BS EN ISO 24014-1:2015

BSI Standards Publication

Public transport — Interoperable fare management system

Part 1: Architecture

National foreword

This British Standard is the UK implementation of EN ISO 24014-1:2015. Together with PD CEN ISO/TR 24014-2:2013 and PD CEN ISO/TR 24014-3:2013 it supersedes BS EN ISO 24014-1:2007 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Intelligent transport systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 85451 4

ICS 03.220.01; 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2015.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 24014-1

November 2015

ICS 03.220.01; 35.240.60

Supersedes EN ISO 24014-1:2007

English Version

Public transport - Interoperable fare management system - Part 1: Architecture (ISO 24014-1:2015)

Transport public - Système de gestion tarifaire interopérable - Partie 1: Architecture (ISO 24014-1:2015)

Öffentlicher Verkehr - Interoperables Fahrgeldmanagement System - Teil 1: Architektur (ISO 24014-1:2015)

This European Standard was approved by CEN on 10 July 2015.

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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, 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: Avenue Marnix 17, B-1000 Brussels

Foreword

This document (EN ISO 24014-1:2015) 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 May 2016, and conflicting national standards shall be withdrawn at the latest by May 2016.

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

This document supersedes EN ISO 24014-1:2007.

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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 24014-1:2015 has been approved by CEN as EN ISO 24014-1:2015 without any modification.

Contents

Page

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 European Committee for Standardization (CEN) Technical Committee CEN/TC 278 *Road transport and traffic telematics*, in collaboration with ISO/TC 204, *Intelligent transport systems*, in accordance with the agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO 24014-1:2007), which has been technically revised.

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) 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.

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 three main benefits.

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

b) 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.

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

The work has benefited from the architecture work done in Electronic Fee Collection (CEN/TC 278/WG 1) and other domains including the following:

— ISO/TS 14904, *Road transport and traffic telematics — Electronic fee collection (EFC) — Interface specification for clearing between operators*;

— ISO/TS 17573, *Electronic fee collection — Systems architecture for vehicle-related tolling*;

— existing international data security standards.

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.

While this part of ISO 24014 does not imply that existing interoperable fare management systems need to be changed, it applies so far as it is practically possible to extensions of these.

This part of ISO 24014 covers the definition of a conceptual framework which is independent of organisational and physical implementation. Any reference within this part of ISO 24014 to organisational 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 application,
- 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;
- a generic model of IFMS describing the logical and functional architecture and the interfaces within the system and with other IFMSs;
- 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 physical medium and its management;
- 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

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

2.1
action list
list of items related to IFM applications or *products* (2.24) downloaded to *medium access devices* (2.18) (MADs) processed by the MAD if and when a specific IFM application or product referenced in the list is encountered by that MAD

2.2
actor
person, an *organisation* (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)

2.3
application rules
application owner requirements

2.4
application specification
specification of functions, data elements, and security scheme according to the *application rules* (2.3)

2.5
application template
executable technical pattern of the *application specification* (2.4)

2.6
application
implemented and initialised *application template* (2.5)

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

Note 2 to entry: The application houses *products* (2.24) and other optional customer information (customer details, customer preferences).

Note 3 to entry: The application can be fully installed on a customer media or distributed on the customer media and the IFM back offices.

2.7
commercial rules
rules defining the settlement and commission within the IFMS

2.8
component
any piece of hardware and/or software that performs one or more functions in the IFMS

2.9
component provider
anyone who wants to bring a *component* (2.8) to the IFMS

2.10
IFM functional model
model to define functions of *IFM-roles* (2.12) and how they interact

2.11
IFM policies
commercial, technical, security, and privacy objectives of IFM

2.12
IFM-role
abstract object performing a set of functions in an *IFM functional model* (2.10)

2.13
interoperable fare management
IFM
all the functions involved in the fare management process such as management of application, *products* (2.24), security and certification, registration, and identification to enable customers to travel with participating service operators using a single portable electronic medium

2.14
interoperable fare management system
IFMS
all technical, commercial, security, and legal elements which enable an *interoperable fare management* (2.13)

2.15
medium
physical carrier of *applications* (2.6)

2.16
message
set of data elements transferred between two *IFM-roles* (2.12)

2.17
customer medium
medium (2.15) initialised with an *application* (2.6) through an application contract

2.18
medium access device
MAD
device with the necessary facilities (hardware and software) to communicate with a *customer medium* (2.17)

2.19
organisation
legal entity covering the functions and implied responsibilities of one or more of the following operational *IFM-roles* (2.12): application owner, application retailer, product owner, product retailer, service operator, and collection and forwarding

2.20
pricing rules
rules defining the price and payment/billing relationships to the customer

2.21
product rules
set of usage, pricing, and *commercial rules* (2.7) defined by the product owner

2.22
product specification
complete specification of functions, data elements, and security scheme according to the *product rules* (2.21)

2.23
product template
technical pattern of the *product specification* (2.22)

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

2.24
product
instance of a *product template* (2.23) stored in an *application* (2.6)

Note 1 to entry: It is identified by a unique identifier and enables the customer to benefit from a service provided by a service operator.

2.25
role
abstract object performing a set of functions

2.26
security policy
objectives of the IFM to secure the public interests and the assets within the IFM

2.27
set of rules
regulations for achieving *IFM policies* (2.11) expressed as technical, commercial, security, and legal requirements and standards relevant only to the IFMS

2.28
trigger
event that causes the execution of a *use case* (2.30)

2.29
usage rules
rules defining the usage time, the usage area, the personal status, and the type of service

2.30
use case
description of a process by defining a sequence of actions performed by one or more *actors* (2.2) and by the system itself

3 Abbreviated terms

IFM	Interoperable Fare Management
IFMS	Interoperable Fare Management system
MAD	Medium Access Device
PP	Protection Profile
PT	Public Transport
SSS	Security SubSystem
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.

Specific requirements of the IFMS model are as follows.

— A customer shall be able to travel with all participating 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 transport operators.
- The same medium may carry additional applications. Conversely, other media may carry the IFM application.
- The ticketing 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 identify the customer while protecting their privacy as appropriate.
- The IFMS model shall protect the privacy of the customer.
- 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 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), independent of access technologies].
- The IFMS model shall be functionally neutral regarding specific transport organization structures.

5 Conceptual framework

The IFMS may be run 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 organisations within an IFM. This may be a necessary condition to allow the cooperation of existing IFMSs. An example is shown in B.3. The example also shows how a new common set of rules for the joint IFMS is built upon the existing sets of the cooperating IFMSs.

5.1 Description of IFM-roles

IFM-roles are identified by capitalized initial letters.

Product Owner

The Product Owner is responsible for his Products.

Functions of ownership:

— Specifying pricing, Usage Rules, and Commercial Rules.

Functions of clearing:

— Trip reconstruction

— Product aggregation based on received usage data using Product definition rules;

— 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.

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

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 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 The "ON US and NOT ON US" concept 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 held by a specific COLLECTION AND FORWARDING function is either "ON US" or "NOT ON US" data.

— 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.

Service Operator The Service Operator provides a service to the customer against the use of a Product.

Application Owner The Application Owner holds the Application contract for the use of the Application with the customer.

Customer Service
Subject to commercial agreements, Customer Service may provide "helpline" and any similar facilities including replacement of stolen and damaged Customer Medium and consequent Product reinstalling.

Customer
The Customer holds an Application and acquires Products in order to use the public transport services.

Security Manager
The Security Manager is responsible for establishing and coordinating the Security Policy and for

— certification of Organisations, Application Templates, Components, and Product Templates,

— auditing of Organisations, Application Templates/Applications, Components, and Product Templates/Products,

— monitoring the system, and

— operation of the security of the IFMS, e.g. key management.

Registrar
After the certification, the Registrar issues unique registration codes for Organisations, 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.

5.2 Basic framework of the generic IFM functional model

The links between the operational IFM-roles of the IFMS are illustrated in Figure 1. These links represent information flows. Optional links and IFM-roles are drawn in dotted lines. It is assumed that the customer already has a medium or is provided with one by the application retailer, therefore, the model considers only application and product issues. Within an IFMS, there may be several organisations performing the functions of the IFM-roles.

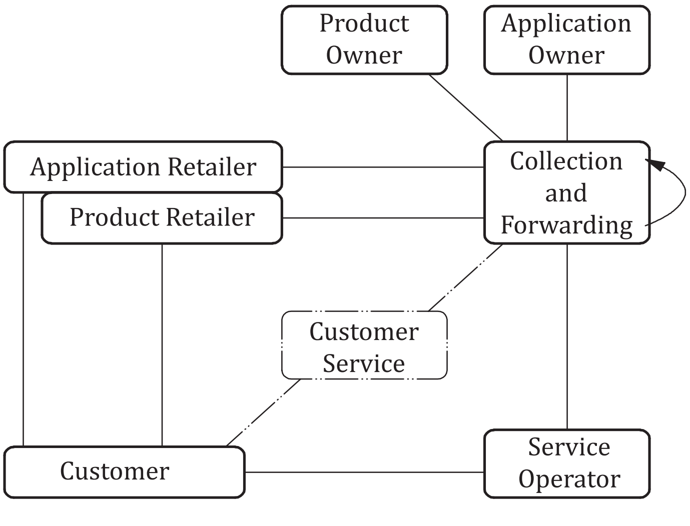


Figure 1 — Links between operational IFM-roles within the IFMS

An IFM manager establishes and manages the IFM policies on behalf of the IFM. These policies are embedded in the set of rules. The IFM manager will have relationships with media issuers. The customer will have a relationship with the issuer of the customer medium they hold. Also, the application owner will have relationships with media issuers.

To manage the elements, the IFM functional model includes two management IFM-roles:

— the registrar — the IFM-role for the identification of any organization, component, application template and application, product template, and product involved in the IFMS;

— the security manager — the supporting IFM-role responsible for the secure operation of the IFMS.

Figure 2 shows the two domains of IFM-roles of the IFM and the connection between them.

The interactions between IFM-roles are described in detail in Clause 6.

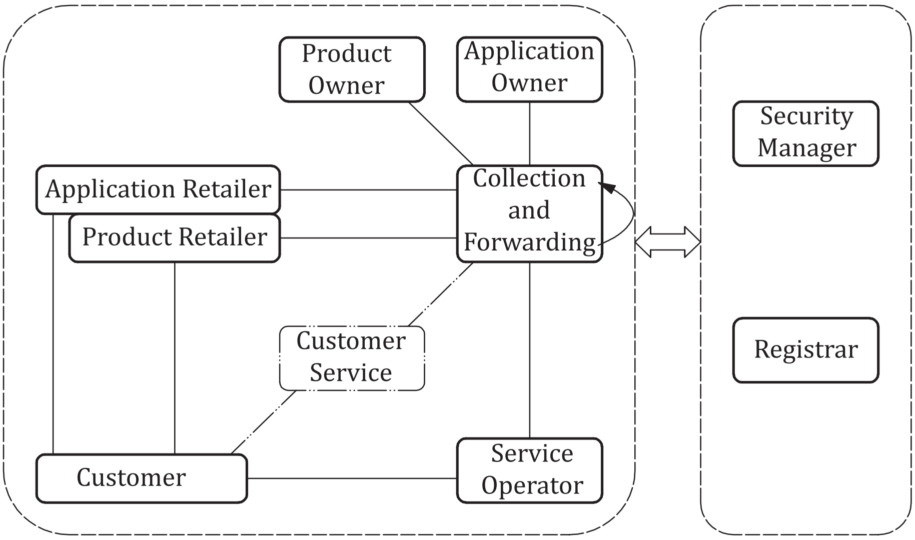


Figure 2 — Two IFM domains (operational and management IFM-roles)

6 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/A Application/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 Application and Product are done between a Medium and MAD.

Back-office centric management:

Main processes of management of Application and/or Product are done in the back-office.

The following Use Cases describe functional aspects of the IFM. Contractual matters are outside the scope of this part of ISO 24014, but a prerequisite to implementation.

All Actors in the Use Cases are written in UPPER CASE characters.

6.1 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

- Organisations,
- security-related Components,
- Application Specification and Template, and
- Product Specification and Template.

The Security Manager is responsible for the certification.

6.1.1 Certification of Organization

Use Case name	Certification of Organization
Outline	Each Organization which wants to participate in the IFM shall agree to abide by the Set of Rules.
Triggered by	ORGANIZATION
Actor(s)	SECURITY MANAGER ORGANIZATION
Use Case description	If the SECURITY 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.

6.1.2 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)	SECURITY MANAGER COMPONENT PROVIDER
Use Case description	The SECURITY 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.

6.1.3 Certification of Application Specification and Template

Use Case name	Certification of Application Specification and Template
Outline	Each Application Specification and Template to be brought into the IFMS shall meet the IFM requirements. Proof of this is given by checking this Application Specification and Template against a Set of Rules.
Triggered by	APPLICATION OWNER
Actor(s)	SECURITY MANAGER APPLICATION OWNER

Use Case name	**Certification of Application Specification and Template**
Use Case description	The SECURITY MANAGER checks the Application Specification and Template against the Set of Rules. If the Application Specification and Template is compliant with the Set of Rules, — the Application Specification and Template will be certified, — else the Application Specification and Template will not be certified.

6.1.4 Certification of Product Specification and Template

Use Case name	**Certification of Product Specification and Template**
Outline	Each Product Specification and Template to be brought into the IFM shall meet the IFM requirements. Proof of this is given by checking this Product Specification and Template against a Set of Rules.
Triggered by	PRODUCT OWNER
Actor(s)	SECURITY MANAGER PRODUCT OWNER
Use Case description	The SECURITY MANAGER checks the Product Specification and Template against the Set of Rules. If the Product Specification and Template is compliant with the Set of Rules, — the Product Specification and Template will be certified, — else the Product Specification and Template will not be certified.

6.2 Registration

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

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

- Organisations,
- Components,
- Application Template and Application, and
- Product Template and Product.

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

6.2.1 Registration of Organization

Use Case name	**Registration of Organization**
Outline	A unique identification is given to each Organization.
Triggered by	ORGANIZATION
Actor(s)	REGISTRAR ORGANIZATION
Use Case description	The ORGANIZATION sends the Organization certification to the REGISTRAR. The REGISTRAR returns a unique Organization identifier to the ORGANIZATION.

6.2.2 Registration of Component

Use Case name	**Registration of Component**
Outline	A unique identification is given to each Component.
Triggered by	COMPONENT PROVIDER
Actor(s)	REGISTRAR COMPONENT PROVIDER
Use Case description	The Component certification is sent to the REGISTRAR. The REGISTRAR returns a unique Component identifier to the Organization which asked for registration.

6.2.3 Registration of Application Template

Use Case name	**Registration of Application Template**
Outline	A unique identification is given to each Application Template.
Triggered by	APPLICATION OWNER
Actor(s)	REGISTRAR APPLICATION OWNER
Use Case description	The APPLICATION OWNER sends the Application Template certification to the REGISTRAR. The REGISTRAR returns a unique Application Template identifier to the APPLICATION OWNER.

6.2.4 Registration of Application

Use Case name	**Registration of Application**
Outline	A unique identification is given to each Application.
Triggered by	APPLICATION RETAILER
Actor(s)	REGISTRAR APPLICATION RETAILER
Use Case description	a) The APPLICATION OWNER sends the Application Template identification to the REGISTRAR and asks for an Application identification. The REGISTRAR sends a unique Application identifier to the APPLICATION OWNER. This can be done for a single identifier as well as for a batch of identifiers. b) The APPLICATION RETAILER sends the Application Template identification to the APPLICATION OWNER throughthrough the COLLECTION AND FORWARDING and asks for an Application identification. The APPLICATION OWNER sends the unique Application identifier throughthrough the COLLECTION AND FORWARDING to the APPLICATION RETAILER. The processes described in a) and b) could happen at any time in any order.

6.2.5 Registration of Product Template

Use Case name	**Registration of Product Template**
Outline	A unique identification is given to each Product Template.
Triggered by	PRODUCT OWNER
Actor(s)	REGISTRAR PRODUCT OWNER

Use Case name	**Registration of Product Template**
Use Case description	The PRODUCT OWNER sends the Product Specification certification to the REGISTRAR. The REGISTRAR returns a unique Product Template identifier to the PRODUCT OWNER.

6.2.6 Registration of Product

Use Case name	**Registration of Product**
Outline	A unique identification is given to each Product.
Triggered by	PRODUCT RETAILER
Actor(s)	REGISTRAR PRODUCT RETAILER
Use Case description	a) The PRODUCT OWNER sends the Product Template identification to the REGISTRAR and asks for a Product identification. The REGISTRAR sends a unique Product identifier to the PRODUCT OWNER. This can be done for a single identifier as well as for a batch of identifiers. b) The PRODUCT RETAILER sends the Product Template identification to the PRODUCT OWNER throughthrough the COLLECTION AND FORWARDING and asks for a Product identification. The PRODUCT OWNER sends the unique Product identifier throughthrough the COLLECTION AND FORWARDING to the PRODUCT RETAILER. The processes described in a) and b) could happen at any time in any order.

6.3 Management of Application

The Management of Application comprises

- dissemination of Application Templates,
- acquisition of Applications,
- termination of Application Templates, and
- termination of Applications.

Only certified and registered Application Templates shall be disseminated.

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

6.3.1 Dissemination of Application Template

Use Case name	**Dissemination of an Application Template**
Outline	Dissemination of an Application Template enables the authorized Retailer to sell an Application and an authorized Service Operator to access this Application.
Triggered by	APPLICATION OWNER
Actor(s)	APPLICATION RETAILER COLLECTION AND FORWARDING SERVICE OPERATOR APPLICATION OWNER

Use Case name	**Dissemination of an Application Template**
Use Case description	Dissemination of Application Template comprises — distribution of registered Application Template by APPLICATION OWNER to the APPLICATION RETAILER throughthrough the COLLECTION AND FORWARDING, and — distribution of registered Application Template by APPLICATION OWNER to the SERVICE OPERATOR through the COLLECTION AND FORWARDING.

6.3.2 Acquisition of Application

Use Case name	**Acquisition of Application**
Outline	An Application is loaded on the Customer Medium.
Triggered by	CUSTOMER
Actor(s)	APPLICATION RETAILER APPLICATION OWNER COLLECTION AND FORWARDING CUSTOMER
Use Case description	The authorized APPLICATION RETAILER installs an instance of a registered Application Template on a Medium. The APPLICATION RETAILER performs — installation of the instance of the registered Application Template, and — distribution of the Application identifier and the Application acquisition data to the APPLICATION OWNER throughthrough the COLLECTION AND FORWARDING.

6.3.3 Termination of Application Template

The Use Case "Termination of Application Template" comprises the following:

- regular termination of Application Template;
- forced termination of Application Template.

6.3.3.1 Regular termination of Application Template

Use Case name	**Regular termination of Application Template**
Outline	An Application Template is terminated in the IFM by request of the Application Owner.
Triggered by	APPLICATION OWNER
Actor(s)	APPLICATION RETAILER COLLECTION AND FORWARDING SERVICE OPERATOR PRODUCT RETAILER SECURITY MANAGER REGISTRAR APPLICATION OWNER

Use Case name	**Regular termination of Application Template**

Use Case description	The APPLICATION OWNER wants to terminate the Application Template. This comprises
	— distribution of Termination of registered Application Template to the APPLICATION RETAILER through the COLLECTION AND FORWARDING;
	— distribution of Termination of registered Application Template to the SERVICE OPERATOR through the COLLECTION AND FORWARDING;
	— distribution of Termination of registered Application Template to the PRODUCT RETAILER through the COLLECTION AND FORWARDING;
	— distribution of Termination of registered Application Template to the SECURITY MANAGER;
	— distribution of Termination of registered Application Template to the REGISTRAR;
	— (optional) distribution of Termination of registered Application Template to the CUSTOMER SERVICE through the COLLECTION AND FORWARDING;
	— (optional) the MAD reports the Application Template identifier and Application Template termination data to the APPLICATION OWNER and SECURITY MANAGER through the COLLECTION AND FORWARDING.

6.3.3.2 Forced termination of Application Template

Use Case name	**Forced termination of Application Template**
Outline	Termination of Application Template by request of the IFM Manager.
Triggered by	IFM MANAGER
Actor(s)	SECURITY MANAGER
Use Case description	The IFM MANAGER sends the request for termination of an Application Template to the SECURITY MANAGER.

6.3.4 Termination of Application

The Use Case “Termination of Application” comprises the following:

- regular termination of Application;
- forced termination of Application.

6.3.4.1 Regular termination of Application

Use Case name	**Regular termination of Application**
Outline	An Application is terminated on the Customer Medium.
Triggered by	CUSTOMER
Actor(s)	APPLICATION RETAILER APPLICATION OWNER COLLECTION AND FORWARDING REGISTRAR CUSTOMER

Use Case name	**Regular termination of Application**
Use Case description	The CUSTOMER wants to terminate the APPLICATION. The APPLICATION RETAILER — de-installs the Application on the Customer Medium; — sends the de-installed Application identifier to the APPLICATION OWNER through the COLLECTION AND FORWARDING. The APPLICATION OWNER sends Application identifier to the REGISTRAR.

6.3.4.2 Forced termination of Application

Use Case name	**Forced termination of Application**
Outline	Application is put on a security list by request of the APPLICATION OWNER.
Triggered by	APPLICATION OWNER
Actor(s)	APPLICATION OWNER COLLECTION AND FORWARDING SECURITY MANAGER
Use Case description	The APPLICATION OWNER wants to terminate an Application and sends the Application identifier to the SECURITY MANAGER through the COLLECTION AND FORWARDING.

6.4 Management of Product

The management of Product comprises the following:

- dissemination of Product Template;
- termination of Product Template;
- management of Action List;
- acquisition of Product;
- modification of Product parameter;
- termination of Product;
- use and inspection of Product;
- collection of data;
- forwarding data;
- generation and distribution of clearing reports.

6.4.1 Dissemination of Product Template

Use Case name	**Dissemination of Product Template**
Outline	Dissemination of registered Product Template enabling authorized Actors to handle the Product.
Triggered by	PRODUCT OWNER
Actor(s)	COLLECTION AND FORWARDING PRODUCT RETAILER SERVICE OPERATOR PRODUCT OWNER

Use Case name	Dissemination of Product Template

Use Case description	Dissemination of Product Template comprises the following:
	— distribution of Product Template by PRODUCT OWNER to COLLECTION AND FORWARDING;
	— distribution of Product Template by COLLECTION AND FORWARDING to authorized PRODUCT RETAILER;
	— distribution of Product Template by COLLECTION AND FORWARDING to authorized SERVICE OPERATOR.

6.4.2 Termination of Product Template

The Use Case “Termination of Product Template” comprises the following:

— regular termination of Product Template,

— forced termination of Product Template.

6.4.2.1 Regular termination of Product Template

Use Case name	Regular termination of Product Template
Outline	Termination of Product Template on decision of the PRODUCT OWNER.
Triggered by	PRODUCT OWNER
Actor(s)	COLLECTION AND FORWARDING PRODUCT RETAILER SERVICE OPERATOR PRODUCT OWNER
Use Case description	Termination of Product Template comprises the following: — distribution of request for termination of a Product Template by PRODUCT OWNER to COLLECTION AND FORWARDING; — distribution of request for termination of Product Template by COLLECTION AND FORWARDING to authorized PRODUCT RETAILER; — distribution of request for termination of Product Template by COLLECTION AND FORWARDING to authorized SERVICE OPERATOR; — sending of the request for termination of Product Template by the PRODUCT OWNER to the SECURITY MANAGER; — (optional) sending of the identifier of the terminated Product Template by the PRODUCT OWNER to the REGISTRAR.

6.4.2.2 Forced termination of Product Template

Use Case name	Forced termination of Product Template
Outline	Termination of Product Template on decision of the IFM Manager.
Triggered by	IFM MANAGER
Actor(s)	SECURITY MANAGER
Use Case description	The IFM MANAGER sends the request for termination of a Product Template to the SECURITY MANAGER.

6.4.3 Management of Action List

Use Case name	Management of Action List
Outline	Management of an Action List enables actions related to Products or Applications.

Use Case name	**Management of Action List**
Triggered by	APPLICATION RETAILER or PRODUCT RETAILER or CUSTOMER
Actor(s)	APPLICATION RETAILER PRODUCT RETAILER COLLECTION AND FORWARDING CUSTOMER
Use Case description	Management of Action List consists of — adding an item to the Action List, which will result in the one-time addition of a Product/Application to the Customer Medium; — adding an item to the Action List, which will result in the one-time removal of a Product/Application from the Customer Medium; — removing an item from the Action List; — aggregation of Action List data; — distribution of Action List to any MAD, which is able to update Products/Applications into the Customer Medium through the COLLECTION AND FORWARDING. After a Customer Medium is updated, the MAD sends information back to the Action List.

6.4.4 Acquisition of Product

Use Case name	**Acquisition of Product**
Outline	Acquisition of PRODUCT enabling CUSTOMER to benefit from a transport service.
Triggered by	CUSTOMER
Actor(s)	PRODUCT RETAILER COLLECTION AND FORWARDING PRODUCT OWNER CUSTOMER
Use Case description	The authorized PRODUCT RETAILER installs an instance of a registered Product Template on a registered Application. The Product Retailer performs the following: — detection and verification of registered Application; — verification of Application according to Security Policies; — installation of the instance of the registered Product Template; — distribution of Product identifier and Product acquisition data to the PRODUCT OWNER through the COLLECTION AND FORWARDING.

6.4.5 Modification of Product parameter

Use Case name	**Modification of Product parameter**
Outline	Modifying changeable Product parameters for an existing Product.
Triggered by	CUSTOMER
Actor(s)	PRODUCT RETAILER COLLECTION AND FORWARDING PRODUCT OWNER CUSTOMER
Use Case description	The authorized PRODUCT RETAILER modifies changeable Product parameters of an existing Product. The Product Retailer distributes the Product identifier and Product modification data to the PRODUCT OWNER through the COLLECTION AND FORWARDING.

6.4.6 Termination of Product

A Product which can be extended or recharged is covered by 6.4.5. Once a Product has been terminated, it shall not be extended or recharged.

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

The Use Case “Termination of Product” comprises

— regular termination of Product, and

— forced termination of Product.

6.4.6.1 Regular termination of Product

Use Case name	**Regular termination of Product**
Outline	Termination of Product by request of the CUSTOMER.
Triggered by	CUSTOMER
Actor(s)	CUSTOMER PRODUCT RETAILER COLLECTION AND FORWARDING PRODUCT OWNER
Use Case description	The authorized PRODUCT RETAILER de-installs/terminates a Product. The Product Retailer distributes the Product identifier and Product termination data to the PRODUCT OWNER through the COLLECTION AND FORWARDING.

6.4.6.2 Forced termination of Product

Use Case name	Forced termination of Product
Outline	Product is put on a security list by request of the PRODUCT OWNER.
Triggered by	PRODUCT OWNER
Actor(s)	PRODUCT OWNER SECURITY MANAGER COLLECTION AND FORWARDING
Use Case description	The PRODUCT OWNER wants to terminate a Product and sends the Product identifier to the SECURITY MANAGER through the COLLECTION AND FORWARDING.

6.4.7 Use and inspection of Product

Use Case name	**Use and inspection of Product**
Outline	SERVICE OPERATOR checks and collects the data of a Customer Medium using the public transport service.
Triggered by	SERVICE OPERATOR
Actor(s)	CUSTOMER SERVICE OPERATOR COLLECTION AND FORWARDING PRODUCT OWNER

Use Case name	**Use and inspection of Product**
Use Case description	A CUSTOMER who uses a PRODUCT on public transport. The Use Case consists of several processes performed by the SERVICE OPERATOR: — detection and verification of Application; — detection, selection and verification of Product; — verification of Application and Product according to Security Policies; — processing of Product data; — communication between Customer Medium and MAD; — computation of Product rules; — collection of the Product usage and inspection data; — distribution of Product usage and inspection data to the PRODUCT OWNER through the COLLECTION AND FORWARDING. Inspection consists of — simple detection, — detection and verification, or — detection, verification and further processing.

6.4.8 Collection of data

Use Case name	**Collection of data**
Outline	The COLLECTION AND FORWARDING receives data and checks the completeness and integrity of the data.
Triggered by	APPLICATION OWNER PRODUCT OWNER APPLICATION RETAILER PRODUCT RETAILER SERVICE OPERATOR other COLLECTION AND FORWARDING SECURITY MANAGER REGISTRAR
Actor(s)	COLLECTION AND FORWARDING APPLICATION OWNER PRODUCT OWNER APPLICATION RETAILER PRODUCT RETAILER SERVICE OPERATOR other COLLECTION AND FORWARDING SECURITY MANAGER REGISTRAR

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

6.4.9 Forwarding data

Use Case name	**Forwarding data**
Outline	The COLLECTION AND FORWARDING forwards data.
Triggered by	COLLECTION AND FORWARDING
Actor(s)	APPLICATION OWNER PRODUCT OWNER APPLICATION RETAILER PRODUCT RETAILER SERVICE OPERATOR COLLECTION AND FORWARDING other COLLECTION AND FORWARDING SECURITY MANAGER
Use Case description	The forwarding of data consists of the following: — forwarding “NOT ON US” data to other COLLECTION AND FORWARDING; — forwarding “ON US” data to the APPLICATION OWNER; — forwarding “ON US” data to the PRODUCT OWNER for clearing and reporting; — forwarding clearing reports, Application Template, Product Template and security list data to the PRODUCT RETAILER and SERVICE OPERATOR; — forwarding Application Templates and security list data to the APPLICATION RETAILER and SERVICE OPERATOR; — forwarding forced termination requests to the SECURITY MANAGER.

6.4.10 Generation and distribution of clearing reports

Use Case name	**Generation and distribution of clearing reports**
Outline	The PRODUCT OWNER performs the clearing procedure and distributes the results to relevant IFM-roles.
Triggered by	PRODUCT OWNER
Actor(s)	PRODUCT RETAILER SERVICE OPERATOR COLLECTION AND FORWARDING PRODUCT OWNER

Use Case name	**Generation and distribution of clearing reports**
Use Case description	The generation and distribution of clearing reports consist of the following: — clearing of the Product data (acquisition and usage data) and generating reports for the PRODUCT RETAILER and SERVICE OPERATOR by the PRODUCT OWNER; — distribution of the clearing report to the PRODUCT RETAILER through the COLLECTION AND FORWARDING; — distribution of the clearing report to the SERVICE OPERATOR through the COLLECTION AND FORWARDING. The distribution of clearing reports can also be done by direct transmission from the PRODUCT OWNER.

6.5 Security management

The Security Policy secures the assets in the IFMS, the privacy of the customers, and the integrity and non-repudiation of the transaction data.

Conformance with the Security Policy is based on adherence to the Set of Rules, in particular the security rules, by the IFM members.

The SECURITY MANAGER is responsible for the operation of the security of the IFMS.

The functions of SECURITY MANAGER are performed by a central body in the IFM and, possibly and by delegation of this body, by other trusted Organisations.

The SECURITY MANAGER will be responsible for the implementation of the Security Policy by all Actors concerned. The responsibility will commence at the start of the IFMS.

Whenever a new Actor joins the IFMS, he will have to accept and implement the IFM Security Policy.

Security management consists of

— monitoring processes,

— managing security keys, and

— managing security lists.

6.5.1 Monitoring of IFM processes and IFM data life cycle

Use Case name	**Monitor IFM processes and IFM data life cycle**
Outline	The monitoring of the processes and data life cycle (generation of data, movement of data, storage of data, use of data, changes of data, and deletion of data) shall guarantee the secure operation of the IFMS, providing the required trust by the customers and operators concerning handling and protection of assets and sensitive information.
Triggered by	SECURITY MANAGER
Actors	ALL
Use Case description	The SECURITY MANAGER participates in the collection of information regarding the general security level from all Organisations and audits both the processes and the IFMS Components from which the data are generated until they are deleted. The Security Manager may collect targeted information from all the Use Cases and may monitor both the processes as well as the life cycle of the IFM data.

6.5.2 Management of IFM security keys

Use Case name	**Management of IFM security keys**
Outline	The generation, distribution, storage, and termination of IFM security keys.
Triggered by	SECURITY MANAGER
Actor(s)	SECURITY MANAGER ORGANISATIONS using IFM security keys
Use Case description	Security keys management covers the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation, and destruction of public or secret keying material in accordance with the IFM Security Policy at the general security level. The Use Case is Triggered by any ORGANIZATION that will receive, install, store, and use IFM security keys or by the SECURITY MANAGER as part of his security implementation tasks. The possibility of attacks must be taken into consideration.

6.5.3 Management of security lists

6.5.3.1 Provision of security lists

Use Case name	**Provision of security lists**
Outline	Provision of a security list by the Security Manager.
Triggered by	SECURITY MANAGER
Actors	SECURITY MANAGER APPLICATION OWNER PRODUCT OWNER APPLICATION RETAILER PRODUCT RETAILER SERVICE OPERATOR CUSTOMER
Use Case description	SECURITY MANAGER provides a new security list to — APPLICATION OWNER, — PRODUCT OWNER, — APPLICATION RETAILER, — PRODUCT RETAILER, — SERVICE OPERATOR, — REGISTRAR, and — (optional) CUSTOMER SERVICE through the COLLECTION AND FORWARDING.

6.5.3.2 Updating security list data

Use Case name	**Updating security list data**
Outline	Aggregation of security list data concerning Components, Customer Medium, installed Products, and installed Applications.

Use Case name	**Updating security list data**
Triggered by	SECURITY MANAGER ORGANIZATION APPLICATION OWNER PRODUCT OWNER APPLICATION RETAILER PRODUCT RETAILER SERVICE OPERATOR CUSTOMER
Actors	SECURITY MANAGER ORGANIZATION APPLICATION OWNER PRODUCT OWNER APPLICATION RETAILER PRODUCT RETAILER SERVICE OPERATOR CUSTOMER
Use Case description	The Use Case covers the activities of the Security Manager concerning the generation and maintenance of security lists.

6.5.3.3 Add or remove a Component to/from security list

Use Case name	**Add or remove a Component to/from security list**
Outline	The adding of a Component to, or removing of a Component from, a security list.
Triggered by	SECURITY MANAGER ORGANIZATION APPLICATION OWNER PRODUCT OWNER APPLICATION RETAILER PRODUCT RETAILER SERVICE OPERATOR CUSTOMER
Actors	SECURITY MANAGER ORGANIZATION APPLICATION OWNER PRODUCT OWNER APPLICATION RETAILER PRODUCT RETAILER SERVICE OPERATOR CUSTOMER
Use Case description	An ORGANIZATION may request that a Component be added to or removed from the security list, e.g. a stolen card-issuing machine or a ticketing machine.

6.5.3.4 Add or remove an Application Template to/from security list

Use Case name	**Add or remove an Application Template to/from security list**
Outline	The adding of an Application Template to or removing of an Application Template from a security list.
Triggered by	SECURITY MANAGER
Actors	SECURITY MANAGER
Use Case description	The SECURITY MANAGER requests the addition/removal of an Application Template to/from a security list. NOTE In the case of a prohibition list, the IFM Manager will later receive from the SECURITY MANAGER an acknowledgement of the termination.

6.5.3.5 Add or remove an Application to/from security list

Use Case name	**Add or remove an Application to/from security list**
Outline	The adding of an Application to or removing of an Application from a security list.
Triggered by	APPLICATION OWNER
Actors	SECURITY MANAGER APPLICATION OWNER
Use Case description	An APPLICATION OWNER requests the addition/removal of the installed Application to/from a security list. NOTE In the case of a prohibition list, the APPLICATION OWNER will later receive through COLLECTION AND FORWARDING an acknowledgement of the termination by an APPLICATION RETAILER.

6.5.3.6 Add or remove a Product Template to/from security list

Use Case name	**Add or remove a Product Template to/from security list**
Outline	The adding of a Product Template to or removing of a Product Template from a security list.
Triggered by	SECURITY MANAGER
Actors	SECURITY MANAGER
Use Case description	A SECURITY MANAGER requests the addition/removal of a Product Template to/from a security list. NOTE In the case of a prohibition list, the PRODUCT OWNER will later receive through COLLECTION AND FORWARDING an acknowledgement of the termination.

6.5.3.7 Add or remove a Product to/from security list

Use Case name	**Add or remove a Product to/from security list**
Outline	The adding of a Product to or removing of a Product from a security list.
Triggered by	PRODUCT OWNER or RETAILER
Actors	PRODUCT OWNER PRODUCT RETAILER SECURITY MANAGER
Use Case description	A PRODUCT OWNER or RETAILER requests the addition/removal of a Product to/from a security list. NOTE In the case of a prohibition list, the PRODUCT OWNER or RETAILER will later receive through COLLECTION AND FORWARDING an acknowledgement of the termination.

6.6 Customer Service Management (optional)

Use Case name	**Customer Service Management (optional)**
Outline	CUSTOMER SERVICE provides “helpline” and any similar facilities.
Triggered by	CUSTOMER
Actor(s)	CUSTOMER CUSTOMER SERVICE COLLECTION AND FORWARDING

Use Case name	**Customer Service Management (optional)**
Use Case description	CUSTOMER SERVICE receives a request from a CUSTOMER. The CUSTOMER SERVICE forwards the request to the relevant IFM-roles through the COLLECTION AND FORWARDING and receives the reply. CUSTOMER SERVICE answers the request.

7 System interface identification

All interfaces described in Annex A, except those with the Customer Medium, will be specified in further standards.

The interfaces with the Customer Medium are out of the scope of this part of ISO 24014 and are under the responsibility of other standardization committees.

8 Identification

8.1 General

By identification is meant a set of attributes that describes a specific person or object in a unique and unambiguous way. A person can, for instance, be described by name, birth date, sex, address, etc. to be uniquely identified. An object, e.g. a ticketing machine, can be identified by owner, type, and serial number.

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

- Security — Identification of IFM-roles, objects, Applications, Products, etc. enables the use of Security lists, e.g. to record stolen Components. The identification may also be used in an authentication procedure by including a unique ID.

- Communication — In an IFM network, there will be many entities like Organisations, companies, and Components that will be acting as a sender and/or a receiver of information. A unique identification is needed for addressing the different entities in a communication network.

- Auditing — There is a strong requirement on being able to audit any transaction and any piece of information in an IFMS, e.g. following a usage transaction from creation by the service operator until it is cleared and refunded by the Product Owner. If something goes wrong or any information is changed during its lifetime, it is important to be able to investigate what happened and where in the IFMS it happened.

8.2 Numbering scheme

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

- all Actors (Organisations) involved in the IFMS, e.g. all Product and Application Owners, Retailers, and Service Operators;

- all Application Templates;

- all Applications (implemented and initialised Application Templates);

- all Product Templates;

- all Products (instances of Product Templates);

- all Components.

8.3 Prerequisites

- There is one Registrar within the IFMS.

- Any object, e.g. Templates and Components, have an owner who will be one of the Actors in the IFMS.
- 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.

9 Security in IFMSs

IFMSs are subject to fraud by customers and operators, but also by people outside the IFMS. The Security Policy for an IFMS shall enable the protection of the public interests and the assets in the system.

9.1 Protection of the interests of the public

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

- Quality of Service — The IFMS shall be used as an instrument to ensure that national/local public transport service strategic goals are met.
- Fairness of payment — Customers shall be convinced that everyone is paying the correct amount according to valid tariff principles.
- Public Trust — Customers shall be convinced that they pay the correct amount for the desired service.
- Public Moral — Deliberate sabotage and fraud should be discouraged and considered illegal. This is related to the principles of fairness and public trust.
- Privacy — Information generated by the IFMS shall be protected as required by applicable laws.

These principles are of general nature and are not further specified in this part of ISO 24014, but should nevertheless be accounted for and followed within any Organization responsible for public transport services.

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

- only relevant personal data needed for the operation of the IFMS shall be requested from the Customer;
- the itemised disclosure of service consumption on an invoice shall be an option that can be chosen by the Customer;
- an IFM Actor might not disclose Customer-related information to third parties without specific authorization from the Customer;
- within the IFMS, the Customer-specific data shall be handled only in connection with the identification number of the contract (implicit or explicit) between the Customer and Product Owner. A link between the contract number and the name of the Customer can only be achieved by the contractual partner at the request of the Customer.

9.2 Assets to be protected

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

- physical assets — Computers, servers, communication systems, storage media, customer media, ticketing machines, validators, etc.;
- software assets — All software in the IFMS including software on the customer media;

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

The information assets can be further divided into the following:

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

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

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

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

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

9.3 General IFM security requirements

An IFMS shall fulfil the following general security requirements:

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

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

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

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

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

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

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

h) manage security lists including, but not limited to

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

   2) add or remove Customer Medium to/from security list,

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

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

Annex A
(informative)

Information flow within the IFM

A.1 General

This Annex will describe the information flow in the IFM. A.2 deals with the interfaces to the general IFM functions: certification and registration. The interfaces between the IFM-roles inside the IFM are described in A.3 to A.7.

A.2 Interface of the IFM-roles with the Security Manager and the Registrar

The security Management comprises the certification and auditing of the IFM and the Management of security lists.

In the context of certification and auditing, the interfaces between the IFM-roles and the Security Manager are on an organisational base. These processes are specified in 6.1.

In the context of security list management, the interfaces described in Figure A.1 are relevant.

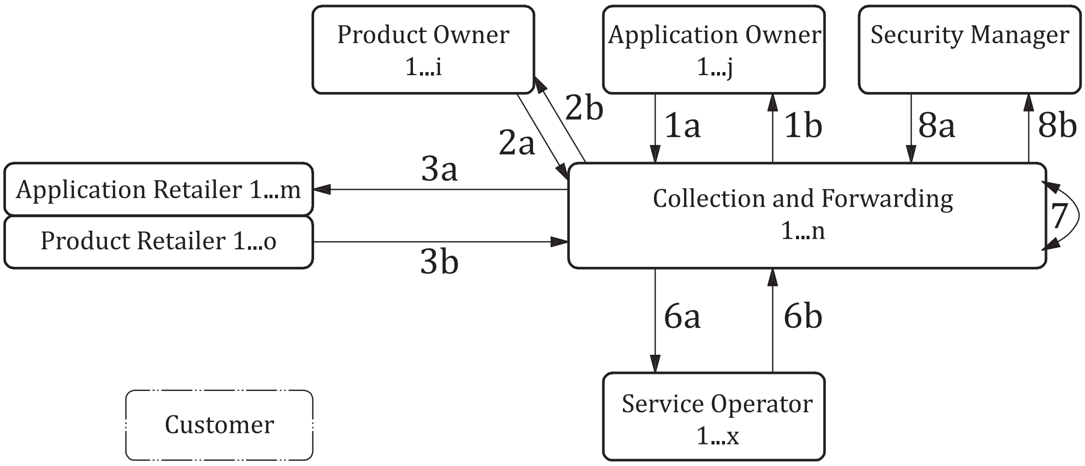


Figure A.1 — Interfaces between Security Management and the IFM-roles

Table A.1 — Interfaces between Security Management and the IFM-roles

Interface	Use Case name	Information flow
1a	Forced termination of Application:	Application identifier
1b	Forced termination of Application Template: Forced termination of Application:	3b and/or 6b information 3b and/or 6b information
2a	Forced termination of Product:	Product identifier
2b	Forced termination of Product Template: Forced termination of Product:	3b and/or 6b information 3b and/or 6b information
3a		8a information

Table A.1 *(continued)*

Interface	Use Case name	Information flow
3b	Forced termination of Application Template:	Application Template identifier and Application Template termination data
	Forced termination of Application:	Application identifier and Application termination data
	Forced termination of Product Template:	Product Template identifier and Product Template termination data
	Forced termination of Product:	Product identifier and Product termination data
6a		8a information
6b	Forced termination of Application Template:	Application Template identifier and Application Template termination data
	Forced termination of Application:	Application identifier and Application termination data
	Forced termination of Product Template:	Product Template identifier and Product Template Termination data
	Forced termination of Product:	Product identifier and Product termination data
7		1a, 2a, 3b, 6b, 8a information (transfer of Not On Us data to On Us data COLLECTION AND FORWARDING)
8a	Provision of security lists:	Security lists
8b	Forced termination of Application Template:	3b and/or 6b information
	Forced termination of Application:	1a information
	Forced termination of Product Template:	3b and/or 6b information
	Forced termination of Product:	2a information

In the context of registration, all Organisations performing one or more functions of the IFM-roles and Components within the IFM will receive a unique identifier. These processes are specified in 6.2.1 and 6.2.2. Also, the information flow related to Application and Product will receive a unique identifier.

The data exchange between Application/Product Owner and the Registrar can be carried out in different ways depending on the organisational and technical structure of the IFM to allow an online as well as an offline registration process. The interfacing to the Registrar can be processed through the Collection and Forwarding or through a direct link between each IFM-role and the Registrar.

The interfaces for

— the Template registration processes are described in Figure A.2 and in Table A.2, and

— the Application and Product registration processes are described in Figure A.2 and in Table A.3.

Table A.2 — Interfaces for Template registration

Use Case name	Information flow	Sequence
Registration of Application Template:	Application Owner request to Registrar: — Application Template certificate	1
	Return from Registrar: — Application Template identifier	2

Table A.2 *(continued)*

Use Case name	Information flow	Sequence
Registration of Application Template:	Product Owner request to Registrar: — Product specification certificate Return from Registrar: — Product Template identifier	1 2

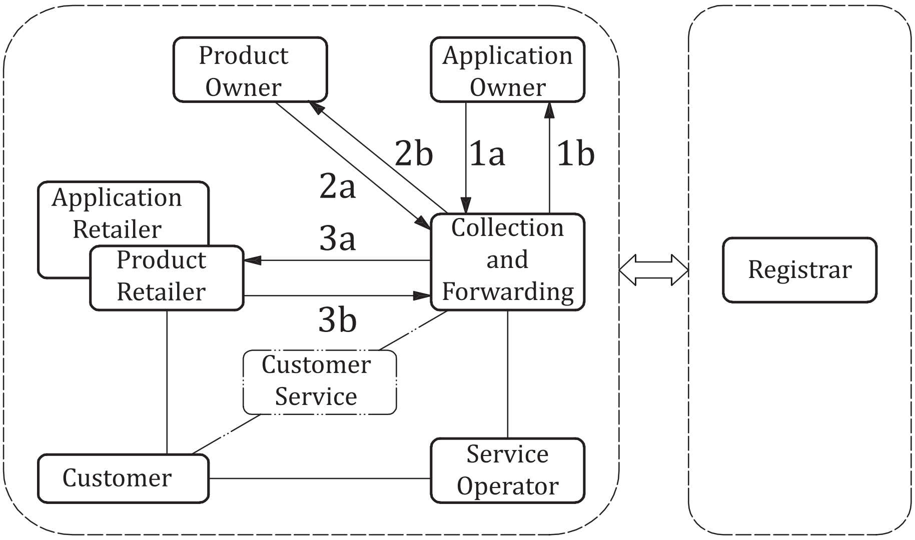


Figure A.2 — Interfaces between Registrar and Application Owner and Product Owner for the registration of applications and products

Table A.3 — Interfaces for registration of application and registration of product

Interface	Use Case name	Information flow	Sequence
1a		Application identifier	3
1b		3b information	2
2a		Product identifier	3
2b		3b information	2
3a		1a and 2a information	4
3b	Registration of Application: Registration of Product:	Application Template identifier Product Template identifier	1
		Send to Registrar: — Application Template identifier Return from Registrar: — Application identifier	
		Send to Registrar: — Product Template identifier Return from Registrar: — Product identifier	

A.3 Interface between the IFM-roles

Figure A.3 describes the interfaces between the IFM-roles inside an IFMS concerning the handling of certified and registered Application Templates, Applications, Product Templates, and Products. Interfaces to the Security Manager and the Registrar are not considered.

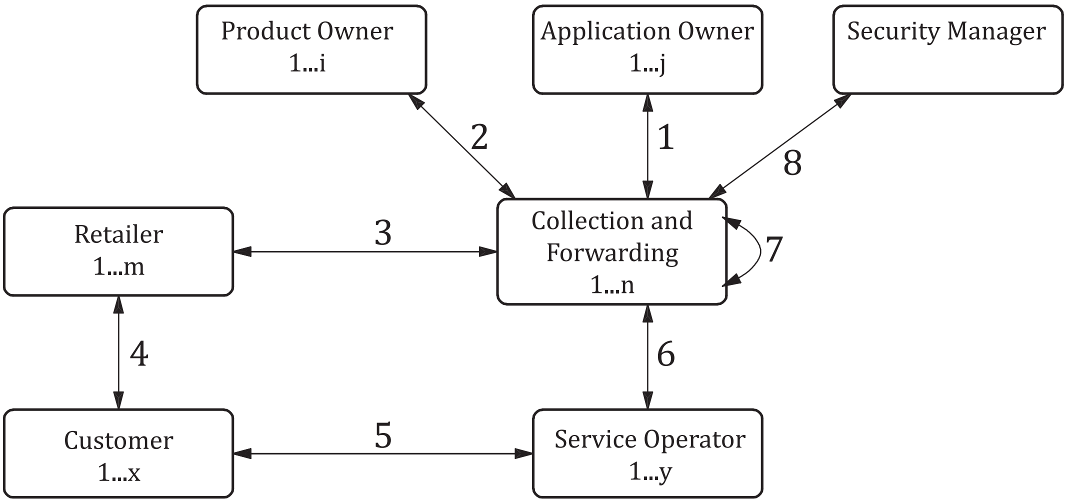


Figure A.3 — Interfaces between Actors within an IFMS

Each IFM-role shall be connected to only one Collection and Forwarding. Several Collection and Forwardings can coexist in one IFMS.

A.4 Interfaces between IFM-roles for Application Template management

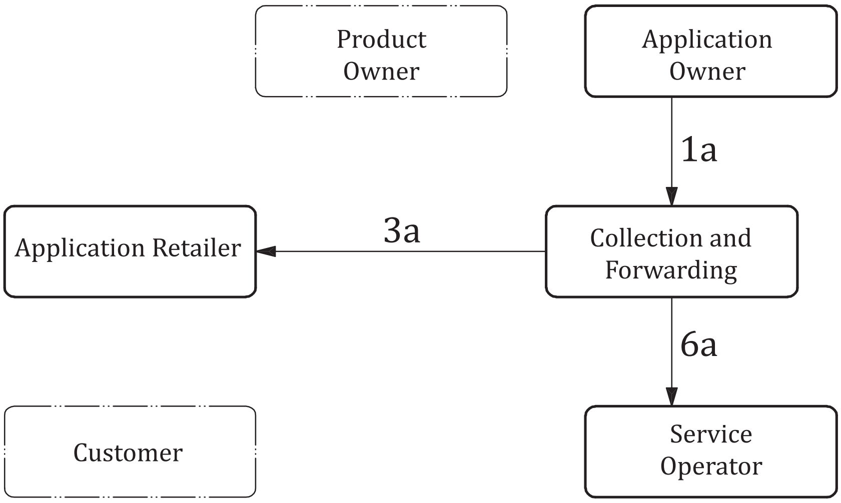


Figure A.4 — Application Template management

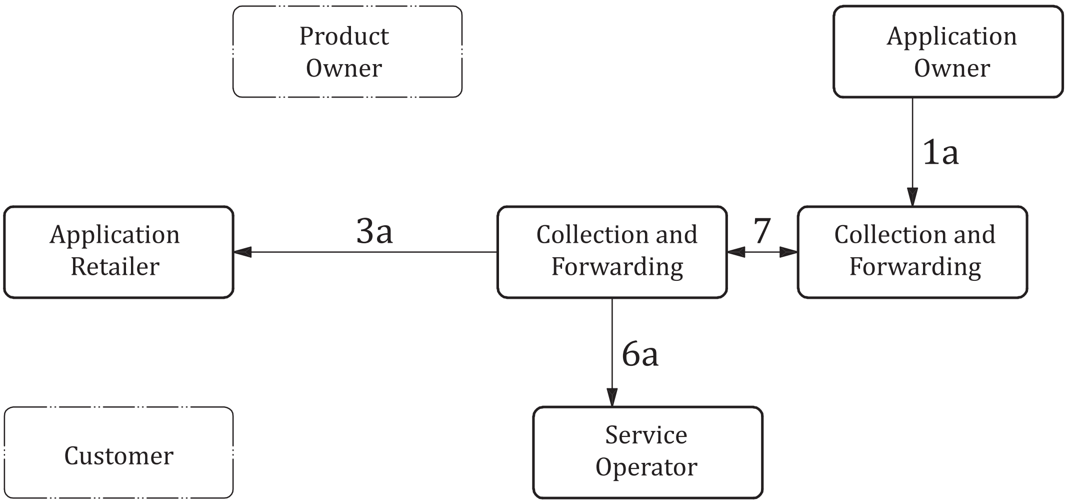


Figure A.5 — Application Template management with Not On Us data

Table A.4 — Application Template management

Interface	Use Case name	Information flow	Sequence Figure A.4	Sequence Figure A.5
1a	Dissemination of Application Template: Regular termination of Application Template	Application Template Request for Termination of Application Template	1	1
3a		1a information	2	3
6a		1a information	2	3
7		1a information (transfer of Not On Us data to On Us data COLLECTION AND FORWARDING)		2

A.5 Interfaces between IFM-roles for Application management

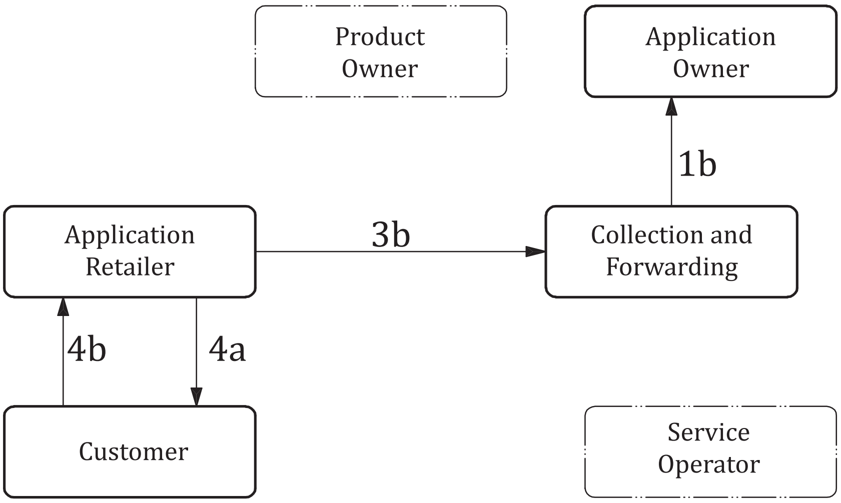


Figure A.6 — Interfaces between IFM-roles for Application management

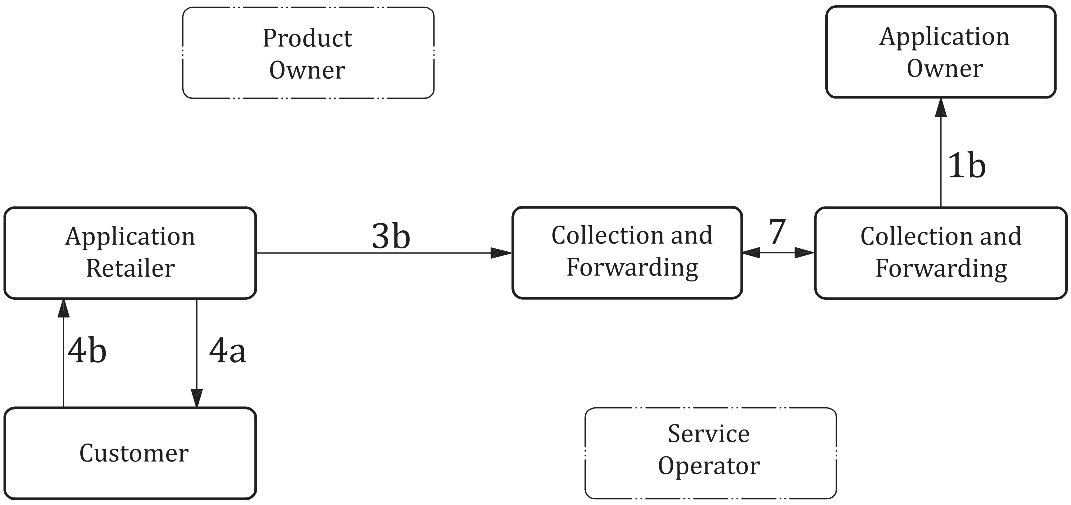


Figure A.7 — Interfaces between IFM-roles for Application management with Not On Us data

Table A.5 — Interfaces between IFM-roles for Application management

Interface	Use Case name	Information flow	Sequence Figure A.6	Sequence Figure A.7
1b		3b information	4	5
3b		Application identifier and 4b information	3	3
4a	Acquisition of Application: Regular termination of Application:	Application Template and Application identifier Termination instruction	2	2
4b	Acquisition of Application: Regular termination of Application:	Medium identifier (optional), Application acquisition data Application identifier, Medium identifier (optional), Application termination data of terminated Application	1	1
7		3b information (transfer of Not On Us data to On Us data COLLECTION AND FORWARDING)		4

A.6 Interfaces between IFM-roles for Product Template Management

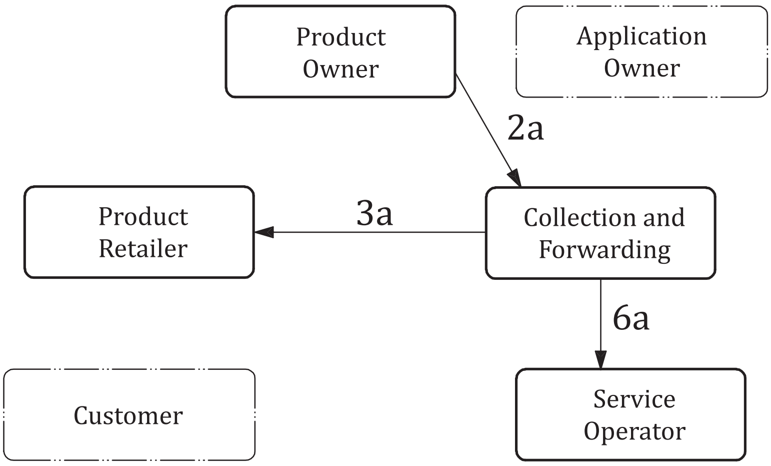


Figure A.8 — Product Template Management

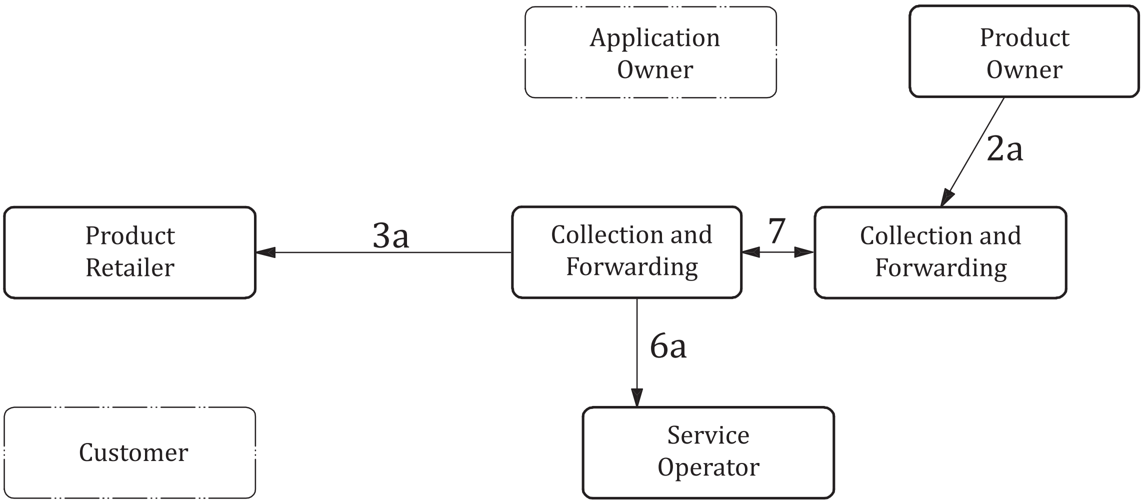


Figure A.9 — Product Template Management with Not On Us data

Table A.6 — Product Template Management

Interface	Use Case name	Information flow	Sequence Figure A.8	Sequence Figure A.9
2a	Dissemination of Product Template: Regular termination of Product Template:	Product Template Request for Termination of Application Template	1	1
3a		2a information	2	3
6a		2a information	2	3
7		2a information (transfer of Not On Us data to On Us data COLLECTION AND FORWARDING)		2

A.7 Interfaces between IFM-roles for Product management

Remark: According to the definition of Product, a Product can be a contract (i.e. charge to account Product) as well as a Product in the classical sense (ticket).

For clarity, the interfaces for Product management are divided into two basic cases:

a) acquisition/modification/termination of a Product, and

b) using a Product and distribution of clearing reports.

A.7.1 Acquisition/modification/termination of a Product

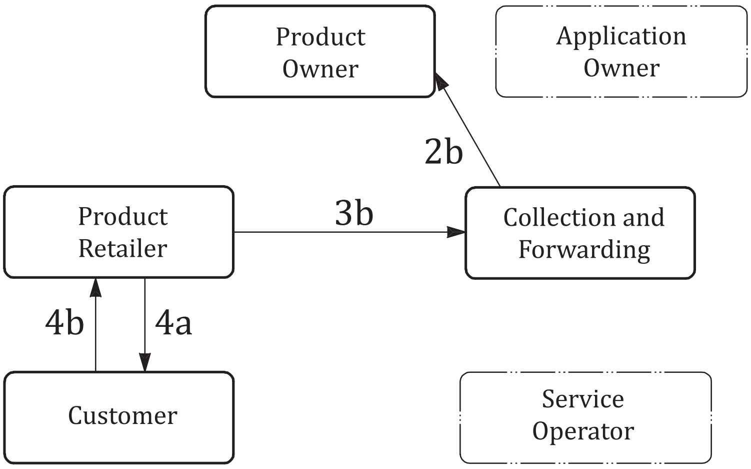


Figure A.10 — Interfaces for acquisition/modification/termination of a Product

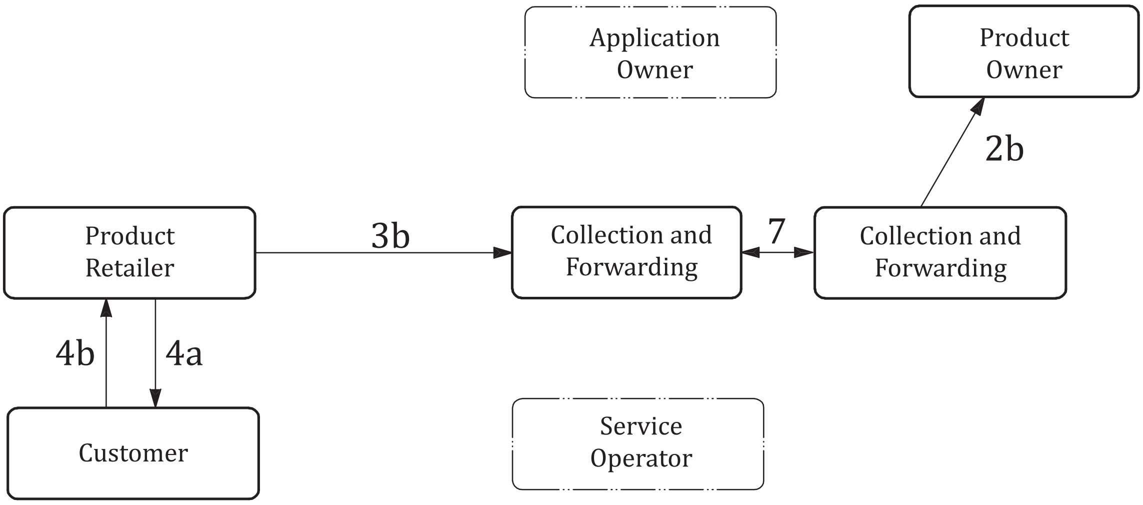


Figure A.11 — Interfaces for acquisition/modification/termination of a Product with not on us data

Table A.7 — Interfaces for acquisition/modification/termination of a Product[a]

Interface	Use Case name	Information flow	Sequence Figure A.10	Sequence Figure A.11
2b		3b information	4	5

[a] In this table, it is assumed that Product identifiers do not contain the Retailer and Product Owner information. If these identifiers contain this information already, it is not necessary to provide Retailer and Product Owner ID separately.

Table A.7 *(continued)*

Interface	Use Case name	Information flow	Sequence Figure A.10	Sequence Figure A.11
3b		Product identifier and 4b information	3	3
4a	Acquisition of Product: Modification of Product parameter: Regular termination of Product:	Product Template and Product identifier Product parameter Termination instruction	2	2
4b	Acquisition of Product(optional): Modification of Product parameter: Regular termination of Product:	Product acquisition data Product parameter Product identifier Medium identifier (optional) Product termination data of terminated Product	1	1
7		3b information (transfer of Not On Us data to On Us data COLLECTION AND FORWARDING)[a]		4

[a] In this table, it is assumed that Product identifiers do not contain the Retailer and Product Owner information. If these identifiers contain this information already, it is not necessary to provide Retailer and Product Owner ID separately.

A.7.2 Using a Product and distribution of clearing reports

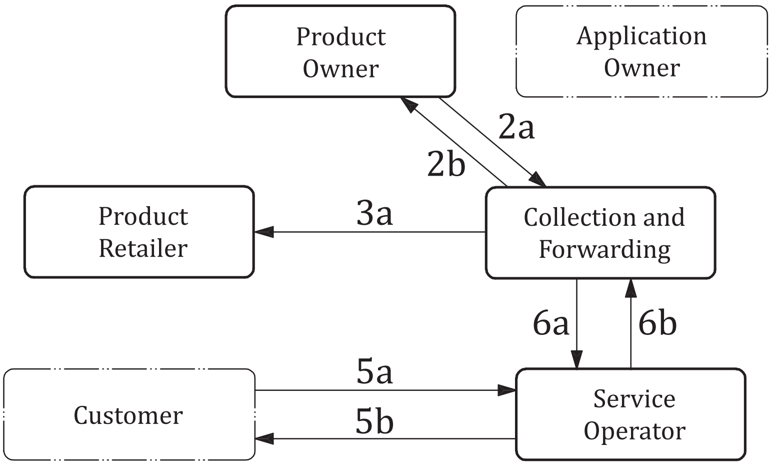


Figure A.12 — Interfaces for using a Product and distribution of clearing reports

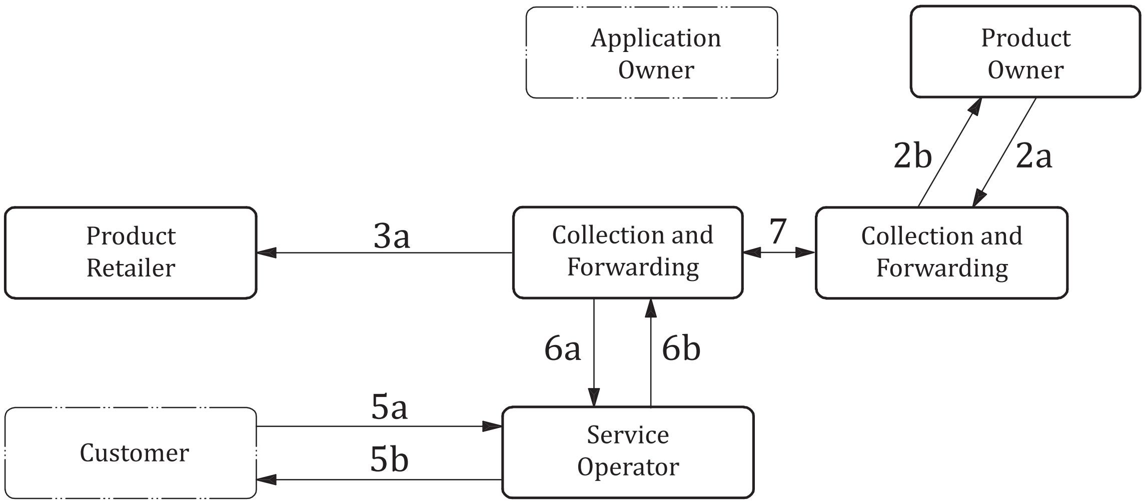


Figure A.13 — Interfaces for using a Product and distribution of clearing reports with Not On Us data

Table A.8 — Interfaces for using a Product and distribution of clearing reports

Interface	Use Case name	Information flow	Sequence Figure A.12	Sequence Figure A.13
2a	Generation and distribution of clearing reports	Clearing reports	5	6
2b	Forwarding data	6b information	4	5
3a	Forwarding data	2a information	6	7
5a	Use and inspection of Product	Application identifier, Product data (Retailer and Product Owner identifier, Usage Rules, etc.)	1	1
5b	Use and inspection of Product	Usage data (Product validation), service operator identifier	2	2
6a	Forwarding data	2a information	6	7
6b	Collection of data	Application identifier, Product identifier, Retailer identifier, 5b data objects, inspection data	3	3
7		6b information (transfer of Not On Us data to On Us data COLLECTION AND FORWARDING)		4

Annex B
(informative)

Examples of implementation

B.1 Interoperability in the Oslo region

B.1.1 General

This example describes how the generic IFM functional model has been implemented in the Oslo region (Norway). There are two main operators in the region.

— NSB Norske Statsbaner (Norwegian State Railways).

— Ruter Major Public transport operator in the Oslo region consisting of previous *Stor-Oslo Lokaltrafikk* (Great Oslo local traffic) and OS – *Oslo Sporveier* (Oslo metro/tram/bus).

Each of the operators will have their own electronic ticketing system purchased from different suppliers, but they have both signed an agreement to adhere to a common specification ensuring interoperability between the two fare management systems.

The two operators will together form the IFM Manager and they have appointed the functions of the Security Manager and the Registrar to a common entity called Oslo Interoperable Organization (OiO) which will have several other IFM functions as well (see B.1.2).

Figure B.1 shows the graphic presentation of the IFM-roles and their functions described below.

B.1.2 Operators and functions

Product Owners

Both operators will function as Product Owners with their own suite of Products including all the Products that are to be interoperable Products. One of the functions of the Product Owner is clearing. The two operators have decided to allocate all the clearing to OiO.

OiO (Oslo Interoperable Organization)

The OiO covers the functions of the following IFM-roles:

— Registrar which is the IFM-role that will register all companies, Products, Applications, security equipment, ticketing equipment, networks, etc. that are involved and/or included in the two interoperable ticketing systems;

— Security Manager which is the IFM-role responsible for security in the two interoperable ticketing systems, including security key management;

— Application Owner which is the IFM-role that owns the Application on the Customer Medium where the two Product Owners will install their Products;

— Collection and Forwarding which implies amongst other things the collection of all sale and use transactions in both companies, passing on common data related to Applications, and Products and passing on security lists. The Collection and Forwarding also includes communication with other IFMSs (future solution);

— Part of the Product Owner functions which in this case mean that the OiO performs the clearing between the Product Owners, Retailers, and Service Providers involved in the Oslo region IFM. All Use, Price, and Commercial rules are stored in the OiO enabling OiO to do the clearing.

Application Retailers

Both operators will function as Application Retailers, i.e. they will initialise the Customer Medium for further issuing of Products from the two operators on the Customer Medium.

Product Retailers

Both operators will function as Product Retailers for interoperable Products in addition to their own Products. This implies storing Product data on the Customer Medium and changing these data, e.g. storing electronic values on the Customer Medium or updating a period ticket.

Service Providers

Both operators will function as Service Providers which means they will provide the transport of the Customer from A to B. In addition to the two operators, Ruter will purchase services from other bus operators who will act as if they were a Service Provider of Ruter in the IFMS.

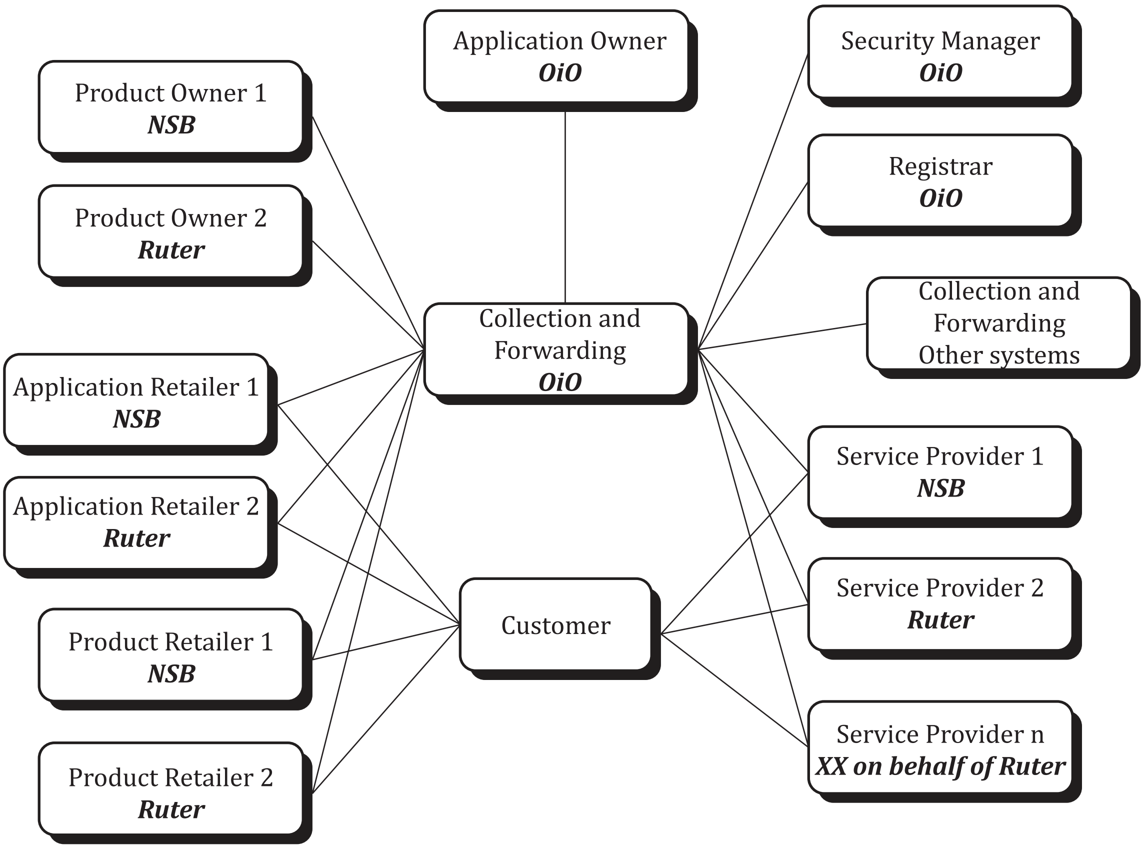


Figure B.1 — IFM functional model applied for an interoperable fare management system in Oslo

B.2 Interoperability in Paris (France) and its suburban region

B.2.1 General

This example describes how the generic IFM functional model has been implemented in Paris (France) and its suburban region.

In this area, the IFM Manager is STIF (*Syndicat des Transports d'Ile-de-France*). It has responsibility for organizing public transport in the Ile-de-France. Local Service Providers have signed an agreement with STIF to ensure interoperability for the customers. These companies are

- RATP (*Régie Autonome des Transports Parisiens*, Paris transport facilities company),
- SNCF (*Société Nationale des Chemins de fer Français*, French railway company), and
- OPTILE (Association of private bus companies).

Functions covered by each partner of the IFM are described in B.2.2.

B.2.2 Partners and functions

B.2.2.1 STIF

STIF is the IFM Manager. It covers the following functions:

- Registrar which registers all companies, Products, Applications, security equipment, ticketing equipment, networks, etc. that are involved and/or included in the three interoperable ticketing systems;
- Security Manager which is responsible for the security lists;
- Application Owner and Product Owner which owns the Application and Products that will allow customers to travel seamlessly among the networks provided by the three Service Providers;
- Collection and Forwarding which gathers data (aggregated use and acquisition data) from other partners.

NOTE The clearing function of Products is processed by STIF.

B.2.2.2 Other partners (RATP, SNCF, and OPTILE)

The functions covered by the other partners of the IFMS are as follows.

Application Retailers

All three operators will function as Application Retailers, i.e. they will initialise Customer Media for further issuing of Products from STIF on the Customer Media.

Product Retailers

All three operators will function as Product Retailers for interoperable Products from STIF in addition to their own Products. This implies storing Product data on the Customer Medium and changing these data, e.g. storing electronic values on the Customer Medium or updating a period ticket.

Product Owners

All three operators will function as Product Owners with their own suite of Products, but these Products give access only to the network owner.

Service Providers

All three operators will function as Service Providers which mean they will provide the transport for the Customer Seamless Travel for interoperable Products and local travel for their own Products.

Collection and Forwardings

They gather acquisition and usage data related to interoperable Products. They aggregate the data and transmit them to STIF.

Security Managers

They are responsible for the security in their own ticketing and control systems including security key management.

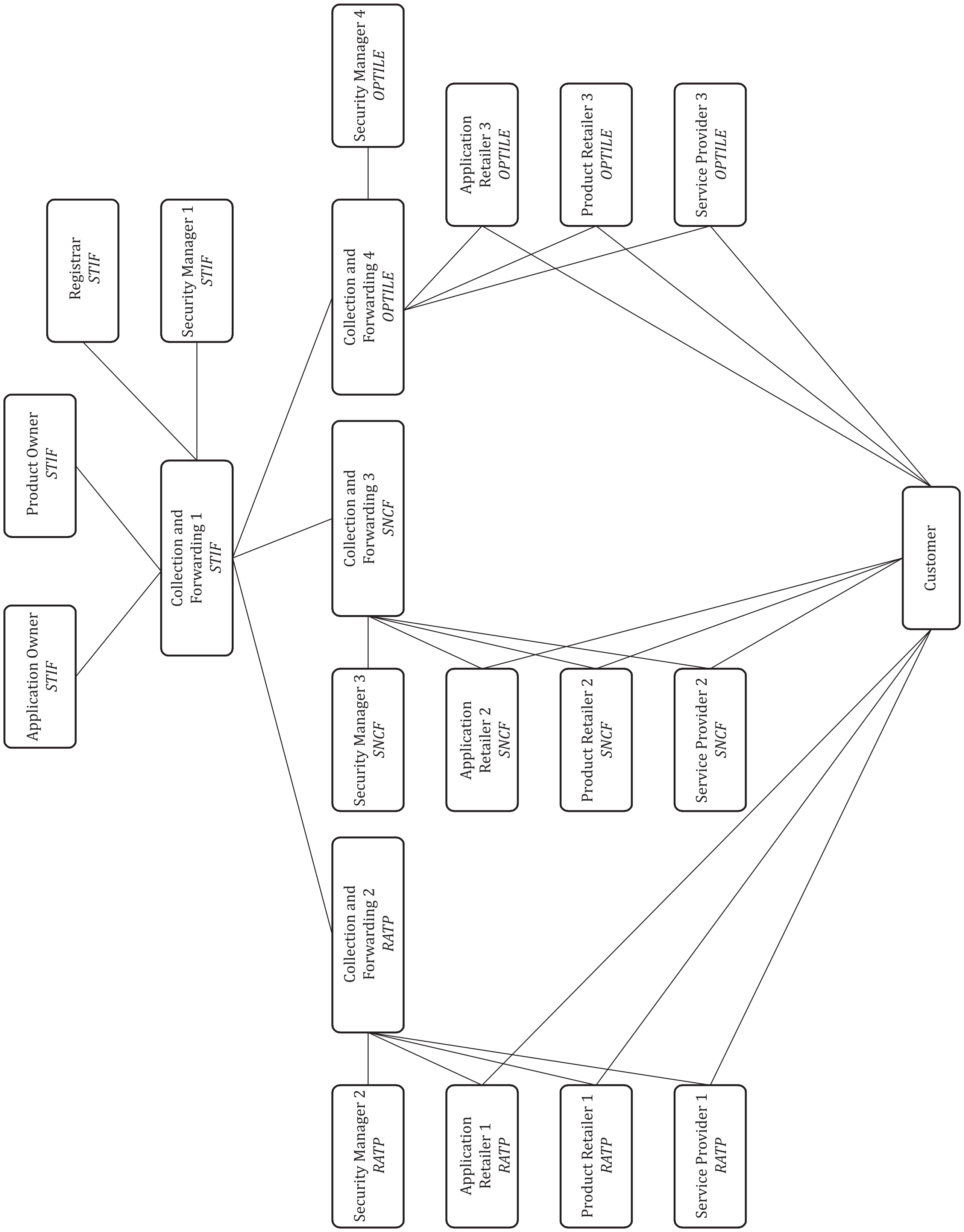

Application Owner STIF
Product Owner STIF
Registrar STIF
Security Manager 1 STIF
Collection and Forwarding 1 STIF
Collection and Forwarding 2 RATP
Collection and Forwarding 3 SNCF
Collection and Forwarding 4 OPTILE
Security Manager 4 OPTILE
Application Retailer 3 OPTILE
Product Retailer 3 OPTILE
Service Provider 3 OPTILE
Security Manager 3 SNCF
Application Retailer 2 SNCF
Product Retailer 2 SNCF
Service Provider 2 SNCF
Security Manager 2 RATP
Application Retailer 1 RATP
Product Retailer 1 RATP
Service Provider 1 RATP
Customer

Figure B.2 — IFM functional model applied for an interoperable fare management system, Paris and Ile de France

B.3 Interoperability in Japan

B.3.1 Interoperable states for a joint IFMS

The probable distribution of the functions and the responsibilities of the Security Manager and the Registrar to several Organisations within an IFM are stated in Clause 5. It is also stated that this distribution may be a necessary condition to allow the cooperation of the existing IFMSs. This may need additional explanation to properly understand the meaning of these sentences. This Japanese example is prepared for this purpose as stated in Clause 5 as well as to show the cooperation of the existing IFMSs in Japan in accordance with this part of ISO 24014.

Any IFMS can be functionally described by a Set of Rules which are subdivided into a management part which relates to the management IFM-roles and an operational part which is the rest of the Set of Rules.

There should be a single management part of the Set of Rules of a functional IFMS which can be distributed to the existing IFMSs for efficiency and effectiveness. On the other hand, the operational part of the Set of Rules need not have a common part, although actual interoperable state will be expanded by integrating the operational part of the Set of Rules of existing IFMSs, mainly an integration of Application/Product Specification/Templates. Figure B.3 explains this.

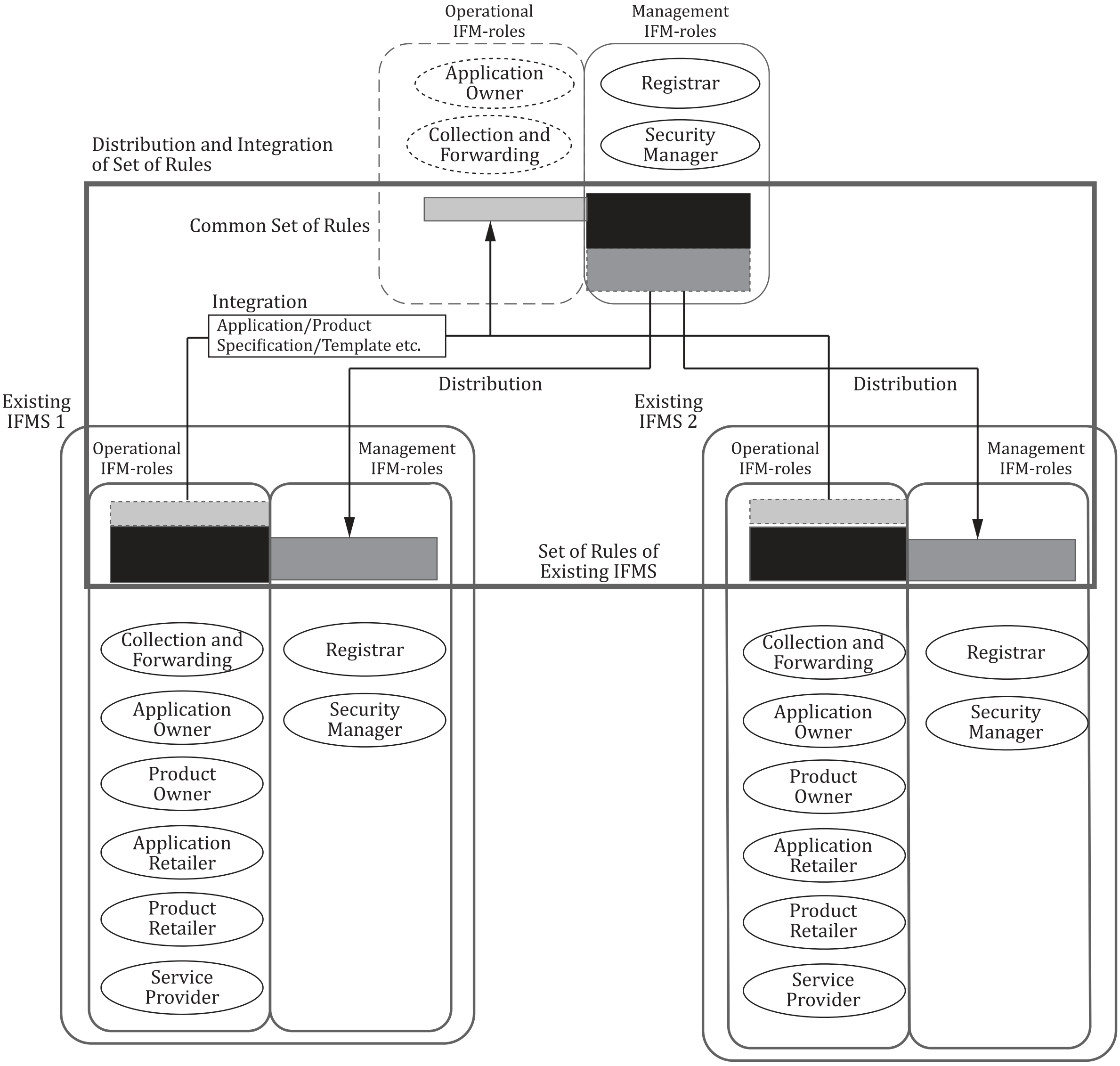


Figure B.3 — Distribution and integration of the Set of Rules of an IFMS after coordination of the existing IFMSs

From this view point, there are several interoperable states of a joint (functional) IFMS that consists of the cooperating existing IFMSs as shown in Figure B.4. Within a joint IFMS, one pair of existing IFMSs may traverse each state to some other one whereas another pair of existing IFMSs may stay at one of the states depending upon the environment and situation surrounding the joint IFMS.

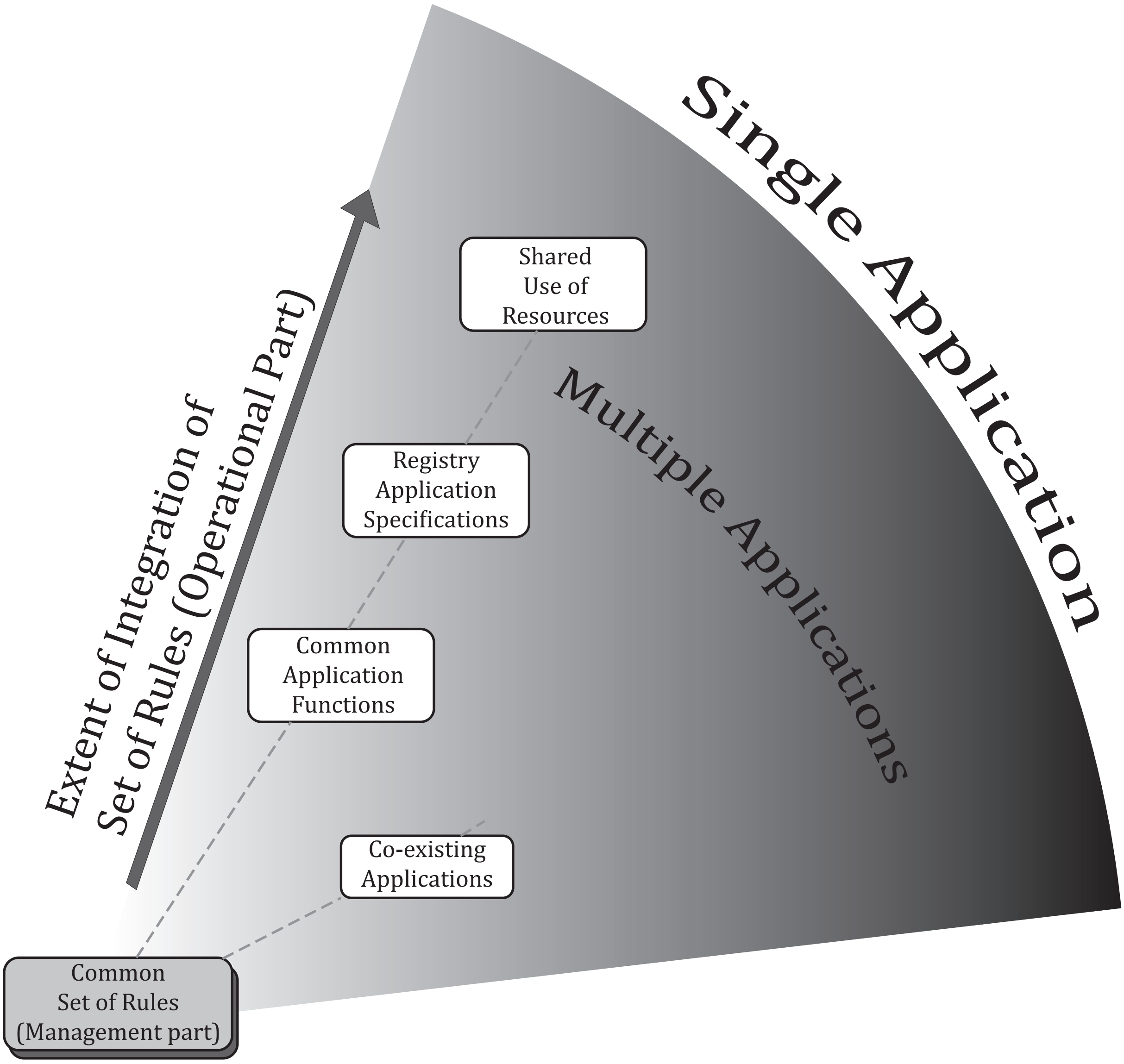

Single Application
Multiple Applications
Extent of Integration of Set of Rules (Operational Part)
Shared Use of Resources
Registry Application Specifications
Common Application Functions
Co-existing Applications
Common Set of Rules (Management part)

Figure B.4 — Interoperable states for an IFMS: Different pairs of existing IFMSs in Japan stay at one of the states within a dotted circle

Interoperable states are as described below.

a) Common Set of Rules

For a joint IFMS, the management part of the Set of Rules is agreed and created considering those of the existing IFMSs in most cases. The agreed Set of Rules can be distributed into the cooperating existing IFMSs.

This is a basic requirement for an IFMS. From this state, there are several possibilities for change. Any state can work as an IFMS.

NOTE State is defined by the extent of integration of a pair of the Set of Rules of existing IFMSs.

b) Common Application functions

In addition to having the common management part of the Set of Rules, the cooperating existing IFMSs can integrate their Application functions, e.g. by discussing the maximum set of Applications which can be used at one of the cooperating existing IFMSs. If they have this maximum set, they could agree with the physical architecture of Customer Media and other functions in an IFMS for multiple Applications.

c) Co-existing multiple Applications/Products

This is the other way of introducing multiple Applications. Instead of the agreement of physical architecture of an IFMS, all Applications can co-exist on a single Medium.

d) Registry for Application/Product Specifications and Templates

Actual Applications and Products are registered as interoperable Specifications and Templates.

e) Shared use of resources based upon the common Set of Rules

If possible, shared use of resources based upon the common Set of Rules, particularly Application/Product Specifications/Templates, reduces the introduction and maintenance costs. For example, common software for MAD and shared use of resources for Collection and Forwarding.

f) Single Application

B.3.2 Interoperability in Japan in accordance with this part of ISO 24014

B.3.2.1 General

This example describes how the generic IFM functional model explained here can be implemented in Japan.

The IFM Manager is a committee representing most of the public transport in Japan. The name is IC Card Interoperability Committee (CIC) and it is responsible for coordination in Japanese public transport. The existing IFMSs have signed an agreement whereby they follow the rules and the decisions of the CIC. These existing IFMSs are the following:

— Suica (main operator: JR EAST);

— PASMO (main operators: subway/private railway/bus operators in Tokyo);

ICOCA (main operator: JR WEST);

— PiTaPa (main operators: subway/private railway/bus operators in Osaka, Kyoto and Kobe).

Functions of the existing IFMSs are described in B.3.2.2.

NOTE As of 2013, the number of existing IFMSs becomes 10.

B.3.2.2 Functions of the existing IFMSs

B.3.2.2.1 IC Card Interoperability Committee

IC Card Interoperability Committee is the IFM Manager.

IC Card Interoperability Committee covers the following functions which are actually distributed into each existing IFMS:

— Registrar as a committee — As a part of the Set of Rules, it decides fundamental rules for registration of all companies, Products, Applications, security equipment, ticketing equipment, networks, etc. that are involved and/or included in the existing IFMSs. Actual registrations are distributed to the Registrar of each existing IFMS. Registration data are collected and forwarded;

— Security Manager, as a committee, is responsible for the security lists strategy and policy as a part of the Set of Rules. Actual work is distributed to the Security Manager of each existing IFMS;

- Interoperable Application Templates and Product Templates are integrated and registered in a registry;
- Collection and Forwarding — In Tokyo Metropolitan area, all the messages are forwarded to appropriate existing IFMSs through CIC in addition to Collection and Forwarding. Calculation of clearing of interoperable Products is processed by CIC.

B.3.2.2.2 Other functions of existing IFMSs

The functions of the existing IFMSs are as follows.

Application Owners

The transport operators, as a single company or a unity of them, function as Application Owners of the existing IFMSs.

Application Retailers

The transport operators in the existing IFMSs function as Application Retailers, i.e. they initialise Customer Media for further issuing of Products on the Customer Media.

Product Owners

The transport operators in the existing IFMSs function as Product Owners with interoperable Products with or without their own modifications/additions and their own suite of Products.

Product Retailers

The transport operators in the existing IFMSs function as Product Retailers for interoperable Products in addition to their own Products.

Service Providers

The transport operators in the existing IFMSs function as Service Providers which means they provide the transport for the Customer Seamless Travel for interoperable Products and local travel for their own Products.

Collection and Forwarding

The Collection and Forwarding of the each existing IFMSs aggregate the data and exchange data of interoperable Applications/Products.

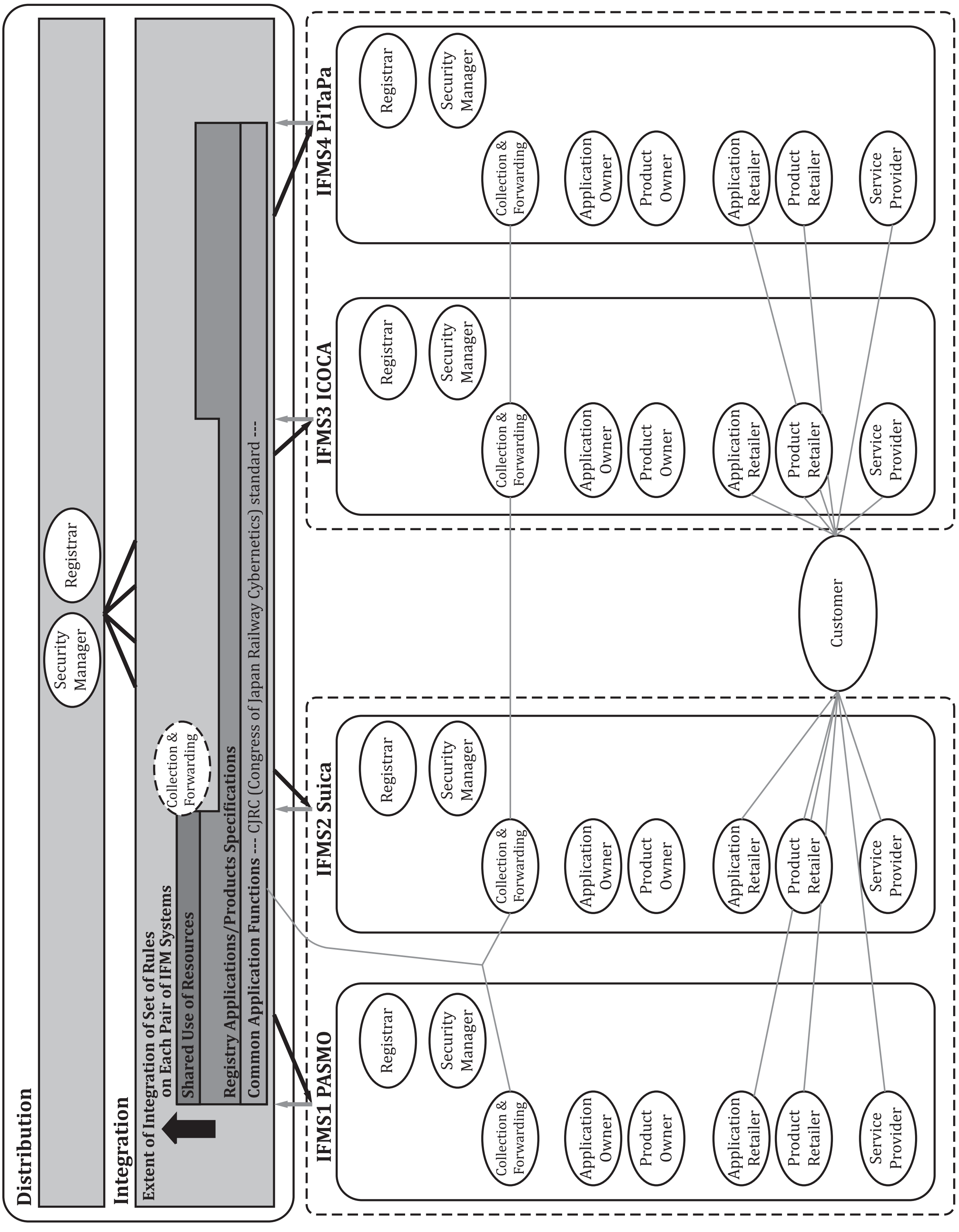


Figure B.5 — IFM functional model applied for the Japanese interoperable fare management system

Annex C
(informative)

List of terms which are defined both in this part of ISO 24014 (IFMSA) and in APTA — UTFS

C.1 General

The APTA (American Public Transportation Association) – UTFS (Universal Transit Farecard Standards) programme develops a series of documents that provides industry guidance for the creation of an open fare collection architecture that promotes greater access and convenience to the public transport network in the USA.

Table C.1 presents terms which are defined both in this part of ISO 24014 (IFMSA) and in UTFS.

Table C.1 — Cross-reference list of terms defined in IFMSA and in the APTA – UTFS

IFMSA term	IFMSA definition	UTFS term	UTFS definition
Action List	list of items related to IFM Applications or Products downloaded to Medium Access Devices (MADs), actioned by the MAD if and when a specific IFM Application or Product referenced in the list is encountered by that MAD	Action List	A list of issued cards that are to have some action performed on them if presented to any applicable Card Interface Device (CID) in the system. The Action List is distributed to the necessary CIDs.
Application	implemented and initialised Application Template on a Customer Medium NOTE 1 The Application is identified by a unique identifier. NOTE 2 The Application houses Products and other optional Customer information (Customer details, Customer preferences).	Application	Sometimes known as a client or an “app”, this is a self-contained program that performs a well-defined set of tasks. The Application can reside on a smart card, PC, browser, etc.
Medium	physical carrier of Applications	Proximity Integrated Circuit Card (PICC)	A plastic card containing an integrated circuit with contacts or antenna for communications on and off the integrated circuit. This integrated circuit can be microprocessor and/or memory logic.
Medium Access Device (MAD)	device with the necessary facilities (hardware and software) to communicate with a Customer Medium	Card Interface Device (CID)	A device that allows cards to be read and encoded through a contactless interface with the card. Also known as validators, readers, etc.
Product	instance of a Product Template on a Medium stored in an Application NOTE It is identified by a unique identifier and enables the customer to benefit from a service provided by a Service Operator.	Fare Product	A feature of the Transit Application cardholder (PICC) profile that authorises transportation with individually specified privileges permitting the CID to determine any special fares to be charged.

Annex D
(informative)

Example of Action List processes

D.1 Interpretation of “action list”

In addition to the definition of Action List in 2.1, the following possible interpretation is given as an example.

An Action List is a list of items related to IFM media, Applications, or Products downloaded to a selection of MADs which shall be actioned by the MAD if and when a specific IFM Application or Product referenced in the list is encountered by that MAD.

Explanation:

The actions are executed by the MADs without user interaction. The Action List is generated from Action List directives. The Action List directives are generated

a) by one of the Actors while in contact with the customer but not in contact with the card (e.g. call centre, website, processing received mail), and

b) in the back office of an Actor based on internal information.

Purpose:

The purpose of an Action List is

a) to service the customer through those channels where the customer cannot physically present a Medium, and

b) to implement measures in Applications and/or Products without forcing customers to visit a service point.

Clarification of scope:

The process of automatically recharging or topping up a Product triggered by the properties of the Product itself is not an enactment of Action Listing.

Process details:

By means of an Action List, one can split transactions into two parts. The first part is order and payment, the second is delivery. This is due to the fact that two parts are separated in space and time and can involve different Actors.

The object of an action could be a Medium, an Application on a Medium, or a Product within an Application.

Contents details:

The items on an Action List can be

a) add a Product;

b) modify a Product, for example:

   1) add/deduct value to/from stored value Product,

   2) modify topping-up settings for a stored value Product, and

3) unblock a Product.

c) terminate a Product (as part of refund);

d) add an Application;

e) modify Application (e.g. add or change a holder profile);

f) terminate an Application.

The only case where the object of an action is a Medium is where the action is adding an Application.

D.2 Comparison of Action Lists and security lists

One could consider that since Action Lists and security lists utilize the same distribution mechanisms, from an engineering perspective security listing is a subset of Action Listing. This is different from the business view which considers that Action List concerns planned actions and security list comprises reactive responses to security incidents.

D.3 Examples of information to be communicated in Action Lists

An Action List will always include the following:

- unique identifier of the Medium, Application, or Product;
- unique identification of the action;
- type of action that is required to be taken (add Product, add stored value to a Product, etc.);
- any parameter that is associated with this action (e.g. amount, if action is to add stored value to a Product).

The actions could be the following.

a) add Product;

   1) Add new Product (Application, Product ID, Product parameters).

   2) Renew Product (old Product ID, new Product ID, Product parameters).

b) modify Product;

   1) Add stored value to stored value Products (Product ID, value).

   2) Deduct stored value from stored value Products (Product ID, value).

   3) Remove stored value from stored value Products (Product ID).

   4) Initialise topping-up parameters of a stored travel rights Product (Product ID, Product parameters).

   5) Modify topping-up parameters of a stored travel rights Product (Product ID, Product parameters).

   6) Stop topping up for a stored travel rights Product (Product ID).

   7) Unblock a blocked Product (Product ID).

c) Terminate Product (Product ID);

d) Modify Application.

   1) Add holder profile (Application, parameters).

2) Terminate holder profile (Application, parameters).

3) Change user preferences (Application, parameters like class).

Additionally, the Action List directive can contain data such as the following:

- one or more identifiers for a selection of MADs which will carry out the action;
  - service operator(s);
  - location(s);
  - zone(s);
  - transport mode(s);
  - line(s);
- the period during which the action is to be taken;
- the type of directive: a new action or revocation of previous action;
- an identification of a previous action (in case of revocation).

D.4 Examples of Use Cases

This clause describes examples of Use Cases for Action List operation. The set of examples of Use Cases described here provides a toolbox for the implementation of such Action Lists in IFMSs. The examples of Use Cases below are detailing the Use Case Management of Action List as described in the main text. The Use Cases are not considered to be comprehensive.

This description uses the term Action List administrator. Action List administration is, in these examples, a function of aggregation of actions into one list, identifying each action uniquely, and controlling the action through its life cycle.

Action List administration as a function can be part of the functions of Product or Application Retailer, Product or Application Owner, and Collection and Forwarding. For the purpose of this Annex, we use the term Action List administrator for the entity/entities responsible for this function.

Use Case name	**Creating an action request**
Outline	Issuing an action request for adding an item to an Action List.
Triggered by	CUSTOMER, PRODUCT RETAILER, APPLICATION RETAILER
Actor(s)	PRODUCT RETAILER, APPLICATION RETAILER, COLLECTION, AND FORWARDING
Use Case description	The PRODUCT RETAILER or the APPLICATION RETAILER — issues an action request to add an action to an Action List. The action could be either — the one time addition/modification/removal of a Product to/from the customer Application, or — the one time modification of an Application on the customer Medium and could be restricted to a selection of MADs, e.g. depending on location/line/service operator. — Depending on the type of action, either — the Product information is sent to the PRODUCT OWNER through the COLLECTION AND FORWARDING, or — the Application data are sent to the APPLICATION OWNER through the COLLECTION AND FORWARDING. Note that the actual implementation of the action has not taken place yet which makes the information at this stage different from a normal retail transaction.

Use Case name	**Aggregation of Action Lists**
Outline	Assemble Action Lists based on action requests.
Triggered by	PRODUCT RETAILER, APPLICATION RETAILER
Actor(s)	PRODUCT RETAILER, APPLICATION RETAILER, ACTION LIST ADMINISTRATOR, COLLECTION, AND FORWARDING
Use Case description	The action request is sent by the PRODUCT RETAILER or APPLICATION RETAILER by Collection and Forwarding to the ACTION LIST ADMINISTRATOR who aggregates the list and issues a unique action number for each action.

Use Case name	**Distribution of Action Lists**
Outline	Assemble and distribute Action Lists.
Triggered by	ACTION LIST ADMINISTRATOR
Actor(s)	APPLICATION RETAILER, PRODUCT RETAILER, ACTION LIST ADMINISTRATOR, COLLECTION, AND FORWARDING
Use Case description	The ACTION LIST ADMINISTRATOR distributes periodically to the APPLICATION RETAILER and/or PRODUCT RETAILER and on a needs basis, either a full Action List or an incremental list to those Organisations, which are owners of the respective MADs. The Organisations distribute the Action List to the selected MADs (see 6.4.3). An action will be distributed only for a limited time or until the status is changed (by execution or removal).

Use Case name	**Executing actions**
Outline	Updating the Customer Media, Application, and/or Product based on the type and data of the action.
Triggered by	CUSTOMER
Actor(s)	APPLICATION RETAILER, PRODUCT RETAILER, COLLECTION, AND FORWARDING.

Use Case name	**Executing actions**
Use Case description	The CUSTOMER presents a Medium to the MAD. The MAD has an action for the Medium, Application, or Product. The MAD updates the Application or Product and sends back information to the ACTION LIST ADMINISTRATOR. Depending on the type of action, the APPLICATION RETAILER and/or PRODUCT RETAILER distributes the Product identifier data or Application data to the PRODUCT OWNER and/or APPLICATION OWNER through the COLLECTION AND FORWARDING.

Use Case name	**Removing item from Action List**
Outline	Issuing a request to remove an item from the Action List.
Triggered by	PRODUCT RETAILER, APPLICATION RETAILER
Actor(s)	PRODUCT RETAILER, APPLICATION RETAILER, COLLECTION, AND FORWARDING
Use Case description	The Use Case is invoked by — the PRODUCT/APPLICATION RETAILER requesting the ACTION LIST ADMINISTRATOR to remove an item from the Action List. The ACTION LIST ADMINISTRATOR no longer distributes the action or actively signals its removal.

Use Case name	**Action item flushing**
Outline	Removal of Action List items based on expiration of the time assigned to an action item.
Triggered by	ACTION LIST ADMINISTRATOR
Actor(s)	ACTION LIST ADMINISTRATOR, COLLECTION, AND FORWARDING
Use Case description	The ACTION LIST ADMINISTRATOR registers all actions and their status. When an action can no longer expect to be executed (due to expiration or removal), the result is sent back to the initiator of the action and the action is removed from the list.

Annex E
(informative)

Security domain, threats, and Protection Profiles

E.1 Security domain

In order to secure the assets, the owners of an IFMS have to recognize what the threats are, how the threats shall be met and which measures and mechanisms shall be implemented. Hence, it is important to define and limit the domain that includes the assets to be protected.

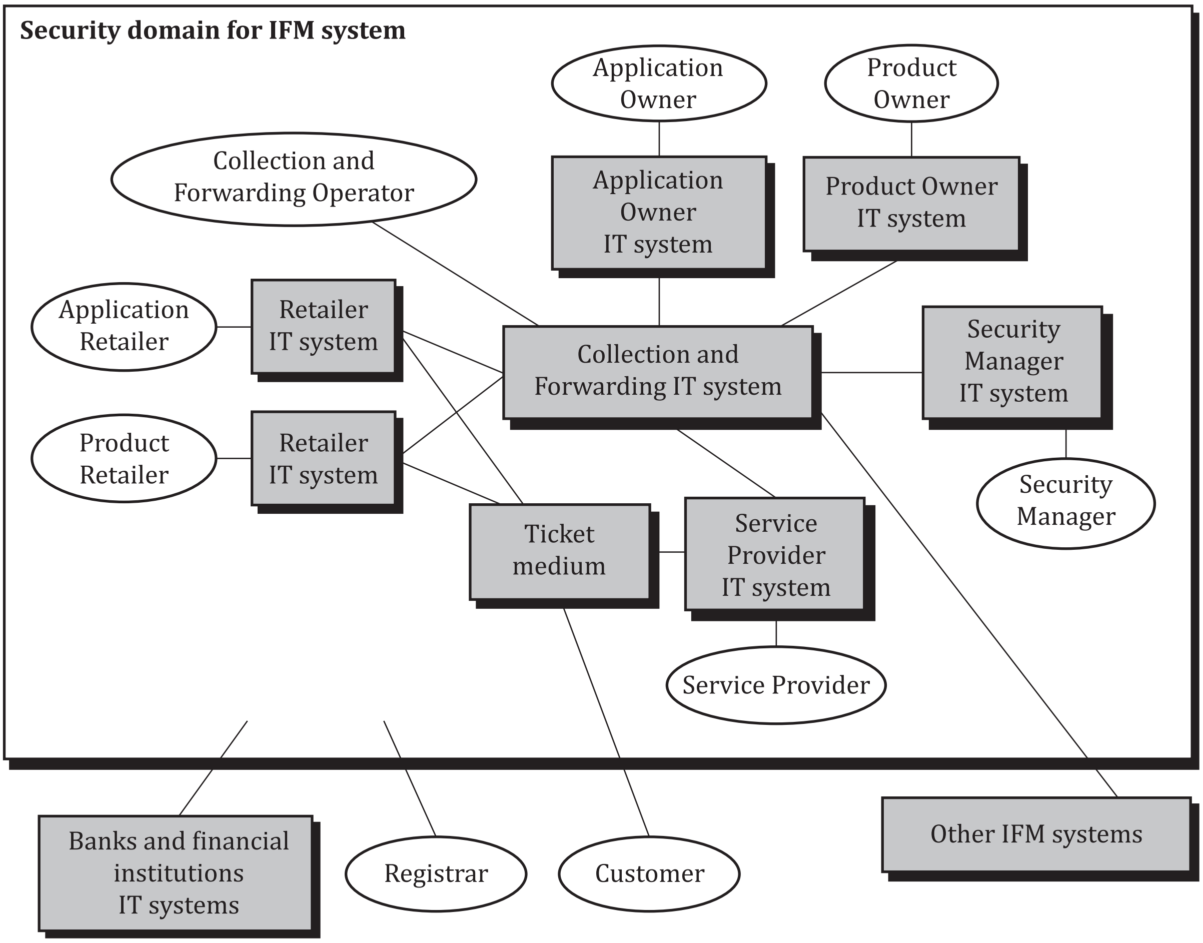

Security domain for IFM system
Application Owner
Product Owner
Collection and Forwarding Operator
Application Owner IT system
Product Owner IT system
Application Retailer
Retailer IT system
Collection and Forwarding IT system
Security Manager IT system
Product Retailer
Retailer IT system
Security Manager
Ticket medium
Service Provider IT system
Service Provider
Banks and financial institutions IT systems
Registrar
Customer
Other IFM systems

Figure E.1 — IFM security domain

Figure E.1 shows the security domain for an IFMS. The inside square boxes represent Components and the ovals represents Component users.

Banks and financial institutions are outside the domain as they are regarded as trusted entities. The Registrar is outside because it is regarded as trustworthy and the information managed by the Registrar does not require confidentiality. Other IFMSs are outside because the owner(s) of one IFMS has no influence or control over other systems. The Customer is also outside because nobody inside the domain can control the behaviour of the Customer.

E.2 Threats

The main motivation of threat and vulnerability analysis is to proactively minimize the risks associated with implementing and operating an IFMS. Threat and vulnerability analysis covers an overall assessment of the most probable threats and the system's vulnerability to these threats.

The threat analysis includes definition of possible attackers and threat targets (containing assets) and an assessment of the targets' vulnerability towards methods that attackers apply to access and change, use, copy, and/or retrieve the assets.

Attackers can be classified as follows.

— Class 1: Clever outsiders

  Might be skilled and have tools intended for attacks, but have insufficient knowledge of the system and exploit known weakness of the system to meet their objectives.

— Class 2: Knowledgeable outsiders

  Possess specialized technical education, experience, and specialized tools intended for attacks and potentially have access to the whole system.

— Class 3: Funded Organisations

  Groups of outsiders possessing specialists, possibly also using Class 2 attackers, with state-of-the-art tools intended for attacks and sufficient funding.

— Class 4: Insiders

  Insiders have access to sensitive information, processes, and modules that might be exploited by them or any other outsiders.

The classification of attackers (ranging from 1 to 4) is included to indicate that the higher the class, the higher the likelihood that severities of the attack are high. On the other hand, the higher the class, the lower the number of people that might be able to carry out the attack and vice versa. This can be used later to assess the likelihood of whether threat results in an actual attack.

The attack strategies can be decomposed into classical security attack methods as given in Table E.1.

Table E.1 — Classification of attacks and attack methods

Attack strategy	Primary attack methods	Secondary attack methods
Repudiation	Denial of used service	None further
Sabotage	Set Service Operator MAD into non-operational state	None further
Product masquerade	Eavesdropping	None further
	Manipulation of data	Alteration of hardware (HW) and/or software (SW) and/or Application and/or Product data
	Disclosure of sensitive information	Theft of MAD
Message replay	Record and replay	Eavesdropping and timing attacks
Cloning of Products	Product media segment tampering	Theft of Products in manufacturing, distribution, or issuance
	Disclosure of sensitive information	Insider abuse such that information assets (e.g. security keys) are disclosed
		Alteration of HW and/or SW
		Theft of MAD to retrieve security keys

Table E.1 *(continued)*

Attack strategy	Primary attack methods	Secondary attack methods
Cloning of messages	Message replay	Eavesdropping and timing attacks
	Disclosure of sensitive information	Insider abuse such that information assets (e.g. security keys) are disclosed
		Alteration of HW and/or SW and/or Application data
		Theft of MAD to retrieve critical information (e.g. security keys)

E.3 Protection Profiles (PP)

The security threats have to be met by different types of security measures including security requirements specifications.

In ISO/IEC 15408 and ISO/IEC/TR 15446, a set of security requirements specifications is referred to as a Protection Profile (PP).

By a Protection Profile (PP) is meant a set of security requirements for a category of Products or systems which meet specific needs. A typical example would be a PP for a Customer Medium to be used in an IFMS and in this case, the PP would be an implementation-independent set of security requirements for the Customer Medium meeting the operators' and users' needs for security.

The main purpose of a PP is to analyse the security environment of a subject and then to specify the requirements meeting the threats being the output of the security environment analysis. The subject studied is called the target of evaluation (TOE).

The contents of a PP is always organized in the following way:

1) Introduction;

2) Target of evaluation (TOE) — The scope of the TOE, e.g. a validator, shall be specified;

3) Security environments — Development, operation, and control methods of TOE are described to clarify the working/operation requirements. Regarding these requirements, IT assets which TOE shall protect and security threats to which TOE is exposed shall be specified;

4) Security objectives — Security Policies for threats to TOE are determined. The policies are divided into technical policy and operational/control policy. Security objectives should be consistent with the operational aim or Product purpose of the TOE. Operational/control policy is defined as personnel and physical objectives in the status in which TOE is used or operated. The operational/control policy includes control and operational rules for operators;

5) Security requirements — In accordance with the security objectives defined in item 4) of the PP, concrete security requirements for security threats stated in item 3) of the PP are specified. The security requirements consist of functional requirements (technical requirements) and assurance requirements for security quality. Functional requirements are provided selecting necessary requirements from ISO/IEC 15408-2 and determining parameters. Regarding assurance requirements, those designated in ISO/IEC 15408-3 are adopted by determining evaluation levels (EAL) for assurance requirements which are provided in ISO/IEC 15408;

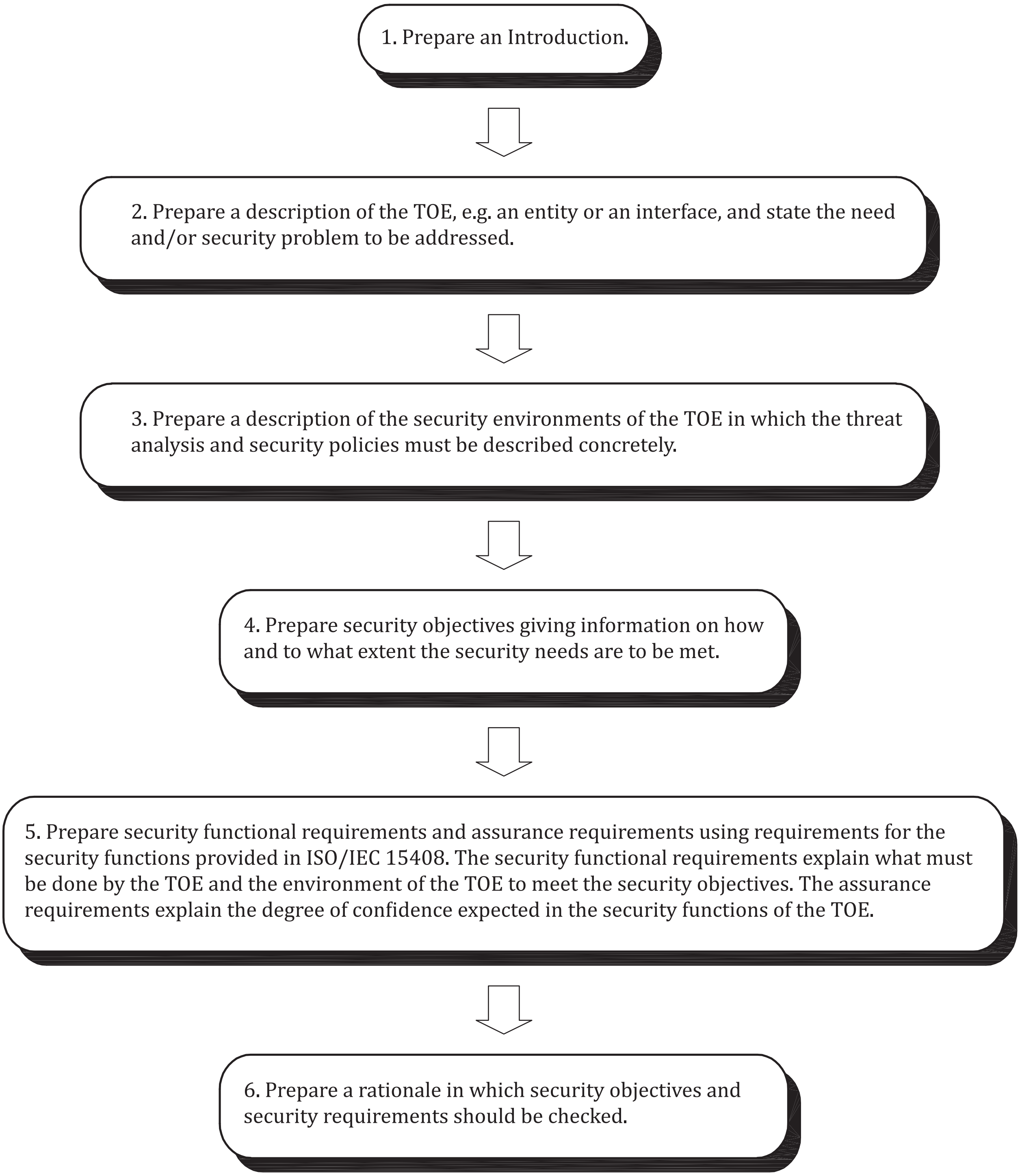
6) Rationale of justification/effectiveness — The contents of the PP is checked when necessary and covers security requirements for TOE. The checked items are shown as follows:

   i) all security environments needed are covered;

   ii) security objectives should completely meet the security environments;

   iii) security requirements should implement security objectives.

The process of preparing a PP is shown in Figure E.2.



1. Prepare an Introduction.

2. Prepare a description of the TOE, e.g. an entity or an interface, and state the need and/or security problem to be addressed.

3. Prepare a description of the security environments of the TOE in which the threat analysis and security policies must be described concretely.

4. Prepare security objectives giving information on how and to what extent the security needs are to be met.

5. Prepare security functional requirements and assurance requirements using requirements for the security functions provided in ISO/IEC 15408. The security functional requirements explain what must be done by the TOE and the environment of the TOE to meet the security objectives. The assurance requirements explain the degree of confidence expected in the security functions of the TOE.

6. Prepare a rationale in which security objectives and security requirements should be checked.

Figure E.2 — PP preparation process

Annex F
(informative)

Media centric management and back-office centric management

F.1 General

An/A Application/Product can be managed either in a media centric or back-office centric way. Any variation or combination between these two approaches can be possible.

In a media centric management, main processes (e.g. fare calculation, billing) of management of Application and Product are done between a Medium and MAD.

In a back-office centric management, main processes of management of Application and/or Product are done in the back-office system.

When Product(s) in an Application is/are under a complete media centric Management, the whole Application and Product(s) should be stored in a Customer Medium (see Figure F.1).

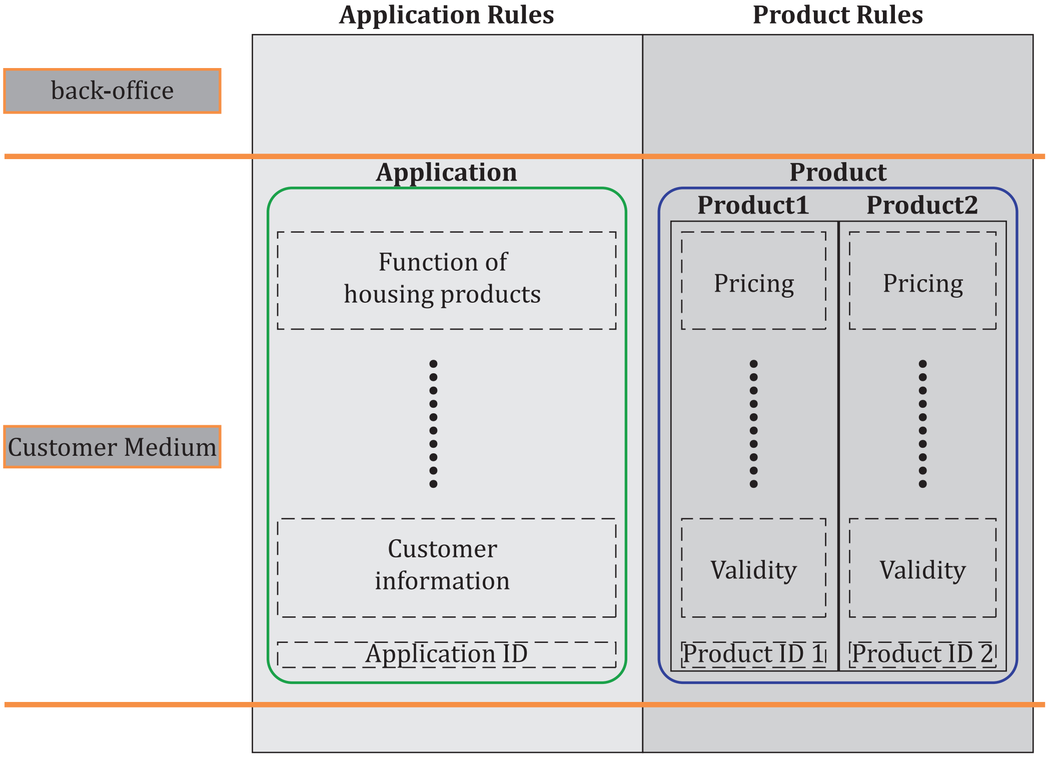
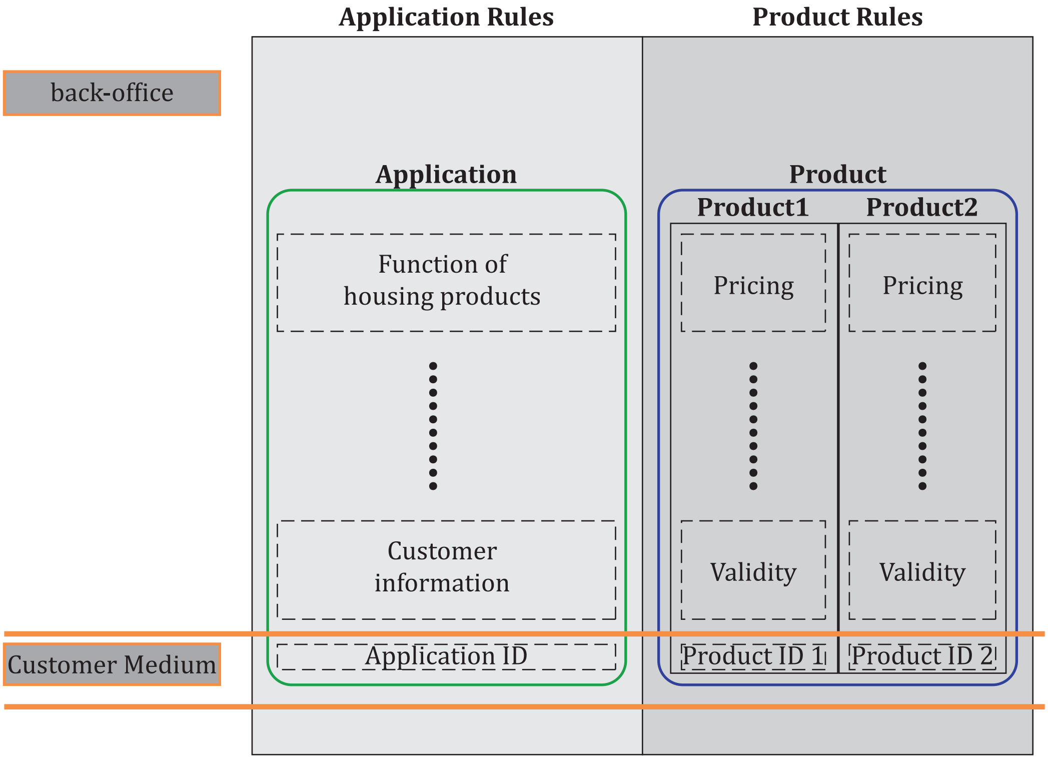


Figure F.1 — Complete media centric management

When all Products in an Application are under a complete back-office centric Management, only Application/Product IDs should be stored in a Customer Medium (see Figure F.2).



NOTE Application ID/ Product ID(s) can be same.

Figure F.2 — Complete back-office centric management

However, in existing Application/Product, various patterns of management can be possible. Depending upon management patterns, ranges of stored Application and Product (s) on a Customer Medium can vary (see Figure F.3).

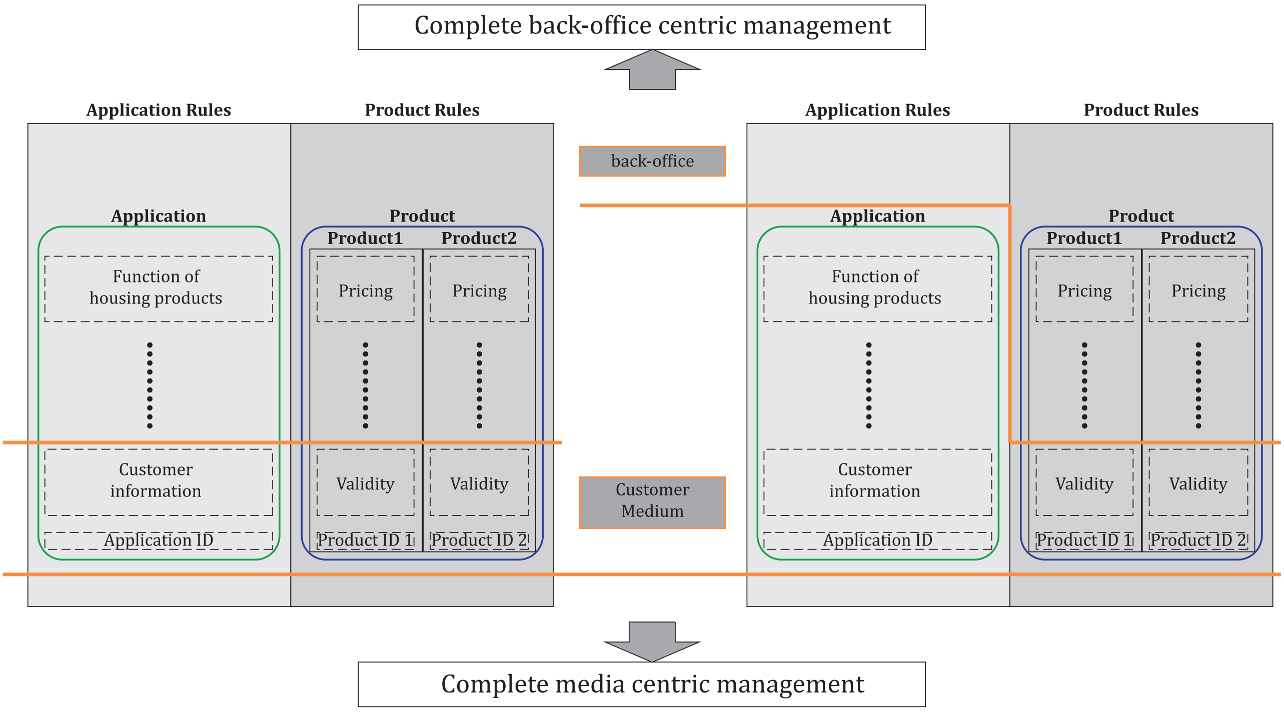


Figure F.3 — Examples of pattern of management

Bibliography

[1] ISO/TS 14904, *Road transport and traffic telematics — Electronic fee collection (EFC) — Interface specification for clearing between operators*

[2] ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

[3] ISO/IEC/TR 15446, *Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets*

[4] ISO/TS 17573, *Road Transport and Traffic Telematics — Electronic Fee Collection (EFC) — Systems architecture for vehicle related transport services*

[5] ITSO TS 1000 (all parts), *Interoperable public transport ticketing using contactless smart customer media*, ISBN 0-9548042, http://www.itso.org.uk

[6] EN 1545 (all parts), *Identification card systems — Surface transport applications*

[7] EN 12896, *Road transport and traffic telematics — Public transport — Reference data model*

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™