State of the art on interoperable media and multi-application management

Deliverable 3.1

February 2009

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 3 leader

RATP

Michel Barjansky (Work package leader)
Phone: +33 1 58 77 93 85
E-mail: Michel.Barjansky@ratp.fr

Main authors

Michel Barjansky, RATP
François GUILLAUME, RATP
Jean-Philippe Amiel, Nextendis

For further information on the 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 4165
Fax +49 221 806 3496
E-mail: oliver.althoff@de.tuv.com

Visit the webpage **www.ifm-project.eu** .

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

Table of contents

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

1 Introduction

The IFM project aims to make public transport more user-friendly by facilitating seamless accessibility to different public transport networks. The objective of the "Interoperable Fare Management Project (IFM Project)" is to provide travellers with common styles of contactless media throughout Europe which can be used for multiple transport products in different geographic areas and for sustainable modal switching, such as the use of "Park and Ride'- unlike existing smart cards which are restricted to specific city or regional geographies.

A number of Public Transport Operators have commenced path towards the vision of seamless travel and the creation of IFMs. It requires common business rules and organisations, and involves linked or hierarchical back offices with structure cooperation between transport authorities and operators to share security and privacy issues, and eventually create common products and organize their settlement when the market needs it and can afford it. The customer can therefore only use his smartcard media in the networks that have already joined these agreements and use common or joined back-office ICT systems.

IFM project has a long term vision where common products will help each customer finding exactly the same interface and processes through his journey all over Europe for purchasing and using his transport fare products. In this paper, we will focus on a first step based on the usage of interoperable media that can be accepted by any IFM scheme and on which customers can download the applications they need as they move, should it be an existing local transit application or a future common EU application when available.

Additionally, customers should be able to benefit from their status all over Europe thanks to the download of a common EU Status Application. Upon customer demand, his home network will download and export the appropriate customer data status into this EU Application. Those statuses will be accessible by others IFM schemes, allowing the customer to eventually benefit from specific rights linked to its status all across Europe.

This work package studies the path for introducing interoperable media to provide access to networks that are part of different IFM schemes:

- by defining common requirements to the media themselves and
- by using the media as multi-application devices.

This first deliverable aims at providing a state of the art vision of the benefits for multi application media for end users, a description of multi application management functions.

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

2 Version Control

1.0	First draft.	October 17th 2008
2.0	Revised version following WP3 & WP4 workshop discussion on Dec 18th.	February 13th 2009
2.2	2nd version including remarks from EC reviewers	February 18th 2009
2.3	Version including remarks from IFM members	March 4th 2009
2.4	Final version for publication	March 5th 2009

3 Reference documents

[R1] ISO 24014-1:2007 - Public transport - Interoperable fare management system - Part 1: Architecture (IFMS)

[R2] GlobalPlatform Card Specification 2.2 – March 2006

[R3] GlobalPlatform Messaging Specification 1.0 – October 2003

[R4] JCP - Java Card Platform Specification 2.1

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

4 Glossary

Definitions referring to the IFM specifications ([R1]) are marked with **[IFM]**.
Definitions referring to the Global Platform specifications ([R2]) are marked with **[GP]**.

Application	[IFM] Implemented and initialised Application Template on a Customer Medium. It is identified by a unique identifier. The Application houses Products and other optional Customer information (Customer details, Customer preferences). [GP] Instance of an Executable Module after it has been installed and made selectable.
Application Provider	[GP] Entity that owns an application and is responsible for the application's behaviour.
(Card) Issuer	[GP] Entity that owns the card and is ultimately responsible for the behavior of the card.
Controlling Authority	[GP] A Controlling Authority has the privilege to keep the control over the Card Content through the mandating of DAP Verification.
ICT	Information and Communication Technologies
(Customer) Medium	[IFM] Medium initialised with one or more Applications through an Application Contract
Medium Access Device	[IFM] A device with the necessary facilities (hardware and software) to communicate with a Customer Medium. The Medium Access Device in fact a "reader" or a "coupling reader" and the term reader is also used in this document.
Product	[IFM] Instance of a Product Template on a Medium stored in an Application. It is identified by a unique identifier. Enables the customer to benefit from a service provided by a Service Operator.
SAM	Secure Application Module, used to store and manage the distribution of transport application keys.
Secure Channel	[GlobalPlatform] A communication mechanism between an off-card entity and a card that provides a level of assurance, to one or both entities
Security Domain	[GlobalPlatform] On-card entity providing support for the control, security, and communication requirements of an off-card entity (e.g. the Card Issuer, an Application Provider or a Controlling Authority)

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

5 Benefits of multi application media for end users

5.1 History and concepts of Transport Fare Management Systems

The present chapter aims at presenting the evolution of media from dedicated objects to open objects and the necessary development of interfaces with IFMs.

5.1.1 Legacy context of Transport Fare Management systems

All over Europe, transport ticketing is going contactless. For various reasons, different ways to set up contactless ticketing schemes have been rolled out:

- In the Netherlands, Translink has specified all detailed parts of a whole national information system,
- In the UK, ITSO has specified some parts only that where necessary for providing interoperability including some SAM and supervision architecture and a list of various accepted Customer Medias,
- For numerous EU projects, Calypso applications have been released allowing compliance in the card /terminal exchanges and in some cases with appropriate key sharing process bringing interoperability between different public transport networks ,
- In Germany, VDV is proposing a core application (Kernapplication) which is a data and interface standard to be largely used nationwide for electronic fare management.

All these different approach have different level of impacts on the Transport Fare Management system architecture as shown in the table below which is extracted from a report from Syntigo, the IT subsidiary of SNCB, the Belgium National Railways Operator:

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

Level	Component	Topic	Calypso	ITSO	Kern-Application
0	Card	Multi application	Yes	Yes	Yes
		Data Model	Free (recommended building on EN 1545)	Specified and built using EN 1545	Specified and built using EN 15320 & 1545
		Data Integrity	Free	Digital Signature	Digital Signature
		Data security	Number of symetric key/app. Rest free	free	Integrated jkey management, mix symetric and PKI
		Commands	ISO 7816-4 + calypso specifc for contactles	Defined per customer media in Customer Media definition	ISO7816-4 + Kern-application specific
		Communication	ISO 14443 A&B	Defined per customer media in Customer Media definition	A&B are allowed
		Card Types	Microprocessor native mask & Java applications	Customer media: Mifar, calyspso cards	Siemens JavaCard, banking card
1	Terminal	SAM	Calypso specific	ISAM, Defined per customer media in Customer Media definition	Only 1 supplier but open to more if needed
		Business rules	free	Functional rules registration	Organisational & functional rules registration
		Communication collector/back office	free		
2	Collector		free		
3	Back Office		free		
4	Common Platform		free		

As seen from the above table, a Customer Media must fulfil some specific requirements to be accepted by a Fare Management System. Those requirements concerns:

- the communication protocol used to communicate between the Customer Media and the terminal,
- the format of the data exchanged with the terminal,
- the security scheme used to protect those data and eventually authenticate the Customer Media to the terminal,
- the commands used to carry the exchanged data.

Additionally some systems are closed systems built on proprietary technical specifications whereas others are open systems relying on public or open standards.

Unfortunately and regardless of closed/open systems consideration, **those set of requirements are largely different and not compatible between each others, then preventing the usage of the same transport application across Fare Management Systems built according different schemes.**

5.1.2 Transport organization and impact on Fare Management System

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

A Fare Management System is an IT System tailored to the task of managing the relationship between a Public Transport System and its clients using (or wishing to use) transport services, through an array of distribution channels.

Virtualization of the (fare) product (as defined by IFM [R1]) organizes the customer relationship around a transaction between a collection of electronic media (held by the clients) and a defined acceptance infrastructure of electronic terminals implemented by product retailers & service operators.

Behind each Public Transport System there is an "Organization".
In most of the European countries, the organisation of public transport services is controlled by Transport Organisation Authorities are responsible for the assignment and coordination of public transport fares and consistent in the associated transport companies. Transport Organisation Authorities can be:

- *Local authorities* responsible for urban transport (bus, metro, tram, LRT,…),
- *Regional authorities* responsible for public transport between towns and cities within a given region (interurban bus& railways lines),
- *National Authorities*, responsible for the national transport companies when it exits and for its interconnection with the different public transport networks.

Each "Organization" has a decisive role towards ticketing system implementation.

The Transport Operators who run these networks act in most of the case with the authority of the Transport Organization Authorities. Those organization authorities have then large influence on the investment made on the transport network, including of course the ticketing system. Ticketing system is hence an important part within the global transport system as it implements some key features for the transport organizations like:

- The transport fare policy according to geographical zone, origin/destination, end user social profile… and hence must be flexible enough to cope with tariff evolution,
- The brand image of the transport organization and then must be in line with the main values that the organization wish to convey towards en users:
    - Reliability, security may lead to microprocessor based media and/or strong security algorithm implementation
    - Seamless access & interoperability may drive towards contactless media with multiple keysets or multi applications capabilities,
    - Sustainable development may orient the choice for reloadable e-ticket rather than paper ticket,
    - …

"Organization" attitude towards risk is largely influencing the Customer Media choice.

Transport Organization Authorities may have different policies towards risk acceptance and mitigation. Depending whether the public service or largely subsidized or not, according to the importance given to the protection of the customer data privacy, the key drivers for Customer Media selection may largely differs:

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

- Some Organizations will have low or medium intolerance toward risk and may consider that "the cheapest, the best" is the most appropriate approach in their context.
- Some Organizations will have high intolerance toward risk and may consider a more risk savings ROI oriented approach.
- Some Organizations will have the requirement that an interoperable use of the medium must be ensured that the transactions are trusted secured for each participating company data because every transaction means ultimately money values.

Moreover, Organizations can have an attitude towards customer risk information that ranges from "customers will not accept to pay price for security" to "customers will pay if they understand what they get for their money". Therefore, the Customer Media choice and customer risk communication are usually closely linked. This is an important point as usually, when different systems want to work together, they have to have a common understanding of risk before they can mutually accept their customer medias.

5.1.3 Organization and Customers Media Subsystems within Fare Management System

From the previous consideration, a Fare Management system can be then seen as a 2 part system and divided into two Sub-Systems:

- The Organization Subsystem (Osub)
- The Customers media Subsystem (CMsub)

The Organization Subsystem (Osub) remains permanently under the custody of the Organization. It is also a subsystem that is always local, tailored to the local needs, according to the local conceptions and prejudices. The Osub is an "infrastructure" and as such will be difficult and costly to modify.

The Customers Media Subsystem (CMsub) is the part of the whole system that is in the hand of the customers and is only under custody of the PT Organization when it is linked to the OSub. A CMsub is made up of a series of **Customer Media (CM)** that can be of numerous and various kinds such as: paper tickets, contact or contactless smart cards, contactless tickets, magstripe tickets, NFC phones, contactless key fobs, contactless USB keys…

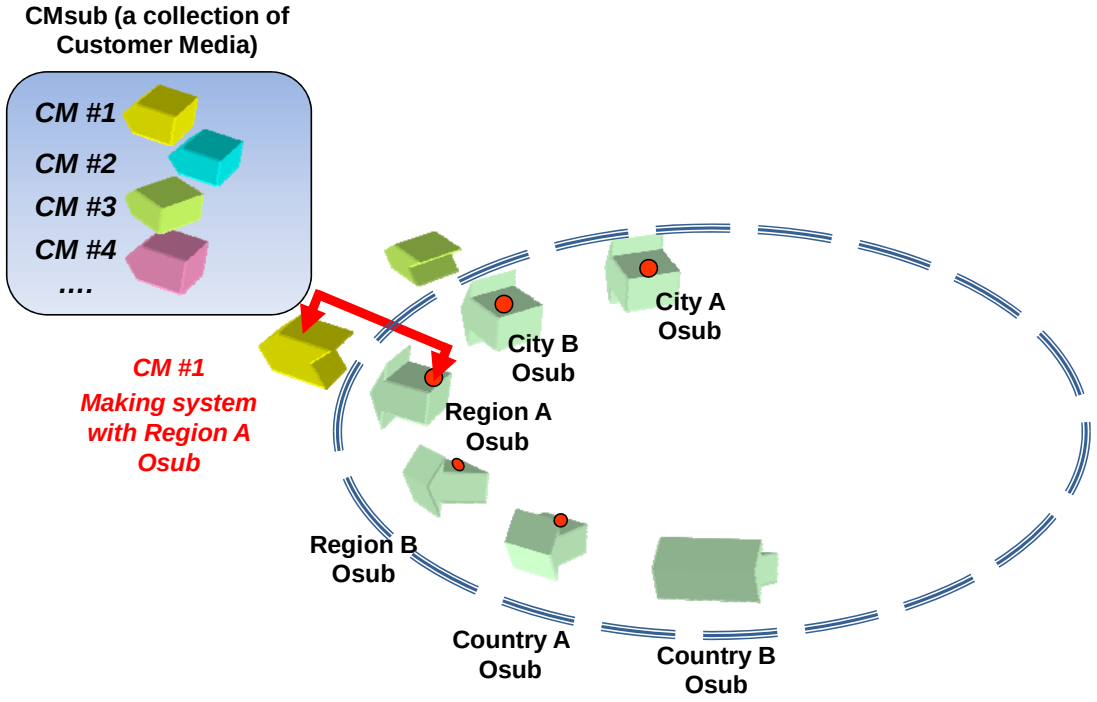
The purpose of those 2 subsystems is to « make system » with each other.

By "making system" we mean here that the CMsub has the capability to communicate with the Osub. This does not necessarily include the ability to support a set of commands, to interpret some data format or to establish a secure connection, which are features dependent on Customer Media's application and/or personalisation.

The purpose of the Customer Medium (CM) is then to "make system" with one or several Organization subsystems through a Medium Access Device.

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

CMsub "Making system" with OSub



Organization Subsystem (Osub) can be characterized according 4 different criteria:

- **On line/ off line system:**
  - On line: every element of the OSub is permanently linked to a central system, that in real time monitors its state and that is involved in the transaction process. This permanent link is provided either through a wired or wireless network. Online systems can implement central or distributed security schemes. In all cases, the Medium Access Device must have online capabilities.
  - Off line: all the components of an off line system are not permanently linked to a central server and supervised in real time. Transactions are processed locally between the Medium Access Device, part of the Osub, and the CMsub. Off line systems are relying on distributed security scheme.

- **Single/ multiple operating entities :**
  - An Osub can be operated by a single entity or by several transport operators.
  - When several actors are operating an Osub, they usually share some common specifications to ensure that any Customer Medium can "make system" with the Organization subsystem through any Medium Access Device:
    - Whoever have provided the Customer Media,
    - Whoever has sold and loaded the Product into the CM,
    - Whoever is operating the part of the Organization subsystem the CM can make system with.

    This usually leads the different actors operating the same Osub to have:
    - the same, high, level of competence towards designing, procuring, running and maintaining an Information system,
    - more or less the same respect towards recommended practices in dealing with public procurement.

Two main kinds of Customer Media can be considered:

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

- **Passive CMs :**
  A passive CM is just storing data that can be securely read/write from the Osub. A Passive CM doesn't have the ability to process a set of commands, even when linked to an energy source. Examples of Passive CMs are contactless paper tickets, memory cards, …

- **Active CMs.**
  An Active CM is hosting an application, i.e. it has the ability, when linked to an energy source, to process a set of commands carrying application data. Active CM contains both data and application code. Examples of Active CMs are microprocessor cards, USB keys, NFC phones, …

With regard to this difference, a CMSub can be either homogenous or heterogeneous.

- CMsub is homogeneous when all the CM of a CMsub can "make system" with any Osub
- CMSub is heterogeneous, when within stated conditions (*starting at the physical level*):
  - the whole of a CMSub can "make system" with a given OSub
  - but only part (or none) of it can "make system" with another OSub,

5.1.4 IFM project vision for building interoperability

From the previous considerations, we can assume that merging existing IFM schemes to achieve a global EU IFM requires decisions by the Transport Organisations and may occur gradually and progressively.

A phased approach to reach gradual levels of interoperability starting from common interoperable media and ending ultimately with common EU products has therefore been agreed as a common input to all WPs and appears as a structuring result of the first year of the project.

- **Step 0 : Existing IFMs**

  At the present, there are several different schemes for Fare Management Systems in operations that are not interoperable between each other at any sense of the word.
  Customer Media are mainly native (i.e. application are non downloadable). Customer Media interoperability can only be achieved if :
  - Common core technology (Mifare, Calypso, VDV KA, …) is accepted across the Fare Management System of the different Transport networks,
  - Mutual business agreements are signed between Transport Organizations to accept each other's media.

- **Step 1: Multi application Customer Media**

  By introducing multi application Customer Media, customers won't need any more to get a dedicated media for each transport network. Customers will download on multi application Customer Media, the transport applications they need as they move across EU.
  - There have to be technical agreements for the usable chip technology and communication standards between reader and medium (p.e. 14443 A or B) and

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

- organisational agreements for example on security matters between the partners.

- **Step 2: EU Status Application**

Customers can benefit from their status all over Europe., but due to the respect of privacy only with their consent

A common EU Status Application is defined. The customer can have this application downloaded in his media (based on the agreed chip technologies, security and communication standard). His home network will export the appropriate data into this EU Status Application according to a common data model.

Any other Transport Operator will be able to read the customer status from the EU Status Application and to use them for the benefit of the customer.

- **Step 3 : Common Web Portal**

Customers can find help and guidance from a common European web-portal to download the applications and purchase the products they need. This portal will provide a link to each transport network existing site that proposes download and purchase services and can allow to develop mutualised service between different transport networks.

- **Step 4 : Common template for local products**

Inside the common EU IFM application, a standardised template is specified. It is in a first step used to host local products. Customers don't need any more to download several local applications for their occasional trips across different IFM schemes. The EU IFM application will be used for hosting all the local products that the customer may need during his journey across EU.

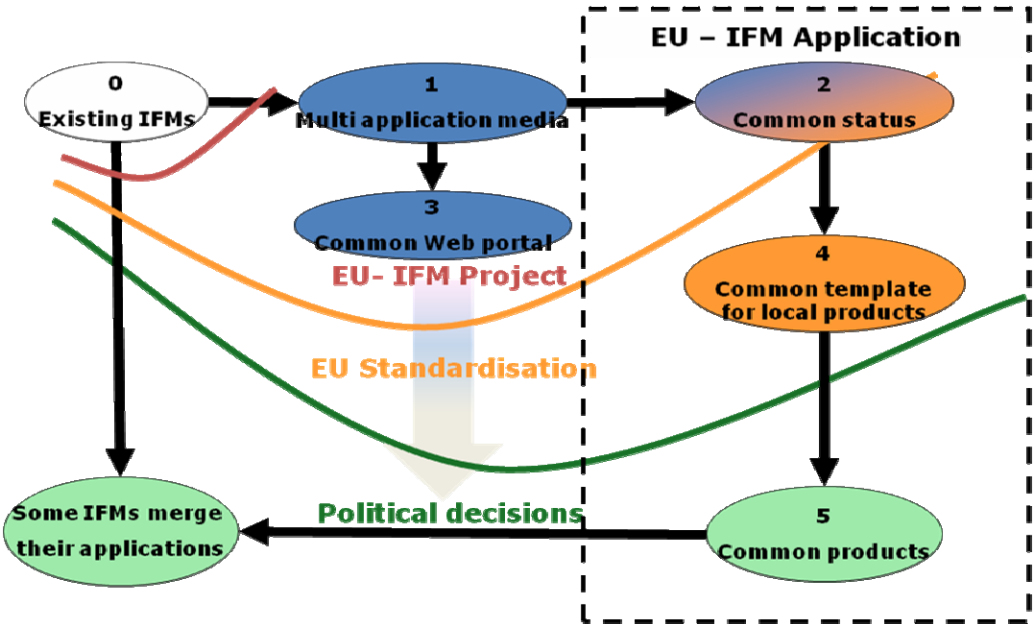
- **Step 5 : Common template for common products**

Common products are proposed and can be loaded into the EU IFM application. Those products can be used on any Transport networks which are EU IFM compliant. These products include interoperable transport payment-schemes.

- **Step 6: Common application**

In an ultimate phase when all / a part EU transport networks will be EU IFM compliant, IFM schemes may decide to stop maintaining their initial applications and to use only the EU IFM application.

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



Steps 1 and 3 can be defined within the scope of the IFM project and made available for use.

Steps 2 and 4 require further standardisation.

The crucial step is the creation of the EU IFM application as a nucleus for ulterior decisions.
It needs a common standardised data model and data structure which was the objective of part 2 of IOPTA standard as defined by CEN TC 224 WG11.
The defined migration path, which proposes the EU IFM application as an add-on to all existing applications doesn't changes the deal from three or four years ago when the proposal was to replace existing applications by a new one. Consensus therefore appears as possible to collaborate to build that standard.

Steps 1 to 4 will make possible the ulterior steps which will then depend upon decisions from Transport Organizations and Operators and hence remain out of scope of IFM project.

The present document will cover the need for multi application and interoperable customer media as described in the step 1 of the present vision.

5.1.5 Payment transactions related to transport product purchase

According IFM 24014-1 ([R1]), transport application is defined as an "Application [that] houses Products and other optional Customer information (Customer details, Customer preferences)".

In all cases, a payment transaction is made in relation with the purchase of transport products. This payment process may vary largely according to IFM schemes and transport application types;

- Pre payment of products using cash, credit/debit card, …
- Post payment with charging on customer banking account or credit card, …

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

- Purchasing of units of credit for reloading the stored value purse of the transport application,
- ….

The use of the payment-process chosen by the customer from the offered range for all transport-related purchases, is a very important issue of interoperability.
Each IFM should pay attention when offering remote loading of its transport application and remote purchase of its products, that adequate payment means are available to the customer via this remote sales channel.

Payment application and payment transaction related to transport ticketing are out of scope of the present work package, so no recommendations will be made here to favour one of them, and ideally all the payment process in place should remain applicable for product purchase.

Additionally, usage of multi application media can be seen as an advantaged as it can also offer to the customer the ability to load jointly in its customer media both transport and payment applications, extending in this case payment possibilities.

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

5.2 General benefits of multi application media

Multi application Customer Media will bring benefits both to the end user and to Transport Operators or Organizations.

Benefits from the end user stand point:

The usage of multi application media for end users brings them some obvious benefits:

- **Greater utility :**
  - The same portable object will bring more usage value as it includes different applications.
  - The types of applications that can be considered in a multi application contactless media goes far beyond the sole transport industry needs, Because contactless applications also exist for payment, access control, event ticketing, loyalty, … a smart multi application Customer Media should be able to host any type of contactless application, hence strengthening its utility.
  - The multiple usage of the same device will raise its level of acceptance by the end user, as they will consider its acceptance not based on a single usage but on the sum of all the potential usages that a multiple application media may provide.
  - Downloading payment applications in the same media as banks propose them and as transport operators may agree to accept them, can allow customer to pay and travel with the same media.

- **Customized usage :**
  - Benefits of storing multiple applications in the same media make sense only if the end user can select the application present in the media.
  - Each end user should be able to install and remove the application he wants, being able to customize its portable object into a tailored made set of applications according to its life style.
  - Even if multi application media may be provided with pre loaded applications, end user should be able to install and remove application at any time.

- **Convenience:**
  - One of the limits of single application objects is that you are quickly limited by the number of objects that you're ready to bring with you on a daily basis in your wallet.
  - Combining multiple applications in the same physical device will offer you the convenience to have always with you the transport card, the loyalty card, the event ticket you need whatever frequent usage or not you make of them.
  - This may remove some barriers for travelers that do not wish for example to have additional transport passes for PT network frequented only occasionally.
  - Additionally, it offers a common ergonomic for different usages in different activities, making the end user feeling in confidence even for a first usage at a new place.

To ensure that those benefits are fulfilled, the following high level requirements must be hence taken into account for multi application Customer Media:

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

- *A multi application media must be able to support the largest possible types of contactless applications (not only the transport ones),*
- *A multi application media must support a dynamic application management.*

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

Benefits from the transport operator stand point:

- **Customer Relationship Optimization Tool:**
  - By leaving the latitude to the end user to manage the contents of its multi application media, transport operators move from Customer Management to Customer Empowerment.
  - This is granting a freedom of choice and comparison-through a dynamic portfolio of personally relevant, evolving services.
  - The end user can for example be proposed with comparison services between private car and public transportation usage, allowing him afterwards to download the public transport application on its Customer Media if he likes too.

- **Partnership Tool:**
  - At a time where transport authorities are looking at enabling additional services likely loyalty programmes, car sharing, park & ride, bike & ride, etc … a multi application Customer Media can be a media where such services can be leverage onto.
  - Multi application Customer Media can be then a powerful partnership tool allowing the coexistence of multiple applications from multiple business partners through a wide range of relationship models.

- **Mutualizing the media distribution cost:**
  - Till now, the cost for transport Product distribution includes the Cost of Ownership for the medium. The media cost may be high compared to the fare value, especially when addressing non frequent visitors that may travel only once in the visited PT network.
  - By extending the usage of the media beyond a single PT network, the cost of ownership of the media can be reduced through the partnership revenues or even zeroed if the end user has already be given (or sold) such a media from another transport network or service provider.
  - Distribution cost itself can be also mutualized and reduced by using some shared remote distribution channel for the media Applications and Products like the internet, Wi-Fi, 3G/GSM networks... and through the set up of a common web portal for facilitating the download of application from different IFM schemes as presented in step 3 of IFM Vision.
  - Multi application media must rely on international standards and open technologies to ensure the largest possible adoption by service providers. The easiest to buy (or to get) the media will be, the seamless it will be for end user to enter into transport network, achieving the ultimate goal of removing the barriers for EU citizens to use public transport whenever possible during a EU journey.

- **Interoperability:**
  - By enabling the co existence of different Applications and by consequence the co existence of Transport Products from different IFMS in the same device, multi application CM is allowing interoperability between different IFMS. This is a first step that is looked at through the EU-IFM project and this topics is developed in the next chapter.

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

5.3 Multi application media as a mean for enhancing interoperability

The aim of this chapter is to identify the benefits of multi-application media for customers who use transport in different IFMs and to iidentify the benefits of multi-application media to enlarge interoperability.

5.3.1 Define interoperability needs

For a passenger, the main objectives of interoperability are:

- the ability to **travel on all the networks within a region of interoperability using the same Customer Media**;
- the access to a **range of interoperable services and products (tariff rights, tickets etc.), distributed and usable equally with several different modes of transport and different operators**, making it as easy as possible to change from one mode of transport to another regardless of the operator and to ensure seamless travel for the end user..

Even if the dubious assertion that the need for interoperability by customers could be the same everywhere, we will have to answer two queries:

- **Interoperability for how many clients ?**
- **Interoperability for how much money ?**

Whenever interoperability has been assessed as a key service for the seamless travelling of the citizens within a given geographical area, Interoperable Fare Management systems have been set up. However, to extend interoperability beyond the existing IFM schemes, the technical gap to close is generally much more bigger than a secret key exchange process, specially when the IFM schemes are different.

Then to help answering these 2 questions, we can assume that generally a single customer acts in fact in 2 zones of interoperability:

- **Zone1: every day uses**
- **Zone2: rest of Europe**

5.3.1.1 Zone1: every day uses

This generally coincides with “first tier Transport Authority” domain (city, region, etc). In that zone, interoperability is a must have service and even more if it’s an “integrated Fare Zone” to be delivered at the lowest possible short & long term cost.

A ‘Local best way’ prevails in the ”every day uses” zone, which means:

- Common fares & price rules apply within the zone.
- Same contracts apply between Authorities & operators
- Same application & security management is used within the zone
- Customer Products are the same and accepted everywhere, even if the PT is operated by several entities.

There is nevertheless **some open doors to “external” admission**, through a shared Application support but **only when all the Fare Management Systems are relying on the same set of technical specifications**. In this case, the admission of frequent out of domain

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

uses can be easily achieved, as technology today allows to solve the question, without having to build any costly, secure failure prone and complex back office system. A shared Application in a single Customer media can be used by any transport operator to load Product or to make use of existing Product in the media, even if the Product has been purchased to a different entity (such as defined by the Triangle European Project).

5.3.1.2 Zone2: rest of Europe

Interoperability here should be more a "Service On Demand" proposed to interested customers. It may be sold for the whole or only part of its costs depending on how much several, adjoining or not, organizations can be interested by having peoples from somewhere else.

This ability is called **"Interoperability On Demand"**. Any one should be able for a just cost, to be delivered to his own Customer Media, what is needed to use public transport where he needs or wants to.

That means using local contracts, bought locally, or at a distance but from the local system saves the cost of a transport clearing system while achieving the goal of *"Everybody local everywhere". The payment process is depending on other facilities.*

The recommended approach is simply to **"use the local transaction"**. Until something else is proven to be more cost and security efficient, the local transactions is used based on:

- Local (even if distant) infrastructures
- Local Application & Product
- Local security principles
- Local payment process

Such approach has the benefit to make void any need for clearing interconnection between IFMS. Application and Product retails remain under the sole control of the originating IFM. Only common requirement on multi application Customer Media must be shared and implemented by the IFMS that want to provide their end user with interoperable media.

5.3.2 Interoperability for application download

Then the purpose of this deliverable is to stress the characteristics of a Customer Media that will be able to "make system" with the OSubs of two kinds:

1) That of an organization that has a very low intolerance to risk, that evinces a low level of sophistication in business matters (the cheapest the best), and doesn't want customer to pay for "complicated things". It uses an heterogeneous, passive devices based CMSub. It's OSub is off line, is operated by a single entity, and deal with suppliers with business as usual rules.

And

2) An organization that has a very high intolerance to risk, that has a high level of sophistication in business matters, and want customers to pay their fair share. It uses an homogenous active devices based CMSub. It's OSub is off line, and is operated by a federation of entities under exacting rules of management & security.

Without driving the first one to support the cost of the care that the second needs, or the second having to bear the cost of the lax management of procurement by the first one.

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

Previous exposed complexity and difficulties to carry out a migration of current Osubs to be capable of sharing common media, force to find solution in the media itself.

The objective is then to define a multi application CM able to be operated:

- (A) In all existing or future CM subsystems,
- (B) Immediately with no predictable registration in a new Osub,
- (C) Without any dedicated modification in this new Osub

Due to the deep connection at the application level between CM sub & OSub:

(A) could be partially provided with a limited number of Osub (as it not possible to load all the existing EU applications in a single media)

(B) & (C) never could be.

As we propose to reach interoperability in a first step by enabling the CM to implement local transaction, application interoperability requirements are then simply translated into requirements for an **interoperability for application download on CM.**
Each IFM willing to propose easy access to visitors, will then provide a new distribution channel to allow the downloading of its application onto multi application CM or can rely on a common web portal mutualised between different FM schemes.

Product loading within the CM can be then performed according to the local rules trough existing distribution channels as the multi application CM will behave like a local CM from the Osub side. If needed, product loading capabilities can be also offered through a new remote distribution channel.

Later on, when some EU IFM application will be available, the downloading process will remain applicable to load the EU IFM application onto the CM.

5.3.3 From Static to Dynamic Application Management

As seen, to reach interoperability through application download, we need to introduce the new concept of a Dynamic management of application by & in the media.

A Dynamic application management gives the key for a real and wholehearted mobility, through the concept of an 'interoperability on demand'.

Dynamic application management removes & brings nothing regarding ""Do we have something to propose for roamers ? & what common security should be used", but it's the first step to avoid all predicated constraints & organisation of transport applications in mobility schemes.

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

6 Description of multi application management functions

This chapter defines common requirements on interoperable contact less media and multi-application management for Public Transport.

It suggests an additional level as a contribution to ISO EN 24014-1 (IFM) functional model to describe the links between the platform issuers and managers and the application issuers and managers and additional guidelines to the GlobalPlatform specifications for reaching an interoperability of transport application download on multi application contactless Customer Media..

6.1 Requirements for interoperable Customer Media

Requirements for an interoperable Customer Media can be divided in 2 parts:

- Interoperability at application level :
  By nature, the customer media is interoperable in its home IFM, i.e. the "every day uses" zone. Extended interoperability will be achieved by the coexistence of several local transport applications in the same media. Further interoperability at application level can be achieved by the acceptance of a common EU IFM application, but as explained previously, this phase require standardization work at EU level to define such application.

  ⇨ **Except the fact that the application must exist in a package form that can be downloaded and Security measures for the download of the application are prepared on the medium , no further requirement is defined for transport application in the IFM project**

  NB: As the IFM is an evolving system, dynamic application management can allow to the CM to follow up and be upgraded according to technical changes in the IFM system.

- Interoperability at application downloading level :
  This is the interoperability on demand for "Rest of Europe" zone.

  ⇨ **Requirements will be defined hereafter for the multi application Customer Media and for the application downloading process.**

6.2 Requirements for multi application Customer Media

The following functional requirements must be fulfilled by multi application CM as recommended by the IFM project.

R1: The multi application Customer Media must bring new functionalities to public transport ticketing to make customers' lifes easier:

1) The customer can load and manage several transport applications in the same device,
2) Customer media enables customers to select, buy and load a transport product through the existing product retailing channels,

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

3) Optionally, customer media can enable customers to select, buy and load a transport product remotely, at the user's chosen place and time by its own (mobile phone) or via a PC internet connection,
4) The customer can access the transport network directly with the media,
5) Optionally, if the media provides such interactivity, the customer can select the transport ticket or the transport application he wants to use. The capability for some CM type to be interactive (like NFC phones for example) can allow a more important mix of applications or products on it.

R2: Multi application media must rely on open industry standard for contactless multi application devices:

1) Microprocessor based device
2) Java Card 2.1 or later as open multi application OS
3) GlobalPlatform Card Specification 2.2 (and amendments) for application management
4) ISO/IEC 7816 as APDU interfaces to the IC (microprocessor)
5) ISO/IEC 14443 type A or B as RF communication protocols
6) A set of standard crypto algorithms (DES, 3DES, RSA, ….) needed by the transport applications
7) The chip must be evaluated to specific protection profiles
8) The chip must have a minimum required memory and velocity

Memory card haven't been considered for multi application devices as they can only implement some predefined family of applications (or more precisely data structure), whereas a microprocessor based device can host any type of application including those emulating memory card.

Relying on open and international standard is the best way for operator to favor an approach that will insure multi sourcing capability to get:

- Competition leading to lowest cost for implementing these principles (avoid / stress on proprietary solutions and favor an open technology),

- Durability for getting products or services from the market (i.e. if one supplier disappear, there are still others available),

- Availability of objects used and distributed by others actors like NFC mobiles, USB contactless keys, …

Java Card and GlobalPlatform are the most used standard in the smart card industry for contactless device whatever the form factor may be: key fob, contactless USB token, Secure Elements (SE) for NFC mobiles should it be an embedded SE, a UICC (SIM) or a secure memory card. GlobalPlatform is an application management standard in the banking industry since end of 1990's, is field proven for multi application and work on specs enhancements to support contactless applications. More, Java cards & GP are offering the maximum access to multi application media for banking and telecoms industries compared to which the transport world may currently look small in term of volume of smart devices.

Java Card technology is offering limited development and seamless deployment for application providers, thanks to the "Develop once, Run everywhere" Java promise.

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

For interoperability, GlobalPlatform provides not only an external interface but also defines the roles of the various actors and different scenarios required to manage, at a large scale, an administration of downloading applications.

To sum up, GP contribution to IFM project could be divided in 3 pillars:

- **API & commands** to manage each application & its associated life span,
- **Security Domains** as on board representatives in the CM of external actors & certificated parties,
- **Secure Channels** to ensure Application authentication & confidentiality from loading to personalisation phases over the air or over the contactless interface.

In addition to the security mechanism provided by GP for the application loading and personalization, Java Card environment is also providing a security framework that offers application firewalling.

R3: Customer media's form factor has no importance provided that the transport application is stored in a smart card component that matches with R1 & R2 requirements. A non exhaustive list of possible form factors for customer media is given hereafter:

1) Contactless smart card
2) Dual (contact & contactless) smart card
3) NFC mobile phone with application stored in the UICC
4) NFC mobile phone with application stored in an embedded Secure Element
5) NFC mobile phone with application stored in a removable Secure memory Card
6) Contactless USB key with application stored in an embedded Secure Element
7) …

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

6.3 Requirements for interoperable downloading process

6.3.1 Introduction

To achieve a global interoperability, different levels of interoperability must be considered:

Interoperabiity Level	*Domain/Tasks*
Business Data	Common vocabulary
Business Process	Roles and Responsibilities
	Process and Constraints
Data Exchange	Data Structure
	Mutual authentication
	Integrity and Security of information
	Error Handling

The different interoperability levels are defined hereafter:

Business Data

Common Vocabulary:

- ➔ clear understanding and agreement of terms being used
- ➔ clear rules about how and where the terms can be used in a way that remains meaningful

Benefits

- ➔ Simplify relations with partners
- ➔ Ensure that information exchanged is used the way it was intended by the creator of that information
- ➔ Enable systems to aggregate information from different sources and process it in a meaningful manner

Business Process

Roles

A Role is an abstract model which specifies a set of duties and tasks

Responsibilities

Comprehensive list of

- ➔ Actions / Functions to perform
- ➔ Business data to exchange
- ➔ Role assignment is dynamic

Benefits

- ➔ Independent of entity/partner
- ➔ A role can be perform by one or multiple entities
- ➔ One entity can perform multiple roles

Data Exchange

Data Structure

- ➔ XML Structure
- ➔ XML Schemas for validation
- ➔ Protocol independent

Benefits

- ➔ Platform independent
- ➔ Describe only the content, not the protocol
- ➔ Easy conversion to and from legacy format

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

➔ Support specialization

6.3.2 Business Data requirements

Business Data requirements define what should be downloaded. For ensuring application download the following set of data must be considered:

- Application code (Java Card Applet package)
- Loading keys (i.e. keys allowing an access to the Medium)
- Personalization data including application keys

6.3.3 Business Process requirements

Business Process requirements define who should be part of the downloading process (as part of new & existing IFM roles):

- Application owner
- Product owner
- Application retailer
- Media owner
- Media loader

Product loading is considered as out of scope of the downloading interoperability requirements. Once an Application is loaded in a media, the way the media interact with the Osub is based on local transaction and then doesn't need additional requirements to the existing local ones.

GP technology is open to allow different business process for application loading. Loading and security checking can be performed by different entities. Security scheme can be set up to ensure mutual authentication, data integrity checking and confidential data loading. Those security schemes can be based on secret key or public key mechanisms.

Those requirements will be refined in WP3.2.

6.3.4 Data exchange requirements

The data exchange requirements aim at defining the format of data exchanged between the different roles.

They will be based on GP messaging format and GP profiles exchanges.

They will not be defined at this level of documents but specified later on in the WP3.2.

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

6.4 New roles to be considered in the IFM Conceptual model

6.4.1 Introduction to the IFM as it is

The IFMS ISO 24014 - Part 1 standard [R1] defines a functional reference architecture for interoperable transport ticket management systems.

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

- management of Application;
- management of (Fare) Products;
- security management;
- certification, registration and identification.

This IFMS defines the following main elements:

- identification of the different functional entities in relation to the overall fare management system;
- a generic model of IFMS describing the logical and functional architecture and the interfaces within the system and with other IFMSs;
- Use Cases describing the interactions and data flows between the different functional entities;
- security requirements.

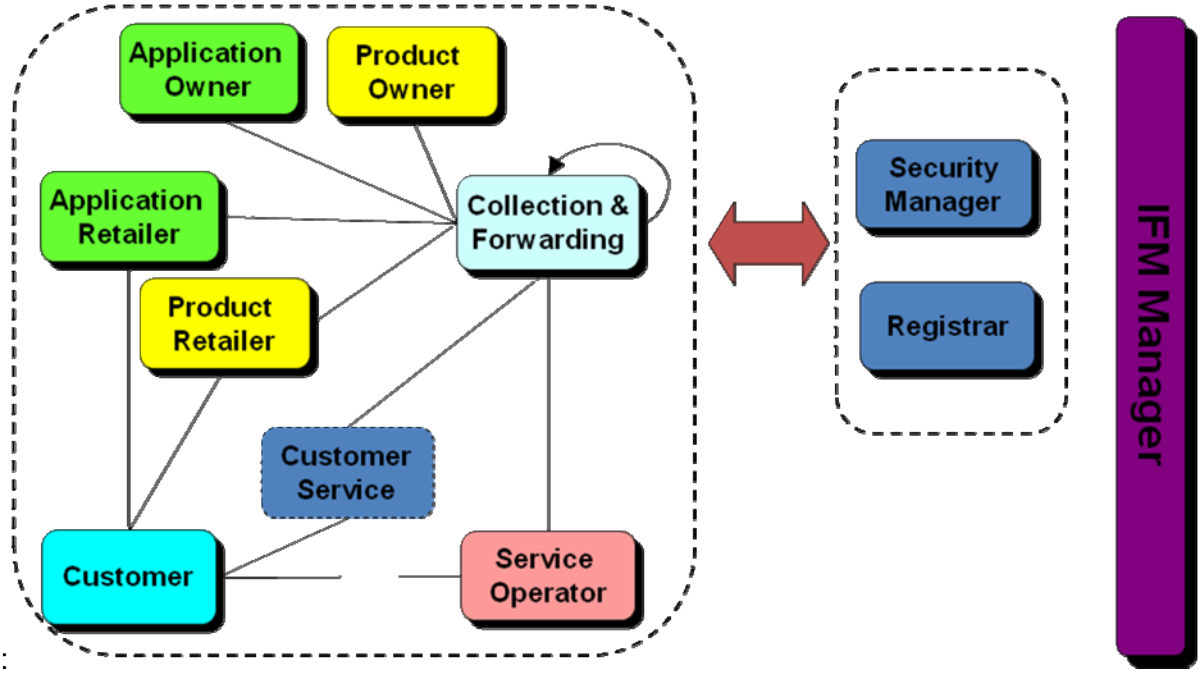
But excludes consideration of:

- the physical Medium and its management;
- the technical aspects of the interface between the Medium and the Medium Access Device;
- the data exchanges between the Medium and the Medium Access Device;
- the financial aspects of fare management systems (e.g. customer payments, method of payment, settlement, apportionment, reconciliation).

The IFM functional reference architecture is described as followed in [R1]

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

IFM model as it is (ISO 24014)



:

6.4.2 New IFM roles and impacts on the IFM model

The Customer Medium is the physical carrier for Applications.

The need for a multi application Customer Media implies to introduce into the existing IFM model, new roles linked to the media distribution process and to describe the impact on the existing roles.

We propose to introduce 3 new IFM roles related to the Medium handling:

- Medium Owner :
  - The Media Owner authorizes application retailer to access a security domain in the media, to download an application and to operate it.
- Medium Retailer
  - The Media retailer has a business relationship with the end user
  - The Media retailer defines the contractual conditions of usage of the services on the media.
- Medium Loader
  - The Media Loader manages the remote access to the media.

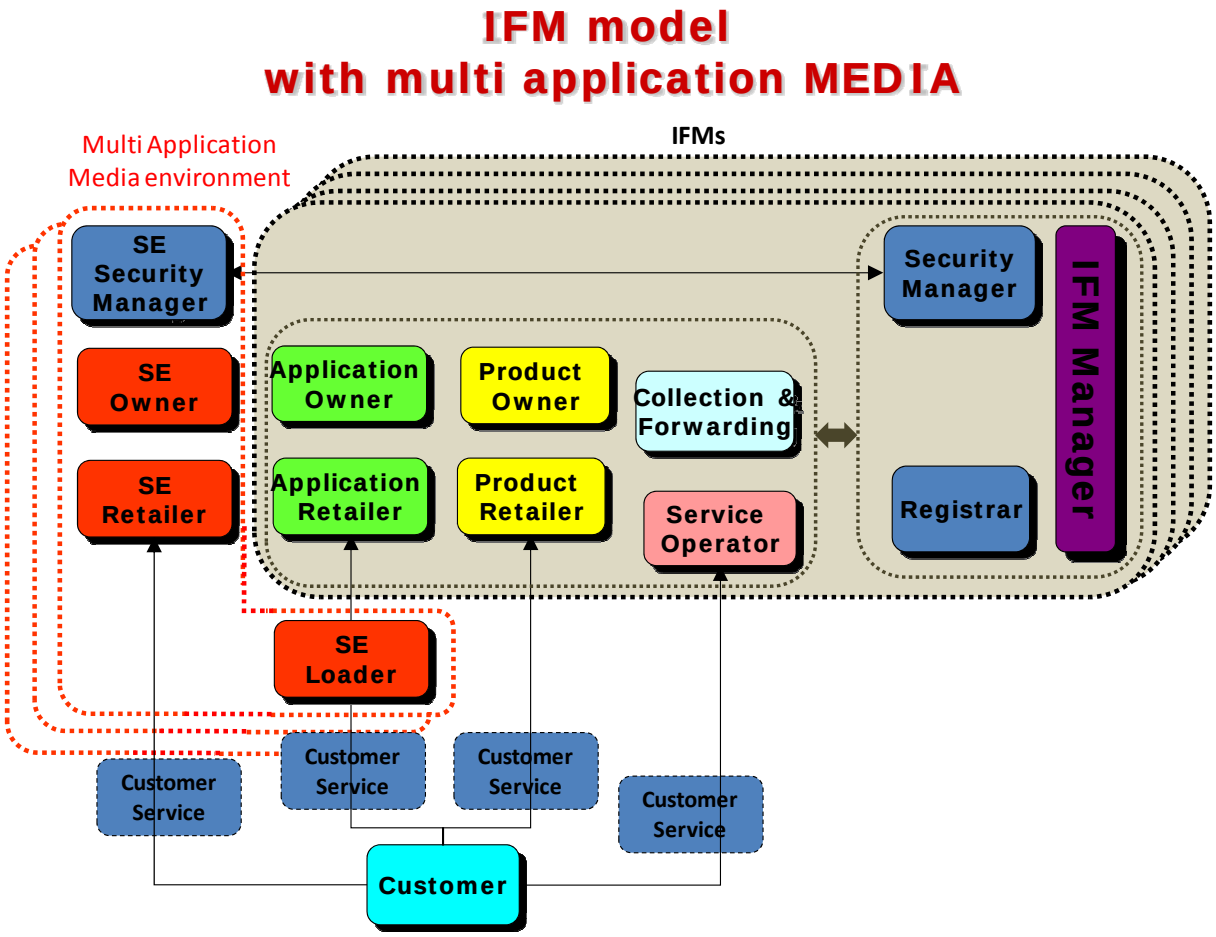
Those new roles have also some impacts on existing IFM roles:

- The Medium Owner, Medium retailer and Medium Loader roles must be linked to the Collection & Forwarding Agent role.
- We can also imagine that the Registrar and Security Manager may be involved in the issuance process of the Media.

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

- The scope of the roles for IFM manager, Application Owner, Application Retailers and Product retailers may also be impacted by the new Medium roles.

A proposed evolution of the IFM Model may look like:

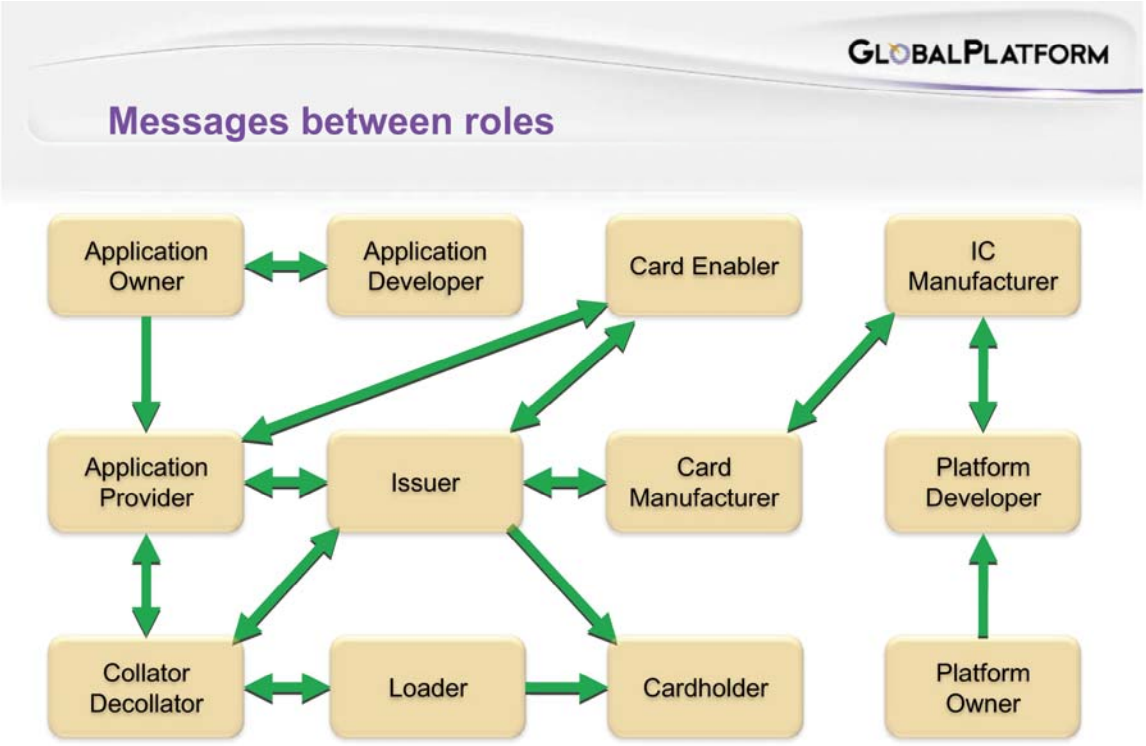


These suggestion for IFM model evolution will be discussed within the ISO EN 24014-1/ CEN/TC 278 work group. It's also recommended as far as possible to combine IFM and GP terminologies for the next phase.

6.4.3 Correlation with GlobalPlatform standard

The different roles for multi application media issuance as defined by Global Platform Systems Specifications are shown hereafter. Specifications are also defining GP messaging between some entities (green arrows).

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



Global Platform roles are defined in [R3] and a brief definition is given hereafter:

- **Application Developer**

The Application Developer writes application code.

- **Application Owner**

The Application Owner defines and maintains the application specifications.

- **Application Provider**

The Application Provider procures the necessary components to load a complete application on to a card (i.e., application code, application data, application keys and/or certificates, and data belonging to a specific Cardholder). The Application Provider has a direct business relationship with the Cardholder and provides a card-based service to that Cardholder.

- **Card Issuer**

The Card Issuer holds ultimate responsibility for the GlobalPlatform card. A Card Issuer may be the only authority that allows load, install, delete, extradition or personalization of applications or the Card Issuer may delegate load, install, extradition or personalization of the applications to a third party such as an Application Provider, via the SSD manager.

The Card Issuer issues cards to the Cardholders. The Card Issuer is responsible for securely managing all the pre-issuance production processes culminating in a card specifically prepared for a Cardholder, and for many post-issuance processes, including final decommissioning of a card.

The Card Issuer determines a portfolio of applications to be supported and offered to its card base. The Issuer manages authorization of applications permitted to reside on its cards.

- **Card Holder**

The Cardholder is the entity that receives the card. A Cardholder maintains the contents of the chip with the authorization of the Card Issuer.

- **Card Enabler**

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

The Card Enabler performs pre-personalization functions, specifically the loading of the initial Issuer, a Controlling Authority Security Domain and if any, Application Provider Security Domains. Furthermore, the Card Enabler can personalize the Security Domain with Issuer, Controlling Authority or Application Provider specific data. The Card Enabler prepares the platform for subsequent application loading.

- **Collator/Decollator**

The Collator/Decollator performs the collation of multi-application personalization data for each Cardholder into a single data stream for processing by a Loader. After personalization, the Collator/Decollator performs the decollation function to return information to the Issuer and the appropriate Application Providers about the results of the personalization process. The functionality of the Collator/Decollator in the context of NFC and post-issuance is to do collating/decollating of the personalization data between the SSD Manager and the Loader.

- **Loader**

The Loader loads Card Issuer specific cards with applications and/or personalization/customization data according to the instructions of the Application Provider [complying with security policies and procedures set by the Card Issuer]. It may also place the final Security Domains keys on the card.

- **Card Manufacturer**

The Card Manufacturer is the entity that manufactures (fabricates) cards to the requirements of the Card Issuer.

- **IC Manufacturer**

The entity that fabricates wafers containing chips with a specified ROM configuration.

- Platform Specification Owner

The Platform Specification Owner defines and maintains the card platform operating system specifications.

- **Platform Developer**

The Platform Developer is responsible for the development of the GlobalPlatform cards according to the Specifications provided by the GlobalPlatform consortium.

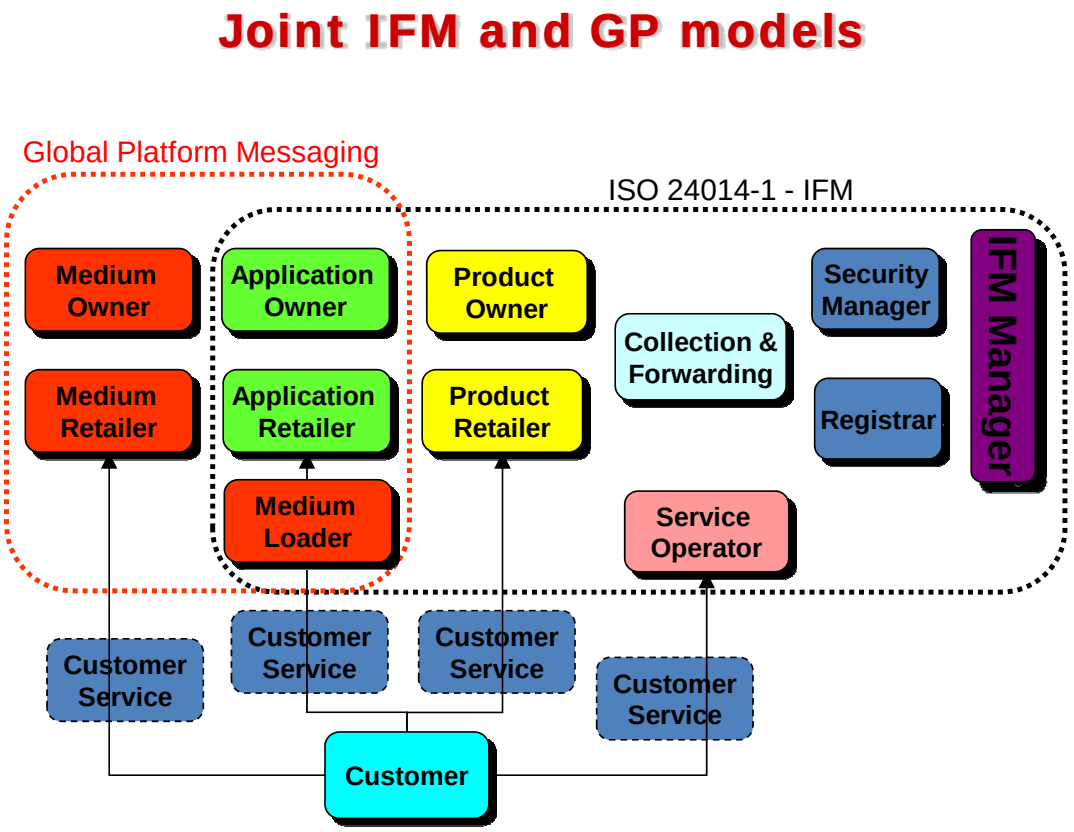
There are some correspondences between IFM and GP Conceptual models even if the scope of the 2 documents are slightly different:

IFM Definition	*Global Platform Definition*
Medium Owner	**(Card) Issuer & Card Manufacturer & IC Manufacturer & Platform Developer & Platform Owner**
Medium Retailer	n.a.
Medium Loader	**(Card) Loader & Card Enabler**
Application Owner	**Application Owner & Application Developer**
Application Retailer	n.a.
Product Owner	**Application Provider**
Product Retailer	n.a.
Customer	**Cardholder**
Service Operator	n.a.
Collection & Forwarding	**Collator/Decollator**
Registrar	n.a.
Security Manager	n.a.

(*) Some roles are out of scope of the GP Messaging conceptual model which only describes a technical solution. They are then indicated as not applicable (n.a.).

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

It is then easy as a next step to imagine to use the GP messaging specifications to describe the different interface between the media issuance actors. Then, the global conceptual model combining the transport IFM specific model with the cross industry GP model can look like as follows:



Advantage of such approach is that the guidelines for GP messaging usage in the transport IFM environment may likely be valid for the issuance of any type of application.

A further description of applications download requirements based on GP messaging will be made in the next WP3 deliverable.

---------- End of document ----------

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