darf, die kein hohes Vertrauensniveau gewährleistet.

3.14**extern**

(en: external)

Objekt, welches nicht den Regeln des *IFMS* (3.20) folgt und für das spezielle Aktivitäten notwendig sind, Interoperabilität und Security mit dem IFMS zu implementieren

3.15**Identität****ID**, en: identity

Information, welche eine spezifische Person oder ein Objekt in einer eindeutigen und unmissverständlichen Art und Weise beschreibt

Anmerkung 1 zum Begriff: Eine Person kann beispielsweise mit den Attributen Name, Geburtstag, Geschlecht, Adresse usw. beschrieben werden. Eine unmissverständliche Identifizierung einer Person benötigt typischerweise zusätzlich einen eindeutigen Bezeichner, welcher von dem Identitätsanbieter ausgestellt wird. Ein Objekt, z. B. ein Fahrkartenautomat, kann über Besitzer, Typ und Softwareversion beschrieben werden. Eine eindeutige Seriennummer kann als Bezeichner dienen.

3.16**IFM-Funktionsmodell**

(en: IFM functional model)

Modell zur Festlegung von *IFM-Rollen* (3.18) und deren Interaktion**3.17****IFM-Richtlinie**

(en: IFM policy)

kommerzielle, technische, sicherheitsrelevante und Vertraulichkeitsziele für ein *IFM* (3.19)**3.18****IFM-Rolle**

(en: IFM-role)

abstraktes Objekt, welches eine Funktionsmenge in einem *IFM-Funktionsmodell* (3.16) ausführt**3.19****interoperables Fahrgeldmanagement****IFM**, en: interoperable fare management

alle Funktionen, die in den Prozess zum interoperablen Fahrgeldmanagement eingebunden sind, wie die Verwaltung der *Anwendungen* (3.7), *Produkte* (3.30), Sicherheit und Zertifikate sowie Registrierung und Identifikation, um dem Kunden, unter Verwendung eines einzelnen tragbaren elektronischen *Mediums* (3.22), die Reise mit teilnehmenden Dienst Anbietern zu ermöglichen

3.20

interoperables Fahrgeldmanagement System

IFMS, en: interoperable fare management system

alle technischen, kommerziellen, sicherheits- und gesetzgeberischen Elemente, die *interoperables Fahrgeldmanagement* (3.19) ermöglichen

3.21

Vertrauensniveau

LoA, en: level of assurance

Niveau der Widerstandsfähigkeit von *IFMS-Komponenten* (3.20, 3.9) und -prozesse gegen festgelegtes Angriffspotential

Anmerkung 1 zum Begriff: Vertrauensniveau wird typischerweise vom Security Manager für alle Komponenten des IFMS festgelegt und in der *Menge von Regeln* (3.33) für Security Zertifikate spezifiziert.

3.22

Medium

(en: medium)

physikalischer *Anwendungsträger* (3.7)

3.23

Botschaft

(en: message)

Menge von Datenelementen, die zwischen *IFM-Rollen* (3.18) übertragen werden

3.24

Medium Zugriffsgesetz

MAD, en: medium access device

Gerät mit den notwendigen Einrichtungen (Hardware und Software) zur Kommunikation mit einem *Kundenmedium* (3.12)

3.25

Organisation

(en: organization)

juristische Einheit, die Funktionen und deren Verantwortlichkeiten für ein oder mehrere der folgenden betrieblichen *IFM-Rollen* (3.18) umfasst: Anwendungsbesitzer, Anwendungsverkäufer, Produkteigentümer, Dienstleister, sowie Sammlung und Weiterleitung usw.

3.26

Regel zur Preisgestaltung

(en: pricing rule)

Regeln, die Beziehungen zum Kunden bzgl. Preise und Bezahlung/Abrechnung festlegen

3.27

Produktregel

(en: product rule)

Nutzungs-, Preisgestaltungs- und *kommerzielle Regeln* (3.8), die vom Produkteigentümer festgelegt werden

3.28

Produktspezifikation

(en: product specification)

vollständige, nach den *Produktregeln* (3.27) festgelegte Spezifikation für Funktionen, Datenelemente und Sicherheitsschemata

3.29**Produktvorlage**

(en: product template)

technische Vorlage für eine *Produktspezifikation* (3.28)

Anmerkung 1 zum Begriff: Die Produktvorlage wird durch einen eindeutigen Bezeichner bestimmt.

3.30**Produkt**

(en: product)

Vorgang, bei dem eine *Anwendung* (3.7) in einer *Produktvorlage* (3.29) abgelegt wird

Anmerkung 1 zum Begriff: Ein Produkt legt das kommerzielle Angebot an einen Kunden fest. Durch den Kauf eines Produktes, wird der Kunde berechtigt, spezielle Dienste zu erhalten, die vom Produktbesitzer festgelegt wurden.

Anmerkung 2 zum Begriff: Es wird durch einen eindeutigen Bezeichner bestimmt und erlaubt dem Kunden, von einem Dienst eines Diensteanbieters zu profitieren.

3.31**Rolle**

(en: role)

abstraktes Objekt, das eine Menge von Funktionen durchführt

3.32**Sicherheitsrichtlinie**

(en: security policy)

Grundsätze des *IFMS* (3.20) zur Sicherstellung der öffentlichen Interessen und des Kapitals innerhalb des IFMS**3.33****Menge von Regeln**

(en: set of rules)

Bestimmungen zur Einhaltung von *IFM-Richtlinien* (3.17), ausgedrückt als technische, kommerzielle, Sicherheit oder gesetzliche Anforderungen und Normen, die nur für das IFMS relevant sind**3.34****Auslöser**

(en: trigger)

Ereignis, das die Ausführung eines *Anwendungsfalles* (3.36) veranlasst**3.35****Nutzungsregel**

(en: usage rule)

Regel, die die Nutzungszeit, den Nutzungsbereich, den persönlichen Status und Art des Dienstes festlegt

3.36**Anwendungsfall**

(en: use case)

Prozessbeschreibung durch Festlegung einer Ausführungssequenz, die von einem oder mehreren *Akteur(en)* (3.3) und von System selbst, festgelegt ist

— Leerseite —

English Version

Public transport - Interoperable fare management system -
Part 1: Architecture (ISO 24014-1:2021)

Transport public - Système de gestion tarifaire
interopérable - Partie 1: Architecture (ISO 24014-
1:2021)

Öffentlicher Verkehr - Interoperables
Fahrgeldmanagement System - Teil 1: Architektur (ISO
24014-1:2021)

This European Standard was approved by CEN on 19 November 2020.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

This document (EN ISO 24014-1:2021) has been prepared by Technical Committee ISO/TC 204 "Intelligent transport systems" in collaboration with Technical Committee CEN/TC 278 "Intelligent transport systems" the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by July 2021, and conflicting national standards shall be withdrawn at the latest by July 2021.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO 24014-1:2015.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 24014-1:2021 has been approved by CEN as EN ISO 24014-1:2021 without any modification.

Contents

Page

Foreword	vi
Introduction	vii
1 Scope	1
2 Normative references	2
3 Terms and definitions	2
4 Abbreviated terms	6
5 Requirements	6
6 System environment for IFMS	7
6.1 General	7
6.2 Mobility platforms	7
7 Conceptual framework for IFMS	7
7.1 General	7
7.2 Description of IFM roles and external roles	8
7.3 Basic framework of the generic IFM functional model	12
8 Use case description for the IFM functional model	13
8.1 Description of IFM-roles and external roles	13
8.2 Define set of rules	14
8.2.1 General	14
8.2.2 Define set of rules for Customer accounts	14
8.2.3 Define set of rules for media	14
8.2.4 Define set of rules for ID services	15
8.2.5 Define set of rules for payment services	15
8.3 Certification	15
8.3.1 General	15
8.3.2 Certification of organizations	16
8.3.3 Certification of components	16
8.3.4 Certification of media	16
8.3.5 Certification of ID services	16
8.3.6 Certification of payment services	17
8.3.7 Certification of application specifications and templates	17
8.3.8 Certification of product specifications and templates	17
8.4 Interaction with external objects	18
8.4.1 General	18
8.4.2 Interaction with external media	18
8.4.3 Interaction with external applications	19
8.4.4 Interaction with external ID services	20
8.4.5 Interaction with external payment services	21
8.5 Registration	22
8.5.1 General	22
8.5.2 Registration of organizations	22
8.5.3 Registration of components	22
8.5.4 Registration of ID services	22
8.5.5 Registration of customer accounts	23
8.5.6 Registration of payment services	24
8.5.7 Registration of media	24
8.5.8 Registration of customer media	24
8.5.9 Registration of application templates	25
8.5.10 Registration of applications	25
8.5.11 Registration of product templates	25
8.5.12 Registration of products	25
8.6 Managing ID services	26

8.6.1	General.....	26
8.6.2	Enrolment and update of Customer ID data via an application form.....	26
8.6.3	Enrolment and update of Customer ID data via an external ID service.....	27
8.6.4	Update of Customer ID data via an online account.....	27
8.6.5	Re-use of incumbent Customer ID data.....	28
8.6.6	Management and maintenance of Customer ID data.....	28
8.6.7	Providing the ID service to IFMS internal and external organizations.....	29
8.7	Management of customer accounts.....	29
8.7.1	General.....	29
8.7.2	Secure login to customer online accounts.....	30
8.7.3	Connect/disconnect customer media to/from the customer online account.....	30
8.7.4	Transfer of products between connected customer media.....	31
8.7.5	Connect system generated account with a customer account.....	32
8.7.6	Termination of customer accounts.....	32
8.8	Management of customer media.....	33
8.8.1	General.....	33
8.8.2	Provisioning of media.....	33
8.8.3	Termination of customer media.....	34
8.9	Management of applications.....	35
8.9.1	General.....	35
8.9.2	Dissemination of application templates.....	35
8.9.3	Acquisition of applications.....	36
8.9.4	Termination of application templates.....	36
8.9.5	Termination of applications.....	37
8.10	Management of products.....	38
8.10.1	Dissemination of product templates.....	38
8.10.2	Termination of product templates.....	39
8.10.3	Management of action lists.....	40
8.10.4	Acquisition of products.....	40
8.10.5	Modification of product parameters.....	40
8.10.6	Termination of products.....	41
8.10.7	Use and inspection of products.....	41
8.10.8	Collection of data.....	42
8.10.9	Forwarding data.....	43
8.10.10	Generation and distribution of clearing reports.....	43
8.11	Security management.....	44
8.11.1	General.....	44
8.11.2	Monitoring of IFM processes and IFM data life cycle.....	44
8.11.3	Management of IFM security keys.....	45
8.11.4	Management of security lists.....	45
8.12	Customer Service management (optional).....	48
9	System interface identification.....	48
10	Identification.....	48
10.1	General.....	48
10.2	Numbering scheme.....	48
10.3	Prerequisites.....	49
10.3.1	There is one Registrar within the IFMS.....	49
10.3.2	All objects, e.g. templates and components, have an owner who is one of the actors in the IFMS.....	49
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.....	49
11	Security in IFMSs.....	49
11.1	General.....	49
11.2	Protection of the interests of the public.....	49
11.3	Assets to be protected.....	50
11.4	General IFM security requirements.....	50

Annex A (informative) Mobility Platform – German example	52
Annex B (informative) Pay-As-You-Go (PAYG) roles and relationships in an IFMS	57
Annex C (informative) Mobility ID service example	63
Annex D (informative) Examples of IFMS implementations	73
Annex E (informative) Media centric management and back-office centric management	79
Bibliography	81

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 information.

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.

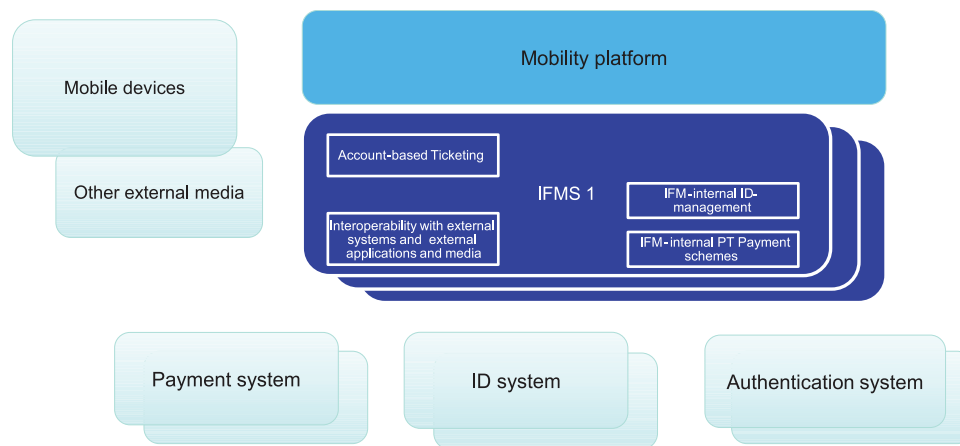


Figure 1 — System environment for IFMS

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	<p>The Account Provider supports the following functions:</p> <ul style="list-style-type: none">— provisioning and hosting of Customer accounts;— creates and validates Customer login credentials for access to a customer online account.
Application Owner	<p>The Application Owner holds the application contract and specifies the application rules for the use of the application with the Customer.</p>
Application Retailer	<p>The Application Retailer sells and terminates applications, collects value, and refunds value to a Customer as authorized by an Application Owner.</p> <p>The Application Retailer is the only financial interface between the Customer and the IFMS related to applications.</p>

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	<p>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.</p> <p>The Customer may acquire customer media, applications and products for himself/herself or other Passengers. Examples:</p> <ul style="list-style-type: none">— 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	<p>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.</p>
Identity Provider	<p>The Identity Provider is an IFM role which:</p> <ul style="list-style-type: none">— 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; <p>External Identity Providers may offer external ID services which are used by the IFM internal Identity Provider as a source of trustworthy ID data.</p>
Media Provider	<p>The role of Media Provider:</p> <ul style="list-style-type: none">— is to provide and release the media for use with one or more applications.
Media Retailer	<p>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:</p> <ul style="list-style-type: none">— 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	<p>The Passenger uses a product to obtain the service provided by the Service Operator.</p>

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	<p>The Security Manager is responsible for establishing and coordinating the security policy and for:</p> <ul style="list-style-type: none">— 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.

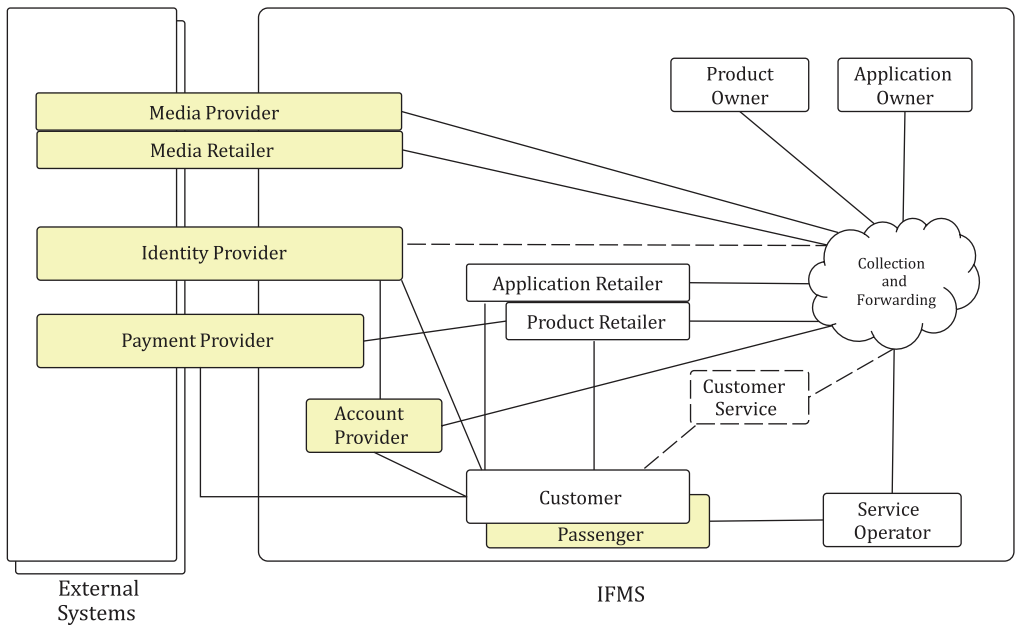


Figure 2 — Links between operational roles

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.

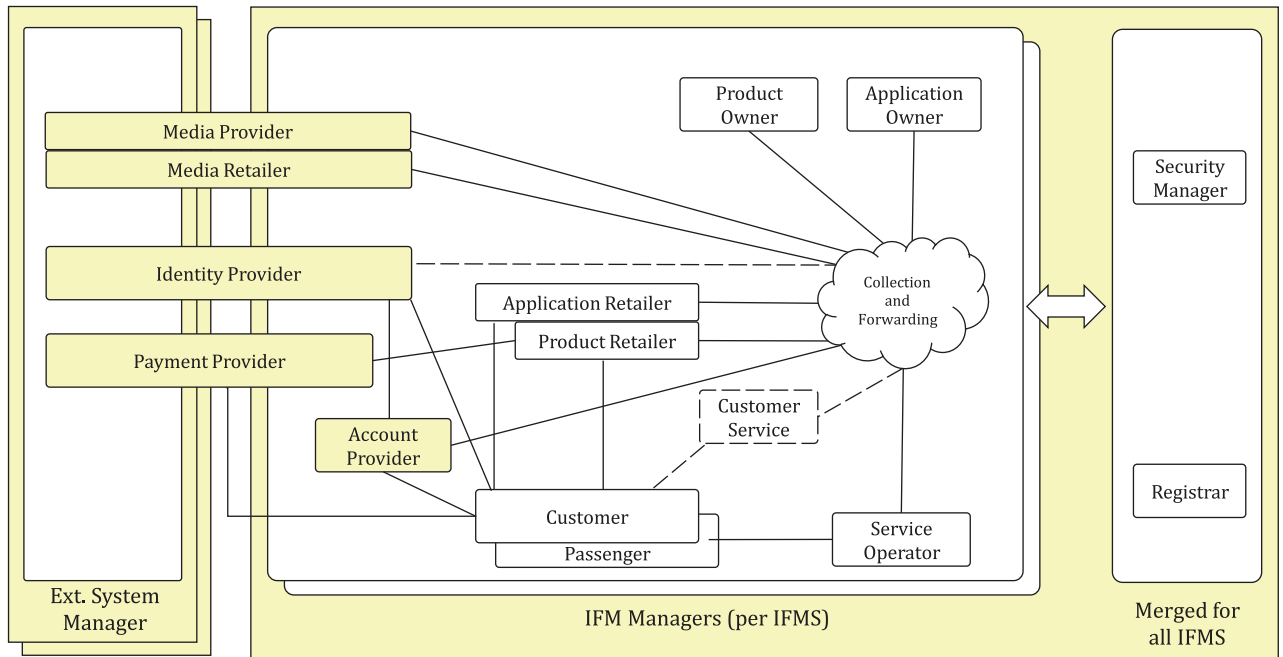


Figure 3 — Interaction of IFM domains and with external systems (operational and management roles)

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 <ul style="list-style-type: none">– 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: <ul style="list-style-type: none">– 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.