Documentation of Use Cases for

Interoperable Fare Management System data exchanges

Version 1.0

Contents

1 Introduction 3
1.1 Applicable Documents or References 4
1.2 Administration 4
1.3 Special Word Usage 4
1.4 Abbreviations, glossary 4
1.5 Revision History 5

2 Purpose of this document 6

3 Documentation of business processes 7
3.1 Description of a roaming journey 7
3.2 Description of an interlining journey 9
3.3 Scope of IFMS data exchanges 10
3.4 Description of business objectives 12

4 Description of Use Cases 13
4.1 Main criteria for consideration 13
4.2 List of targeted Use Cases 14

5 Identification of exchanged data per use case 15
5.1 List of identified messages 15
5.1.1 Sales messages 15
5.1.2 Fulfilment messages 16
5.1.3 Customer data messages 16
5.1.4 Usage messages 16
5.1.5 Security update messages 17
5.1.6 Configuration messages 18
5.2 List of messages per use cases 18
5.2.1 Roaming journey 19
5.2.1.1 Use case 1 Roaming journey – MCT 19
5.2.1.2 Use case 2 Roaming journey – ABT 20
5.2.2 Interlining journey 23
5.2.2.1 Use case 3 Interlining journey – MCT – occasional users 23
5.2.2.2 Use case 4 Interlining journey – ABT – occasional users 25
5.2.2.3 Use case 5 Interlining journey – MCT – frequent users 27
5.2.2.4 Use case 6 Interlining journey – ABT – frequent users 29

1 Introduction

Interoperable Fare Management Systems (IFMS) are becoming more and more interconnected. This need for connections between IFMS comes from different factors:

- Ticketing interoperability areas are expanding and operational data exchanges between ticketing systems are required for revenue sharing or traffic planning purposes,
- Account Based Ticketing (ABT) is developing and creates the need for back office data exchanges as the proof of entitlement to travel is held in the IFMS back office, and not in the media,
- The increasing economic pressure on local authorities is encouraging them to build ticketing revenue sharing models based on actual passenger journeys rather than on predefined pro-rata calculations, and this mandates the need for sharing operational usage data.

Many initiatives defining specifications for IFMS data exchanges do exist but most of them are at best implemented at a regional or domestic level. Anticipating that data exchanges between IFMS will only increase in the future, the Smart Ticketing Alliance has resolved to describe the list of use cases that PT stakeholders want to see addressed through IFMS data exchanges.

The documentation of such use cases is seen as a necessary prerequisite to the later development of a EU wide specification for an IFMS Back Office interface that should help to seamlessly interconnect ticketing systems and hence favour the development of ticketing interoperability on a broader EU scale.

This document aims to identify the business processes and related use cases that IFMS data exchange should cover. Beyond the business and functional requirements, the regulatory and legal aspect of data exchanges are also taken into account to cope with regards to user data privacy, responsibility of data storage, ownership of the exchanged data ….

Note: STA estimates that it would be valuable to assign roles – as defined in ISO 24014-1 – to the use cases described in this document. However, since the current version of ISO 24014-1 doesn't address Account Based Ticketing architecture, an updated release of this STA document may be issued once the ISO 24014-1 revision 3 is published.

1.1 Applicable Documents or References

Document	Short name	Version / date	Issuer
Documentation of Use Cases for NFC Mobile Devices in Public Transport	STA_Mobile_UC	1.7.4 / December 2016	STA
ISO 24014-1 Public transport — Interoperable fare management system — Part 1: Architecture	ISO_24014-1	2015	ISO/TC 204

1.2 Administration

Documentation of Use Cases for IFMS data exchanges

Smart Ticketing Alliance INPO
c/o UITP, rue Sainte Marie 6
B – 1080 Brussels

Tel.: +32 (0)2 673 61 00

www.smart-ticketing.org

Editors: **Jean-Philippe Amiel** jean-philippe.amiel@nextendis.com
Mike Eastham mike.eastham@itso.org.uk
Caroline Berthomieu berthomieu@vdv.de

1.3 Special Word Usage

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119.

1.4 Abbreviations, glossary

ABT	Account Based Ticketing
Account	Customer account in the IFMS where transit entitlements are stored
Authorised List	List of items that are authorised access to the PT network.
CICO	Check-In / Check-Out
Denial List	List of items that are temporarily denied access to the PT network.
IFMS	Interoperable Fare Management System
MCT	Media Centric Ticketing
PT	Public Transport
PT Network	a PT network operated via the same IFMS system that may include one or several modes of transportation.
Refused List	List of items that are permanently denied access to the PT network. In some networks, this list may be also used for temporary access denial.

SAM	Secure Access Module
STA	Smart Ticketing Alliance

1.5 Revision History

Version	Description of update or change	Date	Author
STA Document V1.0	**First public version**	**July 2017**	**STA**

2 Purpose of this document

This document aims at listing the business process and use cases that requires data exchanges between Interoperable Fare Management Systems (IFMS).

Whereas in the past and still today, most IFMS have a media centric architecture in which interoperability is achieved by accessing data held and stored inside the customer media, the emergence of account based ticketing architecture and the attraction of passengers to smartphone mobility and ticketing applications create a disruption in the way data circulates from one PT network to another one, as they can be now exchanged between IFMS at back office level.

As specifications for data exchanges between IFMS with media centric architecture already exist for enabling ticketing interoperability intra-border or locally between PT networks from the same ticketing scheme, the present document doesn't address these use cases in detail.

The document does however pay attention to the specific cases where data exchange occurs:

- between IFMS with account-based ticketing architecture,
- between cross border IFMS,
- between IFMS using different data exchange specifications.

These 3 cases are not mutually exclusive to each other.

The need for implementing messages or to update the existing ones should be identified through these use cases description.

The present document focuses only on data exchanges that occur between the back offices of IFMS. Data exchanges between media and front office equipment, between media and IFMS back office, between front office equipment and IFMS back office or between IFMS back office and external systems such as central registrar systems, payment gateways, mobile application downloading platforms etc … **are out of scope of the present document** but have definitely to be considered as soon as cooperation with product retailers is in place.

The first part of the document describes the business processes that underlie the need for IFMS data exchanges at back office level.

For each business process, a list of associated uses cases is documented and for each use case, the description of the functional and regulatory requirements applying to data exchanges between IFMS is given.

The present document is not intended to define a technical specification of data exchange between IFMS. Based on STA business, functional and regulatory requirements expressed in this document, the development of such a technical standard is supported by the STA, but it shall be legitimately developed within a PT standardisation body such as CEN TC278 WG3 SG5.

3 Documentation of business processes

Identified business processes for IFMS data exchanges are mainly driven by **ticketing interoperability**, i.e. giving to passengers the opportunity to seamlessly travel through different PT networks with a single medium, if not a single fare product.

Business processes shall encompass the following interoperability scenarios:

- Roaming journey:
    - A customer travels inside a PT network using a single medium (or fare product) issued by another PT network.
- Interlining journey:
    - A customer starts his journey in one PT network and terminates it in another PT network using a single medium (or fare product).

3.1 Description of a roaming journey

A customer of a PT network is usually provided with a medium (contactless card, smartphone application …) that allows travel on this PT network.

The medium can be used to store the proof of entitlement to travel, should it be a fare product (media centric IFMS) or a token (account based IFMS). In either case, the entitlement to travel comes from either the purchase of fare products (prepaid policy) or from an enrolment of customer credentials allowing post journey payment for completed journeys (post paid policy).

The “Roaming journey” business process aims at addressing the case when a customer already equipped with a PT medium from his home network (Network A) can use this medium to travel within another PT network (Network B).

In a roaming journey, the product sold by Network A is only usable in Network B, and therefore cannot be qualified as an interoperable fare product. However, customer profile may be known by Network A and mapped with tariff conditions provided by Network B, offering the possibility to the passenger to benefit from a special tariff if applicable.

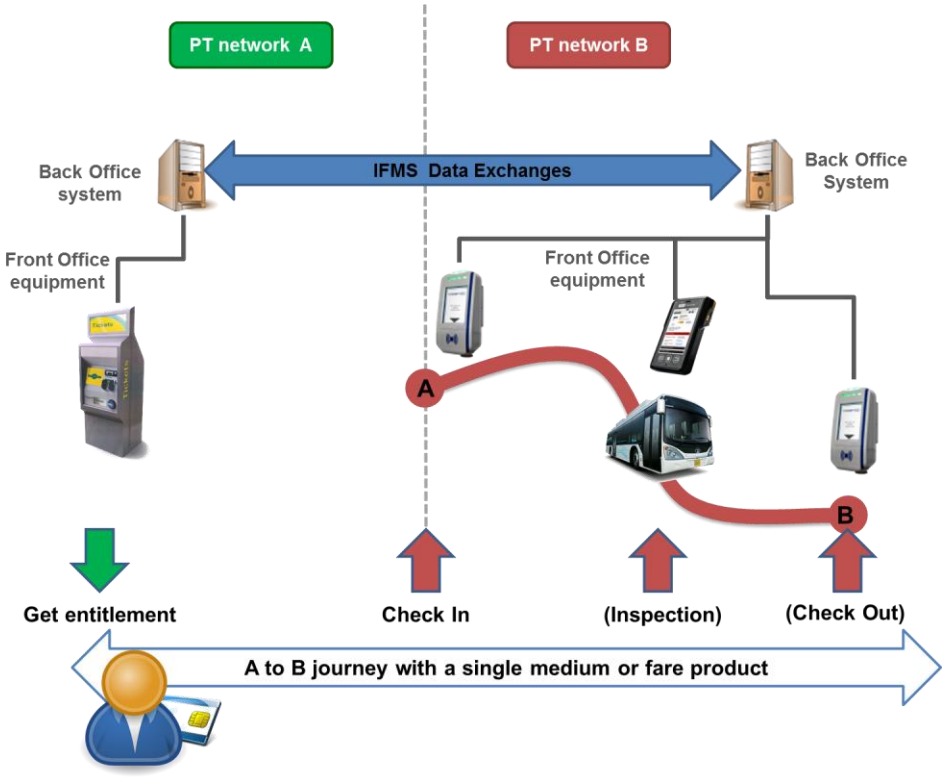

Figure 1 : Description of a Roaming journey

The passenger may achieve the following operations during a roaming journey:

• When in Network A	• Enrol with customer personal details (customer profile and payment related parameters) • Get an entitlement to travel within PT Network B • Update customer personal details
• When in Network B	• Check in • Inspection • Check out
• At any place (Network A or B physical channels, internet or mobile channels)	• Access to journey history • Access to product information (balance) • Claim for a product restoration / refund • Report a defective media • Report lost or stolen media

3.2 Description of an interlining journey

The “Interlining journey” business process deals with the case when a customer has purchased an interoperable fare product or is equipped with interoperable media allowing travel within several PT networks.

The difference with the previous use case is that the provided fare product enables the passenger to use transportation services in Network A and B with the same entitlement. Such entitlement to travel comes from either the purchase of fare products (prepaid policy) or from an enrolment of customer credentials allowing post journey payment for completed journeys (post paid policy).

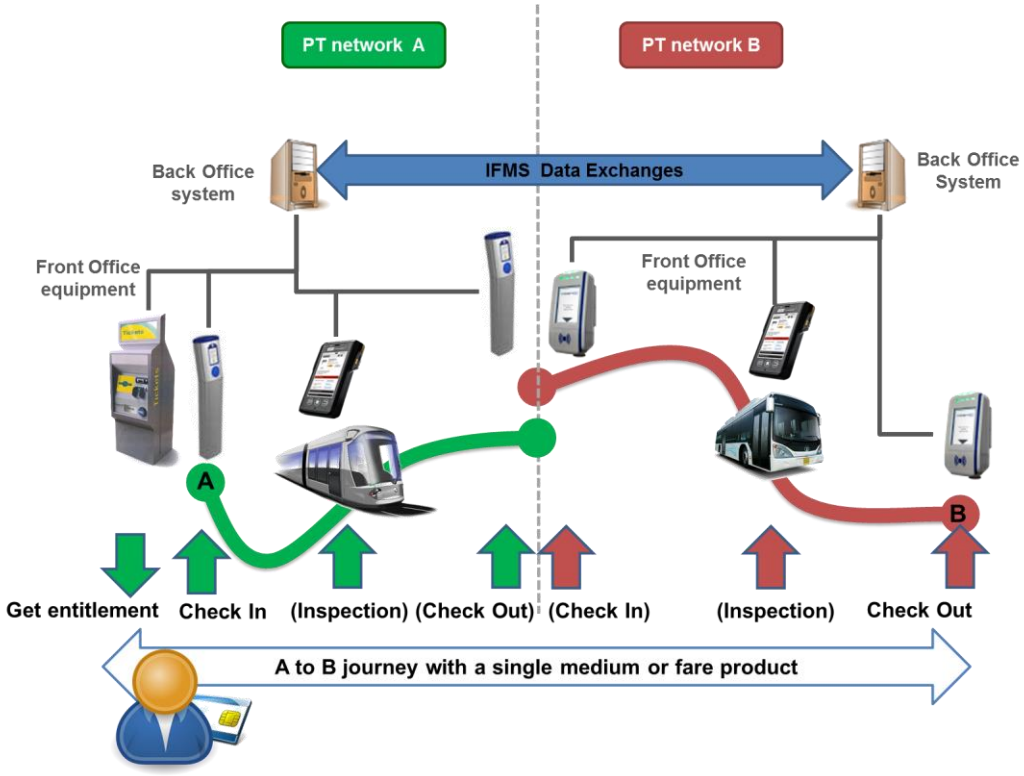

Figure 2 Description of an interlining journey

The passenger may achieve the following operations during an interlining journey:

• When in Network A	• Enrol with customer personal details (customer profile and payment related parameters) • Update customer personal details • Get an entitlement • Check in • Inspection • Check out
• When in Network B	• Check in • Inspection • Check out
• At any place (Network A or B physical channels, internet or mobile channels)	• Access to journey history • Access to product information (balance) • Claim for a product restoration / refund • Report a defective media • Report lost or stolen media

3.3 Scope of IFMS data exchanges

IFMS data exchanges that may occur for the identified business processes shall address the following situations:

- Scope of ticketing interoperability:
  - The business processes cover the case of an interoperable journey for any situation where two or more IFMS need to exchange data: from the case where two or more IFMS are operated for the same PT network, to local, regional, domestic or cross border interoperability situations.
  - According to the case, data may be sent to only one IFMS or to the entire set of IFMS partners.
  - The integration of other sustainable transportation modes shall be possible, assuming that the other ticketing system can exchange data in the same way as an IFMS will do.
- Supported interoperable fare products
  - Interoperable fare products may include single ticket, season tickets for occasional travellers, season tickets for frequent travellers or all of them.

    - According to the list of supported interoperable fare products, the type and frequency of IFMS data exchanges may widely differ.
- Supported ticketing media technology
    - The IFMS data exchanges shall be agnostic to the media technology used (contactless transit cards, 3rd party ID or payment cards, mobile phones etc.).
    - The customer media must be able to be authenticated in all of the IFMS.
    - The use cases for NFC mobile devices documented in [STA_Mobile_UC] shall be covered by the IFMS data exchanges.
- Supported IFMS architecture
    - The IFMS data exchanges shall be applicable to media centric, account based or hybrid (i.e. combining media centric and account based) IFMS architectures.
    - Data exchanges shall be possible in synchronous (i.e. pseudo real time) or asynchronous modes according to the nature of exchanged data and IFMS capacities.
    - Data exchanges can be achieved in a point to point mode between 2 IFMS systems or through a central system to which several IFMS are connected.
- Supported business policy
    - The IFMS data exchanges shall remain valid independently from the validation and inspection policy (check in only, check in check out, no CICO ...)
    - The different business policies linking the IFMS partners (revenue allocation based on usage, sales commission, reverse charging ….) shall be covered.
- Supported institutional organisation
    - The IFMS data exchanges shall be valid for different institutional organisations (central or distributed IFMS management, PT service delegation to a private operator …)
- …

3.4 Description of business objectives

Setting up ticketing interoperability between PT networks requires that data is exchanged between IFMS for serving the following business objectives:

- **Seamless travel across several PT networks,** i.e. enabling passengers through the purchase of a single interoperable fare product to use the transportation services of several PT networks,
- **Ticketing revenue sharing**, i.e. offering PT authorities the ability to split revenue collection on a per usage basis when a single fare is used to travel across PT networks operated by distinct [and different] PT operators,
- **Remote fare product distribution**, i.e. giving the possibility to third party PT networks to issue tickets on behalf of the owning PT authorities,
- **Revenue collection protection**, i.e. that a medium reported as lost or stolen, cannot be used in other PT networks,
- **Passenger journey monitoring**, i.e. allowing PT authorities to optimise the usage and the routing of their vehicles' fleet to better address the mobility needs of the travellers,
- **Customer care improvement,** i.e. allowing any customer touch point to perform after sales operation independently of the place of issuance of the media or of the fare product,
- **Facilitating mobility combining one or several PT modes,** i.e. providing passengers and PT operators' value propositions for seamless travel interoperability,
- …

4 Description of Use Cases

4.1 Main criteria for consideration

IFMS using common or different data exchange specifications

IFMS data exchanges are already specified for addressing most of the needs expressed in the previous section when IFMS are belonging to the same STA ticketing scheme. ITSO specifications, VDV-KA specifications and a French standard InterBob, Calypso based, already exist to cover such cases.

STA estimates that there is a need for specifying IFMS data exchanges when they belong to different ticketing schemes, as this is today more or less a green-field area.

However whether the 2 IFMS belong [or not] to the same ticketing scheme has no impact on the use case description and the types of message that are required. It only has an impact on the specifications that can be used for data exchanges.

Hence no distinction will be made in the use cases and message descriptions that are given in the following sections.

IFMS architecture: media centric or account based ticketing

In media centric ticketing architecture, the product related data – and sometimes also, the customer related data - are hosted within the media itself. They are then immediately available to any front-end equipment for sales, fulfilment, validation or inspection operations. This creates a limited need for exchanging data between IFMS back office, which may happen on a daily or a less frequent periodic basis.

In account based ticketing architecture, the data stored in the media only aims at authenticating a transit account holder. This creates the need for front-end equipment to be able to access account information in a back office in pseudo-real time or to store into the equipment an up to date list of authorised/denied accounts, requiring a different type and frequency of IFMS data exchanges for enabling interoperable journeys.

Interoperable fares for frequent or occasional users

Offering interoperable fare products for frequent or regular users, such as season tickets, creates specific needs for IFMS data exchange. Exchanging lists of authorised media or tokens generally takes place in this case.

When offering interoperable fare products for occasional users, such as single tickets, validation data exchanges are usually required.

NB: The distinction regarding the type of interoperable fare product only applies to interlining journeys. In a roaming journey, the product sold by Network A is only usable in Network B, and therefore cannot be qualified as an interoperable fare product.

4.2 List of targeted Use Cases

STA has focussed in this documentation on the following use cases:

	Use case title	Short description
UC1	Roaming journey – MCT	Roaming journey as described in §3.1 Network A & B have Media Centric Ticketing IFMS
UC2	Roaming journey – ABT	Roaming journey as described in §3.1 Network A & B have Account Based Ticketing IFMS
UC3	Interlining journey – MCT – occasional users	Interlining journey as described in §3.2. Network A & B have Media Centric Ticketing IFMS Interoperable fare products are for occasional users only.
UC4	Interlining journey – ABT – occasional users	Interlining journey as described in §3.2. Network A & B have Account Based Ticketing IFMS Interoperable fare products are for occasional users only.
UC5	Interlining journey – MCT – frequent users	Interlining journey as described in §3.2. Network A & B have Media Centric Ticketing IFMS Interoperable fare products are for frequent users only.
UC6	Interlining journey – ABT – frequent users	Interlining journey as described in §3.2. Network A & B have Account Based Ticketing IFMS Interoperable fare products are for frequent users only.

5 Identification of exchanged data per use case

This section describes the data exchanged between the involved IFMS for the Use Cases listed in the Roaming and Interlining journeys.

5.1 List of identified messages

Implementation of data exchanges will rely on the exchange of one or several messages between the involved IFMS.

This section aims at listing the messages and describing the functional, security, privacy and regulatory requirements applying to these messages.

Data exchanges should happen via sending and receiving messages either in an asynchronous mode (by secure file transfer overnight for instance) or in a synchronous mode (through authenticated WEB services for instance).

Each message comes as a request that shall receive a response. According to the type of protocol, a first level of answer can be received for technical (message receipt) acknowledgement, and a subsequent response may come later on containing the requested information, or the response may be received immediately with the requested information.

There is no requirement to have real time data exchanges between IFMS capable of matching the performance requirements for check in or check out operations (which are usually in the order of magnitude of hundreds of ms).

Messages may include sensitive data, especially when dealing with authorisation lists, or fare product fulfilment. In these cases, security mechanisms shall be applied to the message data to prevent any fraudulent usage and alteration of such data. This may require data encryption and/or digital signature to provide data confidentiality and integrity. Security mechanisms may be applied at message level or at network level (by using a VPN connection over a public network for instance)

IFMS data exchange shall comply with the EU and local regulations in terms of protection of personal data. This requirement shall apply specially when customer data, or personal validation data are exchanged between IFMS. Security mechanisms shall apply in order to prevent any eavesdropping of personal data. This may be also complemented by commitments from each IFMS manager to obtain the acknowledgment from the user to distribute their personal data to other IFMS, or to delete personal data after processing them if there is no reason to store permanently such data.

5.1.1 Sales messages

The following messages relate to a **sale or customer care operation**:

Msg.1. Declare the sale of a medium / installation of an application

Msg.2. Declare the sale of a product

Msg.3. Declare the refund of a medium

Msg.4. Declare the [full] refund of a product.

This is used for the annulment of the sale of a product as in Msg.2.

Msg.5. Declare the restoration of a product

Msg.6. Declare the replacement of a medium

Msg.7. Declare the sale of a product extension (including the automated or manual top up of a stored value product).

Msg.8. Declare the partial refund of a product.

This is used for the annulment of a product extension event, as in Msg.7.

5.1.2 Fulfilment messages

The following messages relate to a **fulfilment operation** following the purchase of a product:

Msg.9. Get a fare product

Get script commands enabling storage of a fare product on the customer medium, following the purchase or an update of a product.

5.1.3 Customer data messages

The following messages relate to a **customer data operation**:

Msg.10. Request customer data

Request customer information about an unknown media

Msg.11. Share customer data

Share customer data to a common customer management platform

Msg.12. Request customer data removal

Request removal of customer data (termination by customer)

Msg.13. Modify customer parameters

Modification of customer personal details (customer profile and payment related parameters)

5.1.4 Usage messages

The following messages relate to validation or inspection operations:

Msg.14. Share validation or inspection data

Share validation and inspection data related to the usage of interoperable fare products, with restrictions regarding the purpose of the exchanged information (anonymisation)

Such data exchanges shall enable the sharing of revenues for interoperable fare products on a usage basis between PT networks.

Msg.15. Request customer charging

Request sent for charging customer usage in a visited PT network.

Such data exchanges are used when a post-paid or Pay As You Go policy applies in the visited network. The message is sent by the visited PT network to the home network of the customer. Subsequent payment operations, following a customer charging request or the sharing of validation data, are normally out of scope of IFMS data exchange as they happen through payment clearing systems.

5.1.5 Security update messages

The following messages relate to an **access authorisation or denial of access** to the PT network:

Msg.16. Add/remove a media to/from an authorised list (white list)

Msg.17. Add/remove a media to/from a denial list (denial list)

Msg.18. Add/remove a media to/from a refused list (black list)

Msg.19. Add/remove a token to/from an authorised list (white list)

Msg.20. Add/remove a token to/from a denial list (denial list)

Msg.21. Add/remove a token to/from a refused list (black list)

Msg.22. Add/remove SAM or organisation IDs from/to a refused list (black list)

Front end equipment may manage different lists:

- An authorised list (or white list) enumerates the media or tokens that have access to the PT network. This is often used for media holding season tickets.
- A refused list (or black list) enumerates the media or tokens that don't have permanently access to the PT network. This is often used for lost or stolen media.
- A refused list may be set up for blacklisting lost or stolen SAMs (and hence issued application or product from this SAM) or fraudulent/closed organisations.
- A denial list (or denial list) enumerates the media or token that are temporarily denied access to the PT network. This is often used for media linked to a user account that has been suspended due to an insufficient balance or unpaid debts.

Some items of information may be managed centrally at the back office and may not need to be exchanged and handled within equipment.

Two sub cases shall be distinguished for the add/remove messages:

- When such message is sent **by** the media owner or account owner, the recipient shall execute the request and update the list of its equipment.
- When such message is sent **to** the media owner or account owner, the media/owner shall instruct the request and answer back with an approval or refusal. The lists in the equipment are only updated when the request is approved.

5.1.6 Configuration messages

The following messages relate to **configuration** operations:

Msg.23. Get fare set

Get the fare set data including all the available fare products and their associated parameters: pricing, validity period and area, supported payment and fulfilment methods, eligible customer profile, validation and inspection policies…

Fare set information exchanges make sense mainly in the roaming journey case when Network A is selling prepaid fare products from Network B. If a post-paid or Pay As You Go policy is applied by Network B, there is no need for fare set exchanges.

For interlining cases, interoperable fare tariffs are jointly defined by all the involved parties. So, one can assume that there is no need for exchanging fare data already known by each party.

Msg.24. Share credential data

The authentication of media or tokens issued by another network shall require the exchange of credentials. For IFMS with media centric architecture using symmetric keys, credentials are usually implemented inside the SAM provisioned in the equipment of each accepting network, and therefore keys are not circulated in any other form than through SAM delivery. However, networks may exchange credential related data to be informed about which SAM key set shall be used, which URL shall be used for online authentication …

5.2 List of messages per use cases

The following tables list the required messages to execute the use case.

Message may circulate from Network A to B, from Network B to A or in both directions.

Message transmission can be done in asynchronous mode (Async.) – usually when there is no immediate need for transferring the data, or in synchronous mode (Sync.) if the transmission shall happen in real time. In some cases, mainly due to the fact that legacy data exchange still requires asynchronous messaging, some cases where synchronous mode would be preferred may be still handled in asynchronous mode, provided that networks agree to accept the related risk of delayed information transfer.

Note 1: Messages left in italic grey are unused for the considered use case.

Note 2: Messages listed hereafter may end up into being split into several messages in data exchange specifications.

5.2.1 Roaming journey

The customer purchases a fare product to travel in PT Network B at one of the point of sales of Network A.

The customer is equipped with a medium issued by Network A (ABT or MCT cases) or issued by a 3rd party but registered by Network A (ABT case).

5.2.1.1 Use case 1 Roaming journey – MCT

As a prerequisite to fare product sales, the selling Network A shall be aware of the fare set applicable to Network B.

When customer profile is known, Network A may retrieve through the fare set of Network B, the eligibility parameters in order to determine according to the customer profile, the adequate fare product price.

This is managed with *Get fare set* message exchanges.

Due to the Media Centric Ticketing architecture of Network B, the fare product shall be provisioned into the customer medium of the end user.

Depending on the fulfilment method used for provisioning the fare product in the media, some script data may be passed on to Network A by Network B (in the case for instance where Network A doesn't have the credentials required to perform a secure writing into a contactless card medium).

This can be managed with *Get a fare product* message exchanges.

Depending on the commercial agreement linking networks A & B, fare product (sales restoration, or refund) information may be reported to PT Network B in order to manage the fare revenue distribution.

This can be managed with *Declare the sale of a product; Declare the refund of a product; Declare the restoration of a product; Declare the sale of a product extension; Declare the partial refund of a product* message exchanges.

	Message	Dir.	Mode
Sales messages	*Declare the sale of a medium / installation of an application*		
	Declare the sale of a product	A->B	Async.
	Declare the refund of a medium		
	Declare the refund of a product	A->B	Async.
	Declare the restoration of a product	A->B	Async.
	Declare the replacement of a medium		
	Declare the sale of a product extension	A->B	Async.
	Declare the partial refund of a product	A->B	Async.
Fulfilment messages	Get a fare product	A->B	Async.
Customer data messages	*Request customer data*		
	Share customer data		
	Request customer data removal		
	Modify customer parameters		
Usage messages	*Share validation or inspection data*		
	Request customer charging		
Security update messages	*Add/remove a media to/from an authorised list (white list)*		
	Add/remove a media to/from a denial list (denial list)		
	Add/remove a media to/from a refused list (black list)		
	Add/remove a token to/from an authorised list (white list)		
	Add/remove a token to/from a denial list (denial list)		
	Add/remove a token to/from a refused list (black list)		
	Add/remove SAM or organisation IDs from/to a refused list		
Configuration messages	Get fare set	A->B	Async.
	Share credential data		

Table 1: List of messages applicable to Roaming journey – MCT

5.2.1.2 Use case 2 Roaming journey – ABT

When a prepaid fare policy applies to network B:

As a prerequisite to fare product sales, the selling Network A shall be aware of the fare set applicable to Network B.

When the customer profile is known, Network A may retrieve through the fare set of Network B, the eligibility parameters in order to determine according to the customer profile, the appropriate fare product price.

This is managed with *Get fare set* message exchanges.

Sales (or refund) information shall be reported as soon as possible to PT Network B, that will register the fare product in the back-office account of the user (and potentially update the authorised list in the front-end equipment of Network B).

This is managed with *Declare the sale of a product; Declare the refund of a product; Declare the restoration of a product; Declare the sale of a product extension; Declare the partial refund of a product* message exchanges.

Network A and Network B may exchange credential data to allow the proper authentication of Network A's media/token within Network B.

This is managed with *Share credential data* message exchanges.

When a post-paid fare policy applies to network B:

A customer may submit a request in Network A for using Network B services. This request may be implicit depending on the commercial agreement linking the 2 networks, the type of customer profile and charging method, in which case the customer is authorised by default to use Network B services.

Due to the Account Based Ticketing architecture of Network B, the sale (or request) shall be registered into the user account associated to the presented media at Network A's points of sale. This is achieved by requesting the addition of the customer media/token to an authorised list.

This is managed with *Add/remove a media to/from a xx list; Add/remove a token to/from a xx list* message exchanges (where xx means authorised, denied or refused).

After a given period, Network B will request payment for provided services to visiting customer form Network A.

This is managed with *Request customer charging* message exchanges.

Network A and Network B may exchange credential data to allow the proper authentication of Network A's media/token within Network B.

This is managed with *Share credential data* message exchanges.

See Table 2 (on next page).

	Message	Dir.	Mode
Sales messages	*Declare the sale of a medium / installation of an application*		
	Declare the sale of a product	A->B	Sync.
	Declare the refund of a medium		
	Declare the refund of a product	A->B	Sync.
	Declare the restoration of a product	A->B	Sync.
	Declare the replacement of a medium		
	Declare the sale of a product extension	A->B	Async.
	Declare the partial refund of a product	A->B	Async.
Fulfilment messages	*Get a fare product*		
Customer data messages	*Request customer data*		
	Share customer data		
	Request customer data removal		
	Modify customer parameters		
Usage messages	*Share validation or inspection data*		
	Request customer charging	B->A	Async.
Security update messages	Add/remove a media to/from an authorised list (white list)	A->B	Async.
	Add/remove a media to/from a denial list (denial list)	A->B	Async.
	Add/remove a media to/from a refused list (black list)	A->B	Async.
	Add/remove a token to/from an authorised list (white list)	A->B	Async.
	Add/remove a token to/from a denial list (denial list)	A->B	Async.
	Add/remove a token to/from a refused list (black list)	A->B	Async.
	Add/remove SAM or organisation IDs from/to a refused list		
Configuration messages	Get fare set	A->B	Async.
	Share credential data	A->B	Async.

Table 2: List of messages applicable to Roaming journey – ABT

5.2.2 Interlining journey

The passenger purchases an interoperable fare product at one of the points of sale of Network A. The interoperable fare product allows travel within PT Networks A & B.

The customer is equipped with a medium issued by Network A (ABT or MCT cases) or issued by a 3rd party but registered by Network A (ABT case).

5.2.2.1 Use case 3 Interlining journey – MCT – occasional users

As a prerequisite to fare product sales, the selling Network A shall be aware of the interoperable fare set applicable to Networks A & B. But as the interoperable fares are jointly defined, there is usually no need to exchange this information as it is already known by each network.

Getting customer data may also be a prerequisite to the fare product sale, but is not considered here as only occasional users are addressed.

Due to the Media Centric Ticketing architecture of Networks A & B, the fare product shall be provisioned into the customer medium of the end user.

Whatever the fulfilment method used for provisioning the fare product in the media, Network A shall be autonomous to handle this task.

Depending on the commercial agreement linking Networks A & B, sales (or refund) information may be reported to PT Network B in order to manage the fare revenue distribution.

This is managed with *Declare the sale of a product; Declare the refund of a product; Declare the restoration of a product; Declare the sale of a product extension; Declare the partial refund of a product* message exchanges.

When the revenue distribution is based on usage, validation and inspection data may need to be exchanged too.

This is managed with *Share validation or inspection data* message exchanges.

If a SAM is reported lost/stolen, or an organisation is reported as acting fraudulently or ceases to operate, the related information needs to be distributed to the networks that could accept such product or media.

This is managed with *Add/remove SAM or organisation IDs from/to a refused list (black list)* message exchanges.

All messages can be exchanged in asynchronous mode (i.e. on a daily or longer period basis).

See Table 3 (on next page).

	Message	Dir.	Mode
Sales messages	*Declare the sale of a medium / installation of an application*		
	Declare the sale of a product	A<->B	Async.
	Declare the refund of a medium		
	Declare the refund of a product	A<->B	Async.
	Declare the restoration of a product	A<->B	Async.
	Declare the replacement of a medium		
	Declare the sale of a product extension	A<->B	Async.
	Declare the partial refund of a product	A<->B	Async.
Fulfilment messages	*Get a fare product*		
Customer data messages	*Request customer data*		
	Share customer data		
	Request customer data removal		
	Modify customer parameters		
Usage messages	Share validation or inspection data	A<->B	Async.
	Request customer charging		
Security update messages	*Add/remove a media to/from an authorised list (white list)*		
	Add/remove a media to/from a denial list (denial list)		
	Add/remove a media to/from a refused list (black list)		
	Add/remove a token to/from an authorised list (white list)		
	Add/remove a token to/from a denial list (denial list)		
	Add/remove a token to/from a refused list (black list)		
	Add/remove SAM or organisation IDs from/to a refused list	A<->B	Async.
Configuration messages	*Get fare set*		
	Share credential data		

Table 3: List of messages applicable to Interlining journey – MCT – occasional users

5.2.2.2 Use case 4 Interlining journey – ABT – occasional users

As a prerequisite to fare product sales, the selling Network A shall be aware of the interoperable fare set applicable to Networks A & B. But as the interoperable fares are jointly defined, there is usually no need to exchange this information as it is already known by each network.

Getting customer data may also be a prerequisite to the fare product sales, but is not considered here as only occasional users are addressed.

Due to the Account Based Ticketing architecture of Networks A & B, the sale shall be registered into the user account associated to the presented media at Network A's points of sale. Additionally, sales (or refund) information shall be reported as soon as possible to PT Network B, that will register the fare product in the back-office account of the user (and potentially update the authorised list in the front-end equipment of Network B).

Depending on the commercial agreement linking Networks A & B, sales (and / or refund) information may be reported to PT Network B in order to manage the fare revenue distribution.

This is managed with *Declare the sale of a product; Declare the refund of a product; Declare the restoration of a product; Declare the sale of a product extension; Declare the partial refund of a product* message exchanges.

The exchange of usage data is required when the revenue distribution is based on usage.

This is managed with *Share validation or inspection data* message exchanges.

If a SAM is reported lost/stolen, or an organisation is reported as acting fraudulently or ceases to operate, the related information needs to be distributed to the networks that could accept such product or media.

This is managed with *Add/remove SAM or organisation IDs from/to a refused list (black list)* message exchanges.

See table 4 (on next page).

	Message	Dir.	Mode
Sales messages	*Declare the sale of a medium / installation of an application*		
	Declare the sale of a product	A<->B	Sync.
	Declare the refund of a medium		
	Declare the refund of a product	A<->B	Sync.
	Declare the restoration of a product	A<->B	Sync.
	Declare the replacement of a medium		
	Declare the sale of a product extension	A<->B	Async.
	Declare the partial refund of a product	A<->B	Async.
Fulfilment messages	*Get a fare product*		
Customer data messages	*Request customer data*		
	Share customer data		
	Request customer data removal		
	Modify customer parameters		
Usage messages	Share validation or inspection data	A<->B	Async.
	Request customer charging		
Security update messages	*Add/remove a media to/from an authorised list (white list)*		
	Add/remove a media to/from a denial list (denial list)		
	Add/remove a media to/from a refused list (black list)		
	Add/remove a token to/from an authorised list (white list)		
	Add/remove a token to/from a denial list (denial list)		
	Add/remove a token to/from a refused list (black list)		
	Add/remove SAM or organisation IDs from/to a refused list	A<->B	Async.
Configuration messages	*Get fare set*		
	Share credential data		

Table 4: List of messages applicable to Interlining journey – ABT – occasional users

5.2.2.3 Use case 5 Interlining journey – MCT – frequent users

As a prerequisite to fare product sales, the selling Network A shall be aware of the interoperable fare set applicable to Networks A & B. But as the interoperable fares are jointly defined, there is usually no need to exchange this information as it is already known by each network.

Getting customer data may also be a prerequisite to the fare product sale in order to determine according to the customer profile, the appropriate fare product price. Usually, such information is stored within the medium itself and doesn't require back office exchanges.

Getting customer data may also be key to offer unified customer care services, should the customer touch point be at Network A or Network B.

This is managed with *Request customer data; Share customer data; Request customer data removal; Modify customer parameters* message exchanges.

Due to the Media Centric Ticketing architecture of Networks A & B, the fare product shall be provisioned into the customer medium of the end user.

Whatever the fulfilment method used for provisioning the fare product in the media, Network A shall be autonomous to handle this task.

Sales and usage data shall be exchanged between the 2 networks in order to manage the fare revenue distribution.

This is managed with *Declare the sale of a product/medium; Declare the refund of a product/medium; Declare the restoration of a product; Declare the replacement of a medium; Declare the sale of a product extension; Declare the partial refund of a product* message exchanges.

The exchange of usage data makes sense when the revenue distribution is based on usage.

This is managed with *Share validation or inspection data* message exchanges.

Exchange of action lists is needed to offer unified customer care services and to prevent fraudulent access of lost, stolen and suspended media.

This is managed with *Add/remove a media to/from a xx list; Add/remove a token to/from a xx list* message exchanges (where xx means authorised, denied or refused).

If a SAM is reported lost/stolen, or an organisation is reported as acting fraudulently or ceases to operate, the related information needs to be distributed to the networks that could accept such product or media.

This is managed with *Add/remove SAM or organisation IDs from/to a refused list (black list)* message exchanges.

All messages can be exchanged in asynchronous mode (i.e. on a daily or longer period basis).

See table 5 (on next page).

	Message	Dir.	Mode
Sales messages	Declare the sale of a medium / installation of an application	A<->B	Async.
	Declare the sale of a product	A<->B	Async.
	Declare the refund of a medium	A<->B	Async.
	Declare the refund of a product	A<->B	Async.
	Declare the restoration of a product	A<->B	Async.
	Declare the replacement of a medium	A<->B	Async.
	Declare the sale of a product extension	A<->B	Async.
	Declare the partial refund of a product	A<->B	Async.
Fulfilment messages	*Get a fare product*		
Customer data messages	Request customer data	A<->B	Async.
	Share customer data	A<->B	Async.
	Request customer data removal	A<->B	Async.
	Modify customer parameters	A<->B	Async.
Usage messages	Share validation or inspection data	A<->B	Async.
	Request customer charging		
Security update messages	Add/remove a media to/from an authorised list (white list)	A<->B	Async.
	Add/remove a media to/from a denial list (denial list)	A<->B	Async.
	Add/remove a media to/from a refused list (black list)	A<->B	Async.
	Add/remove a token to/from an authorised list (white list)		
	Add/remove a token to/from a denial list (denial list)		
	Add/remove a token to/from a refused list (black list)		
	Add/remove SAM or organisation IDs from/to a refused list	A<->B	Async.
Configuration messages	*Get fare set*		
	Share credential data		

Table 5: List of messages applicable to Interlining journey – MCT – frequent users

5.2.2.4 Use case 6 Interlining journey – ABT – frequent users

As a prerequisite to fare product sales, the selling Network A shall be aware of the interoperable fare set applicable to Networks A & B. But as the interoperable fares are jointly defined, there is usually no need to exchange this information as it is known by each network.

Getting customer data may also be a prerequisite to the fare product sales in order to determine according to the customer profile, the adequate fare product price. If implemented, message transmission shall occur in synchronous mode to satisfy any query that happens during the sales process.

This is managed with *Declare the sale of a product/medium; Declare the refund of a product/medium; Declare the restoration of a product; Declare the replacement of a medium; Declare the sale of a product extension; Declare the partial refund of a product* message exchanges.

Getting customer data may be also key to offer unified customer care services, should the customer touch point be at Network A or Network B.

This is managed with *Request customer data; Share customer data; Request customer data removal; Modify customer parameters* message exchanges.

Due to the Account Based Ticketing architecture of Network A & B, the sale shall be registered into the user account associated to the presented media at Network A's points of sale. Additionally, sales (or refund) information shall be reported as soon as possible to PT Network B, that will register the fare product in the back-office account of the user (and potentially update the authorised list in the front-end equipment of Network B).

This is managed with *Declare the sale of a product/medium; Declare the refund of a product/medium; Declare the restoration of a product; Declare the replacement of a medium; Declare the sale of a product extension; Declare the partial refund of a product* message exchanges.

Whatever the fulfilment method used for provisioning the fare product in the media, Network A shall be autonomous to handle this task.

Sales and usage data shall be exchanged between the 2 networks in order to manage the fare revenue distribution.

This is managed with *Declare the sale of a product/medium; Declare the refund of a product/medium; Declare the restoration of a product; Declare the replacement of a medium; Declare the sale of a product extension; Declare the partial refund of a product* message exchanges.

The exchange of usage data is required when the revenue distribution is based on usage.

This is managed with *Share validation or inspection data* message exchanges.

Exchange of action lists is needed to offer unified customer care services and to prevent fraudulent access of lost, stolen and suspended media or token.

This is managed with *Add/remove a media to/from a xx list; Add/remove a token to/from a xx list* message exchanges (where xx means authorised, denied or refused).If a SAM is reported lost/stolen, or an organisation is reported as acting fraudulently or ceases to operate, the related information needs to be distributed to the networks that could accept such product or media.

This is managed with *Add/remove SAM or organisation IDs from/to a refused list (black list)* message exchanges.

Most of the messages shall be exchanged in synchronous mode (i.e. in nearly real time) as identified in the table 6.

	Message	Dir.	Mode
Sales messages	Declare the sale of a medium / installation of an application	A<->B	Async.
	Declare the sale of a product	A<->B	Sync.
	Declare the refund of a medium	A<->B	Async.
	Declare the refund of a product	A<->B	Sync.
	Declare the restoration of a product	A<->B	Sync.
	Declare the replacement of a medium	A<->B	Async.
	Declare the sale of a product extension	A<->B	Async.
	Declare the partial refund of a product	A<->B	Async.
Fulfilment messages	*Get a fare product*		
Customer data messages	Request customer data	A<->B	Sync.
	Share customer data	A<->B	Sync.
	Request customer data removal	A<->B	Async.
	Modify customer parameters	A<->B	Sync.
Usage messages	Share validation or inspection data	A<->B	Async.
	Request customer charging		
Security update messages	Add/remove a media to/from an authorised list (white list)	A<->B	Sync.
	Add/remove a media to/from a denial list (denial list)	A<->B	Sync.
	Add/remove a media to/from a refused list (black list)	A<->B	Sync.
	Add/remove a token to/from an authorised list (white list)	A<->B	Sync.
	Add/remove a token to/from a denial list (denial list)	A<->B	Sync.
	Add/remove a token to/from a refused list (black list)	A<->B	Sync.
	Add/remove SAM or organisation IDs from/to a refused list	A<->B	Async.
Configuration messages	*Get fare set*		
	Share credential data		

Table 6: List of messages applicable to Interlining journey – ABT – frequent users

§§ End of document §§