

# DRAFT INTERNATIONAL STANDARD

## ISO/DIS 24014-1

ISO/TC 204

Secretariat: ANSI

Voting begins on:  
2020-02-21

Voting terminates on:  
2020-05-15

---

---

## Public transport — Interoperable fare management system —

### Part 1: Architecture

*Transport public — Système de gestion tarifaire interopérable —  
Partie 1: Architecture*

ICS: 35.240.60; 03.220.01

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/469b9a80-a79e-4a0f-a7a3-7ab973d4009d/iso-dis-24014-1>

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

**ISO/CEN PARALLEL PROCESSING**



Reference number  
ISO/DIS 24014-1:2020(E)

© ISO 2020

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/469b9a80-a79e-4a0f-a7a3-7ab973d4009d/iso-dis-24014-1>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Fax: +41 22 749 09 47  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

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

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

## 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](http://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](http://www.iso.org/patents)).

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

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

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

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

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

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

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

## Introduction

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

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

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

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

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

Interoperability also requires the definition of a security scheme to protect privacy, integrity, and confidentiality between the actors to ensure fair and secure data flow within the IFM system (IFMS). The overall architecture is the subject of this part of ISO 24014 which recognizes the need for legal and commercial agreements between members of an IFM, but does not specify their form. The Technical Specifications of the component parts and, particularly, the standards for customer media (e.g. smart cards) are not included.

Note that there is not one single IFM. Individual operators, consortia of operators, public authorities, and private companies can manage and/or participate in IFMSs. An IFM can span country boundaries and can be combined with other IFMSs. Implementations of IFMSs require security and registration functionalities. This part of ISO 24014 allows for the distribution of these functions to enable the coordination/convergence of existing IFMSs to work together.

This part of ISO 24014 intends to provide the following benefits.

- a) It defines a common definition of terms and roles that shall constitute the basis for the other parts of ISO 24014 and technical specifications and technical reports from ISO TC204 which address mobility platforms, fare management and interoperability between IFM and other systems.
- b) It provides a framework for an interoperable fare management implementation with minimum complexity.
- c) It provides guidance on how IFM Managers can benefit from external devices and services and how interoperability and appropriate security level can be established in cooperation with system from other markets.
- d) It aims to shorten the time and lower the cost of IFM procurement as both suppliers and purchasers understand what is being purchased. Procurement against an open standard reduces cost as it avoids the need for expensive bespoke system development and provides for second sourcing.
- e) It aims to simplify interoperability between IFMSs to the benefit of all stakeholders.

In its informative annex, this part of ISO 24014 provides a framework for mobility platforms that integrate fare management and travel information for inter- and multimodal travel.

# Public transport — Interoperable fare management system —

## Part 1: Architecture

### 1 Scope

This part of ISO 24014 provides the basis for the development of multi-operator/multi-service interoperable public surface (including subways) transport Fare Management Systems (IFMSs) on a national and international level.

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

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

The objective of this part of ISO 24014 is to define a reference functional architecture for IFMSs and to identify the requirements that are relevant to ensure interoperability between several actors in the context of the use of electronic tickets.

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

- management of media,
- management of applications,
- management of products,
- security management, and
- certification, registration, and identification.

This part of ISO 24014 defines the following main elements:

- identification of the different set of functions in relation to the overall fare management system and services and media from non-transport systems which interact with fare management systems;
- a generic model of IFMS describing the logical and functional architecture and the interfaces within the system, with other IFMSs and with services and media from non-transport systems;
- use cases describing the interactions and data flows between the different set of functions;
- security requirements.

This part of ISO 24014 excludes consideration of the following:

- the technical aspects of the interface between the medium and the medium access device;
- the data exchanges between the medium and the medium access device;

**NOTE** The data exchanges between the Medium and the Medium Access Device are proposed by other standardization committees.

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

## 2 Terms and definitions

The following terms and definitions apply.

### 2.1

#### **account-based ticketing (ABT)**

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

### 2.2

#### **action list**

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

### 2.3

#### **actor**

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

### 2.4

#### **application rules**

application owner requirements

### 2.5

#### **application specification**

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

### 2.6

#### **application template**

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

### 2.7

#### **application**

implemented and initialised *application template* (2.6)

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

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

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

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

### 2.8

#### **commercial rules**

rules defining the settlement and commission within the IFMS

### 2.9

#### **component**

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



**2.10****component provider**

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

**2.11****customer account**

Data space hosted by the IFMS (typically the product retailer) that contains all information which is relevant for the business relationship between the Customer and the IFMS.

Note 1 to entry: Accounts are maintained and managed by the responsible stakeholder in the IFMS. Accounts which are accessible online can be established and managed by the customer as well.

**2.12****customer medium**

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

**2.13****derived identity (derived ID)**

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

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

**2.14****external**

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

**2.15****identity (ID)**

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

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

**2.16****IFM functional model**

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

**2.17****IFM policies**

commercial, technical, security, and privacy objectives of IFM

**2.18****IFM-role**

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

**2.19****interoperable fare management****IFM**

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

**2.20**

**interoperable fare management system**

**IFMS**

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

**2.21**

**level of assurance**

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

**2.22**

**medium**

physical carrier of *applications* (2.7)

**2.23**

**message**

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

**2.24**

**medium access device**

**MAD**

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

**2.25**

**organization**

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

**2.26**

**pricing rules**

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

**2.27**

**product rules**

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

**2.28**

**product specification**

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

**2.29**

**product template**

technical pattern of the *product specification* (2.28)

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

**2.30**

**product**

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

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

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

**2.31****role**

abstract object performing a set of functions

**2.32****security policy**

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

**2.33****set of rules**

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

**2.34****trigger**

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

**2.35****usage rules**

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

**2.36****use case**

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

**3 Abbreviated terms**

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

**4 Requirements**

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

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

Specific requirements of the IFMS model are as follows.

- A customer shall be able to travel with all participating service operators (the seamless journey) using a single medium.

- There shall be a capability to extract data appropriate to the revenue-sharing and statistical requirements of the service operators.
- The same medium may carry additional applications in addition to the IFM application. Conversely, external media may carry the IFM application.
- The methods associated with the application shall offer the opportunity to reduce the current time taken to enter/exit the public transport system and may reduce payment handling costs significantly.
- The IFMS model shall comply with data protection and financial services laws/regulations (e.g. privacy).
- The IFMS model shall provide the capability to accommodate new product specifications as required regardless of those already in existence.
- The IFMS model shall recognize and prevent internal or external fraud attacks.
- The IFMS model shall facilitate a balance between measures for security and fraud avoidance against the need to offer Customer convenience and performance.
- The IFMS model shall have the capability to identify the Customer while protecting their privacy as appropriate.
- The IFMS model shall ensure the integrity of exchanged data.
- The IFMS model shall enable the implementation of additional services: loyalty programmes, car sharing, park and ride, bike and ride, etc.
- The IFMS model shall provide interface definitions between identified functions within public transport or other modes of transportation to enable different operator networks to interoperate.
- The IFMS model shall describe interfaces which are essential to enable data-forwarding functions between different operator networks allowing revenue-sharing agreements to be met.
- The IFMS model shall provide a framework from which commercial agreements may be developed.
- The IFMS model shall be neutral with regard to different technologies which can be deployed [e.g. contact medium, contactless medium (short range, wide range), external devices, independent of access technologies, account-, cloud- or ID-based concepts].
- The IFMS model shall be functionally neutral regarding specific transport organization structures.
- The IFMS model shall support the introduction and migration to new technologies and architecture concepts and interoperability with media, applications and systems from other market sectors.

## 5 System environment for IFMS

ISO 24014-1 focused so far on interoperability between fare management systems. However, recent trends and market developments require enhancements of the IFMS architecture, interoperability with other PT systems and also interoperability with systems, customer media and applications from other market sectors.

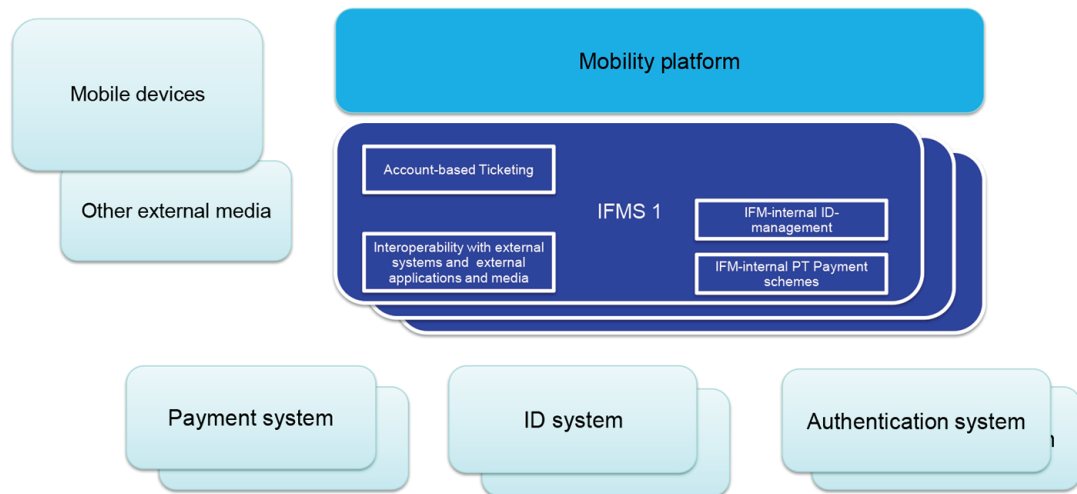


Figure 1 — System environment for IFMS

## 5.1 Mobility platforms

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

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

This edition of ISO 24014-1 documents a possible approach to mobility platforms in the informative part of the specification.

## 6 Conceptual framework for IFMS

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

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

To manage the elements of the IFMS dealt with in this part of ISO 24014, the IFM Manager shall appoint

- a Security Manager, and
- a Registrar.

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

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