

DIN EN ISO 24014-1



ICS 03.220.01; 35.240.60

Entwurf

Einsprüche bis 2020-07-29
Vorgesehen als Ersatz für
DIN EN ISO 24014-1:2016-04

**Öffentlicher Verkehr –
Interoperables Fahrgeldmanagement System –
Teil 1: Architektur (ISO/DIS 24014-1:2020);
Englische Fassung prEN ISO 24014-1:2020**

Public transport –
Interoperable fare management system –
Part 1: Architecture (ISO/DIS 24014-1:2020);
English version prEN ISO 24014-1:2020

Transport public –
Système de gestion tarifaire interoperable –
Partie 1: Architecture (ISO/DIS 24014-1:2020);
Version anglaise prEN ISO 24014-1:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-05-29 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an naautomobil@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Automobiltechnik (NAAutomobil), 10004 Berlin, Postfach 8 04 62 oder Behrenstr. 35, 10117 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 91 Seiten

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

Nationales Vorwort

Dieses Dokument (EN ISO 24014-1:2014) wurde vom Technischen Komitee ISO/TC 204 „Intelligent Transport Systems“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 278 „Intelligente Verkehrssysteme“, dessen Sekretariat vom NEN (Niederlande) gehalten wird, erarbeitet.

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

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) Erweiterungen durchgeführt, welche neu Trends im öffentlichen Verkehr reflektieren;
- b) Erweiterungen durchgeführt, welche die Kollaboration mit anderen marktrelevanten Systemen und Anwendungen berücksichtigen;
- c) redaktionelle Korrekturen.

Nationaler Anhang NA (informativ)

Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

2.1

kontobasierter Fahrkartenverkauf

ABT (en: account based ticketing)

architekturbasierter Ansatz, der Produkte im interoperablen Fahrgeldmanagement-System Backoffice (en: interoperable fare management, IFM) speichert (d. h. den persönlichen Kundenzugang oder einen temporären Zugang) und nicht im Medium des Kunden. Das Kundenmedium führt Authentifizierungsberechtigungen mit sich sowie eine Anwendung, die Referenzen zu kontobasierten Produkten im Backoffice beinhaltet

2.2

Aktionsliste

(en: action list)

Objektliste bezogen auf IFM-Anwendungen oder –produkte (2.28), die auf Zugriffsgeräte (en: medium access devices, MAD, 2.22) heruntergeladen und verarbeitet wird, wenn es eine spezifische IFM-Anwendung oder ein IFM-Produkt betrifft, das in der Liste im Zugriffsgerät referenziert wird

2.3

Akteur

(en: actor)

Person, eine *Organisation* (2.19) oder anderes (Unter)System, welche(s) eine kohärente Menge an Funktionen im IFM-System für einen bestimmten *Anwendungsfall* (2.30) bedient

2.4

Anwendungsregeln

(en: application rules)

Anforderungen an den Besitzer der Anwendung

2.5

Anwendungsbeschreibungen

(en: application specification)

Funktionsspezifikation, Datenelemente und Sicherheitsschemata nach den *Anwendungsregeln* (2.4)

2.6

Anwendungsvorlage

(en: application template)

ausführbare technische Vorlage der *Anwendungsbeschreibung* (2.5)

2.7

Anwendung

(en: application)

implementierte und initialisierte *Anwendungsvorlage* (2.6)

Anmerkung 1 zum Begriff: Die Anwendung kann eine oder mehrere Produkte 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 (Identifikation und Zugriffssteuerungsfunktion) und teilweise sich im IFM-Backoffice befinden (Produkte).

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

Anmerkung 3 zum Begriff: Die Anwendung kann *Produkte* (2.28) und andere optionale Kundeninformationen (Details zum Kunden, Kundenpräferenzen) beinhalten.

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

2.8

kommerzielle Regeln

(en: commercial rules)

Regeln, die das Abkommen und die Vergütung in einem IFMS festlegen

2.9

Komponente

(en: component)

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

2.10

Komponentenlieferant

(en: component provider)

jeder Beliebige, der eine *Komponente* (2.9) in ein IFMS einbringen möchte

2.11

Kundenkonto

(en: customer account)

Datenbereich, der von einem IFMS 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 außerdem vom Kunden aufgesetzt und betrieben werden.

2.12

Kundenmedium

(en: customer medium)

Medium (2.22), welches von einer *Anwendung* (2.7) über einen Anwendungsvertrag initialisiert wird

2.13

abgeleitete Identität (abgeleitete ID)

(en: derived identity, derived ID)

elektronischer Bezeichner, der von einer anderen ID 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.

2.14

extern

(en: external)

Adjektiv "extern" gibt an, dass das bezeichnete Objekt nicht den Regeln des IFMS folgt und das spezielle Aktivitäten notwendig sind, Operabilität und Security mit dem IFMS zu implementieren

2.15

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.

2.16

IFM-Funktionsmodell

(en: IFM functional model)

Modell zur Festlegung von *IFM-Rollen* (2.18) und deren Interaktion

2.17

IFM-Richtlinien

(en: IFM policies)

kommerzielle, technische, sicherheitsrelevante und Vertraulichkeitsziele für ein IFM

2.18

IFMS-Rolle

(en: IFM-role)

abstraktes Objekt, welches eine Funktionsmenge in einem *IFM-Funktionsmodell* (2.16) ausführt

2.19

interoperables Fahrgeldmanagement

IFM (en: interoperable fare management)

alle Funktionen, die in den Prozess zum interoperablen Fahrgeldmanagement eingebunden sind, wie die Verwaltung der Anwendungen, *Produkte* (2.30), Security und Zertifikate sowie Registrierung und Identifikation, um dem Kunden, unter Verwendung eines einzelnen tragbaren elektronischen Mediums, die Reise mit teilnehmenden Dienstleistern zu ermöglichen

2.20

interoperables Fahrgeldmanagement System

IFMS (en: interoperable fare management system)

alle technischen, kommerziellen, sicherheits- und gesetzgeberische Elemente, die *interoperables Fahrgeldmanagement* (2.19) ermöglichen

2.21

Vertrauensniveau

(en: level of assurance)

Niveau der Widerstandsfähigkeit von IFMS-Komponenten und -prozesse gegen festgelegtes Angriffspotential. Wird typischerweise vom Security Manager für alle Komponenten des IFMS festgelegt und in der Regelmenge für Security Zertifikate spezifiziert

2.22

Medium

(en: medium)

physikalischer *Anwendungsträger* (2.7)

2.23

Botschaft

(en: message)

Menge von Datenelementen, die zwischen *IFM-Rollen* (2.18) übertragen werden

2.24

Medium Zugriffsgerät

MAD (en: medium access device)

Gerät mit den notwendigen Einrichtungen (Hardware und Software) zur Kommunikation mit einem *Kundenmedium* (2.12)

2.25

Organisation

(en: organization)

juristische Einheit, die Funktionen und deren Verantwortlichkeiten für ein oder mehrere der folgenden betrieblichen *IFM-Rollen* (2.18) umfasst: Anwendungsbesitzer, Anwendungsverkäufer, Produkteigentümer, Dienstanbieter, sowie Sammlung und Weiterleitung usw.

2.26

Regeln zur Preisgestaltung

(en: pricing rules)

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

2.27

Produktregeln

(en: product rules)

Menge von Nutzungs-, Preisgestaltungs- und *kommerziellen Regeln* (2.8), die vom Produkteigentümer festgelegt werden

2.28

Produktspezifikation

(en: product specification)

vollständige, nach den *Produktregeln* (2.27) festgelegte Spezifikation für Funktionen, Datenelemente und Sicherheitsschemata

2.29

Produktvorlage

(en: product template)

technische Vorlage für eine *Produktspezifikation* (2.28)

Anmerkung 1 zum Begriff: Die Produktvorlage wird durch eine eindeutige Bezeichnung bestimmt.

2.30

Produkt

(en: product)

Vorgang, bei dem eine *Anwendung* (2.7) in einer *Produktvorlage* (2.29) 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 eine eindeutige Bezeichnung bestimmt und erlaubt dem Kunden, von einem Dienst eines Dienstansbieters zu profitieren.

2.31

Rolle

(en: role)

abstraktes Objekt, das eine Menge von Funktionen durchführt

2.32

Sicherheitsrichtlinie

(en: security policy)

Grundsätze des IFM zur Sicherstellung der öffentlichen Interessen und des Kapitals innerhalb des IFM

2.33

Menge von Regeln

(en: set of rules)

Bestimmungen zur Einhaltung der *Richtlinie* (2.17) für das IFM, ausgedrückt als technische, kommerzielle sicherheitsrelevante oder gesetzliche Anforderungen und Normen, die nur für das IFMS relevant sind

2.34

Auslöser

(en: trigger)

Anlass, der die Ausführung eines *Anwendungsfalles* (2.36) veranlasst

2.35

Nutzungsregeln

(en: usage rules)

Regeln, die die Nutzungszeit, das Nutzungsgebiet, den persönlichen Status und Art des Dienstes festlegen

2.36

Anwendungsfall

(en: use case)

Prozessbeschreibung durch Festlegung einer Ausführungssequenz, die von einem oder mehreren *Akteur(en)* (2.3) und von System selbst festgelegt ist

— Leerseite —

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Terms and definitions	2
3 Abbreviated terms	5
4 Requirements	5
5 System environment for IFMS	6
5.1 Mobility platforms	7
6 Conceptual framework for IFMS	7
6.1 Description of IFM-roles and external roles	8
6.2 Basic framework of the generic IFM functional model	12
7 Use case description for the IFM functional model	13
7.1 Define set of rules	14
7.1.1 Define set of rules for customer accounts	14
7.1.2 Define set of rules for media	14
7.1.3 Define set of rules for ID Services	14
7.1.4 Define set of rules for payment services	15
7.2 Certification	15
7.2.1 Certification of organizations	15
7.2.2 Certification of components	16
7.2.3 Certification of media	16
7.2.4 Certification of ID services	16
7.2.5 Certification of payment services	16
7.2.6 Certification of application specifications and templates	17
7.2.7 Certification of product specifications and templates	17
7.3 Interaction with external objects	17
7.3.1 Interaction with external media	18
7.3.2 Interaction with external applications	19
7.3.3 Interaction with external ID services	19
7.3.4 Interaction with external payment services	20
7.4 Registration	21
7.4.1 Registration of organizations	21
7.4.2 Registration of components	22
7.4.3 Registration of ID services	22
7.4.4 Registration of customer accounts	22
7.4.5 Registration of payment services	23
7.4.6 Registration of media	23
7.4.7 Registration of customer media	24
7.4.8 Registration of application templates	24
7.4.9 Registration of applications	24
7.4.10 Registration of product templates	24
7.4.11 Registration of products	25
7.5 Managing ID services	25
7.5.1 Enrolment and update of Customer ID data via application form	25
7.5.2 Enrolment and update of Customer ID data via an external ID service	26
7.5.3 Update of Customer ID data via an online account	26
7.5.4 Re-use of incumbent Customer ID data	27
7.5.5 Management and maintenance of Customer ID data	27
7.5.6 Providing the ID service to IFMS-internal and external organizations	28
7.6 Management of customer accounts	28
7.6.1 Secure login to Customer online accounts	29
7.6.2 Connect/disconnect customer media to/from the customer online account	29

7.6.3	Transfer of products between connected customer media	30
7.6.4	Connect system generated account with a customer account.....	30
7.6.5	Termination of customer accounts	31
7.7	Management of customer media.....	31
7.7.1	Provisioning of media.....	32
7.7.2	Termination of customer media	32
7.8	Management of applications.....	33
7.8.1	Dissemination of application templates	33
7.8.2	Acquisition of applications.....	34
7.8.3	Termination of application templates	34
7.8.4	Termination of applications	35
7.9	Management of products	36
7.9.1	Dissemination of product templates	36
7.9.2	Termination of product templates.....	36
7.9.3	Management of action lists.....	37
7.9.4	Acquisition of products.....	38
7.9.5	Modification of product parameters.....	38
7.9.6	Termination of products.....	38
7.9.7	Use and inspection of products.....	39
7.9.8	Collection of data	40
7.9.9	Forwarding data	41
7.9.10	Generation and distribution of clearing reports	41
7.10	Security management	42
7.10.1	Monitoring of IFM processes and IFM data life cycle.....	42
7.10.2	Management of IFM security keys.....	43
7.10.3	Management of security lists	43
7.11	Customer Service management (optional).....	46
8	System interface identification.....	46
9	Identification.....	46
9.1	General.....	46
9.2	Numbering scheme	46
9.3	Prerequisites.....	47
10	Security in IFMSs.....	47
10.1	Protection of the interests of the public.....	47
10.2	Assets to be protected.....	48
10.3	General IFM security requirements	48
	Annex A (informative) Mobility Platform – German example.....	50
	Annex B (informative) Pay-As-You-Go (PAYG) roles and relationships in an IFMS.....	55
	Annex C (informative) Mobility ID service example.....	60
	Annex D (informative) Examples of IFMS implementations.....	69
	Annex E (informative) Media centric management and back-office centric management.....	76
	Bibliography	79

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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 document 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 and IEC 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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 204, *Intelligent transport systems*.

ISO 24014-1 was prepared by ISO/TC 204, *Intelligent transport systems*.

This third edition cancels and replaces the second edition (ISO 24014-1:2015), which has been enhanced in order to reflect recent trends in Public Transportation and needs for collaboration with systems and applications from other market sectors.

ISO 24014 consists of the following parts, under the general title *Public transport — Interoperable fare management system*:

- *Part 1: Architecture*
- *Part 2: Business practices*
- *Part 3: Complementary concepts to Part 1 for multi-application media*

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 NFC 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.

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 part of ISO 24014 which recognizes the need for legal and commercial agreements between members of an IFM, 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 IFM. Individual operators, consortia of operators, public authorities, and private companies can manage and/or participate in IFMSs. An IFM can span country boundaries and can be combined with other IFMSs. Implementations of IFMSs require security and registration functionalities. This part of ISO 24014 allows for the distribution of these functions to enable the coordination/convergence of existing IFMSs to work together.

This part of ISO 24014 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 TC204 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 system from other markets.
- d) It aims to shorten the time and lower the cost of IFM 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 its informative annex, this part of ISO 24014 provides a framework for mobility platforms that integrate fare management and travel information for inter- and multimodal travel.

Public transport — Interoperable fare management system —

Part 1: Architecture

1 Scope

This part of ISO 24014 provides the basis 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 part of ISO 24014 is applicable to bodies in public transport and related services which agree that their systems need to interoperate.

This part of ISO 24014 covers the definition of a conceptual framework which is independent of organizational and physical implementation. Any reference within this part of ISO 24014 to organizational or physical implementation is purely informative.

The objective of this part of ISO 24014 is to define a reference functional architecture for IFMSs and to identify the requirements that are relevant to ensure 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 part of ISO 24014 defines the following main elements:

- identification of the different set of functions in relation to the overall fare management system and services and media from non-transport systems which interact with fare management systems;
- a generic model of 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 set of functions;
- security requirements.

This part of ISO 24014 excludes consideration of the following:

- 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 Terms and definitions

The following terms and definitions apply.

2.1

account-based ticketing (ABT)

Architectural approach that stores products in the IFM system's back office (i.e. the customer's personal account or a temporary account) and not in the customer medium. The customer medium carries authentication credentials and an application that contains references to the account-based products in the back office.

2.2

action list

list of items related to IFM applications or *products* (2.28) downloaded to *medium access devices* (2.22) (MADs) processed by the MAD if and when a specific IFM application or product referenced in the list is encountered by that MAD

2.3

actor

person, an *organization* (2.19), or another (sub)system playing a coherent set of functions when interacting with the IFM system within a particular *use case* (2.30)

2.4

application rules

application owner requirements

2.5

application specification

specification of functions, data elements, and security scheme according to the *application rules* (2.4)

2.6

application template

executable technical pattern of the *application specification* (2.5)

2.7

application

implemented and initialised *application template* (2.6)

Note 1 to entry: The application may host one or more products 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 (identification and access control function) and partly in the IFM-back office (products).

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

Note 3 to entry: The application may house *products* (2.28) and other optional customer information (customer details, customer preferences).

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

2.8

commercial rules

rules defining the settlement and commission within the IFMS

2.9

component

any piece of hardware and/or software that performs one or more functions in the IFMS

2.10

component provider

anyone who wants to bring a *component* (2.9) to the IFMS

2.11

customer account

Data space hosted by the IFMS (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 can be established and managed by the customer as well.

2.12

customer medium

medium (2.22) initialised with an *application* (2.7) through an application contract

2.13

derived identity (derived ID)

Electronic identifier that was generated from another ID (primary ID).

Note 1 to entry: Typically, the derived ID is generated by an Identity Provider in 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.

2.14

external

The adjective “external” indicates that the named object does not follow the rules of the IFMS and that special activities are necessary to implement interoperability and security with the IFMS.

2.15

identity (ID)

Information that describes a specific person or object in a unique and unambiguous way.

Note 1 to entry: A person can, for instance, 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.

2.16

IFM functional model

model to define functions of *IFM-roles* (2.18) and how they interact

2.17

IFM policies

commercial, technical, security, and privacy objectives of IFM

2.18

IFM-role

abstract object performing a set of functions in an *IFM functional model* (2.16)

2.19

interoperable fare management

IFM

all the functions involved in the fare management process such as management of application, *products* (2.30), security and certification, registration, and identification to enable Customers to travel with participating Service Operators using a single portable electronic medium

2.20

interoperable fare management system

IFMS

all technical, commercial, security, and legal elements which enable an *interoperable fare management* (2.19)

2.21

level of assurance

Level of resilience of IFMS components and processes against a defined attack potential. Typically defined by the Security Manager for all components of the IFMS and specified in the set of rules for security certification.

2.22

medium

physical carrier of *applications* (2.7)

2.23

message

set of data elements transferred between two *IFM-roles* (2.18)

2.24

medium access device

MAD

device with the necessary facilities (hardware and software) to communicate with a *customer medium* (2.12)

2.25

organization

legal entity covering the functions and implied responsibilities of one or more of the following operational *IFM-roles* (2.18): Application Owner, Application Retailer, Product Owner, Product Retailer, Service Operator, Collection and Forwarding etc.

2.26

pricing rules

rules defining the price and payment/billing relationships to the Customer

2.27

product rules

set of usage, pricing, and *commercial rules* (2.8) defined by the Product Owner

2.28

product specification

complete specification of functions, data elements, and security scheme according to the *product rules* (2.27)

2.29

product template

technical pattern of the *product specification* (2.28)

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

2.30

product

instance of a *product template* (2.29) stored in an *application* (2.7)

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.

2.31

role

abstract object performing a set of functions

2.32

security policy

objectives of the IFM to secure the public interests and the assets within the IFM

2.33

set of rules

regulations for achieving *IFM policies* (2.17) expressed as technical, commercial, security, and legal requirements and standards relevant only to the IFMS

2.34

trigger

event that causes the execution of a *use case* (2.36)

2.35

usage rules

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

2.36

use case

description of a process by defining a sequence of actions performed by one or more *actors* (2.3) and by the system itself

3 Abbreviated terms

ID	Identity
IFM	Interoperable Fare Management
IFMS	Interoperable Fare Management system
MAD	Medium Access Device
LoA	Level of Assurance
PP	Protection Profile
PT	Public Transport
SSS	Security Sub System
TOE	Target Of Evaluation

4 Requirements

The purpose of ISO 24014 is to achieve interoperability throughout fare management systems while making sure that participating companies in public transport 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 (the 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 public transport system and may reduce payment handling costs significantly.
- The IFMS model shall comply with data protection and financial services laws/regulations (e.g. privacy).
- 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 public transport 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 and migration to new technologies and architecture concepts and interoperability with media, applications and systems from other market sectors.

5 System environment for IFMS

ISO 24014-1 focused so far 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.

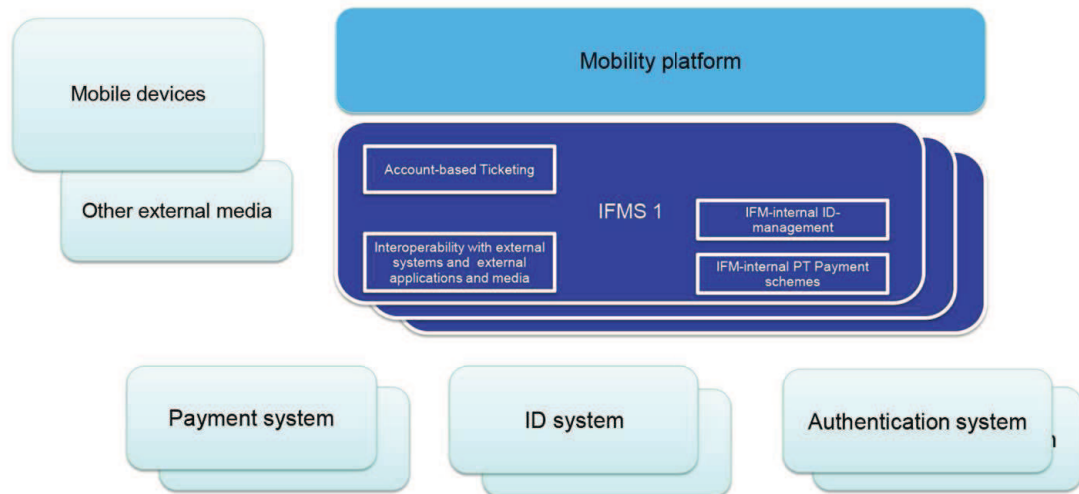


Figure 1 — System environment for IFMS

5.1 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 context of travel information systems and their interdependencies, extensions are needed on the travel information side.

In order to integrate IFM systems 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 edition of ISO 24014-1 documents a possible approach to mobility platforms in the informative part of the specification.

6 Conceptual framework for IFMS

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 part of ISO 24014, the IFM Manager shall appoint

- a Security Manager, and
- a Registrar.

The functions and the responsibilities of the security manager and the registrar can be distributed to several organizations within an IFM.

A 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 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.

6.1 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 for the use of the application with the Customer.

Application Retailer The Application Retailer sells and terminates applications, collects, and refunds value to a Customer as authorized by an Application Owner.

The Application Retailer is the only financial interface between the Customer and the IFMS related to applications.

Collection
and
Forwarding
(set of func-
tions)

The IFM-role of Collection and Forwarding is the facilitation of data interchanges of the IFMS. The general functions are data collection and forwarding. They contain at least the following functions:

Functions of collecting

- Receiving application template from Application Owner.
- Receiving product template from Product Owner.
- Receiving data from Service Operators.
- Receiving data from Product Retailer.
- Receiving data from Application Retailer.
- Receiving data from Media Retailer.
- Receiving data from other collection and forwarding functions.
- Receiving security list data from Security Manager.
- Receiving clearing reports from Product Owner.
- Consistency and completeness check of the data collected on a technical level.
- Receiving the address list of all IFM-roles in the IFM from the Registrar.

Functions of forwarding

- Forwarding “Not On Us” data to other collection and forwarding functions.
- Recording “Not On Us” data.
- Forwarding data with a corrupt destination address to the Security Manager.
- Forwarding “On Us” data to the Product Owner for clearing and reporting.
- Forwarding clearing reports, application template, product template, and security list data to the Product Retailer and Service Operator.
- Forwarding application templates and security list data to the Application Retailer and Service Operator.

Note 1 to entry:

The concept of this connectivity functionality is as follows.

- A specific Collection and Forwarding function is to collect data from one IFM-role and forward it to other IFM-roles.
- Logically, there may be several Collection and Forwarding functions within the IFM.
- IFM-roles may be linked to different Collection and Forwarding functions, but each IFM-role can only be linked to one.

The concept of “ON US and NOT ON US” addresses this connectivity functionality:

- Data collected by a specific Collection and Forwarding function addressed to IFM-roles directly linked to this Collection and Forwarding function is termed “ON US” data.
- Data collected by a specific Collection and Forwarding function addressed to IFM-roles not linked to this Collection and Forwarding function is termed “NOT ON US” data.
- Data held by a specific Collection and Forwarding function is either “ON US” or “NOT ON US” data.

Customer	<p>The Customer holds a customer medium with an application and acquires products in order to use the public transport services. In many cases, the Customer is also a Passenger. The Customer may also hold a personal account and external media or applications which may be used for purposes of the IFMS.</p> <p>The Customer may acquire customer media, applications and products for himself 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 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 the 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.</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	<p>A Payment Provider is the party that provides the function to pay for travel products with electronic transaction.</p> <p>This can for example be a bank account accessed by direct debit or credit transfer, a payment card account accessed through an acquirer, a transport purse held by a Product Owner, or a mobile network operator.</p> <p>One or more Payment Provider may be proposed to the Customer by the Product Retailer and the Customer will choose the one best suited for her/his purposes.</p> <p>This does not apply for virtual accounts which are activated by contactless payment service. In such case, the payment will be conducted via the Payment Provider who is referenced by the contactless payment service.</p> <p>The Account Provider makes payment requests to the Payment Provider on the basis of the travel consumed by the Passenger.</p>
Product Owner	<p>The Product Owner is responsible for his products.</p> <p>Functions of ownership:</p> <ul style="list-style-type: none">— Specifying pricing, usage rules, and commercial rules. <p>Functions of clearing:</p> <ul style="list-style-type: none">— 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. <p>Functions of reporting:</p> <ul style="list-style-type: none">— Detailed:<ul style="list-style-type: none">— 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:<ul style="list-style-type: none">— apportionment data and clearing report.— Total acquisition data.
Product Retailer	<p>The Product Retailer sells and terminates products, collects, and refunds value to a Customer as authorized by a Product Owner.</p> <p>The Product Retailer is the only financial interface between the Customer and the IFMS related to products.</p> <p>Based on his Customer relationship, the role of the Product Retailer may include the role of the Account Provider.</p>

Registrar	After the certification, the Registrar issues unique registration codes for organizations, components, application templates, and product templates. The Registrar function also issues unique identifiers or rules for generating unique identifiers for the applications, products, and messages.
Security Manager	<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.

6.2 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 this edition of ISO 24014-1 are indicated in yellow.

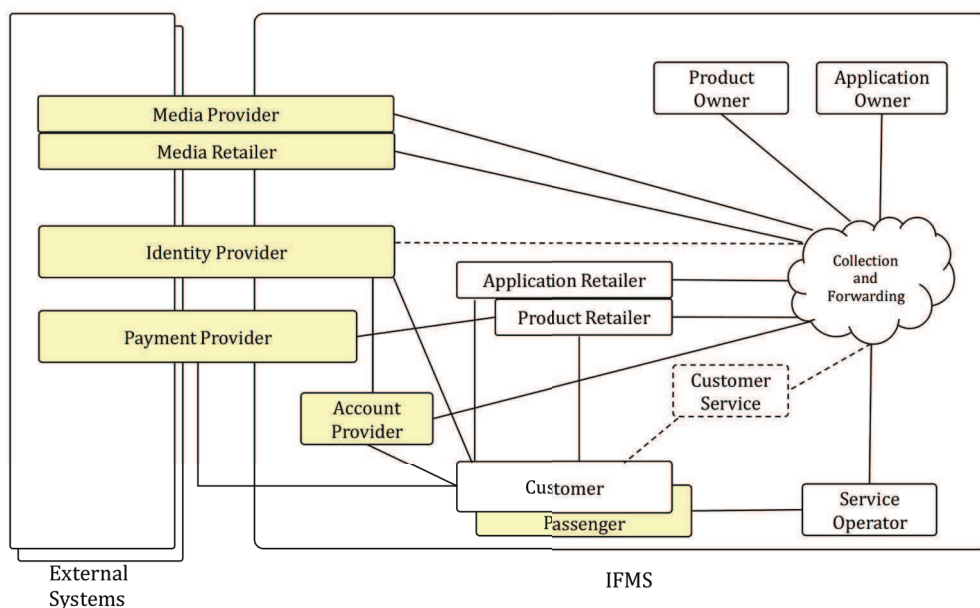


Figure 2 — Links between operational roles

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.

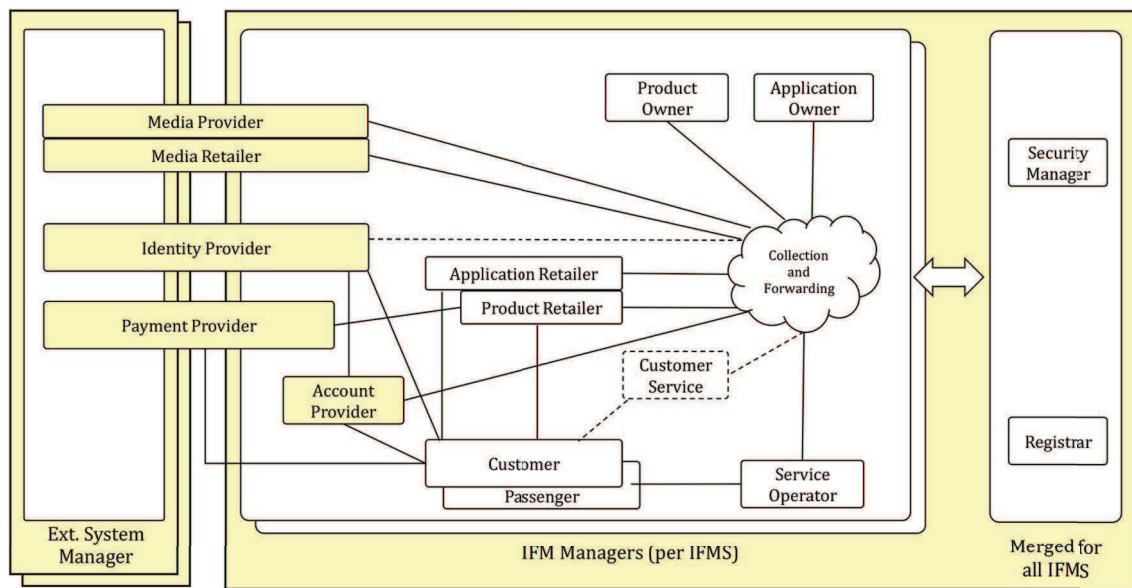


Figure 3 — Interaction of IFM domains and with external systems (operational and management roles)

Figure 3 shows also 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 versions of this standard, there are new roles which are indicated in yellow. The IFM manager will have relationships with Media Retailers. The Customer will have a relationship with the issuer of the customer medium they hold. Also, the Application Owner will have relationships with Media Providers.

The interactions between IFM-roles are described in detail in Clause 7.

7 Use case description for the IFM functional model

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 done between a Medium and MAD.

Back-office centric management / account-based ticketing:

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

The following use cases describe functional aspects of the IFMS. Contractual matters are outside the scope of this part of ISO 24014, but a prerequisite to implementation.

7.1 Define set of rules

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

Within the IFM, Sets of Rules are required for

- Organizations
- Components with specific demand for security or interoperability
- Customer accounts
- Media
- ID service
- Payment service
- Application specification and template, and
- Product specification and template.

The IFM Manager or his representatives defines the sets of rules.

7.1.1 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 – enforces an assurance level as requested by the IFMS for the targeted applications and products.

7.1.2 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 – enforces an assurance level as requested by the IFMS for the targeted applications and products.

7.1.3 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

Use case name	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 <ul style="list-style-type: none">– enforces interoperability with the components and applications of the IFMS– enforces an assurance level as requested by the IFMS for the targeted applications and products.

7.1.4 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 <ul style="list-style-type: none">– enforces interoperability with the components and applications of the IFMS– enforces an assurance level as requested by the IFMS for the targeted applications and products.

7.2 Certification

Each object to be brought into the IFM should meet the IFM requirements. The proof of compliance 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 demand for security or interoperability
- Media
- eID service
- Payment service
- Application specification and template, and
- Product specification and template.

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

7.2.1 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 name	Certification of organizations
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.

7.2.2 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 compliant with the set of rules, — the component will be certified, — else the component will not be certified.

7.2.3 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 compliant with the set of rules, — the medium will be certified, — else the medium will not be certified.

7.2.4 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 description	The IFM Manager checks the ID service against the set of rules. If the eID service is compliant with the set of rules, — the ID service will be certified, — else the ID service will not be certified.

7.2.5 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.