KONTIKI

WG Interoperability

European Interoperability in Electronic Fare Management

A contribution by Kontiki

www.kontiki.net

European Interoperability in Electronic Fare Management

A contribution by Kontiki

Working Group Interoperability, Version 1.0, February 2012

European Interoperability in Electronic Fare Management

A contribution by Kontiki

Table of content

1 List of Abbreviations

AES	Advanced Encryption Standard
ATQ	Answer to Request
AVM	Automatic Vending Machine
BiBo	Be-in / Be-out Technology
CEN	Comité European de Normalisation
CiBo	Check-in / Be-out Technology
CiCo	Check-in / Check-out Technology (= Tap-in / Tap-out)
CTA	Charge to account
CWA	CEN Workshop Agreement
DES	Data Encryption Standard
EMV	Europay Master Visa
EN	European Norm
FSP	Financial Service Provider (e. G. Europay, Mastercard, Visa)
IEC	International Electrotechnical Committee
IFM(S)	Integrated Fare Management (System)
ISO	International Standardisation Organisation
ISSS	Information Society Standardisation System (CEN)
NFC	Near Field Communication
OS	Operating System
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
PT	Public Transport
PWI	Preliminary Work Item in CEN and/or ISO
RSA	Rivest Shamir Adleman (crypto method)

STR	**Stored Travel Rights**
TC	**Technical Committee in CEN or ISO**

2 Introduction

The free movement of people in Europe requires border-crossing, practical solutions for everyday mobility demands of public transport and the services that result from them.

Taking the development of EFM in Europe so far as a base, which is characterized by the creation of national standards (e. g. KA in Germany, TLS in the Netherlands, Rejsekort in Sweden and ITSO in UK), this document deals with possible approaches to creating European interoperable fare management from these existing national solutions.

A detailed consideration of the facets of the term ‘interoperability' in chapter 3 is followed by a description of various models in chapter 4, which is then used in chapter 5 to derive requirements for European interoperability. Chapter 6 deals with the European rules & regulations necessary for the discussion.

3 Interoperability in electronic fare management

3.1 Definition of Interoperability

Interoperability as a term is used in a wide context. Due to European circumstances only effective interoperable systems will allow efficient cross-border services. So far interoperability can be defined in general terms as:

> *....the ability of systems to provide services to and accept services from other systems and to use the services so exchanged to enable them to operate effectively together.*

Restricting this definition to the working group scope and focus on public transport, interoperability in public transport can be defined as:

> ***.....the provision for the passenger of a seamless journey using the same application on the networks of all contractually participating service operators at any moment of time.***

The following extension of the term interoperability - merely referring to electronic ticketing systems - is integrating most of the published documents such as CWA 18092 (CEN/ISSS workshop FASTEST) and national relevant literature from Germany, France, UK and Netherlands.

The understanding of the term interoperability can be treated on four levels:

- Technical
- Procedural
- Contractual
- Usage

3.1.1 Technical Interoperability

Technical interoperability means the capability of different sets of equipment to work together or share resources through physical or wireless interconnection. Technical interoperability includes physical interoperability and syntactical interoperability.

Physical interoperability is the ability to establish communication with the integrated circuit (IC), using electronic and mechanical specifications.

Syntactical interoperability is the ability to create the same functionality using different user media with different protocols and data structures. A high level abstraction of the data objects and access mechanisms is necessary.

The interoperable public transport application has to support all technologies of media acceptance, tariff systems, payment methods and payment means in the networks of all participating service operators. Interoperability can be said to contain three components, each of which in its own right provides a degree of interoperability.

These components are:

- Medium and its software has to be compatible with the terminals in all participating service operators' networks used for loading, reading, validating and inspecting the data on the user media.
- The application on the media has to be accepted by the terminal(s) above.
- The proof of entitlement on the media has to be valid on the host passenger service operator's network.

3.1.2 Procedural Interoperability

Procedural interoperability means the adoption by different sets of equipment (IC and Interface device) of common data element definitions, procedures for data delivery, and presentation formats (common interpretation of the data objects as well as common rules for their manipulation and use).

3.1.3 Institutional and Contractual Interoperability

Institutional and contractual interoperability is generally a common approach, expressed through contracts, to objectives and needs related to the provision for the passenger of a seamless journey using the same application on all contractually participating service operators. These objectives and needs should cover the exchange of information as well as a coherent policy on the use of this information and the making of connections.

A fare product (contract) is interoperable if it can be accepted (not necessary validated) by more than one service operator, whoever sells and loads it. A fare product is a marketable commodity whose specification determines the conditions of access to a passenger transport service or services. These conditions are based on a set of usage and pricing rules.

Multi-operator fare products allow benefit to service operator which they need to take into account for their business strategy. New commercial agreements for cross sale of fare products or commonly shared fare products can be negotiated. Multi-operator fare products include two levels**:** common fare principles (zone, section, distance, time) and common fare offer (season tickets, single tickets …). There are the following fare products usable across schemes:

- All fare products are proprietary and only sold and accepted by one service operator. Operator own fare product.
- All fare products are proprietary and only sold and accepted by one service operator. Operator own fare product. Cross sale are possible.
- All fare products are proprietary and only sold and accepted by one service operator. Operator own fare product. The service operator accepts at least one multi-operator fare product. In case the service operators belong to the same network, the fare product is defined as common fare product. In case they belong to different networks they are defined as shared fare products.

The specification through binding agreements underlines the intention of service operators to co-operate and the processes by which they act accordingly.

For the organising authorities this institutional interoperability allows to offer one integrated fare system with common rules of service contracts and subsidy allocation and revenue sharing enabling:

- Usage statistics for the service operators and authorities.
- Realisation of one customer profile based on social criteria.
- Rules for revenue sharing and compensation.

3.1.4 Usage Interoperability

On this level the customer perception is meant. Which kinds of gestures are necessary when embarking public transport? How and where do the customers buy their tickets, how do they validate tickets, how do they exchange their tickets in case of loss or theft?

- Visual identity on all existing equipment.
- Systematic validation gestures.
- Ergonomic recommendations for hard- and software.
- Local use instructions for electronic purses.
- After sales rules.

3.2 Interpretations

Deriving from this four levels there are two possible interpretations of the term interoperability:

- Closed interoperability concept
- Open interoperability concept

At first glance the term “closed interoperability” appears to be contradictory. Basically it means that a group of service operators can have agreed upon data models and encoding being external to all existing standards. Consequently a convergence scenario is not possible for other service operators as they would have to adopt these definitions. In addition there would be no freedom of choice of supplier.

To avoid this scenario only a concept of open interoperability would be adoptable. Such a concept is legally backed by national ruling like e.g. in UK where competitive supply and multiple sources for devices, equipment and back offices is compulsory.

Resuming the aforementioned definition of interoperability a user media issued for use within one electronic ticketing scheme is technically compatible with the sales, validation (and eventual rewriting for changes) reading and inspection terminals used in another electronic ticketing scheme, then potentially the two schemes are interoperable. In this situation it is technically possible for a customer to use a compatible media in both schemes.

Examples of this could be within a city in a multi-modal environment (train, metro, tram, bus) where a customer can travel with his medium. Extensions of this are possible to regions, nations or within an international context. To achieve this level of comprehension it is necessary to agree on common principles dealing with the interfaces among participating partners. Procurement policy shall be kept to the decision autonomy of each single partner, but still keeping the commitment of open interoperability.

Basic principles for compatible interoperable specifications:

- The authority in charge of public transport in a dedicated region should be in charge of the governing and monitoring of interoperability rules among the participating companies.
- Compliance with this rules guarantees interoperability among any participating company.
- The interoperability rules have to be based on existing standards to ease geographic extension of the scheme.
- Multi source industrial environment shall be guaranteed for all service operators as there is no preferential supplier that will be able to impose its products for subsequent system implementations. An open and fair competitive tendering process will be assured.

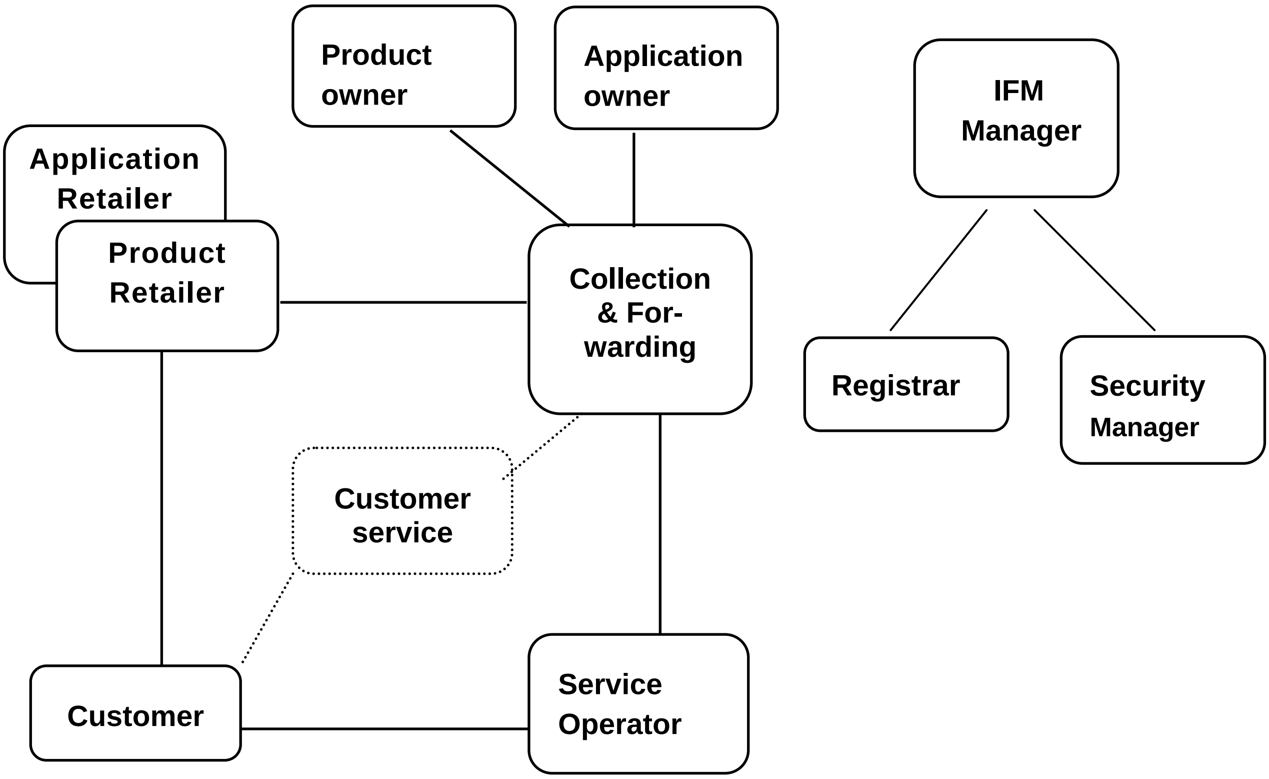
3.3 EN ISO 24014-1 Logical Roles Model

A first approach to an architecture of European interoperability in IFM is the agreement on a common definition of the players involved in IFM. This definition shall abstract from the numerous physical organisations. The EN ISO 24014-1 standard therefore decided to go for a generic roles model.

The following paragraphs are an extract from this standard as published.

3.3.1 Basic Framework of the generic IFM model

- **Relationships** between the entities of the IFM system are described in the following figure.
- The **lines** between the entities represent data exchange. Optional relationship and entities are drawn in dotted lines.
- It is assumed that the Customer has already a **Media** therefore the model considers only application and product issues.



Two transversal entities are added to the IFM model:

- The **Registrar**, indispensable entity for the identification of any organisation, component, application template and application, product template and product involved in the IFM system.
- The **Security Manager**, the supporting entity responsible for the secure operation of the IFM system.

Any other entity is related to the Security Manager and the Registrar.

3.3.2 Description of the Entities

Product owner

He is responsible for his products with the following functions:

- Specifying pricing, usage and commercial rules.

Functions of Clearing:

- Trip reconstruction - product aggregation based on received usage data using product definition rules
- Linking of aggregated usage data with acquisition data
- Preparation of apportionment data based on Product Specification rules

Functions of Reporting:

- Detailed
- acquisition data with no link to usage data within the reporting period
- usage data with no link to acquisition data within the reporting period
- linked aggregated product data within the reporting period

- Summary
- apportionment data and clearing report
- Total acquisition data

Product Retailer

Sells and terminates entitlements or contracts on basis of a given product, collects and refunds value to a customer as authorised by a product owner.

The Product Retailer is the only financial interface between the customer and the IFM system related to products.

Application Retailer

Sells and terminates applications, collects and refunds value to a customer as authorised by an application owner.

The Application Retailer is the only financial interface between the customer and the IFM system related to applications.

Collection & Forwarding

The role of Collection & Forwarding is the facilitation of data interchanges of the IFM. The general functions are data collection and forwarding comprising at least the following functions:

Functions of Collection:

- Receiving Application Template from Application Owner
- Receiving Product Template from Product Owner
- Receiving data from Service Operators
- Receiving data from Product Retailer
- Receiving data from Application Retailer
- Receiving data from other Collection & Forwarding Operators
- Receiving security list data from Security Manager
- Receiving clearing reports from Product Owner
- Consistency and completeness check of the data collected on a technical level
- Receiving address list of all entities in the IFM from the Registrar

Functions of Forwarding:

- Forwarding “Not On Us” data to other Collection & Forwarding Operators.
- Recording “Not On Us” data
- Forwarding data with corrupt destination address to security manager

- Forwarding “On Us” data to the product owner for clearing and reporting
- Forwarding clearing reports, Application Template and Product Template, security list data to the Product Retailer and Service Operator
- Forwarding application templates, security list data to the Application retailer and Service Operator

NOTE: the “ON US and NOT ON US” concept:

- A specific Collection & Forwarding function is to collect data from one IFM entity and forward it to other IFM entities.
- Logically there may be several Collection & Forwarding entities within the IFM.
- IFM entities may be linked to different Collection & Forwarding but each entity can only be linked to one.
- The concept of "ON US and NOT ON US" addresses this connectivity functionality. Data held by a specific Collection & Forwarding is either "ON US" or "NOT ON US" data
- Data collected by a specific Collection & Forwarding addressed to IFM entities directly linked to this Collection & Forwarding is termed "ON US" data.
- Data collected by a specific Collection & Forwarding addressed to IFM entities not linked to this Collection & Forwarding is termed "NOT ON US" data.

Service Operator

The service operator provides service to the customer against the use of a product

Application Owner

Hold the Application Contract for the use of the application with the customer. The entity that owns the application on the Customer Media on which the Product Owners will install their products.

Customer service

Subject to commercial agreements may provide “helpline” and any similar facilities including stolen and damaged Customer Medium replacement and consequential product reinstalling.

Customer

Holds an application, buys products in order to travel.

Security Manager

The Security Manager is appointed by the IFM Manager. He is responsible for establishing the security policy and

- certification of organisations, application templates, components and product templates
- auditing of organisations, application templates/applications, components and product templates/products

- monitoring the system
- operation of the security of the IFM system, e.g. key management.

Registrar

The Registrar is appointed by the IFM Manager. After the certification, he issues unique registration codes for organisations, components, application template, product templates. The Registrar function also issues unique identifiers or rules for generating unique identifiers for the applications, products and messages.

3.4 The role of payment

There are different methods of payment which are related to different types of products like:

- Stored Value , Pre-Paid Contract (STR)
  - Public Transport Tokens (ruled by PT, integrated in the transport application)
  - Open Electronic Purse (ruled by financial sector, not integrated in the transport application but present in the media)
- Charge to Account (CTA)
  - Post-Pay Account (the customer is invoiced after a certain time period and pays then)
  - Pre-Pay Account (the operator is allowed to collect a contracted fixed amount from the customer's bank account in advance whenever a certain floor-limit is reached. All transactions of the customer are then calculated against this pre-paid account)
- Conventional Payment Method
  - Cash
  - Debit-, Credit Card,

The payment method offered to the customer is a decisive factor for the evaluation of interoperability in connection with the technology of media acceptance used. Stored tickets or passes do not provide interoperability unless the product is contractually accepted everywhere. It is the stored payment contract accepted everywhere that grants access to a PT network.

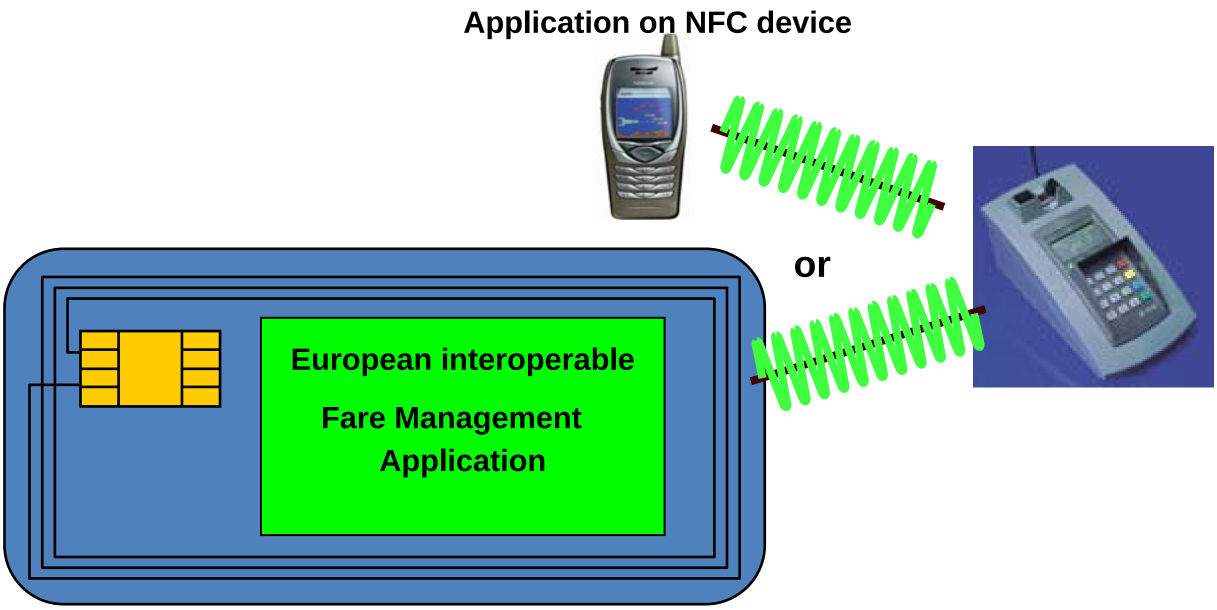
The rules and regulations related to payment are defined by the banking sector. These matters are therefore not in the scope of this document.

4 Models on Interoperability

Depending on the use of public transport by a user four models of interoperability can be distinguished. These models differ in the complexity of the relevant technical solution.

4.1 Model 1: One European IFM area comprising all kinds of fare products

All user media issued to be used in all contractually participating PT networks contain a European wide common accepted IFM application being used everywhere in the referenced area without restriction on the fare structure whatever maybe the native issuer of the media/application. A native home-application is no longer necessary.

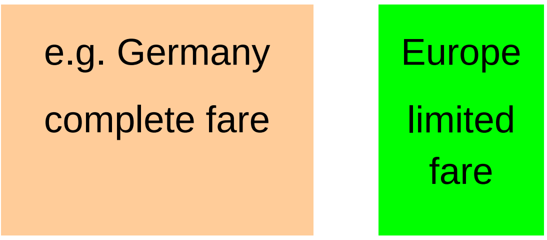


All technologies of acceptance will have to be supported by the media. One single security architecture is required that has to be maintained centrally.

A model for users travelling regularly or occasionally through many IFM areas using the whole range of product offers at any time (provides everyday complete interoperability everywhere).

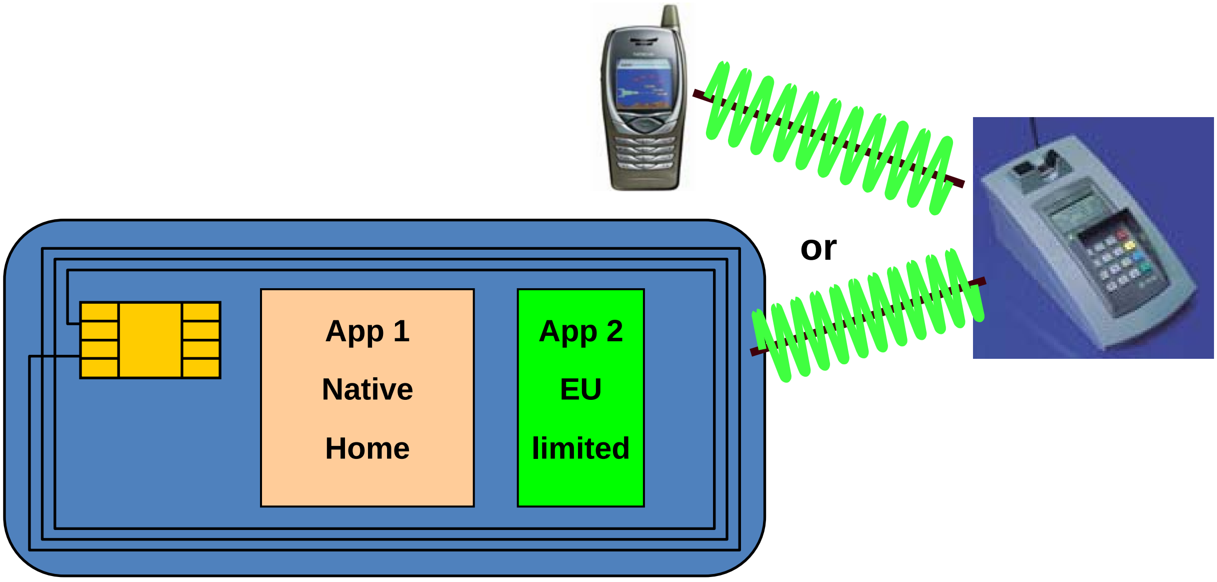
There must be an agreement amongst all participating network operators about the common definition of the product(s) valid to be stored into the application

4.2 Model 2: One European IFM area for limited use products only



A model for users travelling regularly in their home-country but only occasionally through many IFM areas using only a limited offer of products (e. g. single-tickets or daily passes with low demand for interoperability).

Application on NFC device

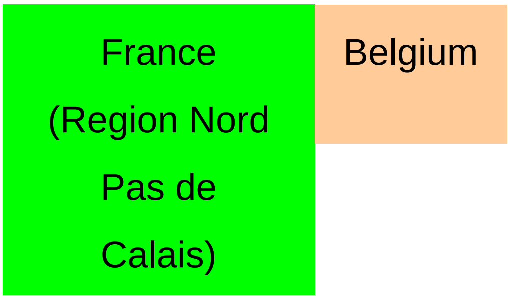


All technologies of acceptance will have to be supported by the media.

Besides their native home-application all user media issued to be used in all contractually participating PT networks contain a European wide common accepted IFM application being used everywhere in the referenced area restricted to less fare products whatever maybe the native issuer of the media/application.

There must be an agreement amongst all participating network operators about the common definition of the product(s) valid to be stored into the application

4.3 Model 3: Coexistence of several different IFM areas for all fare products



Region of Aachen

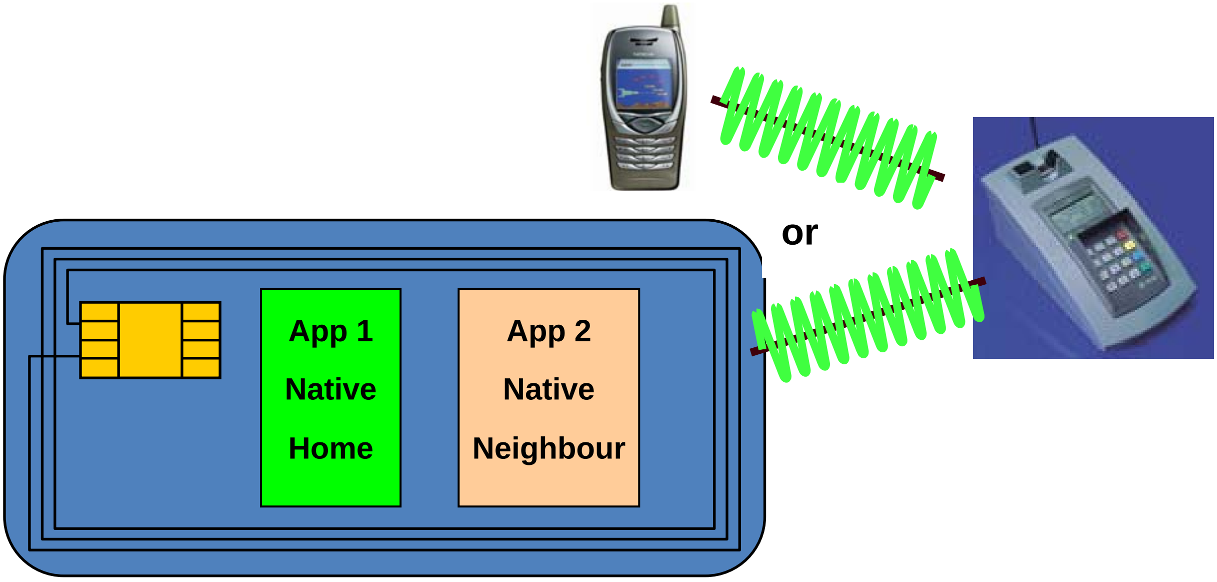
Region of Basle

Region of Nijmegen/Lower Rhine

Region of Padborg

A model for users travelling regularly between two (or few more) different IFM areas. This is the commuter approach (always complete interoperable bilaterally). All fare products of the respective area are offered

Application on NFC device

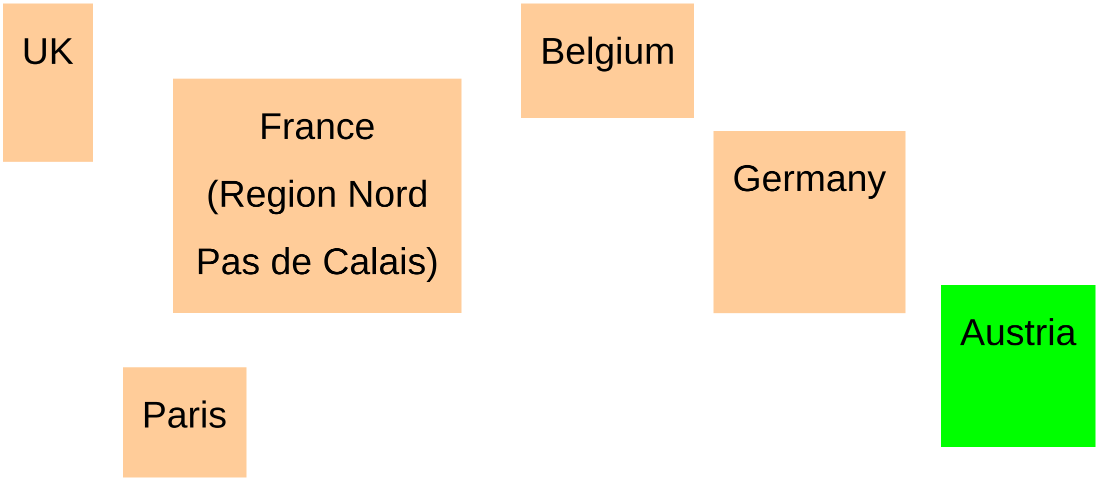


Two (or few more) native applications reside on the media from the beginning. The user uses the native applications of each neighbour area regularly.

The problem of ticket contracts that are valid in both areas (cross-border) is considered in chap.4.5.

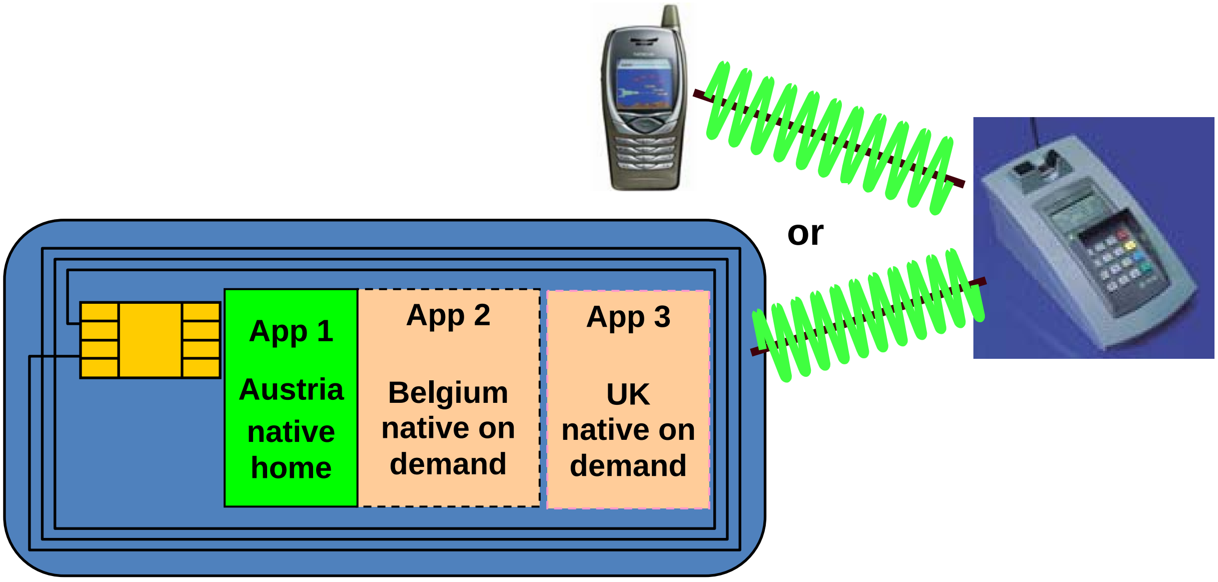
This is the approach taken by IFM Project as first step.

4.4 Model 4: Use of the destination's IFM area on demand



A model for users travelling occasionally in or between many different IFM areas (from time to time complete interoperable everywhere).

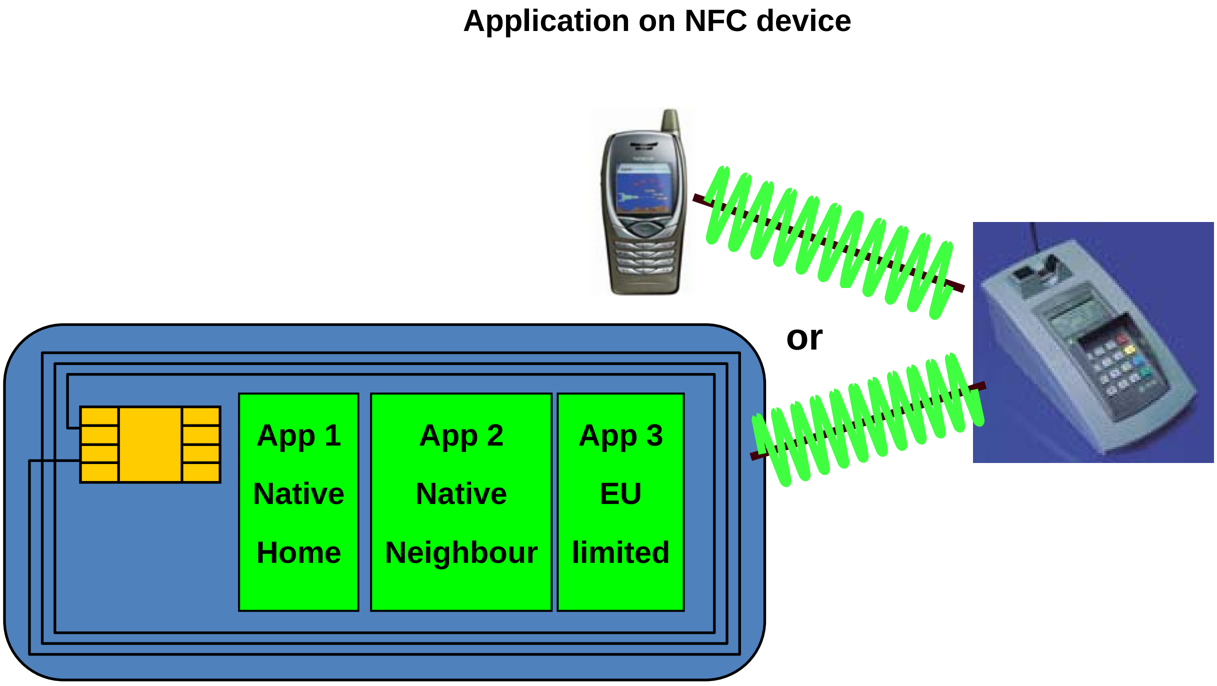
Application on NFC device



The native application of the respective IFM area is loaded on the user media on demand for interoperable use of the complete fares during the stay in the respective area.

The problem of ticket contracts that are valid in both areas (cross-border) is considered in chap.4.5.

4.5 Possible mixture of models 2 and 3



This model could cover a high percentage of all transport cases.

Tariff agreements could create tickets that are valid in both areas – home and neighbour. How to handle these?

- Store the ticket contract on both applications on purchase. In this way inspection in both areas would be guaranteed. Requires secure access to both applications with the right to update records.
- If the payment means used is STR (occasional travel) and not CTA and you want to offer the same level of convenience in both areas a common accessible payment product has to be offered to the user with all complexity in handling this. To avoid this let the occasional user pay cash when user neighbour applications. Must we provide an electronic solution for every possible (probably exceptional) situation?

4.6 Intersector-Model (EMV)

4.6.1 Status of development

In its version MC4 Release 2 the EMV based MasterCard mask offers a small open data container to be used for storing electronic ticket data. This data area is currently only temporary, not separately secured and can be overwritten. This development is not unique and used here only as a reference. The other credit or debit card specifications will – with differentiated schedules – follow the same approach.

It must be noted here that this trend represents an evolution as compared with the first large scale pilots as in those trailblazer exercises, only the financial records are used to define a transport contract in terms of date and time of validity, the value paid being the reference for the kind o contract purchased. On the contrary, the new development make possible the loading of a contract in the form that the transport operator wants to define and record it, this record being if necessary rewritable for change validations or for decrease of the counters (the case of carnet of ten trips) e.g.

Current practice is that the operator only uses the EMV medium to identify the user at his EMV adapted readers. At the end of the day his back-office uses the collected travel pattern to determine the amount this user has to pay. The operator then “sends an invoice” to the Financial Service Provider (FSP) as is typical for any “credit card” transaction. The FSP now guarantees but also controls and shares in the revenue flow

It must be observed that the introduction of an open data storage facility is, in the case mentioned combined with a pre authorized off line payment without pin code or any other action than a voluntary contactless presentation of the media. This means that to adopt EMV media for hosting public transports contracts will be automatically associated with a quick payment means or, in other words, the smart ticketing equipments will need to integrate the local IFM application and, independently, an EMV based authentication process of the media. As those media will represent the next future in terms of payment cards, this adaptation of the ticketing equipments will be “the price to pay” for using a largely distributed – and standardized – media.

Furthermore, this adoption means the recognition by the public transport industry that for really occasional demand, locally adopted IFM systems or supposed interoperable systems, due to the diversity of systems and the non full standard character of some of them, do not represent the most economic solution. Propose specific technical solutions for marginal demand for which only marginal revenue may be expected means to face high structural costs with low revenues. On the contrary to use payment cards for which structural costs are supported by several other payments, often of quite higher value may be the right equation. And the number of low payments for public transport contracts purchases may consist into the critical mass required for the launching of an off line payment mean. So both bank (credit) and public transport industries may find here a ”win-win” situation.

Note 1: Current practice involves considerable effort by the operators to increase the system’s friendliness to occasional users. The FSP’s effort is merely the emission of EMV cards to their specific customers. Since only a small cross-section of all occasional passengers will have an EMV card, the operator will always have to offer an alternative. This makes the “win-win” situation for the operator rather limited but he may still consider it valuable enough.

Note 2: With the strong emergence of NFC enabled devices (in Europe), also the micro payment solution will become an option in this category and may make the implementation of EMV obsolete.

Note 3: The real motivation of FSPs to be present in the public transport domain may be found in their fear for another technology leapfrog experience (compare how Suica Mobile now has the role of the credit card providers in Japan). Public transport can indeed be a *killer* application!

4.6.2 Consequences for Public Transport IFM

- opens the opportunity to use the possibility of recent evolutions in payment cards (contactless available data storage for non-finance transactions)
- allows to integrate the absolute occasional users (e. g. tourists or business travellers) into the implemented IFM system
- avoids the emission of the expensive memory or microprocessor media for these users
- but … adopt the principle that a local IFM system must accept media issued somewhere else
- users may want to reclaim lost products because other systems have overwritten them
- FSPs may want to change business conditions after contracts run out
- operators must follow technical changes as they occur and be backwards compatible.
- Transaction times will increase if the reader has to check multiple applications for a valid product instead of only the local application.
- a media will be presented to PCDs that is not known to PT. So, existing vending channels (AVM, desk) have to be adapted or modified to EMV processing. But, as the majority of operators already use EMV payment it will only be an upgrade.
- It will be mandatory for PT IFM systems to integrate the specifications for time protection of the records (the transport contracts e.g.)
- local contract recognition in container requires either lower security or the adoption of a security architecture based on an another concept that the IFM systems
- the inversion of the “place to recognise and select” the ISO/IEC 14443 protocol as described before will appear as an obligation for the bank (credit) industry as the PT industry provides some ten times more equipment compared with the bank industry.

4.6.3 EMV as parallel standard

At present, this approach is going to be standardized on international level.

ISO TC204 WG8 & CEN TC278 WG3

PWI 14806

IFMS Part 4- Public Transport Requirements for Use of Payment Applications for Fare Media

Objective: Define the regulations and other technical matters needed to provide transport tickets with contactless third party open payment media. The first use case will be EMV. Future use cases: non-EMV bankcards, non-bank-issued payment media (pre-paid credit/debit instruments, etc.), and mobile devices

Above the regulations and other technical matters needed to provide transport tickets with contactless third party open payment media, the introduction of EMV as a parallel standard may lead to future use cases: non-EMV bankcards, non-bank-issued payment media (pre-paid credit/debit instruments, etc.), and mobile devices.

The document will be finalized in January 2012 for the CEN voting procedure.

5 Requirements on Interoperability

This Chapter analyses the requirements on interoperability with respect to each of the four models taking into consideration the role of the different payment products.

5.1 Model 1: One IFM Area comprising all kinds of fare products

- an organisational rule is required to clearly define the necessary identifiers. The establishment of a European central registration body is not needed. Instead, use existing national bodies applying the possibilities of the data standards (EN1545 / EN15320) of creating the necessary identifiers to distinguish the different products and organisations
- ISO/IEC 7812.2 provides standardised numbering to identify both the operator or the transport authority (series given under the authority of national normalisation bodies)
- the customer media must follow the rules described in chap. 5.5 hereunder
- however the ISO/IEC 14443 norm requires that terminals must accept media according to ISO/IEC14443 both Type A and B, a large majority of terminals are limited to one of the two A or B types so, another location of the choice between type A and type B must be found
- the customer has to be registered only once
- mutual authentication is required to guarantee security
- if a native application exists (for what so ever reasons) it must live together with the unique IFM application

5.1.1 Application without payment product

- application is only fitted to store electronic tickets
- in automated fare finding environment only applicable in the allowed fare area of the fare management system
- clearing like today without use of smart ticketing data
- only limited seamless travel within the considered fare area according to the conditions of the respective fare product
- European interoperability needs the creation of Europe wide accepted PT products

5.1.2 Application contains a payment product

The media contains (only) one of the following payment products. This requires the acceptance of these products at all terminals.

Before the decision of offering a payment product to the customer, all payment alternatives have to be analysed with respect to European and national banking law and financial Directives such as eMoney Directive, Money Laundering Directive, Payment Service Directive etc.

a) CTA post-pay

- maximal flexibility ----> seamless travel
- high credit risk affords the installation of a creditability management
- requires the installation of accounting and invoicing procedures
- requires the installation of clearing procedures
- requires the installation of an arbitration management
- requires measures to prevent the delay in obtaining the money for operators

b) CTA pre-pay

- maximal flexibility ----> seamless travel
- requires the installation of accounting and invoicing procedures
- requires the installation of clearing procedures
- requires the installation of an arbitration management
- lower risk without the necessity of a creditability management

c) Transport purse (STR)

- needs loading facilities for value units in the responsibility of the operators
- needs complex clearing procedures between operators
- except for flat fare needs to install complex fare finding procedures at exit in CiCo, BiBo, CiBo environment
- needs to install fare deduction procedures at entrance in case of flat-fare
- except for flat fare needs to install procedures to calculate journey legs at the end of the trip
- except for flat fare needs to install geographical positioning facilities inside the vehicle (however in simplified situations, the change of zone may be manual)

5.1.3 Parallel Open Bank Purse

- a parallel application resides on the media
- does not require clearing procedures between operators
- needs to support automated fare finding procedures
- needs to meet the necessary performance requirements, especially in automated fare finding environment
- needs loading facilities for value units in the responsibility of the banks

- needs the contractual acceptance by the banks to load back access charge at exit
- needs that the ticketing application and the e-purse application, only linked through the terminal activity, work in some extends in parallel to avoid excess of transaction time
- needs the adoption of the security procedures to the requirements of the financial sector

5.2 Model 2: One IFM area for limited use products only

- An existing native application must live together with the unique (limited) IFM application. Both are pre-defined
- an organisational rule is required to clearly define the necessary identifiers. The establishment of a European central registration body is not needed. Instead, use existing national bodies applying the possibilities of the data standards (EN1545 / EN15320) of creating the necessary identifiers to distinguish the different products and organisations
- ISO/IEC 7812.2 provides standardised numbering to identify both the operator or the transport authority (series given under the authority of national normalisation bodies)
- the customer media must follow the rules described in chap. 5.5 hereunder
- however the ISO/IEC 14443 norm requires that terminals must accept media according to ISO/IEC14443 both Type A and B, a large majority of terminals are limited to one of the two A or B types so, another location of the choice between type A and type B must be found
- mutual authentication is required to guarantee security
- as both applications are held separately customers have to register twice

5.2.1 Application without payment product

- application is only fitted to store electronic tickets
- in automated fare finding environment only applicable in the allowed fare area of the fare management system
- clearing like today without use of smart ticketing data
- only limited seamless travel within the considered fare area according to the conditions of the respective fare product
- needs the definition of common accepted EU fare procucts

5.2.2 Application contains a payment product

The EU limited application contains (only) one of the following payment products. This requires the acceptance of all of these products by all terminals.

As of performance reasons the access to an existing payment product within the native application is not considered.

All payment alternatives have to be analysed with respect to European and national banking law and financial Directives such as eMoney Directive, Money Laundering Directive, Payment Service Directive etc.

a) CTA post-pay

- maximal flexibility ----> seamless travel
- high credit risk affords the installation of a creditability management
- requires the installation of accounting and invoicing procedures
- requires the installation of clearing procedures
- requires the installation of an arbitration management
- requires measures to prevent the delay in obtaining the money for operators

b) CTA pre-pay

- maximal flexibility ----> seamless travel
- lower risk without the necessity of a creditability management
- requires the installation of accounting and invoicing procedures
- requires the installation of clearing procedures
- requires the installation of an arbitration management

c) Transport purse (STR)

- needs loading facilities for value units in the responsibility of the operators
- needs complex clearing procedures between operators
- except for flat fare needs to install complex fare finding procedures at exit in CiCo, BiBo, CiBo environment
- needs to install fare deduction procedures at entrance in case of flat-fare
- except for flat fare needs to install procedures to calculate journey legs at the end of the trip
- except for flat fare needs to install geographical positioning facilities inside the vehicle (however in simplified situations, the change of zone may be manual)

5.2.3 Parallel Open Bank Purse

- a parallel application resides on the media
- does not require clearing procedures between operators
- needs to support automated fare finding procedures
- needs to meet the necessary performance requirements, especially in automated fare finding environment
- needs loading facilities for value units in the responsibility of the banks
- needs the contractual acceptance by the banks to load back access charge at exit
- needs that the ticketing application and the e-purse application, only linked through the terminal activity, work in some extends in parallel to avoid excess of transaction time
- needs the adoption of the security procedures to the requirements of the financial sector

5.3 Model 3: Coexistence of several different IFM areas for all fare products

- The content of the media is **pre-defined** with the relevant native applications. Thus the requirements of each application owner are guaranteed as far as the application is concerned (especially key management)
- organisational rules are required to clearly specify who is allowed to read which application and/or to write on it
- The establishment of a European central registration body is not needed. Instead, use existing national bodies applying the possibilities of the data standards (EN1545 / EN15320) of creating the necessary identifiers to distinguish the different products and organisations
- ISO/IC 7812.2 provides standardised numbering to identify both the operator or the transport authority (series given under the authority of national normalisation bodies)
- the customer media must follow the rules described in chap. 5.5 hereunder
- however the ISO/IEC 14443 norm requires that terminals must accept media according to ISO/IEC14443 both Type A and B, a large majority of terminals are limited to one of the two A or B types so, another location of the choice between type A and type B must be found
- mutual authentication is required to guarantee security
- each application lives its own life so, interoperability only exists within the borders of each network where the application is accepted (no network transient interoperability)
- for all services the customer has to be registered in each network (= application)

5.3.1 Application without payment product

- Each application is only fitted to store electronic tickets
- in automated fare finding environment only applicable in the allowed fare area of the fare management system
- clearing like today without use of smart ticketing data
- only limited seamless travel within the considered fare area

5.3.2 Application contains a payment product

Each application contains (only) one of the following payment products. This requires the acceptance of all of these products by all terminals. As of performance reasons a common accessible transport payment product has not been considered.

All payment alternatives have to be analysed with respect to European and national banking law and financial Directives such as eMoney Directive, Money Laundering Directive, Payment Service Directive etc.

a) CTA post-pay

- maximal flexibility ----> seamless travel
- high credit risk affords the installation of a creditability management
- requires the installation of accounting and invoicing procedures
- requires the installation of clearing procedures
- requires the installation of an arbitration management
- requires measures to prevent the delay in obtaining the money for operators

b) CTA pre-pay

- maximal flexibility ----> seamless travel
- requires the installation of accounting and invoicing procedures
- requires the installation of clearing procedures
- requires the installation of an arbitration management
- lower risk without the necessity of a creditability management

c) Transport purse (STR)

- needs loading facilities for value units in the responsibility of the operators
- needs complex clearing procedures between operators
- except for flat fare needs to install complex fare finding procedures at exit in CiCo, BiBo, CiBo environment
- needs to install fare deduction procedures at entrance in case of flat-fare
- except for flat fare needs to install procedures to calculate journey legs at the end of the trip
- except for flat fare needs to install geographical positioning facilities inside the vehicle (however in simplified situations, the change of zone may be manual)

5.3.3 Parallel Open Bank Purse

- a parallel application resides on the media
- does not require clearing procedures between operators
- needs to support automated fare finding procedures
- needs to meet the necessary performance requirements, especially in automated fare finding environment
- needs loading facilities for value units in the responsibility of the banks
- needs the contractual acceptance by the banks to load back access charge at exit
- needs that the ticketing application and the e-purse application, only linked through the terminal activity, work in some extends in parallel to avoid excess of transaction time
- needs the adoption of the security procedures to the requirements of the financial sector

5.4 Model 4: Use of the destination’s IFM area on demand

- Needs application loading and deletion procedures. It has to be stated that each application owner has his own requirements regarding theses procedures (OS, key management)
- To make this model workable it is necessary to transmit the relevant secure elements and/or secret keys. Could this be guaranteed by the channel operator on which transport operators do not have any kind of control?
- The establishment of a European central registration body is not needed. Instead ,use existing national bodies applying the possibilities of the data standards (EN1545 / EN15320) of creating the necessary identifiers to distinguish the different products and organisations
- ISO/IEC 7812.2 provides standardised numbering to identify both the operator or the transport authority (series given under the authority of national normalisation bodies)
- the customer media must follow the rules described in chap. 5.5 hereunder
- however the ISO/IEC 14443 norm requires that terminals must accept media according to ISO/IEC14443 both Type A and B, a large majority of terminals are limited to one of the two A or B types so, another location of the choice between type A and type B must be found
- mutual authentication is required to guarantee security
- each application lives its own life so, interoperability only exists within the borders of each network where the application is accepted (no network transient interoperability)
- for all services the customer has to be registered in each network (= application)
- needs a coordination on EU level with respect to business rules (e.g. which application is allowed to be loaded on which card?)

5.4.1 Application without payment product

- Each application is only fitted to store electronic tickets
- in automated fare finding environment only applicable in the allowed fare area of the fare management system
- clearing like today without use of smart ticketing data
- only limited seamless travel within the considered fare area

5.4.2 Application contains a payment product

Each application contains (only) one of the following payment products. This requires the acceptance of all these products by all terminals. As of performance reasons a common accessible transport payment product has not been considered.

All payment alternatives have to be analysed with respect to European and national banking law and financial Directives such as eMoney Directive, Money Laundering Directive, Payment Service Directive etc.

a) CTA post-pay

- maximal flexibility ----> seamless travel
- high credit risk affords the installation of a creditability management
- requires the installation of accounting and invoicing procedures
- requires the installation of clearing procedures
- requires the installation of an arbitration management
- requires measures to prevent the delay in obtaining the money for operators

b) CTA pre-pay

- maximal flexibility ----> seamless travel
- lower risk without the necessity of a creditability management
- requires the installation of accounting and invoicing procedures
- requires the installation of clearing procedures
- requires the installation of an arbitration management

c) Transport purse (STR)

- needs loading facilities for value units in the responsibility of the operators
- needs complex clearing procedures between operators
- except for flat fare needs to install complex fare finding procedures at exit in CiCo, BiBo, CiBo environment
- needs to install fare deduction procedures at entrance in case of flat-fare

- except for flat fare needs to install procedures to calculate journey legs at the end of the trip
- except for flat fare needs to install geographical positioning facilities inside the vehicle (however in simplified situations, the change of zone may be manual)

5.4.3 Parallel Open Bank Purse

- a parallel application resides on the media
- does not require clearing procedures between operators
- needs to support automated fare finding procedures
- needs to meet the necessary performance requirements, especially in automated fare finding environment
- needs loading facilities for value units in the responsibility of the banks
- needs the contractual acceptance by the banks to load back access charge at exit
- needs that the ticketing application and the e-purse application, only linked through the terminal activity, work in some extends in parallel to avoid excess of transaction time
- needs the adoption of the security procedures to the requirements of the financial sector
  -

5.5 Minimum Requirements on the Media

5.5.1 General technical requirements

The media

- must be equipped with a contactless interface according to ISO/IEC14443
- may be equipped with other standardised interfaces
- shall support certain platforms used to download apps (e.g. ROM based OS according to ISO/IEC 7816-4, programmable OS like Java, Multos or Basic, ROM based OS especially developed for transport purposes) .

In order to achieve the maximum level of interoperability the highest possible level of security is recommended.

The processing specifications at which a terminal processes the user media are:

Processing Level	Interface Specification
9 Terminal application software	Subject to scheme implementation requirements
8 Rules for processing	Subject to scheme organisational and contractual requirements
7 System architecture and security management	Architecture according to EN/ISO24014-1 (IFM) Security management subject to scheme implementation Examples: Common Criteria x Protection profiles (for OS)
6 Model and data instantiation	Covered by EN1545
5 Structure of application data	EN15320 (IOPTA)
4 Data elements used	EN1545
3 Card commands and security mechanisms	Covered by de facto standard and ISO/IEC 7816-4
2 Structuring the application into files/objects	ISO/IEC7816-4
1 Contact and contactless communications interface	ISO/IEC7816-1,2,3 ISO/IEC14443

Possible models for the card – terminal interface should be based on existing standards.

Where standards do not yet cover the scheme requirements the model should guarantee that the system being implemented is a non-proprietary one and that open tendering processes are possible. Taking into account the current status of standardisation open interoperability includes:

- Use of existing standards at the levels 1, 2, 3, 4 and 5 in the above table: ISO/IEC14443 for contactless communication, ISO/IEC7816-4 for the file structure, EN1545 for the coding of transport data
- Development of a data model at level 6 based on EN1545 and EN15320 allowing national and international compatibility. A unique interpretation of identifiers and parameters has to be guaranteed
- Use of a tested and non-proprietary solution for command and terminal security mechanisms for level 3.

Operating systems for cards in transport should include the following features:

- Flexible memory management and file structure
- Initialisation functions
- Application and security management
- Transport card features:
  - High security
  - High operational speed (<300 ms)
  - High data integrity (anti tear)
  - High operation range (5 – 10 cm)
  - File data management (non-proprietary)
  - Reliability
  - Multi-application support (pre-condition for models 2-4)
  - Sufficient EEPROM data size

Microprocessor cards are in the best position to meet these requirements.

As long as native PT applications reside on memory cards OR microprocessor cards only, all PCDs shall be able to interpret the ATQ for all types of cards. This requirement may hinder the development of European interoperability for a long time.

5.5.2 Special technical implication: the communication signal interface

Background: user media have to be accepted in networks of PCDs where the PICCs have not been launched.

ISO/IEC 14443-2 defines two communication signal interfaces: Type A and B. The standard states that the PCD shall alternate between modulation methods when idling before detecting the presence of a PICC of Type A or B. Only one communication signal interface may be active during a communication session until deactivation of the PCD or removal of the PICC.

5.5.2.1 Consequences on existing implementations

- the majority of implementations in PT FM-Systems follow either Type A or Type B, i. e. the PCD accepts only one type and manufacturers surely will not adapt their equipment so easily
- a marginal number of implementations provide a maximum modulation depending on their localisation, i. e. the validation of a non-local protocol takes much longer.

Though being compliant with ISO/IEC 14443, this circumstance may hinder the interoperable acceptance of user media in any environment across Europe.

----> PCDs should treat both chip types equally. At least the polling periodicity should be indicated.

5.5.2.2 Consequences on the use of NFC

ISO/IEC 18092 - the NFC standard - today only supports Type A and Type Felica but not Type B.

----> demand on standardisation

5.5.2.3 A reverse approach

Following ISO/IEC 14443-2, it is the PCD that recognises the observed signal interface type. The PICC remains static either Type A or Type B.

Why not turn the process upside down?

There are developments under way that allow the PICC to recognise and select the observed interface type facing the PCD. So, the PICC will be the master in this process.

Consequences:

- ISO/IEC 14443 has to be opened for the possibility to place the choice between the signal interfaces into the PICC (in cases that a PCD is polling between A and B a technical solution has to be found to avoid that PICC and PCD never meet on one protocol).
- local PICCs could then benefit from a faster transaction With the introduction of mobile phones in e-ticketing such a scenario could become possible - as the end user will select the ticket in advance by using the transit wallet interface. In this case, of course, it would be possible to pre-select either ISO/IEC 14443 Type A or B as with the ticket itself it is a priori known which type of communication is requested. This in the end could solve the problem of an existing infrastructure only being able to serve only type A or B.
- no need to adapt any equipment as far as signal interface switching is concerned
- take into account that there are already more readers in the field that support both Type A and Type B than only single interface readers.
- The number of EMVCo certified readers is continuously growing. These readers will support both type A and B according to ISO/IEC 14443.

5.6 Requirements on Information flow (Transactions)

5.6.1 PICC to PCD

A transaction occurs whenever a customer media has been impacted by a reader (local or remote).

Data elements transmitted in such a transaction must be compliant with EN1545.

5.6.2 PCD to Host or Host to Host

All possible transmission technologies between background systems shall be supported. No restrictions on the choice of transmission technology should be defined, as the security technology is responsible for a secure data transmission through any network.

To guarantee cross-border interoperability transaction data has to be standardised which is not the case yet.

5.6.3 Hotlist procedures

For model 1 a Europe wide hotlist service has to be implemented.

Model 2 does not require any hotlist service (low risk).

Models 3 to 4 benefit from the native hotlist service. We do not see a requirement for a border-crossing hotlist service.

5.7 Requirements on Security

Regarding the described models on interoperability for each of it we would have to mention its own list of such requirements. This would have exceeded the context of this document. So, this chapter wants to hint the reader to the various aspects of security.

In terms of security the overall management should be in the hands of one single legal entity allowing each service operator to have its own security scheme. As different service operators will require specific key management functionalities the legal entity should also cover this issue. The keys of each service operator shall not be distributed to the other service operators. Only some data should be accessible in a reciprocal way. These could be e.g. product issuer identification and expiry date of the proof of contract.

There should be different - but standardized **-** levels of security, suitable to the needs and values of transactions of the different applications.

The applications shall be allowed to negotiate on the security-standards used.

It may be assumed that different European fare management systems will use different security architectures, using own defined security levels. For achieving interoperability, security levels of different systems should be compared in order to allow common functionalities among those systems on comparable security levels. Maybe security levels can be adapted each other to maximise the palette of functionalities.

Also it is recommended to set a security threshold under which no interoperability should be accepted.

Usually transactions overspan a chain of several network components, starting with the media at a customer through to the endpoint, e.g. an abroad back office. It shall be guaranteed that a recognized security level cares for a successful completion of a transaction within that chain. It shall not happen that a customer media is accepted at the one end and the back office cannot accept the transaction at the other end.

5.7.1 The impact of security on interoperability

The security of a ticketing system is built on technical mechanisms and organizational measures ensuring that the ticketing entitlements (contracts) used by the customers have been paid for to the service operator.

The main conditions necessary for this security are:

- During contract validation:
  - Ensure that the contract presented by the customer is authentic, and that a possible debit is genuine.
  - Ensure that the contract and the data generated during the transaction are available later when necessary (e.g. for other contract uses, for controls, etc.)

- Collect the transaction data and be able to prove its authenticity to the central systems.

- Regarding contract loading:
  - Prevent getting a contract without payment (e.g. fraudulent card reloading).
  - Prevent to erase another contract still valid
  - Use signature keys (integrating e.g. the number of the SAM used) for authentication
  - Prevent selling a contract without informing the central systems.
- Have at disposal the means to detect frauds, and to react to them to re-establish the nominal state.
- Data protection
- Privacy

5.7.2 Validation

The validation equipment must be able to distinguish an authorized contract from a counterfeited one.

To do that, a first method is to use sophisticated techniques for the card manufacturing, as for bank notes. This solution is not chosen generally because the terminal costs would be increased considerably to allow an automatic verification. Furthermore, the contract information is too variable and lengthy for this type of technique.

A second method, used by all present e-ticketing systems is to include secret information in the application. This information is then used to authenticate the contracts during validations.

This information is generally a “secret key”, which is different for every application, and which is securely stored in the chip of a smartcard.

5.7.3 Reloading

Reloading a contract into an application consists in creating an object of value in the application. It is therefore necessary to protect the application against fraudulent reloading.

5.7.4 Monitoring

The smartcard ensures a high level of protection of the data and secret it contains. This capacity results from more than 20 years of experience of the smartcard manufacturers, mainly in the banking fields.

No system however can be totally secure, and it is possible that some of the system secrets be found. It is therefore necessary to be able to detect and react to such threats.

In order to detect and assess a fraud, a surveillance system must be established, and possible responses must be planned in advance for the different possible threats.

The heart of this system is a central detection system analyzing the information received from the validation and reloading equipments.

5.7.5 Authentication methods

To be able to authenticate cards and data, various algorithms exist.

Typical examples of suitable crypto-algorithms are:

Algorithm	*Examples*	*Characteristics*
Symmetric	DES DESX Triple-DES AES	The secret key is shared by all the equipment
Asymmetric	RSA Elliptic Curves	A public key ensures the possibility for anyone to check the authenticity without knowledge of the secret key

Asymmetric crypto-algorithms can facilitate the realization of interoperability on EU level, e. g. simplification of key management.

A description of the specific application of these algorithms is not intended.

5.7.6 Interoperability constraints

a) Interoperable platform

For an interoperable system to work, it is necessary for every actor to be able to use the interoperable platform:

- Read the application content and understand it (at least partially).
- Delete obsolete data in the application, to free some chip memory.
- Record some data in the application (e.g. a new contract, a validation transaction result).

It may also require a common visual recognition of a user media, including the holder identity for some media (e.g. nominative contracts).

b) Common Security Policy

An interoperable security requires a common understanding of security issues and a common management of the secrets and of the equipments managing them (SAM).

This Security Policy defines all the procedures of creating, using, storing, and reproducing the security secrets and the SAM containing them. It defines the organization to set up in order to ensure this security management.

It imposes precise rules to all the actors (transit operators, manufacturers). It also defines the test security equipment management.

Finally, it also defines the central surveillance system and the actions required from every actor to allow its correct work (data gathering from various equipment) and the management of a common hotlist of equipment stolen or lost.

c) Common Application Data Management

The interoperable use of a common EU chip application requires a common method for managing the data in the application.

For example, since the chip memory is limited it is necessary for anyone to be able to determine if a data present in the application may be deleted and replaced by some new data.

The security risk is that valuable data present in the application be destroyed intentionally or not.

In order to interoperate, at least the validity information and issuer of some data in the application (e.g. a contract) must be interpretable by all.

d) Application Loading

To be considered in models 3-5: in case of loading the application over the air it is necessary to make this application applicable and to transmit the relevant secure elements (secret keys) over the air as well.

Could this be guaranteed by the channel operator over which transport opeators do not have any form of copntrol?

5.8 Requirements on Man-Machine-Interface

Goals: ease of use, convenience

The applicable definitions of EN 1332 shall be observed

- the system must be comprehensible
- the user should be informed, which action would take place, if the user initiates it (transparency)
- the user should be informed about the result of an upcoming action
- simple actions shall be signalled with red/green colours
- icons/symbols shall be used to achieve the maximum level of recognition
- the selection of languages shall be considered by the operator. He should aim to offer common languages to all users
- if a Hotline-Service is available the offered languages should be displayed

The definitions must be adapted to the underlying technology (BiBo, CiCo, CiBo).

The MMI shall give all relevant information the user needs

Minimum requirements are

Which machines?

Which offered languages? At least English

Logos / Icons

Colours used to indicate actions

Sizes of written messages

Design

Facilities addressing PRM

Communication with call centres

6 Rules & Regulations

Cross-border rules & regulations have to be established to organise data and money flows. As far as financial rules are concerned the following legal considerations have to be checked for relevance:

This document cannot and is not allowed to give any legal proven expertise on the respective subjects. The document instead points out the issues that have to be investigated in depth and need to be confirmed by legal advisers.

The document refers to European Directives only. Maybe national laws will exceed these findings.

6.1 EU e-Money Directive

As far as stored value is concerned according to the

DIRECTIVE 2000/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions (EMD)

it has to be clarified

(1) whether value units in the application have to be considered as electronic money

In Article 1 the Directive states

3. (a) 'electronic money institution' shall mean an undertaking or any other legal person, other than a credit institution as defined in Article 1, point 1, first subparagraph (a) of Directive 2000/12/EC which issues means of payment in the form of electronic money;

(b) 'electronic money' shall mean monetary value as represented by a claim on the issuer which is:

(i) stored on an electronic device;

(ii) issued on receipt of funds of an amount not less in value than the monetary value issued;

(iii) accepted as means of payment by undertakings other than the issuer.

From this it can be derived that

- the value units are monetary value as represented by a claim on the issuer
- the value units are stored on an electronic device
- the value units issued by a retailer, which is not the transport operator, will be accepted by an organisation other than the retailer

Therefore STR have to be regarded as electronic money.

(2) whether the medium-issuing organisation has to act as a financial institution if it is not.

In Article 1 the Directive states

4. Member States shall prohibit persons or undertakings that are not credit institutions, as defined in Article 1, point 1, first subparagraph of Directive 2000/12/EC, from carrying on the business of issuing electronic money.

The requirement for the retailer of applying for a license either as electronic money institution according to Article 1, 3a) or as credit institution according to Article 1, 4 has to be investigated in depth by a legal adviser.

6.2 EU Money Laundering Directive

The rulings of the

DIRECTIVE 2005/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

need to be analyzed by legal advisers whether the refund of any residual amount of STR falls under the restriction of money laundering.

6.3 EU Payment Services Directive

As far as the autoload functionality is concerned a special attention has to be drawn on the

DIRECTIVE 2007/64/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 November 2007 on payment services in the internal market (PSD)

As long as the instance that possesses the money (retailer) is identical to the one that collects the money from the user’s bank there will be no conflict. But if the retailer uses an intermediate service provider the legal requirements of this directive have to be considered.

7 Economics

Interoperability has a price for the service operators and the organising authorities. It has different levels with different costs. It should be based on a business case. Interoperability is a service that has to be marketed to the customers who are ready to pay for it.

European Union has a declared belief in interoperability. With regards to electronic fare management Europe-wide interoperability is the final political target. Key question in this context is where interoperability starts. The definition of this starting point varies from country to country. But commonly the first level or starting point is the region. Therefore it should mandatory be included in the base calculation of the business case.

Extended scenarios of interoperability always involve increasing costs with higher levels of interoperability. Taking into account the experience of the mobile phone case it is remarkable that the cost for the user is huge when using an operator which is not the contractual one.

Roaming prices are rather high and customers often buy cheaper local contracts and not interoperable contracts. Customers going frequently in the same foreign country have two contracts: one in each of those two countries. They only change the “SIM-card” in their phone when they get over the border. This is possible due to the medium - the mobile phone - being interoperable. In terms of public transport this could be realised by putting the focus on the interoperable application. Potentially there are three usage scenarios worth of economic analysis:

a) Customer makes several journeys in one network with one service operator.

b) Customer makes several journeys in one network with more than one service operator.

c) Customer makes several journeys in a) and b) including at least one further network.

Key point today is the interoperability of long distance rail service and the regional services. Some analysts believe that there still needs to be a proof of this customer driven wish of seamlessness. They argue that interoperability is more a technical answer to service operators’ expectations. For the interoperability business case definitely there is a need to analyse what is the exact impact of “over the country” interoperability on the market share of public transport or public transport revenues.

The following table gives an overview of the possible edge marks for a business case:

Usage scenario	**Operators's own fare products**	**Cross sales**	**Shared fare products**	**Common fare products**
Customer makes several journeys in one network with one service operator	Seamlessness limited to a single operator, no commercial and regulatory agreement required	No business case	No business case	No business case
Customer makes several journeys in one network with more than one service operator	Limited seamlessness, no commercial and regulatory agreement required	Limited seamlessness, commercial and regulatory agreement required, but no need for a common fare policy	High seamlessness, commercial and regulatory agreement required, but no need for a common fare policy	Total seamlessness, commercial and regulatory agreement required, apportionment agreement required, need for a common fare policy
Customer makes several journeys in a) and b) including at least one further network	Limited seamlessness, no commercial and regulatory agreement required	Limited seamlessness, commercial and regulatory agreement required, but no need for a common fare policy	High seamlessness, commercial and regulatory agreement required, but no need for a common fare policy	Total seamlessness, commercial and regulatory agreement required, apportionment agreement required, need for a common fare policy

8 Conclusions

8.1 Summary

It is clearly shown that the future of IFM is based on multi-application either with applications being fix stored at the time of personalisation of the media or flexibly organised by the user himself dependant of his individual structure of usage.

Providing the one and only European interoperable application (model 1) is shown as a visionary solution that should guide migration efforts towards a common goal and not to diverge them.

To monitor such future organisation co-operative and consensus based processes amongst multinational partners are required which have to be organised.

A standardised and mutually agreed technological platform has to be implemented with one common operating system and a sufficient level of security that is mutually agreed.

Representatives of existing national standards should meet regularly to discuss the best ways of harmonization. The aforementioned models of interoperability may support this discussion.

With respect to the different models their handling alternatives have to be acceptable and masterable by and transparent and non-discriminatory to the user.

8.2 Some organisational implications of European interoperability

Using the ability of real multi-application procedures that is needed when considering models 2 to 4 some basic questions occur when introducing payment means:

a) PT tokens

considering two ore more independent applications on the PICC with their own PT purse, how will this be organised not confusing the user

b) Bank purse

- usage for ticket contracts only?
- usage in IN / OUT Technology and open PT networks?

8.3 Reflexions on Migration Alternatives

a) Analyse whether the approach of TRIANGLE could bridge the frontiers between national / regional systems without ending in Model 1.

b) Take into account the standardisation work on international level in ISO/TC204/WG8 & CEN/TC278/WG3

PWI 24014-3: IFMS Part 3- Interoperability within a Multi-Application Environment

Objective: A Technical Report addressing multi-application of IFMS, the interoperability and the business practices within a multi-application environment.

Future goal: automatic loading of the relevant applet(s) onto the medium when purchasing a cross-border ticket (model 4)

The deliverable could be an input for the ongoing discussion.

c) There is a strong recommendation to harmonize at first step the various technological card platforms (memory/microprocessor) to avoid too much impact on the PCDs in Europe.