Report and recommendation to Cooperative Organisational Models

Deliverable 4.3

April 2010

Grant Agreement number: IST-2007-214787
Project acronym: IFM PROJECT
Project title: INTEROPERABLE FARE MANAGEMENT PROJECT

Funding Scheme: Support Action

Project Coordinator: John Graham Verity
Head of Compliance
ITSO Limited, United Kingdom

Tel: +44 121 634 3700
Fax: +44 121 634 3737
E-mail: compliance@itso.org.uk
Project website address: http://www.ifm-project.eu

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

For further information please contact:

Work package 4 leader

VDV-Kernapplikations GmbH & Co. KG

Elke Fischer (Work package leader)
Phone +49 30 3999322
E-mail: e.fischer@vdv.de

Main authors

VDV-Kernapplikations GmbH & Co. KG

Elke Fischer
Phone +49 30 39993222
Fax +49 221 57979 8222
E-mail: e.fischer@vdv.de

Dr. Joseph Lutgen
Phone +49 221 57979162
Fax +49 221 57979 8162
E-mail: lutgen@vdv.de

For further information on the EU-IFM Project please contact:

Coordination

ITSO Ltd.

Phone +44 121 634 3700
Fax +44 121 634 3737
E-mail: compliance@itso.org.uk

Secretariat

TÜV Rheinland Consulting GmbH

Phone +49 221 806 4252
Fax +49 221 806 3496
E-mail. izaskun.arenaza@de.tuv.com

Visit the webpage www.ifm-project.eu

Version Control

0.5	First draft for internal review.	August 19th, 2009
0.6	Incorporation of the results of the internal review.	August 22nd, 2009
0.7	Revision in preparation for London Workshop	August 28th, 2009
0.71	Revision after London Workshop	September, 2009
0.9	Integration of French Comments	January, 2010
1.0	Integration of French Comments	April, 2010

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Content

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

List of Figures

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

I Introduction

The key stakeholders of the IFM Forum perceive the “Interoperable Fare Management Project” (IFM Project) as a well-suited framework to coordinate their experience and share it with a wider community of beneficiaries in Europe, which constitute the IFM Forum that is organised by the UITP.

The objective is to avoid the establishment of enduring isolated national solutions and to define roadmaps leading the way toward European interoperability.

The IFM Project aims to be a European wide initiative dedicated to the establishment of attractive public transportation with modern fare management, which is safe, reliable and comfortable for both users and operators. Once achieved, this may serve as a model for many further countries outside Europe faced with the need to strengthen the use of public transport.

The “IFM Project” will be the first step of the IFM initiative. The ultimate goal of the IFM Project at the end of the project is a European-wide agreed concept (Road Map) developing shared back-office rules if cross-border data exchange is needed and the associated European security requirements necessary to achieve cross-border data exchange. It will create a documented framework by 2010 to deliver the requirements for secure, fully interoperable portable object for seamless mobility on public transport accessible to all European Citizens. In a second step comprising Research and Technological Development (RTD) and field operational tests, a European interoperable fare management standard will be developed and implemented.

The objective of the “Interoperable Fare Management Project” (IFM Project) is to provide traveller easy access to travel throughout Europe. Customers should be able to benefit from their status as European Residents, allowing them to use public transport easy and well appointed - as they did accustomed at home - all across Europe.

The goal is to create Interoperable Electronic Fare Management in Europe for that, which permits customers in public transport to travel barrier-free and without ticket limits "door to door".

A first step therefore is done in different European regions with the launch of interoperable-shared styles of contact-less media in regional electronic fare management systems. These media can be used for multiple transport products in different public transport companies and authorities.

An inventory of existing electronic fare management systems in Europe [R3] and the analysis of functions, organisational models and economic issues [R4] have shown that in all of the analysed European systems exist specific National Standards for IFM/EFM. So a good common basis for a migration to an European IFM is given.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

The titles of the corresponding country specific National Standards are:

- INTERCODE; ref. AFNOR NF P99-405 (France) /INTERBOB,
- VDV-Kernapplikation/VDV Core Application for Interoperable Electronic Fare management - (((eTicket Deutschland (Germany)
- Open ticketing Standard (SDOA, Open architecture) for Trans Link Systems (The Netherlands)
- No official title - set of “Regional specifications so called „OTLIS LisboaViva Specification“ (Lisbon wide Region)
- RFK-specification (Sweden)
- ITSO (United Kingdom of Great Britain and Northern Ireland)

The National Standards encompass also data exchange interfaces between reference systems of various roles in France, Germany, the Netherlands, Portugal/Lisbon, Sweden and the UK. National Standards for data exchange interfaces in the different EFM systems of the EFM participants, independent of their roles in the EFM system, exist within INTERBOB, ref AFNOR FD-P 99503VDV Core Application, TLS, Resekortet and ITSO, but not within OTLIS LisboaViva Specification (although it follows standards such as ISO-14904, INTERCODE, EN-1545, etc, to build a data exchange specification).

The basis for all of the various systems is more or less the common IFM System Architecture described in the standard ISO EN 24014-1 ([R1] and Figure1). So this is also the basis for the EU-IFM Organisation Model.

Based on the results of the analysis, of the visions of the working systems and particularly of the results of WP 1 [R5] and WP 3 [R6] cooperative Organisational Models (OMs) for the European IFM area will be described in this report.

Essential for the establishment of interoperability is to use the same customer medium in all EFM systems and guarantee the security, which is required for the connected systems. Necessary organisational units and related rules and procedures of the cooperative OMs will be identified in this report. It is observed that the efficiency of the systems is ensured.

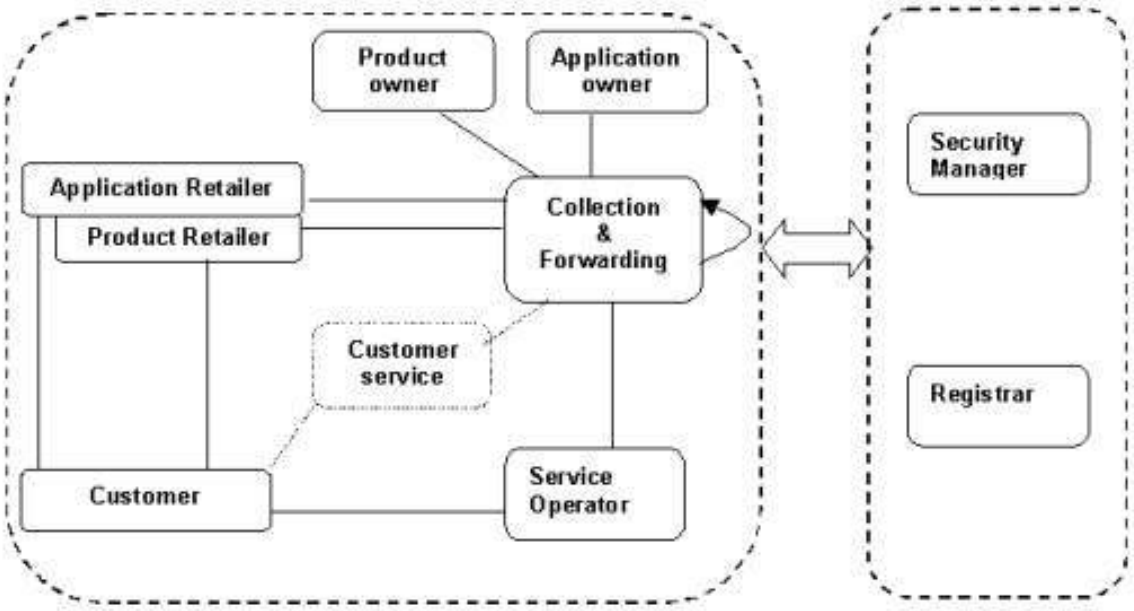


Figure 1 — The two IFM organisational domains (operational and management Entities)[1]

[1] Source: ISO/EN 24014-1:2005

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

II List of abbreviations

AFC	Automated Fare Collection
CALYPSO	Electronic Ticketing Standard for (microprocessor) contactless Smartcard, designed by a group of European transit operators
CBO	Central Back Office
CRL	Certificate Revocation Lists
EFM	Electronic Fare Management (local/regional/national)
EN	European Norm
GPRS	General Packet Radio Service
HOPS	ITSO Back office system
HSM	Cryptographic "Hardware Security Module“ it is the secure central element of the Security Management System that generates (and holds) the key pairs and certificates.
EU-IFM	Interoperable Fare Management (European)
EU-IFMSG	Common EU-IFM Steering Group
IFMS	IFM system
ISO	International Organization of Standardization
ITSO	Integrated Transport Smartcard Organisation; UK Standard for nationwide Interoperable Electronic Fare Management
MO	Mobile operators
PT	Public transport
OTLIS	Consortium of Operators that Specify, Build and Operate the Interoperable Fare Collection System which manages the LisboaViva, 7 Colinas, Viva Viagem and Lisboa Card contactless cards (Lisbon wide Region)
OM	Organisational Model
PC	Personal Computer
PTO	Public transport operator
RKF	Resekortsföreningen i Norden ekonomisk förening, from January 2007 it is Resekortet i Norden AB

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

SAM	Secure Application Module
SIM	Subscriber Identity Module
SE	Secure Element
SM	Security Management Service/Trust Centre (Issuing media certificates)
TA	Transport Authority
TO	Transport operator
UMTS	Universal Mobile Telecommunications System
UICC	Universal Integrated Circuit Card
UMTS	
USIM	Universal Subscriber Identity Module
VDV-KA	VDV Core Application, German Standard for nationwide Interoperable Electronic Fare Management
VDV-KA KG	VDV-Kernapplikations GmbH & Co. KG

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

III Reference documents

[R1] ISO/EN24014-1: 2007 - Public transport - Interoperable fare management system - Part 1: Architecture (IFMS)

[R2] ISO/PrEN 24014-2: [Working draft] -Public Transport - Interoperable Fare Management System - Part 2: Recommended Working draft]

[R3] EU-IFM Project - Inventory of functions, organisational models and economic issues of existing IFM-Systems, Deliverable 4.1 - March 2009

[R4] EU-IFM Project – Report on the organisational structures and the differences of the existing IFM systems, Deliverable 4.2 - March 2009

[R5] EU-IFM Project – Report on the follow-up workshop to explain and disseminate the agreed Common Methodology for preparing a Trust Management Model, Deliverable 1.3 - August 2009

[R6] EU-IFM Project – Common requirements and recommendations on interoperable media and multi-application management, Deliverable 3.2, Version 2.4 - September 2009

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

IV Organisational Model

IV.1 Objective

Interoperability in Public Transport (PT) has to guarantee a continuous journey with different means of transportation of different transport operators between different regions as well as punctual single travels into Electronic Fare Management (EFM) systems of contractually merged transport operators.

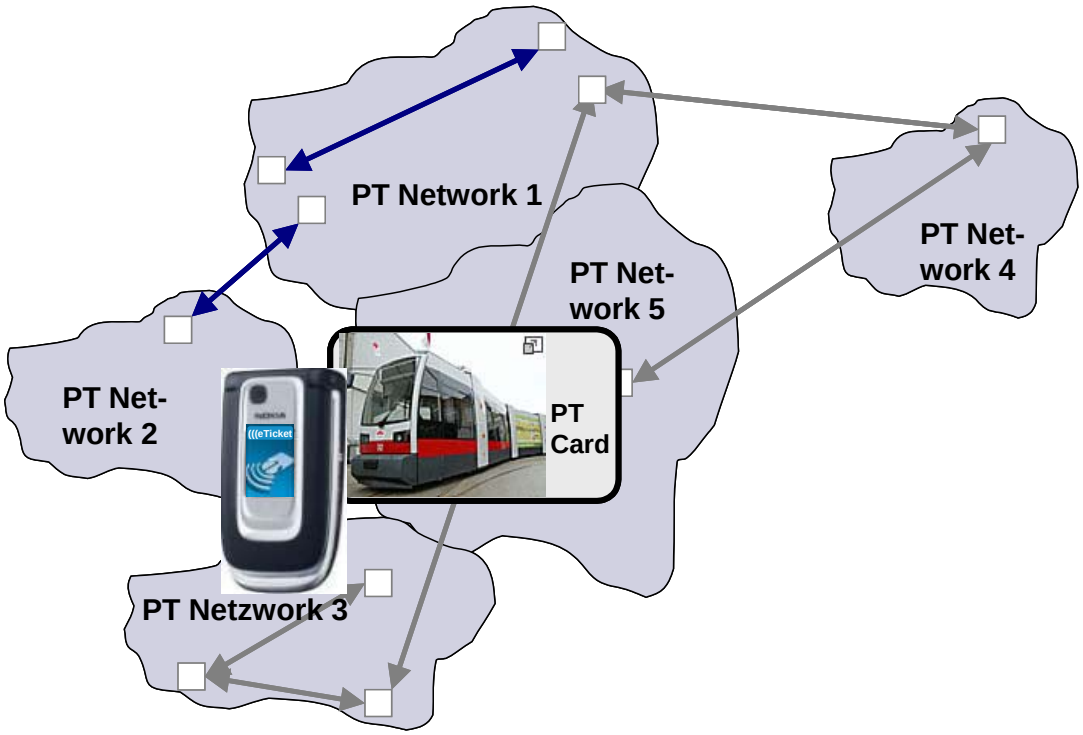


Figure 2 — Interoperability in Public Transport (PT)

As the result of WP 4.2, 7 migration steps of EU-IFM have been developed to get a full interoperable fare management in Europe:
From the organisational point of view, that leads to six scenarios :

- Scenario 0 (Status Quo): Interoperability can be only achieved by mutual agreements between EFM schemes to accept each other's media
- Scenario 1 (EU IFM Media): EU IFM media are issued and customers can download the EFM applications they need as they move.
- Scenario 2 (EU IFM Application): A common EU-Application is defined. The customer can have this application downloaded in his media. Customer profile and EFM products can be loaded into the EU-Application..
- Scenario 3 (EU Web Portal):. Customers will find a common European web-portal from where to download the applications and products they need

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

- Scenario 4. (EU Product); Some common products (EU products) are proposed and hosted in the EU-Application.
- Scenario 5. (Phase out of EFM applications and products): European IFMs use only the EU Application with EU product templates.

The Scenarios can be used to define the necessary organisation models based on the ISO 24014-1 [R1].
This document will define common Organisational Models safeguarding existing national organisations and key regional or city implementations, therefore within the relevant European Standards.
Possible migration paths to and between these cooperative OMs will be identified and determined.

Of course they have to take into account different requirements and different criteria for implementation from the perspective of the customers and the PT companies that provide the service:

- PT companies and authorities need efficiency, costs, independence from other companies, …
- Customers wish comfort, easy access, no searching for the right Ticket, to have all necessary tickets before start of trip, …

Goals are

- to specify an interoperable EU-IFM from the organisation point of view

and

- to define the requirements for these new Organisational Models based on needs of the components of the Fare Management system particularly customer media, trust model and back office system.

Therefore the following conditions must be observed:

- The ISO 24014-1 role model is the basis and can be used in every IFM-System.
- Migration steps should be found, which allow to use interoperable ticketing in different convenience for the EU citizens taking account of the large differences in the technical implementation of EFM systems based on the national standards.
- Bodies, which will decide on migration options, are the existent authorities as they already are in the different Member States..
- The burden on the participating companies at EU-IFM must be acceptable.

Based on the results of WP 3 [R6] is to note:

- The interoperable customer medium is a device able to host several transport applications on demand of the customer from distinct IFM schemes.
- At a longer term, a nucleus EU IFM application will need to be standardised to host EU citizen status, to offer a common template for hosting local products and to ultimately host common products.

- Finally, it will be possible to replace multiple transport applications from separate IFM schemes by a single EU-application on customer media, which all EU citizens can acquire and use.

Based on the results of WP 1 [R5] is to note:

1. The security model of the EU-IFM must ensure that:
    - EU-IFM stakeholders trust that the customers will adopt EU-IFM.
    - Customers trust that EU-IFM system delivers what it claims.

2. Two time periods must be considered for the EU-IFM Trust Model and also for the Organisation Model:
    - The present time, when interoperability of the public transport products do not yet have a prominent presence in the focus of EU residents.
    - The future, when multi-application cards are the norm (possibly owned by the customer), and global markets and operations are also the norm.

Acceptance and customer satisfaction must be ensured.

Under these conditions, the following basic scenarios for migration to an European IFM are identified and agreed within the EU-IFM project participants.

IV.2 Basic Scenarios for Migration to an European IFM

IV.2.1 Scenario 0 (Status Quo)

Scenario 0 represents the current status of EFM systems as reflected in the analysis in accordance with WP 4.1 and 4.2 [R3][R4].
The customer uses the Medium with the PT application he needs in the EFM system, where he is. He owns and uses several media and several applications if necessary.
Even in this scenario it is possible, that EFM system operators from different regions agree a common standard across country borders and that EFM participants agree sharing some components of the system. Also this scenario (0b) is making a first step towards EU interoperability and should be considered further.
Therefore, the following existing conditions are identified and to consider:

Current technical conditions:

- Contactless micro-processor media with IS0/IEC 14443 Interface is partially used.
- The use of customer media with crypto-co-processors remains an exception.
- Applications are issued with the media.
- Application download initiated by the customer is not possible in the regular.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

- Security relates to the used medium/application, application-specific requirements and security methods are implemented.
- The overall system safety is based on application-specific rules.

Current organisational conditions:

- System specifications are available by the central organisations.
- Central security management and registration functions are partially used.
- The financing of the central organization units is handled differently, and has strict limits.
- Certification of components is not a rule for every installed application.
- The rules of participation are very different.

Interoperability between the different national systems can be achieved if system participants accept each other's media with the relevant PT application. Mutual agreements have to be contracted between the system participants (see Figure 3). This is already a part of interoperability within EFM systems in Europe. This development should be pursued and supported also in the EU further, because the desired "door to door" travel with one customer medium from customers view is met. So is an essential requirement for an EU-IFM from the customer perspective fulfilled.

Scenario 0 is now a reality in Europe.
The conditions for the implementation of Scenario 0b "Interoperability between the different national systems" are given. The necessary conditions will need bilateral agreements.

IV.2.2 Scenario 1: Download of existing PT- Applications on EU IFM media

Scenario 1 means that EFM operators in European countries agree to use multi application and interoperable media (so called EU IFM media) issued to customers. This can include media issued by non transport stakeholders.
Customers can download the local existing applications they need onto such EU IFM media as they move.
Common requirements for application downloads and for interoperable media have been specified based on Global Platform specifications in [R6].
The customer uses an EU IFM compatible Medium with the PT application he needs in his home region EFM system. He has received the medium from a Medium Retailer and the application from an Application Retailer. With this PT application the customer can acquire local EFM products. He is contracted with every EFM organizations he needs products from. This gives him access to the public transport networks (to travel) operated by Service Operator. This fully continues the scenario 0.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

In addition, the customer may download other PT-applications into his EU IFM medium, when he travels to other regions or countries. The SE Owner of the medium has ensured the conditions for that with all participating EFM PT Application Owners.

There are different ways to implement the download of the foreign PT application:

1. Customers get the foreign PT application in his home EFM from a local channel (scenario 1a).
2. Customers get the foreign PT application, when he is arrived in the foreign EFM from a local channel (scenario 1b)...
   Every EFM must provide its own application to download at its terminals.
3. Customers get the foreign PT application over the web. A EU roaming Web-portal routes the requests to download EFM PT applications to the web portal of the corresponding EFM scheme (scenario 1c).
   This variant requires the implementation of Scenario 3 (see also Chap. IV.2.4).
4. Customer gets the foreign PT application over the web. A common EU Web-Portal is available and allows directly the download of the EFM PT (scenario 1d).
   This variant requires the implementation of Scenario 3 (see also Chap. IV.2.4).

The following preconditions are to be considered and to meet.

Technical Preconditions:

- Contactless media with IS0/IEC 14443 A **or** B interface is used and fulfils the requirements defined by the EU-IFM organisation (Storage Capacity, performance, OS witch support the download, security evaluation in accordance with EFM-application specifications).
- Application download onto an EU IFM media is specified for PT-applications from every EFM . Application download process is standard & the same for all PT application
- Security and trust requirements for EU IFM media are defined and agreed by the SE Owner and by the EFM PT application owners.
- All EU IFM media must have the ability to support the download of all applications and associated security components (such as keys and certificates)
- Each EFM organisation is providing a web site and/or local channels from where its local application can be downloaded into the visitor's EU IFM media (see also Chap. IV.2.4).
- At least one EU Web-portal must be established and connected with all EFM web sites and/or local channels from where its local application can be downloaded into the visitor's customer media (see also Chap. IV.2.4).
- Media readers have to support ISO/IEC 14443-A **and** B interfaces.
- Only the customer (portable object owner) is allowed to give order to delete a downloaded application

Organisational preconditions:

- EFM Application Owners and SE Owners agreed, that the download of PT application is allowed (see Chap 0).
- It is defined, where the download is possible for every EFM (internet web site, mobile internet web site, service desks and vending machines all or only on special places …).
- The usage and the way of interacting with EU Web-portals are agreed between all participant parties in case of scenario 1c and 1d.
- It is defined where and how the download is possible by the customer (the best for the customer before start of the trip at home, not so likely after arrival in the other country, in the other EFM system).
- Customer service and customer information are attuned between SE Owners and EFM applications owners and available in every participating EFM system.

A first step of interoperability between the different national systems may be realised with this scenario within the EU countries. So this scenario may represent the migration step 1 towards an EU-IFM in Europe.
But in case of the use of Web-solutions it is necessary that the media can use Internet over a Home PC Reader or over a UMTS/GPRS connection.

In this scenario a fist level of an EU-IFM organisation model will be required.

IV.2.3 Scenario 2: Definition of an EU-Application with common Product Template

Scenario 2 contents that an EU-PT application with a common product template has been defined by an EU-Application Owner. Also all necessary Terms of Use.
The customer still uses the EU IFM Medium with the PT application he needs in his home country EFM system (see Chap. IV.2.2).
The customer is able to download the additional EU-application on his medium, which contains the common EU product template.
Application Retailers [2] are able to retail the EU application to the customer medium besides the home PT application of the customer.
The SE owner has ensured the conditions for that with the EU-Application Owner.

The home Application Retailer of the customer will export the customer data profile from local application and products into this EU-Application according to the common EU product template.

[2] May be all retailers who retail the local applications or only some of them or only one of them which is doing that for all participating systems

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

All participating Product Owners are authorised to use the EU product template to retail the products giving access to their networks.

Also in this scenario 2, there are different ways to implement an EU application download:

1. The customer gets the EU-application, when he is in his home EFM or when he arrives in the foreign EFM from local channels (scenario 2a). Every EFM must provide the EU-application to download at its terminals.

2. The customer gets the EU-application over an EU- roaming Web-Portal. According to the EFM products selected by the customer, the request is routed to the corresponding EFM Web Portal. He downloads the EU application from an EU Application Retailer and local products from the local EFM Product Retailer from the local EFM web portal (scenario 2b).
   This variant requires the implementation of Scenario 3 (see also Chap. IV.2.4).

3. The customer gets the EU-application and national products from participating product owners over a common EU-Web-Portal. He downloads the EU application from an EU Application Retailer and local products from the local EFM Product Retailer from the common EU IFM web portal within the EU product template. (Scenario 2c).
   This variant requires the implementation of Scenario 3 (see also Chap. IV.2.4).

The following preconditions are to be considered and to meet.

Technical Preconditions:
In addition to the conditions defined for scenario 1:

- EU-Application specifications must comply with the specifications agreed in scenario 1 (performance, OS, download process).
- Security and trust requirements for EU IFM media are defined and agreed between the SE Owner and every EFM PT application owners.
- There are EFM terminals and/or web retailers that are technically equipped so that they support the EU-Application download
- For the EU-application download, shared security conditions have to be defined by the EU application owner and must be supported by each EU Application Retailer.
- EU-application download process is technically and organisationally supported and so possible for the customer
- The usage and the way of interacting with EU Web-portal are agreed between all participant parties in case of scenario 2b and 2c.
- EU-application template is available for local products and local product can use it technically
- EFM terminals are technically equipped so that they accept EU-application and products within the common product template

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Organisational preconditions:
In addition to the conditions defined for scenario 1:

- It is defined, how the download of the EU-IFM application is possible by the customer
- Products are defined by the Product Owners in the local EFMs
- Customer service and customer information are attuned between SE Owners and EU or EFM application owners and available in every participating EFM system.

Interoperability is given to the customer. Different local systems can handle with the medium of the foreign customer.
The customer can The customer can charge at least one product, which he can use outside his home EFM and take benefit from the relevant data (e.g. his age) outside his home EFM.
He can load local products for foreign use, where available, without the need of downloading the local application.
In case of the use of Web-solutions it is necessary that the media can use Internet over a Home PC Reader or over a UMTS/GPRS connection.

This scenario represents the first step towards borderless public transport in Europe.
The level of an EU-IFM organisation model will be increased further.

IV.2.4 Scenario 3: Additional EU-Application retailed from a common EU Web-Portal

Customers will find a common European WEB-Portal to download the EU-application and local products they need in it.

This is an extension of the scenarios 1c, 1d, 2b and 2c in addition to the download of local applications and local products.

The customer can use the Web-portal to acquire the EU-application and the needed products for the first travel outside his home EFM system.

Preconditions are identically with scenario 2. The EFM terminals in the field must not support the application download respectively only selected terminals in service stations are doing this for the national/regional applications. Additional preconditions are:

Technical Preconditions:

- Web application download procedure is specified
- Web-portal must be established
- Web application and product download procedure are specified in the EFMs

- Web customer service is available
- Web-portal is available to access to the national IFM to download the PT- Application and products into the application
- Media readers supporting ISO/IEC 14443-A **and** B interfaces have be available to use at the Home PC (it is necessary that the media can use Internet over a Home PC Reader)
- Mobile phones with NFC interface and UICC with agreed secure element are available and can be purchased by the customer (it is necessary that the media can use Internet over UMTS or GPRS)

Organisational Preconditions:

- The Web-portal is agreed between all participant parties
- Web customer service is agreed between all participant parties
- Agreements with the SE Owners to use their Secure Element are available under reasonable and non-discriminatory conditions

This scenario is very similar for download from the EFM-PT applications. Instead of the EU application, the desired national or regional application has to be downloaded.
The relevant pre-conditions are also very similar. Scenario 3 therefore is considered in the following both for the downloading of national/regional as well as the EU-application.

Interoperability is given to the customer. The access will be very easy and comfortable. He can get the products he wants before travelling.
Different national systems can handle with the medium of the foreign customer.
The extensive deployment to distribute the downloads at many terminals in the field of every EFM system is not necessary. But it is necessary that the all media can be used within Internet over a Home PC Reader or UMTS or GPRS.

This scenario represents an extensive approach to EU-IFM in public transport of Europe.
The level of an EU-IFM organisation model will be not much larger than in scenario 2.

IV.2.5 Scenario 4: EU-Application is issued by an EU-Application Owner on every PT-Medium, some EU-Products are available

Customers use the EU-application for their occasional trips in public transport. Some common interoperable products agreed between different EFM systems and defined from EU Product Owners, issued by local Product Retailers (including interoperable entitlements for automatic fare calculation) are hosted in the EU-Application.

This Scenario differs to Scenario 3 only by the available products.
Until now, EU-products were local products hosted in the EU-application.

Now the first EU-IFM products are defined. They include products from the three main families: tickets, Stored Value and termed contracts.
The EU-IFM products can be accepted throughout the EU but their usage will remain restricted to the geographical area defined for that product (example: origin/destination ticket, monthly contract for a given zone …).
The Product Owners in the national/regional EFMs will become EU-Product Owner for their local products.

EU-product owners propose EU IFM products that can be accepted in any EU IFM network.
It would be handy for them to exist on both "pre" and "post" paid, and in either fashion should be able to be linked to PT Accounts. Of even greater worth could be the fact to organize a provision allowing the customer to pay at home to a local partner of the EU - IFM, when that is feasible under the "Payment Service Directive" and when the settlement cost can be afforded:
Settlement takes place between the Service Operators involved in the trip, and the Product Retailer (Customer Contract Partner) supported by the Product Owner based on the product definition.
A settlement and liability scheme must be set up and defined between all the participants, and addressing more particularly the case of fraudulent usage of the EU IFM products (lost & stolen case), of non customer payment in case of post paid products …

EU-IFM store value based products would make Check-in/Check-out possible with automatic fare calculation without the need to get a payment product for PT abroad.

Preconditions are identical with scenario 3. Additional preconditions are

Technical Preconditions:

- IFM EU-products are defined and available to issue by the Customer Contract Partner (EU Product Retailer) the customer has chosen

Organisational Preconditions:

- EU Product Owners are there these are the existing EFM product owners and a new EU-IFM product owner to be defined.
- EU-IFM products are supported by the participants of EU-IFM
- The back office interconnection is set up between all the EU IFM product owner/retailers and the settlement of the products is agreed with all European participant parties
- Liability rules must be defined and agreed between all EU IFM product owners and retailers
- An EU wide blacklist process must be set up among all the EU IFM schemes.

The IFM organisation level has been achieved. The national and local systems guarantee the migration to EU IFM by developing their systems towards the EU system and support the issue of the EU-IFM application..

IV.2.6 Scenario 5: EU-Application is issued by an EU-Application Owner on every PT-Medium, all products are available in this EU-Application

European Customer uses the one and only EU-Application with EU-Product templates and common EU-Products within the EU IFM. For the customer, nothing changes compared to scenario 4.
But every EU Customer get and may use a common EU-Products to take part in automatic fare calculation or to buy electronic tickets with them.

Preconditions are identically with scenario 4. Additional preconditions are:

Technical Preconditions:

- All the regional/national products must be translated into EU products
- Phase out of local applications and products is achieved by all EU IFM participants including the migration of all the current existing local product still owned by the customers.

Organisational Preconditions:

- The sales of local product are ended with all the retailers.
- All the previous EU IFM organisational preconditions defined up to scenario 4 must remain the only valid ones.

The national/regional EFM are fully integrated in the EU IFM, so that their own central organisations fully have been convicted into the EU's organisation.

IV.2.7 Scenarios from status Quo EFM to an EU-IFM - Overview

In Figure 3 is shown, that already common scheme rules are required and needed between the described scenarios:

- Cross acceptance needs Set of Rules between the acceptance partners

- To form interoperability in existing EFM systems by merging an application and products is very similar to define common product templates in a joint application.

- Already with the agreement of applications in multi-application media related agreements are necessary between Media Owner, Media Retailer and Application Owners within a set of rules, statutes and contracts.

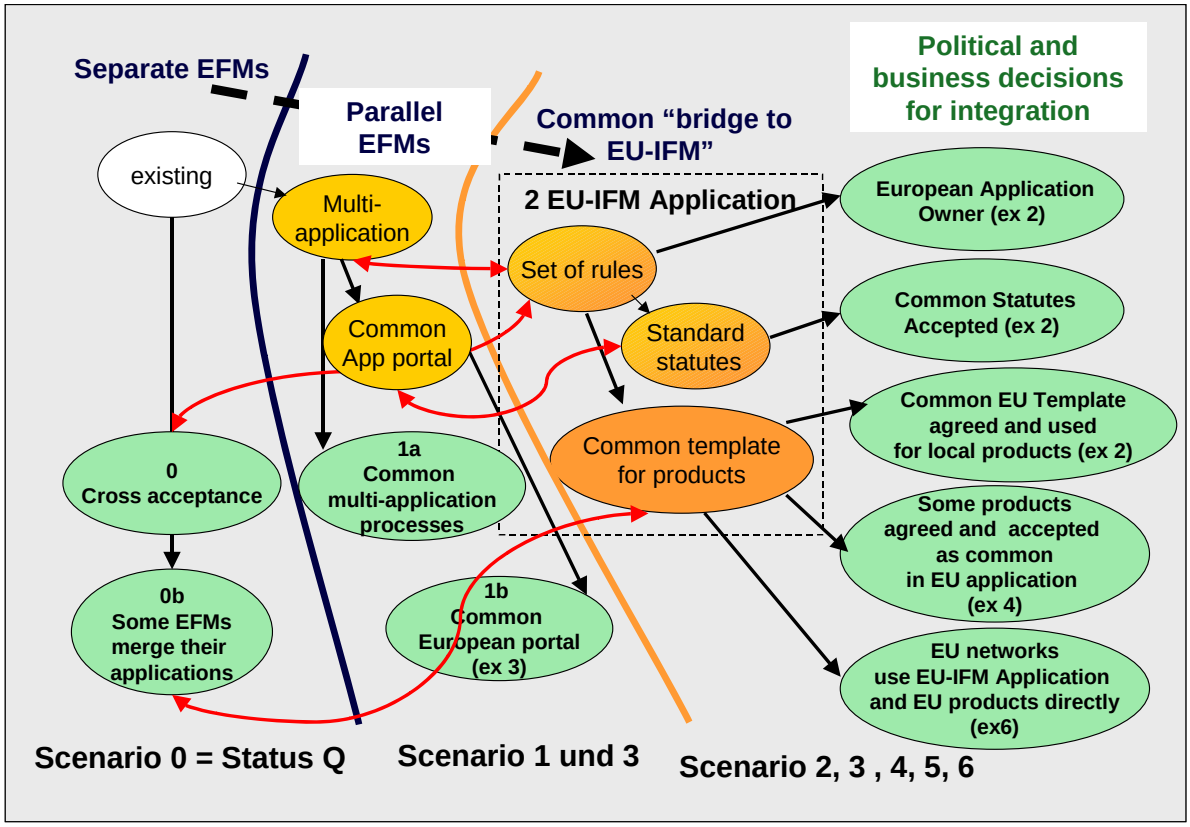


Figure 3 — Scenarios from status Quo EFM to an EU-IFM - Overview

Because of that, it is to be expected that the organisation levels elaborated based on the scenarios (see Chap. IV.2) in some points may differ only slightly, but, for some steps, EU wide agreement and support from the political and business stakeholders will be absolutely required. So the transitions and the migration opportunities between them should largely differ according to the importance that must be given to a EU IFM organisation and to the operational impacts on each EFM scheme.

IV.3 Organisation Levels and Organisational Solution for IFM

IV.3.1 General

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

In WP 4.1 [R3] and WP 4.2 [R4] are shown that the IFM roles model of the ISO/EN Standard [R1] can be applied to all analysed EFM systems and national standards in Europe.
It has to be used as the basis for an EU IFM organisational solution. Uses cases are defined for the functional roles within the standard, which are performed by the organisational unit or units (usually a transport company, a transport authority or a contracted partner enterprise in the IFMS).

Therefore, the role model is used as the basis for the presentation of the to be realised organisational levels regarding the interoperability scenarios for EU-IFM in this chapter. Each role is presented by one or more organisational units (companies), which have to exercise the role in the current context or the future one.

But in addition to the currently well-defined roles for IFM, new actors have to be integrated in the EU-IFM organisation (see also [R2] and [R6]). These are

Media Owner:

- Owner of the user multi-application media
- Releases his media for the use with different applications
- Releases his media for the use of one or more secure elements by Secure Element Owners

Media Retailer:

- Issuer of the user Multi-application media to a customer
- Issues the Secure Element with the medium in conjunction with a Secure Element Retailer
- Is holding the customer contract to the customer in relation to the medium

Secure Element Owner(SE Owner):

- Defines the specifications and design of the SE, complying with the requirements of the SE Security Manager
- Authorises the Application Retailer to access, load and update applications on the SE.

Secure Element Retailer (SE Retailer):

- Provides Secure Element to customers and the related customer service
- Guarantees to customer the compliance of the SE to the requirements set by SE security manager

Secure Element Loader (SE Loader):

- Is required by the Application Retailer to operate loading / deletion / updating of applications in the SE as authorised by SE owner and by Application Owner
- Manages customer's directives as authorised by SE owner and Application owner if conflicts appear when loading/updating an application (e.g. overflow of SE's capacity, conflicting applications, …)

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Controlling Authority:

- Is a trusted third party both for the SE Owner and for the Application Owner
- Enables application code and personalization data confidentiality for Application Owner/Provider towards SE Owner during post issuance loading and personalization of application

The defined roles Security Manager and Registrar [R1] will be occupied for the EU-IFM separately and additionally to the organisations witch fulfil this role in the national or regional EFM system:

EU-Security Manager:

- Specifies security requirements that apply to accepted media for all PT applications and the Secure Elements used for the download process
- Certifies the SE and provides means of authentication

EU-Registrar:

- Registers the SE Owners, the authorised media and secure elements and the participating Application Owners with their PT-applications as well as the participating Application Retailers
- Is responsible for the administration of the participation contracts
- Accredits EU-IFM participants after signing the participation contract

In the following organizational levels will be defined and described on the basis of the advanced role model and the scenarios 1 to 6 to propose the relevant cooperative organisational models.

The analysis has shown, that Scenario 0 became reality in Europe now.
The conditions for the implementation of Scenario 0b “Interoperability between the different national systems” are given. The necessary conditions will need bilateral agreements. Therefore Scenario 0b will not be considered as reasonable EU wide IFM organisational solution in this document (see also Chap. IV.4)!

IV.3.2 Level1 Organisational Solution for Downloading existing PT-Applications

Level 1 organisation is corresponding with Scenario 1.

The shared use of a standard for downloading applications in a first step must be prepared and organised in the form of SE/customer media usage agreements, descriptions of the agreed processes and the individual requirements of the different participants, especially with regard to security. This will be the beginning of a shared security management, which will ensure and monitor the integration of various security processes of the various media

applications in such a first step. The relevant EU-IFM compliant SEs/customer media and PT applications must be registered and released for all IFM participants.

This first migration step for an interoperable ticketing organisation can use the ISO/EN 21014-1 Role Model and create an organisational and contractual basis for such a common and shared Security Management and Registration for the application download to the customer medium.

On this basis it would be possible to permit the download of the different local PT-applications on multi-application customer media in a first joint EU-IFM phase.

Each SE owner shall decide in consultation with the Application Owner, which loads its application to the SE about a Controlling Authority. If in future different SE owners download applications on its SE, also several Controlling Authorities will be involved.

At the download desks (terminals) different relations and download use cases to bring PT-application on the media have to be agreed and will been used.

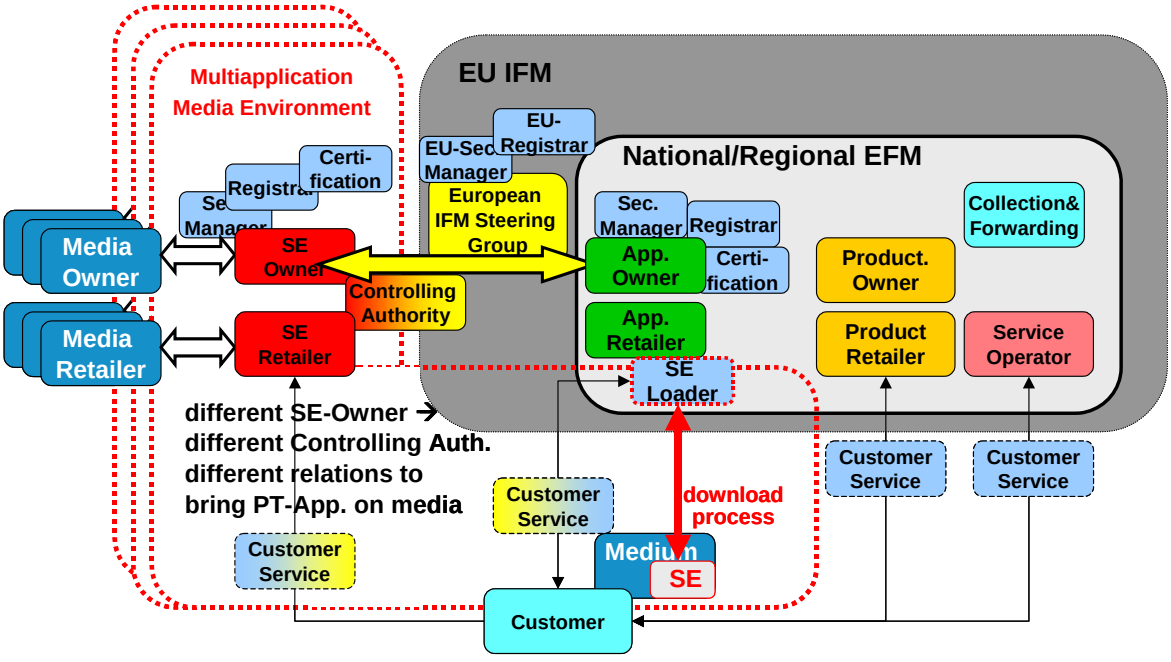


Figure 4 — IFM Roles for related IFM organisations within a Level 1 IFM

Each PT-Application Owner has to deal with each SE Owner and each Control Authority. Therefore it will be necessary to centrally organise

- activities towards the SE Owners
- uniform processes and safety conditions to be negotiated for download for all PT Application Owners within Europe.

An European IFM steering group aims to provide this by creating:

- EU Security Manager role:
  The role of the EU Security Manager is to set up a certification process to allow each PT application owner to identify SE compliant with EU-IFM media requirements stated in [R6]. This role will be quite simple as this level, as all the Security requirements identified for the media are based on existing Java Card, NFC, ISO/IEC 14443 and GlobalPlatform standard and should rely on cross industry existing certification process.

- EU Registrar role:
  The maintenance of a registration list of all the known EU-IFM compliant SEs. Each SE owner remains free to select a Controlling Authority of its choice as well as every PT Application Owner. One ore more joint Control Authority can be authorised as EU-IFM participants in accordance with Global Platform role model.

- The EU Security Management has to ensure, that the safety level of each national/regional application is not jeopardized.
  That means an agreement about security management under a decentralised responsibility of the stakeholders is to organize.

Customer Service for the media issuer and for the PT-Application Owners will be specified uniformly for the relevant GP processes to dominate this. Further organisation of the system remains within it.

During the download Process the security components of the PT-application have to be requested and issued during the download by the EFM Security Manger.

Customer services have to be capable to support the application download procedure.

IV.3.3 Level 2 Organisational Solution for Issuing an Additional EU-Application with Common Template for Products

Level 2 organisation is corresponding with Scenario 2.

Second Level will be the additional issuing of an EU-application. It will be issued within every associated EFM-System. Conditions for acceptable media must be agreed. Authentication of the EU-Template and encryption of personal data are needed (Data Protection!!!), therefore this will require to share EU application keys between all stakeholders (at least EU Application Owner and the EU Application and Product retailers) in addition to the secure link

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

set up between the application download and personalisation server and the customer media already described in [R6] for local application download.

Additional to level 1 therefore will be needed the roles of EU-Application Owner and EU-Application Retailer (see Figure 5).
The role of Application Retailer could be taken over by all or selected national Application Retailers (see Figure 6).
Each EFM Scheme should have the choice to propose the EU application download via its own retailers (which may handle both EFM PT applications and EU IFM PT Applications download) or to rely on a dedicated EU IFM retailer for handling the EU IFM PT application download.

The physical development of a common Security Management and a common Registrar making possible the joint use of security components (keys, certificates, Hardware SAMs) by the EU-IFM participants to support the EU-Application issued by an EU-Application Owner (e.g. Society of national Application Owners in this second level of EU-IFM).
He should initiated from the group of EFM Application Owner, which are already represented in the European IFM Steering Group.
It must be ensured that each of the customers of the associated EFMs can obtain the download.

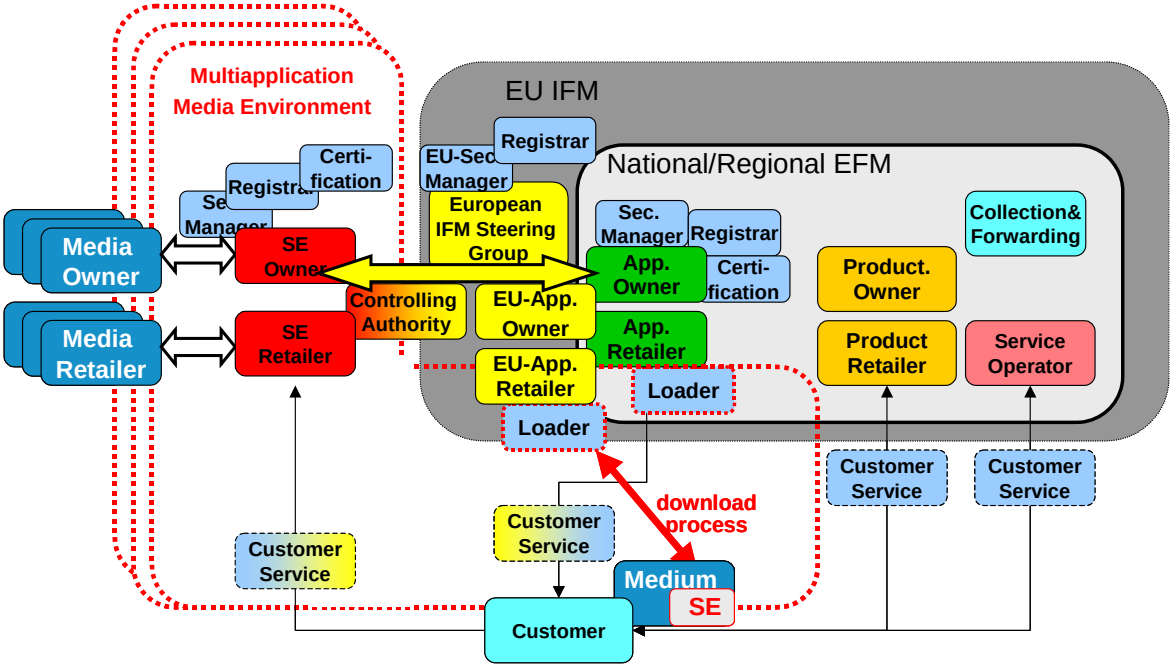


Figure 5 — IFM Roles for related IFM organisations within a Level 2 EU-IFM (1)

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

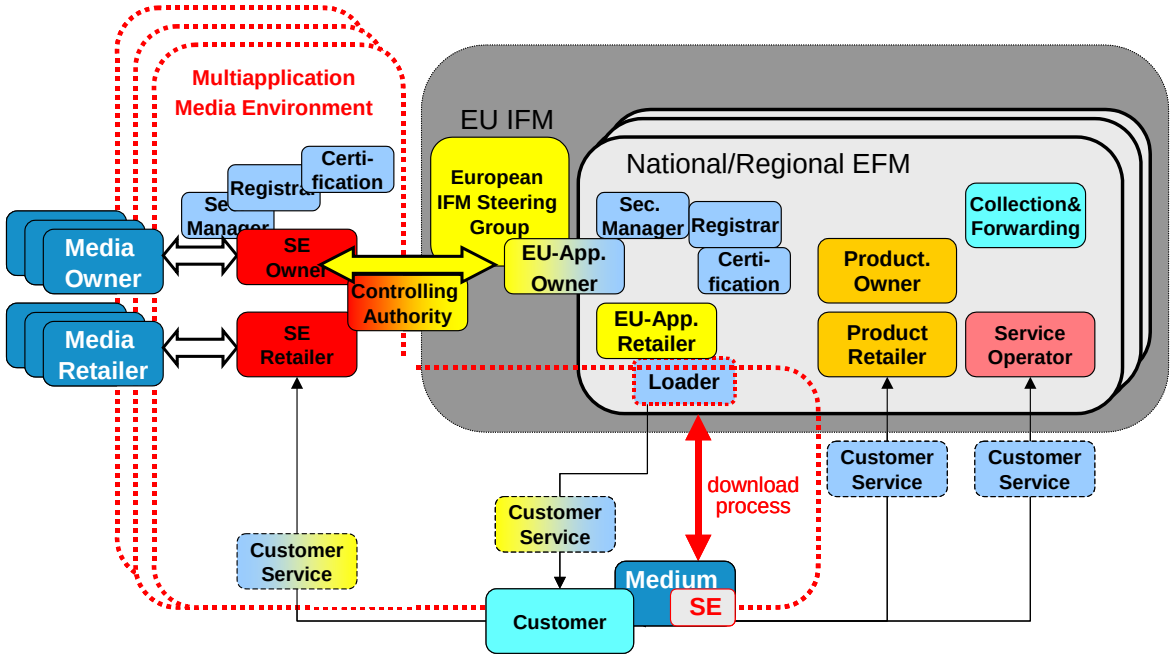


Figure 6 — IFM Roles for related IFM organisations within a Level 2 EU-IFM (2)

This results in the same role model as in national schemes. All EFM organisations (participants) keep their role in their own system and get parallel to part of the EU-IFM system.

IV.3.4 Level 1b/2b Organisational Solution for Application Issuing over Web-Portal and Product Download

Level 1b and 2b organisations are corresponding with Scenarios 1,2 and 3.
Scenario 3 refers to the introduction of a Web-portal that supports the possibility of application downloads of the EU-application. This allows customers to get the application needed to their journey into foreign EFM territory over an Internet access.

This option is an acceptable scenario 1c and 1d within Chap. IV.2.2 and scenario 2b and 2c within Chap. IV.2.3 for download of national/regional PT-applications (see Figure 7) as well as for the EU-application (see Figure 8). This ensures both a high level of customer acceptance as well as an economic solution to the EFM system operators, because the Download can be organised over common Download servers with access to the Security Management to load the necessary security components also in the PT-application.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

The necessary roles and organisations to implement are almost identical for the two variants. Therefore, the download version of the national application is considered together with the download version of the EU-application.

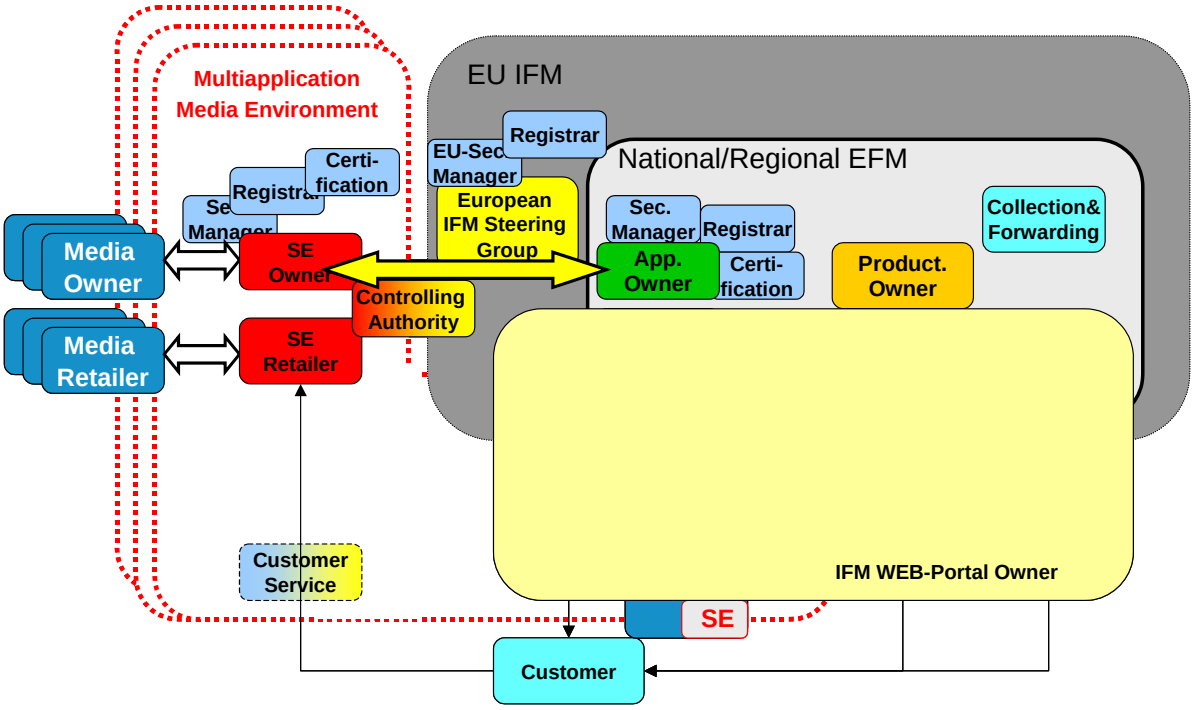


Figure 7 — IFM Roles for related IFM organisations within a Level 1b I EU-IFM

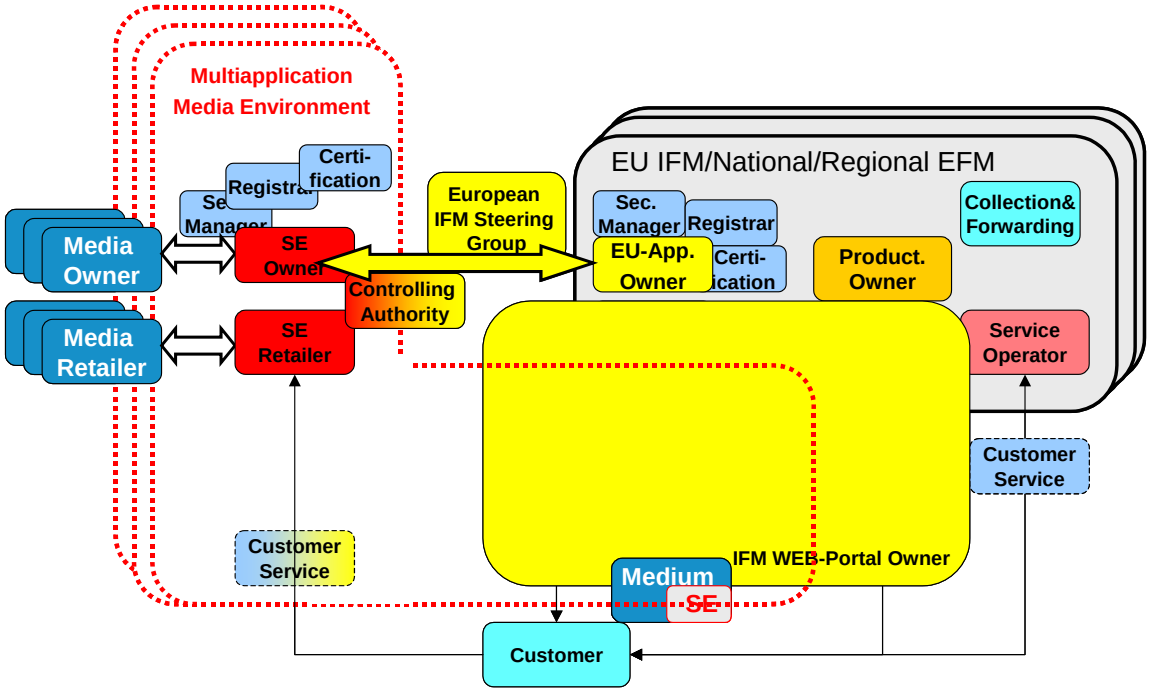


Figure 8 — IFM Roles for related IFM organisations within a Level 2b EU-IFM

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

The agreements for the establishment and operation of the EU Web-Portal (or Portals) must be created and accepted by the EU-IFM participants. The role of IFM WEB-Portal Owner has to be built.

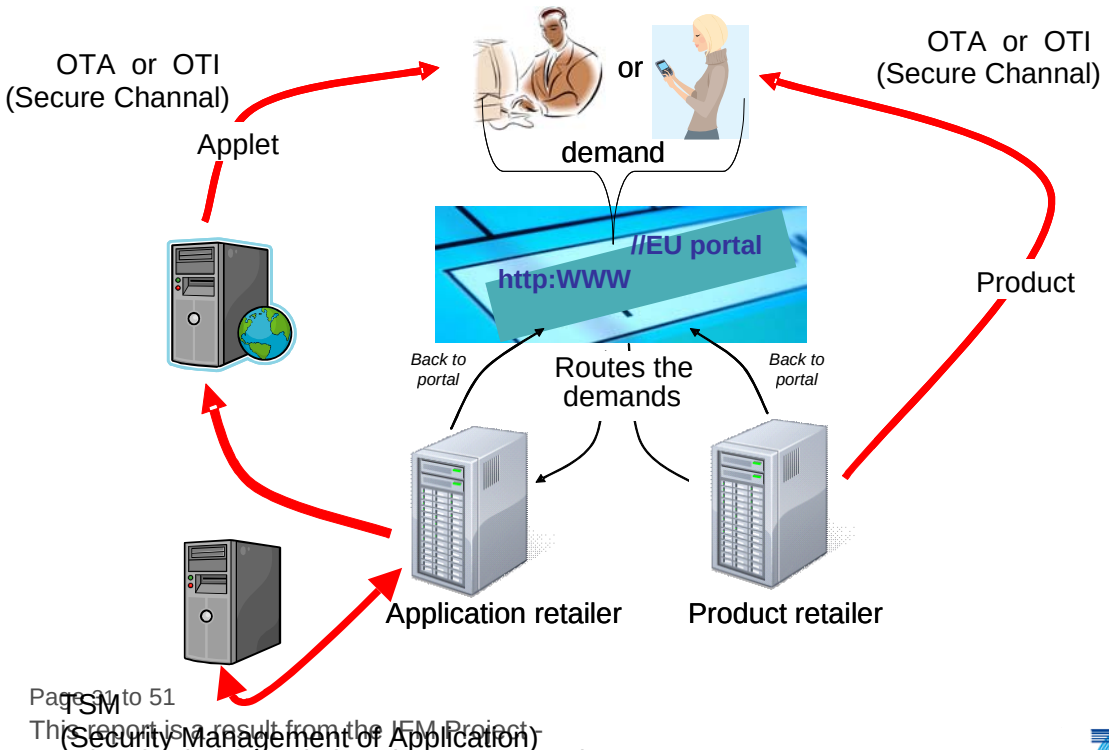
IFM WEB-Portal must be implemented. The portal can be used to acquire EFM application and EFM products linked to an EFM Application Retailer respectively Product Retailer or linked to the EU Application Retailer and after application download to the EFM Product Retailer.
It can offer different possible levels of service for local schemes:

- an entry point to all local web-services, The customer will be routed from the IFM Web-portal to the Application Retailer, the services being rendered on the local web portal of the EFM scheme, (routing as illustrated below in Figure 9). Similarly, the customer gets directly the products he needs through an access to the product download from the server of the Product Retailer.
- a direct download of the applications, including the EU IFM application and potentially the local EFM PT applications.

The IFM Web-portal provides a common access to the application download for the - customer.

The customer will be routed from IFM Web-portal to the Application Retailer.

The servers may be shared by several retailers and operated by an authorised service provider or by each retailer itself.



This report is a result from the IFM Project –
a project funded through the 7th EU Framework Program

Figure 9 — EU-IFM portal – Routing Model

The products that the customer needs, he gets directly through an access to the product download from the server of the Product Retailer.
The product server may be operated shared by several retailers, or via an authorised service provider or by each retailer itself.

IV.3.5 Level 3 EU-Application Issuing by one EU-Application Owner, Issuing of EU-Products by one EU-Product Owner on every PT Medium

All products hosted in the EU-App are EU-products as it has been defined. But at a start, they remain local.

In level 3 some EU-IFM products will also be issued, which can be used to seamless travel between different countries.

Level 3 organisation is according to scenario 3, but at least one EU-IFM Product has to be build, and issued by selected or all EFM Product Retailers.

In EU-IFM participating Service Operators have to accept these EU products – collection and forwarding has to deal with transactions EU wide.

Level 4 will requires regulations for revenue sharing between the associated partners and the corresponding European product clearing as the basis for financial compensation for the transportation services provided with these products.

Customer service must be organised Europe wide. This may be based on the already existing travel information systems.

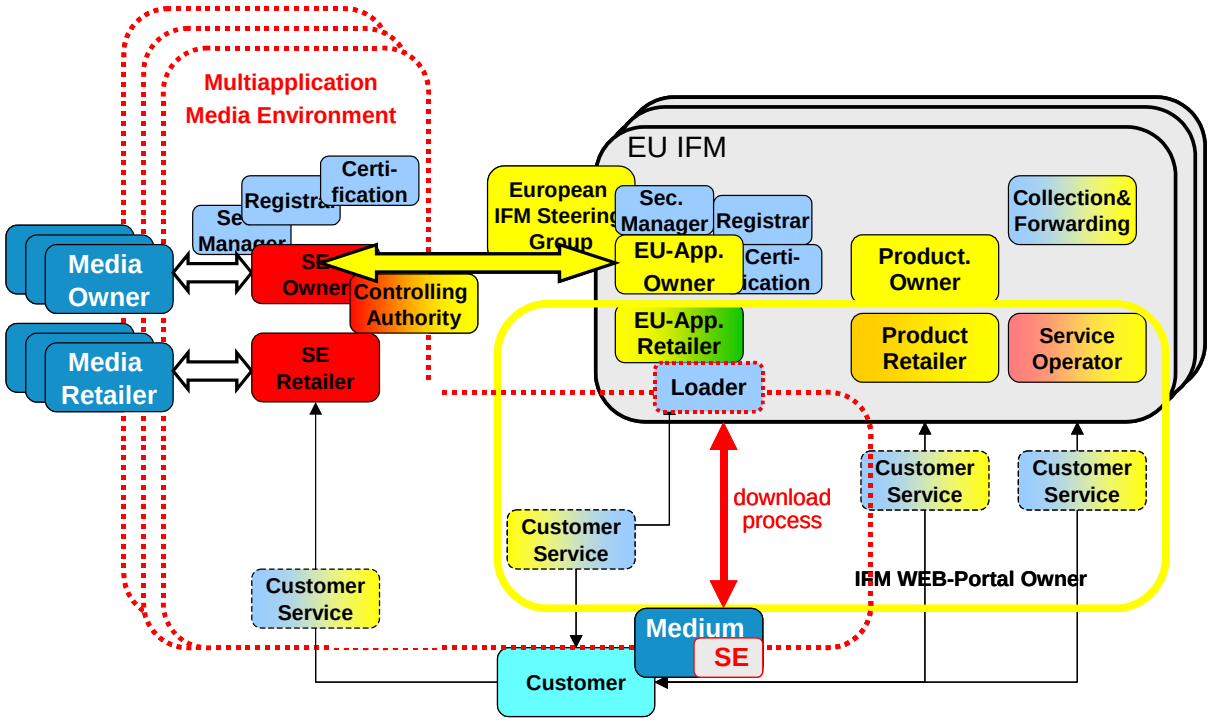


Figure 10 — IFM Roles for related IFM organisations within a Level 3 EU-IFM

IV.3.6 Level 4 Organisational Solution for EU-Application Issuing by one EU-Application Owner, EU-Product(s) by many EU-Product Owner on every PT Medium

Level 4 organisation corresponding with Scenario 5.

The last level means one interoperable IFM standard is applied. All roles have to transfer in full EU roles. The regional/national systems are fully migrated into the EU-IFM now.

Each regional/national scheme keeps the control of its pricing policy but must have translated all its local product into EU IFM compliant product templates.

When EU IFM products are defined, an EU IFM product owner has been defined for each of them.

Level 4 organisation is according to level 3, but all Product Owners become EU-Product Owners. EU-Products have to be issued by each Product Retailer. EU-Products have to be accepted by each Service Operators.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Full interoperability for the PT customer is realised.

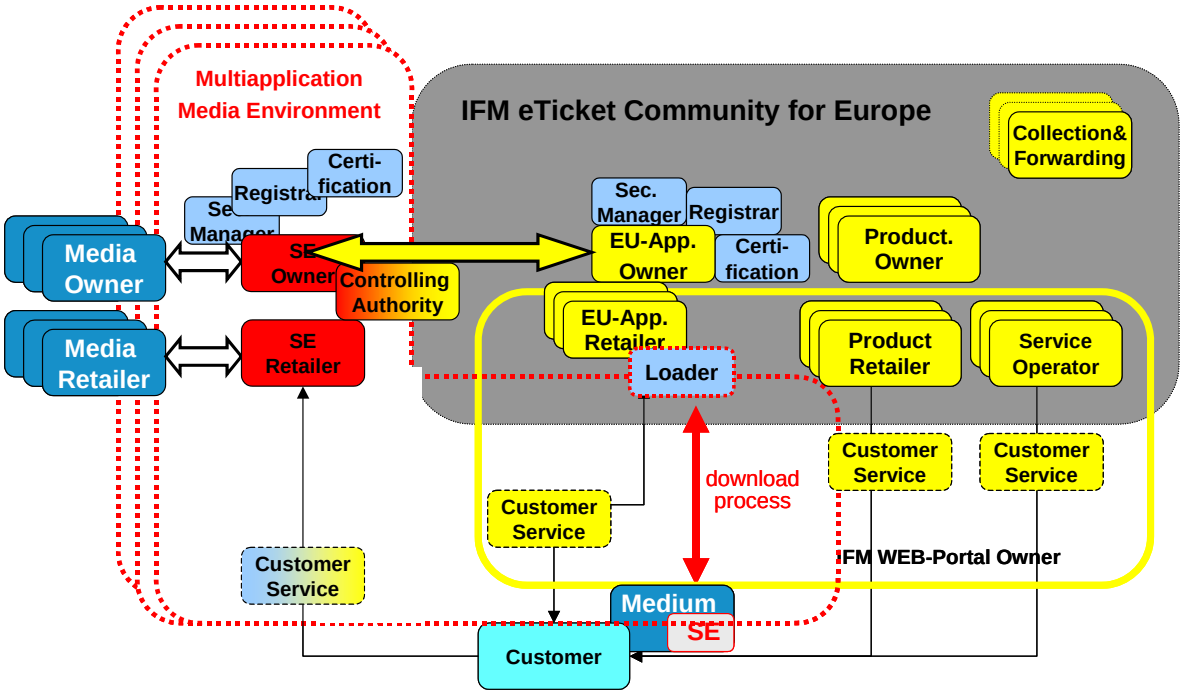


Figure 11 — IFM Roles for related IFM organisations within a Level 4 EU-IFM

IV.4 Qualification of the Organisation Levels

The description of organisations Level 1 to 4 has shown that some of them have very similar or even identical technical and organisational requirements. Therefore the aim is to reduce the organisation levels of economic migration steps.

Based on the “Evaluation of Possible Migration Scenarios based on Effort and Customer Acceptance” in WP 4.2. the Organisational levels are compared against the following criteria:

- Rating Table 3 from WP 4.2
- Organisational Structures
- Conditions of Participation in EU-IFM System
- Certification Procedures for EU-IFM Components
- Economic Basis for the Implementation of the EU-IFM
- Media Requirements
- Products requirements
- Security Requirements
- Back Office requirements

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

- Customer Satisfaction

Therewith a qualification will be done so that only the qualified scenarios are considered with regard to the organisational models to be created.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Organisation Level	Rating Table 3 WP 4.2[1]	Organisational Structures	Conditions of Participation in IFM System	Certification Procedures for IFM Components	Economic Basis for the Implementation of the IFM	Media Requirements	Product Requirements	Security Requirements	Back Office Requirements	Customer Satisfaction
(Status Quo) Interoperability can be achieved by mutual agreements to accept each other's media or Interoperability can be achieved by mutual agreements to accept each other's media or countries agree a common standard across country borders	19	None	N.A.	EFM internal certification		EFM internal certifcation process	Only EFM products used	EFM internal security requirements, EFM SAM	No exchanges needed between EFM back office	No seamless travel over teh border of existing EFM scheme.
Level 1 Downloading existing PT-Applications	22	IFMSG designated/elected representatives of IFM Treaty members + **EU-Security Manager** for EU IFM media certifcation + **EU-Registrar** for EU IFM media registration	EU IFM Participating parties have to agree - Security requirements on SE - Security requirements for application download - Usage agreements	+**EU IFM media** have to be registered by the EU-Registrar and certified by the EU Security Manager	Download over Server **with** switch to the EFM Security Manager	Certified and approved EU IFM media		+ EU- Security Manager agrees the security requirements for EU IFM media	Set up of one or more EFM application download servers.	Application download and product retailing available at the visited EFM only (via local channels or over the web - see level 1b/2b)
Level 2 Issuing of Additional EU-Application (with Common Template for Products)	46	+ **EU Application Owner** for EU IFM application definition + **EU Product Owner** for definition of EFM products based on the EU IFM Common template + EU-Security Manager for EU IFM application certification + EU-Registrar for EU	+ Agreements for : - Certification process for EU-application and EU-product - Blacklist Service	+ **EU IFM application** have to be registered by the EU-Registrar and certified by the EU Security Manager + **EU IFM products** have to be registered by the EU-Registrar and certified by the EU Security Manager	Download over Server **with** switch to the EU IFM Security Manager		+One common product template for EFM products	+ EU-extended EFM-SAM + Blacklist Service for EU-application + Asset Management for EU-SAM	Set up of one or more EU IFM application download servers. **Maintenance of a global EU IFM application black list**	EU application can be natively provided on EU IFM media and then available "at home" Products are only valid per EFM.
Level 1b/2b Application Issuing over Web-Portal and Product Download	22/46	+ organisation of **EU Web Portal**	+Agreement for : - the EU-Web-Portal and Links to EFM-Web Portals		Download **over Server** and **customer equipment** over Internet or GPRS/UMTS				Set up of an EU IFM web portal.	Application "at home" via web donwload. Products are only valid per EFM.
Level 4 EU-Application Issuing by one EU-Application Owner, Issuing of EU-Products by one EU-Product Owner on every PT Medium	47/55	+ **EU Product Owner** for EU IFM products definition + **Collecting &Forwarding** regard. EU-Product Transactions	+Agreements for : - the EU-product acceptance and issuance - **Clearing and revenue sharing agreements** - Risk sharing and liability model				+ Definition of EU IFM product templates	+Security management for EU-Products through EU-Product Owner +additional access rights to the EU-product +monitoring of Product transactions	Set up of a clearing house for EU product settlement.	EU IFM application "at home" EU IFM Products are available and accepted at every participating EU IFM.
Level 5 EU-Application Issuing by one EU-Application Owner, EU-Product(s) by many EU-Product Owners on every PT Medium	55		+Agreements for : -Phasing out of all EFM products		All participants have to support only the EU IFM application, can use the same standardised IFM system components. All the EFM specifc components can be phased out.					Everywhere one medium, one application, interoperable products, one customer contract partner, "everywhere at home"

Table 1: Qualification of the identified Organisation Levels

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

The comparison of the organisation model solutions shows that level 1 to 2 do not differ significantly.

The first interesting step for the customer to EU-IFM represents the general possibility of application downloads. Important here is that he already can get/buy at home application and products.
It does not change much to him to download an other additional EFM application or an additional EU application.

The advantages of the EU application will be available if he can use the one additional EU application everywhere in Europe (at first of course in the participating systems) to Check-in/Check-out or to buy tickets.
Customers may obviously expect a quick migration from level 1a to Level 2b.

This migration however requires the definition of the EU IFM application and its endorsement by EFM schemes already having a local ticketing application fulfilling their current needs. This requires technical standardisation and agreements that may likely need some support form the EU organisation as the short term financial benefit may appear negative to each EFM scheme.

In the prepaid ticket approach, to purchase local EU-products or IFM EU products and load them in the EU IFM application the customer will use the usual means of payment (cash, credit card, ….) .

In the entitlement approach, the customer has to be linked by contract to an EU-IFM Product Owner over which the payment for the trips made will be handled (store value or customer account approach).
The customer uses this contactless entitlement (which may be anonymous in case of the data protection requirements).to an EU IFM product in each EFM to obtain the access permission for all trips

In all cases of EU-IFM products –pre-paid tickets, stored value or customer account- some clearing and settlements must be performed between the EU Product Retailer and the Service Operators providing the transport service and possibly between the EU Product Retailer and the EU-Product owner.

Therefore a migration path can be taken, which leads from scenario 4 to scenario 5, namely, first to retail one EU IFM product by one EU Product Owner over a number of EU Product Retailers. But the organisational model should have the goal to make possible that many Products Owners and Retailers coexist in the EU-IFM scheme in order to guarantee some freedom of choice to customers for the purchase of EU IFM products.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Therefore all active today Product Owners in the EFM and retailers will be given the opportunity to act on European and regional levels of public transport, without providing individual with special privileges.

Therefore, to simplify the further discussion of the general organisational conditions and related issues, only the level 1b/2b and 5 will be considered hereafter. These can be expected also in terms of expected customer acceptance, customer needs and customer satisfaction as well as to guarantee equal treatment for Product Owners and Product Retailers.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

V General Organisational Conditions

V.1 Level 1b/2b Application Issuing over EU Web-Portal and Product Download

Step 1: Existing EFM Applications
Step 2: Additional EU-Application with common Product Template

V.1.1 Step 1 Existing EFM Applications

V.1.1.1 Organisational Structures

PT Application Owners of the existing EFM systems have to build a Common EU-IFM Steering Group (EU-IFM-SG), which is mandated to negotiate with Secure Element Owners or their organisation. It will be supported by an EU- Security Manager and an EU-Registrar.

The Stakeholders of the Common EU-IFM Steering Group (EU-IFM-SG) shall consist of the designated/elected representatives of EU-IFM Alliance members.

EU- Security Manager agrees the security requirements that apply to accepted media for all PT applications and the Secure Elements used for the download process. He accepts SE and provides means of authenticating certified SEs.

EU-Web-Portal is to organise as a roaming portal, and all customer service is processed by the regional servers of Application and Product Retailers.
The download of products have to be performed only via the local / regional Product Retailers, and may rely on a Web-portal which acts as a roaming service to the regional Product Retailer Web portal or on a Web-portal from which the customer uses the download service directly with the regional Product Retailer.

EFM-participants (Application Owner/Application Retailer) have to be registered by the EU-Registrar once their downloading process on a medium as been tested or certified as respectful of the requirements for Application Download Procedure expressed in [R6]. Approved secure elements and media[3] have also to be registered by the EU-Registrar.
Only tested and certified media are covered and guaranteed by the EU Security Management.

[3] Only SE and media have to been used that can demonstrate in according reports all properties and evaluations, required by the application download. The approved base on these media will be retrievable.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

It would make sense that the EU roles should be executed by a selected organisation or a group of representatives from those organisations, which already play this role in the national or regional EFM systems.

V.1.1.2 Conditions of Participation in EU-IFM System

The participating parties have to agree upon and admit

- Security requirements on SE
- Security requirements on Application Download Procedure
- EU Web portal

Usage agreements are available and signed by the participants in form of:

- descriptions/specification of the agreed download processes
- individual requirements of the different Application Owner, especially with regard to security, media evaluation
- the download is done at the risk of the Application Retailers

V.1.1.3 Certification Procedures for IFM Components

The certification of IFM Components will be part of all the national/regional systems.

Common certification of EU IFM Media is necessary. The EU-Registrar designates authorised testing laboratories for the certification of the EU IFM media.
There should be a cross recognition in the EU IFM scheme of media certification performed at any authorised testing laboratory. The release of new certified media should be notified to all the participants within an agreed period.

V.1.1.4 Interoperable Product Templates/Products

Interoperable EU-IFM Products are not necessary.

V.1.1.5 Economic Basis for the Implementation of the EU-IFM

It is suggested that the possibility of promoting of the EU-IFM-SG and the EU-Registrar is to be prove through the EU.

The funding of the EU-Security Manager is to be clarified among the participating parties and the EU. One possibility in countries where a national Security Manager exists, can be that the financial contribution to EU-Security Manager activities is part of the funding of the Security Management in the national context.

The business rationale for each participating EFM to support this first step, is dual as:

- Its offers a first level of ticketing interoperability by allowing coexistence of several EFM ticketing application on the same customer media,
- It enables to deliver EFM ticketing application on 3 rd party EU IFM compliant media like NFC phones, USB keys, or banking cards.

Each participating EFM will support its own cost for accepting to download its EFM application on EU IFM media. This financial effort must be back up by an acceptable business model based on:

- extra revenue from an increased interoperability and a wider media acceptance
- cost reduction on dematerialisation of EFM application and product delivery.

V.1.1.6 Customer perspective

The customer receives an access to the PT in all EU countries with a medium in his possession. He needs an Internet access.

He gets the needed application and products for access “at home” over one or more Web portals. he can buy products for subsequent trips, directly with his medium at the destination.

V.1.2 Step 2: Additional EU-Application with common Product Template

V.1.2.1 Organisational Structures

PT Application Owners of the existing EFM systems have to build a Common EU-IFM Steering Group EU-IFM-SG), which is mandated to negotiate with Secure Element Owners or their organisation. It will be supported by an EU- Security Manager and an EU-Registrar.

The Stakeholders of the Common EU-IFM Steering Group (EU-IFM-SG) shall consist of the designated/elected representatives of IFM Alliance members (see V.1.1.1).

EU Application Owner is instructed by the Common EU-IFM Steering Group (EU-IFMSG). EU Application Owner is responsible for the maintenance of the EU application specifications and for the certification of the EU application in conjunction with the media issued or used for national/regional EFMs. One or more EU application templates can be developed, but all the templates must be certified and approved by the EU Application Owner before being distributed by EU Application retailers.

EU- Security Manager agrees the security requirements that apply to accepted media for all PT applications and the Secure Elements used for the download process. He accepts SE and provides means of authentication.

Security Management has to define the procedure for a secure distribution and usage of the application keys needed for the EU-application.

Security Management has to organise and engage a Blacklist Service needs for the EU-application.

A EU-Web-Portal is to organise. that can at first be directly linked to one EU Application Retailer, who spends applications from the EU-Application Owner. Alternatively, or in a further phase of expansion the EU portal can be realised as a roaming portal, and all customer service is processed by regional servers of Application Retailers that acquire the right to issue the EU's application.
The download of products remains to be performed only via the local / regional Product Retailers, depending from the role of the Web-portal as a roaming the service to the regional Product Retailer Web portal or the customer uses the download service directly with the regional Product Retailer.

EFM-participants (Application Owner/Application Retailer) have to be registered by the EU-Registrar for access to the downloading on the medium. The approved secure elements from SE Owners and SE Retailers have also to be registered by the EU-Registrar.

The clear identification of the issued EU applications must be ensured through the registry by the EU-Registrar or through registered number ranges for the Application Retailers.

Asset Management is built up for tracking of hardware security components (e.g. SAMs) and software objects (applets, certificates) necessary for the EU-application. This also includes the responsibility of the manager to keep an inventory of assets and rules of acceptance and an information classification (definition of confidential and non-confidential information).

Only tested and certified media are covered by the EU Security Management.

It would make sense that the EU roles should be executed from a selected organisation or a group of representatives from those organisations, which already play this role in the national or regional EFM systems.

V.1.2.2 Conditions of Participation in EU-IFM System

The participating parties have to agree upon and admit

- Security requirements on SE
- Security requirements on Application Download Procedure
- Specification of the EU-application and of the available product template
- Certification process for the EU-application and for the related product template Blacklist Service which works with all participating Application Retailer and application acceptors
- EU Web portal

Usage agreements are available and signed by the participants in form of:

- descriptions/specification of the agreed download processes
- individual requirements of the different Application Owner, especially with regard to security, media evaluation
- the download is done at the risk of the Application Retailer(s)

V.1.2.3 Certification Procedures for IFM Components

The certification of IFM Components will be part of all the national/regional systems.

Mutual certification of Media is necessary, including the certification of the EU application. The EU-Registrar designates by national Application Owners authorised testing laboratories for the national certification of the media. The release of the test media should be notified within the agreed period.

V.1.2.4 Interoperable Product Templates/Products

Interoperable Product template is specified and available. National Products can be issued into this template.

Interoperable EU Products are not necessary.

V.1.2.5 Economic Basis for the Implementation of the EU-IFM

It should be suggested that the funding of the IFMSG, the EU Application Owner and the EU-Registrar is to be clarified through the EU.

The funding of the EU-Security Manager should be clarified though the participating parties and the EU. One possibility in countries where a national Security Manager exists can be

that the financial contribution to EU-Security Manager activities is part of the funding of the Security Management in the national context.

Each participating will support its own cost for accepting the EU application with EU product template. This financial effort must be back up by an acceptable business model based on:

- extra revenue from an increased interoperability
- cost reduction on media and front office components procurement.

V.1.2.6 Customer perspective

The customer receives an access to the PT in all EU countries with a medium in his possession. He needs an Internet access.

The needed application for access should be issued in their own EFM. He can use this one application in all participating systems and does not need to download new applications over.

He gets the products for access “at home” over one or more Web portals. He can buy products for subsequent trips, directly with its medium at the travel destination at many terminals in the field.

V.1.3 Step 3 EU-Application Issuing by one EU-Application Owner, EU-Product(s) by many EU-Product Owners on every PT Medium

V.1.3.1 Organisational Structures

The organisational structures for step 3 are built on the already established in step 2 on.

Participating IFM organisations have to build a EU-IFM Application Owner company. It might be built from the Common EU-IFM Steering Group (IFMSG), It is the Application Owner of the EU-application for the EU-IFM.
It is mandated to negotiate with Secure Element Owners or their organisation. It will be supported by the EU-Security Manager and the EU-Registrar. The operational service can be perfomed by external service providers (e.g. Trust EU IFM organisation), which are working ordered by the EU Application Owner.

The Stakeholders of the EU-IFM Application Owner organisation shall consist of the designated/elected representatives of IFM Alliance members.

EU- Security Manager agrees the security requirements that apply to accepted media for the EU-application and the Secure Elements used for the download process. He accepts SE and provides means of authentication.

Specified IFM security concept is realised. The security manager checks this. All EU-IFM participants agreed contractually to work in compliance with for they defined security measures (trust in terminals/back office, communication, data monitoring).

EU IFM-participants (all roles executing organisation units/companies) have to be registered by the EU-Registrar after signing the EU-IFM contracts.
The approved secure elements from SE Owners and SE Retailers have also to be registered by the EU-Registrar.Only tested and certified SE are covered by the EU Security Management.

All IFM hard- and software components have to been certified by accredited testing laboratories. Accreditation is done by the certification body of the Application Owner.

EU-Product Owners are to integrate into the EU-IFM Application Owner organisation. Prices, usage rules and terms of use for products are to be matched on the basis of regional tariff requirements. Clearing and revenue sharing is to organise if the customer buys his products through a payment authorisation/entitlement, which issued its customer contract partner. The doing for the clearing settlement is to fix up (centralised or distributed clearing). Liability rules for payment and data privacy have also to be agreed between the EU-IFM members.

Security Management has to organise and engaging a Blacklist Service needs for the EU-products.

Collecting & Forwarding of transactions of EU-IFM Products must be covered by a contract and are technical supported by all participants.

V.1.3.2 Conditions of Participation in EU-IFM System

The participating parties have to agree upon and admit

- Security requirements on SE
- Security requirements on Application Download Procedure
- EU-IFM participating contract(s) (role related)
- Clearing and revenue contracts
- Settlement contracts
- Liability rules for payment and data privacy

Usage agreements are available and signed by the participants in form of:

- Specification of the-EU-application
- descriptions/specification of the agreed download processes and
- individual requirements of the different Application Owner, especially with regard to security, media evaluation
- risk sharing model

V.1.3.3 Certification Procedures for IFMS Components

The certification of FMS Components will be part of the IFM systems.

Certification of Media holding the EU-application is necessary. The EU-Registrar designates testing laboratories for the EU-IFM certification of the components.

V.1.3.4 Interoperable Product Templates/Products

EU-IFM Products and product templates are available and defined by participating EU Product Owners.

Terms of Use, commissions and revenue sharing are contracted by the participating parties.

The transaction monitoring and auditing must be specified and running so that the collected data allows secure and trusted fare revenue sharing or allocation between the systems.

An interoperable Customer Service must be made available for interoperable products.

V.1.3.5 Economic Basis for the Implementation of the IFM

It will be The funding of the IFM is to be clarified through the EU.

Operating costs must be determined and shared by the national/regional participating EFM.

Each participating EFM will support its own cost for phasing out its remaining local EFM products and turning them into EU IFM products. This financial effort must be back up by an acceptable business model based on:

- extra revenue from an increased interoperability
- cost reduction on shared and EU wide retail channels.

V.1.3.6 Customer Perspective

The customer receives an access to the PT in all EU countries from a single EU application with EU products. Seamless travel “door to door” is possible.

The needed application and products for access can be issued by a unique customer contract partner for all EU regions.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

VI Legal Framework

The first EFM Application Owners join to the EU-IFM contract and represent the participating parties of their systems in the migration Level 1 to 3. They stay the EU-IFM Alliance members.

Every EFM Application Owner in Europe has the right to join if they accept the EU-IFM contracts.

The EU-IFM Alliance members pay an EU-IFM contribution and select the members of the EU-IFM-SG.

The relevant contracts for the national EFM are relevant examples:

- VDV-KA; Participation contracts for Retailer/Customer contract partner, Product Owner, Service Operator, IOP Clearing, issuing (application/entitlements to customer) contracts, conditions of carriage, Regional PT contracts
- ITSO: membership agreement; licensed operator agreement; registered supplier agreement
- Resekortet: Co-operation agreement
- TLS: contracts between TLS (as Scheme Provider) and IFM participants: Framework agreement, participant agreement, load agent agreement. Part of the participant agreement is the services portfolio.

The relevant requirements stemming from data protection acts are observed.

Other legal and political requirements (may be company laws and obligations stemming from monetary regulations (E-Money Directive, banking law (Credit Transaction Law)) are also observed.

All the EU-IFM participating parties join a participation contract for EU-IFM directly, which will to be developed, coordinated and implemented in accordance with the organisational conditions in the described levels.

The EU-IFM Application Owner company is built and financial supported by the IFM Alliance members and by the EU.

The development and coordination of EU-IFM participants contracts and of the Shareholders' agreement of the EU-IFM Application Owner company are not the contents of this project. This is to realise in a follow-up project.
It seems however to make sense that the EU-IFM Application Owner company could be built and financially supported by the IFM Alliance members and by the EU.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

VII Liability

An EU-IFM participant contract should be signed by all participants. The contract should define the liabilities regarding the correctness of specifications and regarding their usage for implementation. It's expected that the EU IFM participants will make no guarantees and refuses all liability with regard to the content of the Specifications, and in particular any breaches of intellectual property rights such as patents, trademarks, copyright or other intellectual property rights belonging to third parties in relation to all or part of the Specifications.

In the case of contract violations by individual EU-IFM participants have to make also financial arrangements in the contracts in relation to the roles that the participants in the overall EU-IFM system occupy.

Liability agreements are also necessary regarding the EU-Security Management.

It should be created basic agreements between the EU-IFM Application Owner organisation and one ore more Security management operators; single supply contracts made with EU-IFM participants and the Security Management Operator. The Security Management Operator takes over the liability for the delivered security components, or security services (keys, security certificates, SAM)

Liability rules must be also clarified and agreed regarding the payment settlement between the EU-IFM participating parties (Owners, Retailers, Services Operator,…).

Liability rules must also be defined and agreed regarding the sharing of personal data linked to an EU IFM application (customer profile, statutes, …).

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

VIII Resume

The analysis of EFM systems in Europe and beyond has shown that current EFM systems operate more at a regional level than a national one. Therefore, the EU-IFM project should be met with great interest throughout Europe as well as elsewhere.

The existing systems and standards used can generally be mapped to the role model from ISO EN 24014-1. So a general basis for the formation of a European organisation model is given, which also includes the existing national organisation units that can fit the role model.

Thus, different scenarios for the introduction of EU-IFM have been developed and discussed, which would also allow a number of other modifications.

The need for downloading PT applications on media appropriate for e-ticketing was identified as the most important prerequisite for a viable EU-IFM. This allows customers to acquire a medium before the start of PT trips, which they can load while still at home with the applications and products necessary for their trips across their home regions and beyond.

The downloading of existing PT applications, which must also be available via the Internet or UMTS / GSM, will require an initial joint organisational level necessary for the creation of a European IFM.

Therefore, the necessary EU-IFM organisational structure should focus on creating these opportunities by identifying the relevant structural, contractual and technical requirements and making the necessary preparations for building an appropriate solution.

Building on these results an organisational model for Europe can be created in the long term to present an attractive public transportation system with modern fare management that is safe, reliable and convenient for both users and operators.

The organisation model must meet the following essential requirements:

- help the customer to find the appropriate application and product(s) (Portal function),
- downloading the application (retail) in a secure manner,
- selling the most appropriate product (retail) in a secure manner,
- support cashless payment in the distribution channel chosen by the customer in a secure manner,
- supporting the acceptance by the service operator,
- supporting the convenient use by the customer on all PT networks and
- ensuring the revenues and revenue sharing between the participating parties.

The present approach developed by the EU IFM project members has been based on a graduate and phased approach that provides the following advantages which are essential for the success of our long term road map:

- The ability for each EFM scheme to join the EU IFM organisation and to move from level to level at their own pace,
- The development of an EU IFM organisation based on the voluntary participation of each EFM local/regional schemes,
- The ability for each EFM scheme to leverage on the investments made at each level for reaching media interoperability, then application interoperability and finally product interoperability.

As explained all along this document, some decisions will require a strong back up and endorsement from the industrial partners, from the transport authorities and from the EU Commission to support the proposed vision for reaching an EU IFM scheme, should it be the massive roll out of EU IFM media, the consensual definition of a EU IFM application or ultimately the universal delivery of EU IFM products. Hence, it would not make sense to start implementing the first steps of the IFM road map without a prior strong endorsement from the main European transportations stakeholders.

This development of the cooperative organisations will be based on three axes for decision and action:

1. A technical cooperation between the existing schemes, based on existing or to-be-agreed standards to define and implement

    - The downloading process
    - The EU-application

2. A fare management cooperation between the relevant authorities to agree common products (tickets, stored value or customer entitlement) and the associated clearing and settlement processes.

3. A distribution cooperation between product owners to ease the access of the customer to the products (portals roaming the demand or common retailers)

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program