

**TAP TSI RETAIL ARCHITECTURE DESCRIPTION**

|  |  |
| --- | --- |
| **Project:** | **TAP Phase One** |
| Release: | 1.0 – To DG MOVE, ERA, TAP Steering Committee |
| Date: | 13 May 2012 |
| Author: | Dominique Margottin (Work Stream Leader) |
| Owner: | TAP Phase One Project Team |
| Client: | DG MOVE, ERA |
| Document Ref: | TAP TSI Retail Architecture Description |
| Version No: | 1.0 |

## Document History

* 1. **Document Location**

This document will be uploaded to the “TAP TSI / TAP Retail Architecture/ Deliverables” folder of the project extranet (members’ area).

* 1. **Revision History**

**Date of delivery: 13 May 2012**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Document History | | | | |
| Date | Version | Description | Author | Modified chapters |
| 06/03/2012 | 0.1 | Initialisation | J.C. Montigny D. Margottin |  |
| 08/03/2012 | 0.2 | Changes during the TAP TSI Architecture meeting on 8mar12 | Architecture Group | * 1. Context and Scope   1.4 TAP TSI Retail Architecture context |
| 20/03/2012 | 1.0 | Version to be discussed and enriched with all architects for the 27mar12 meeting | J.C. Montigny R. Santoro D. Margottin |  |
| 21/03/2012 | 1.1 | Final version presented to meeting | J.C. Montigny  D. Margottin |  |
| 03/04/2012 | 1.2 | Inclusion of all contributions and remarks from architects | J.C. Montigny on behalf of Archi-tecture Group | According to new document structure |
| 05/04/2012 | 1.3 | Tidying and sorting of Non functional Requirements  Rephrasing Use Cases  Minor changes to Glossary | J.C. Montigny | Minor §1; §4.2  Major §6 use cases;  Major §7 |
| 06/04/2012 | 1.3 | Security and service requirements updated | M. Haynes | Changes in red done independently between the 2 v1.3 |
| 09/04/2012 | 2.0 | 4.2 Actor’s Landscape: Replacement with last Anant’s drawing  4.3 Interaction Overview: Replacement with last Anant’s drawing  6.4.2 Flow View: Replacement of last Dominique’s Drawings | D. Margottin | Reference Document for the Architecture meeting on 11 Apr 2012 in Brussels |
| 11/04/2012 | 2.1 | Validation of the document until chapter 4.4.1 List of Resources | Architecture Group |  |
| 14/04/2012 | 2.2 | Inputs from Mick on Registry security are moved to an appropriate chapter | M. Haynes | 6.1 |
| 19/04/2012 | 3.0 | Validation of the document until chapter 6.1.2 “Use Cases” | Architecture Group | 4.1.1, 5.1 and 6.1.1 |
| 20/04/2012 | 4.0 | Validation of the document until the end | Architecture Group | Consistency work between terms is needed;  Chapter 4.4.2 and 4.4.3 need to be reviewed |
| 09/05/2012 | 4.3 | Consolidation and consistency | A. Minhas,  R. Santoro  D. Margottin | Until chapter 6.5.2.6 included |
| 11/05/2012 | F01  (1.0) | Finalisation | A. Minhas,  R. Santoro  D. Margottin |  |

* 1. **Approvals**

This document requires the following approvals.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name/ Entity** | **Title/ Remark** | **Approval** | **Date of Issue** | **Version** |
| Project Team | Project Manager, Work Stream Leaders, Project Assistant | Done | 12 May 2012 | 1.0 |
| TAP Steering Committee | Chairs, members and alternates |  | 15 June 2012 | 1.0 |
| ERA |  |  | 13 July 2012 |  |

* 1. **Distribution**

This document is distributed to:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name/ Entity** | **Title/ Remark** | **Date of Issue** | **Version** |
| DG MOVE, ERA | Official recipients of the TAP Phase One deliverables | 13 May 2012 | 1.0 |
| TAP Steering Committee | Chairs, members and alternates | 13 May 2012 | 1.0 |
| Project Team;  UIC and Ticket Vendor project coordinators | All members of the Project Team and the coordinators involved in the Grant Agreement between DG MOVE and UIC | 13 May 2012 | 1.0 |
| Architecture Group members | Members of the Phase One Architecture Workgroup and other contributors | 14 May 2012 | 1.0 |
| Interested public | On http:\\tap-tsi.uic.org | tbd |  |

* 1. **Document maintenance**

This document is maintained by the European Railway Agency.

Any stakeholder detecting errors or needing clarifications can contact the European Railway Agency (e-mail address to be defined).

.

Proposals for additions or updates can be sent to the same mail addresses, and will undergo the Change Control Management process described in the TAP regulation.

## Table of Contents

[1 Document History 2](#_Toc324670769)

[2 Table of Contents 3](#_Toc324670770)

[3 Purpose 3](#_Toc324670771)

[4 Glossary 3](#_Toc324670772)

[5 Context 3](#_Toc324670773)

[6 Scope 3](#_Toc324670774)

[7 Actors and Landscape 3](#_Toc324670775)

[8 Business Rules 3](#_Toc324670776)

[9 Functional Requirements and Use Cases 3](#_Toc324670777)

[10 Non Functional Requirements 3](#_Toc324670778)

[11 Obligations of Service Providers 3](#_Toc324670779)

[12 ANNEX 3](#_Toc324670780)

## Purpose

Commission Regulation (EU) No 454/2011 requires at the end of Phase One the issuing of deliverables on three areas:

* detailed IT specifications
* governance
* master plan

In particular “The detailed IT specifications shall describe the system and shall indicate in a clear and unambiguous manner how the system fulfils the requirements of the TAP TSI. The development of such specifications requires a systematic analysis of the relevant technical, operational, economic and institutional issues that underpin the process of implementing the TAP TSI. Therefore, deliverables shall include, but shall not be limited to, the following:

1. Functional, technical and performance specifications, the associated data, the interface requirements, the security and the quality requirements.

2. The outline of the global architecture of the system. It shall describe how the requisite components interact and fit together. This shall be based on the analysis of the system configurations capable of integrating the legacy IT facilities, while delivering the required functionality and performance.”

The purpose of this document is to describe the TAP TSI Retail Architecture. It supports interoperability according to the specifications of the TAP TSI Basic Parameters and the provisions described in the Technical Documents (TDs). It facilitates all Actors to comply with the regulation, describes how to fulfil their obligations and allows them to exercise their rights.

## Glossary

|  |  |
| --- | --- |
| **Term** | **Meaning** |
| **Access Method** | Specification of technical means (or interface) by which a system accesses another.  The Registry stores the access methods for each RU and will give to Resource Consumers the needed information for data exchange   * Message format * Transport protocol * Server address and port |
| **Company Codes** | Reference data listing unique identifiers for Companies participating in the TAP TSI Retail Architecture and subject to the TAP TSI Regulation |
| **Control Certificate** | Transactional Resource made available by a Ticket Controlling Organisation (a type of Resource Producer) to support the print@home TAP TSI Regulation process  This is valid for the Carrier Makes Certificate (**CMC)** and Carrier Keeps Contract (**CKC)** e-Fulfilment methods as described in the B7 technical document. |
| **Data Quality Management (DQM)** | A common component of the TAP TSI Retail Architecture providing Data Quality Management services to both Resource Producers and Resource Consumers.  The component performs quality management checks and produces reports to the requester. |
| **European Railway Agency (ERA)** | A community agency created on 20th April 2004 by an EC Regulation. It has 2 missions: Railway safety and Railway Interoperability |
| **Governance Entity** | The body dedicated to TAP TSI, responsible for implementing and operating the TAP TSI regulation through the TAP TSI Governance Process |
| **Partial Schedule** | A partial schedule is integrated with other Partial Schedules of the same service to build the end to end schedule. A Resource Producer is only responsible for the delivery of the Partial Schedules it is in control of. |
| **Notification** | A message generated by the Registry to Resource consumers that have subscribed to receive Notification regarding a specific Resource, upon detection of that Resource being made available or updated by Resource Producers |
| **Passenger Code List** | List of allowed values for specific data types managed by the Governance Entity, centrally stored and available in a computer readable format to both Consumers and Producers.  ERA will make the Passenger code list and location reference data publicly accessible.  This list will be registered as a Resource by the Governance Entity acting as a Resource Producer |
| **Public Key** | Resource made available by an Actor to decrypt a file encrypted by the same actor with its Private key. An application in TAP TSI is for a Distributor (a type of Resource Producer) to support the print@home TAP TSI Regulation process.  This is valid for the Digital Signed Ticket (**DST)**, one of the possibilities of e-Fulfilment methods as described in the B.7 technical document). |
| **Reference location Data** | Reference data listing unique identifiers for Locations used in the TAP TSI Retail Architecture managed by Governance Entity. It will be stored centrally and will be accessible by both Resource Producers and Resource Consumers in a machine readable format.  It will be registered by Governance Entity acting as a Resource Producer |
| **Registrar**  **Registry** | A role in the Governance process charged with administration of the Registry  The Registry is a Central Repository listing Resource names, addresses and Access Methods, made available by Resource Producers for the Resource Consumers.  It also registers subscriptions to Resources by Resource Consumers. |
| **Registry Service Provider**  **Resource** | Organisation selected through a tender process to manage the hardware and software environment implementing the Registry.  Files, interfaces, endpoints or data elements made available by Resource Producers and accessed by Resource Consumers through Access Methods |
| **Resource Delivery** | Delivery of a resource” indicates the operation of making a resource available. The term “delivery” therefore does not imply “sending” data but consists in registration in the Registry |
| **Resource Subscription** | A Resource Consumer is associated with one or more Resource Subscriptions entries, each consisting of the “Resource Name” and, optionally a list of selected Resource Producers of that Resource. |
| **Retail Reference Data (RRD)** | A common component of the TAP TSI Retail Architecture providing Access Methods to Reference Location Data, Passenger Code lists, specific retail codes (Retail Data) and Company Codes |
|  |  |
| **TAP TSI Governance Process** | The process of administering the TAP TSI Regulation |
| **TAP TSI Regulation** | The Commission Regulation (EU) No 454/2011 of 5 May 2011 on the technical specification for interoperability relating to the subsystem ‘telematics applications for passenger services’ of the trans-European rail system, including its Technical Documents |
|  |  |

## Context

Commission Regulation 454/2011 requires at the end of Phase One the issuing of deliverables on detailed IT specifications.

In particular “*The detailed IT specifications shall describe the system and shall indicate in a clear and unambiguous manner how the system fulfills the requirements of the TAP TSI. The development of such specifications requires a systematic analysis of the relevant technical, operational, economic and institutional issues that underpin the process of implementing the TAP TSI. Therefore, deliverables shall include, but shall not be limited to, the following:*

1. *Functional, technical and performance specifications, the associated data, the interface requirements, the security and the quality requirements.*
2. *The outline of the global architecture of the system. It shall describe how the requisite components interact and fit together. This shall be based on the analysis of the system configurations capable of integrating the legacy IT facilities, while delivering the required functionality and performance.*”

TAP TSI Architecture specific Basic Parameters are the following:

*Chapter 4.2.21.1. General architecture*

*The proposed ‘Information Exchange Architecture’:*

* *is designed to reconcile heterogeneous information models by semantically transforming the data that are exchanged between the systems and by reconciling the differences in business processes and application- level protocols,*
* *has a minimal impact on the existing IT architectures implemented by each actor,*
* *safeguards IT investments already made.*

*The Information Exchange Architecture favours a mostly Peer-to-Peer type of interaction between all actors, while guaranteeing the overall integrity and consistency of the rail interoperability community by providing a set of centralised services.*

*A Peer-to-Peer interaction model allows the best distribution of costs between the different actors, based on actual usage and, in general, will pose fewer scalability problems.*

*Chapter 7.2.3*

*Deliverables shall include the outline of the global architecture of the system. It shall describe how the requisite components interact and fit together. This shall be based on the analysis of the system configurations capable of integrating the legacy IT facilities, while delivering the required functionality and performance.*

The document defines consequently the architecture that will be used to exchange rail data according to those Basic Parameters.

This document is intended for the use of:

- RUs when acting as “Resource Producers”, delivering resources such as Timetables, Tariffs/Fares

- Distributors acting as Producers, delivering Public Keys for Digitally Signed Ticket Print@home

- Public Authorities, Ticket Vendors, RUs acting as “Consumers” of Resources

- Governance Entity when acting as the “facilitator” to all Actors in the TAP TSI

In order to come to an accurate identification of the “data exchange architecture” for the Basic Parameters of TAP TSI Phase One, and to generate data exchange Procedures from it, it is important to qualify the expression “data exchange” by identifying type of interactions:

* File exchange. These are used for asynchronous copying of data organised in files across systems. For instance ftp (File Transfer Protocol) for timetable data etc.
* Transactional service requests using a synchronous request/ reply message exchange (i.e. reservation request).

The Architecture is designed as a business logic neutral interoperability infrastructure that can be extended to support the evolution of new Resources and new Technical Documents (i.e. changing from one data structure format to another).

## Scope

This document presents a high level view of the TAP TSI Retail architecture: decentralised exchange of rail business data with a central registry.

The TAP TSI retail architecture covers the exchange of rail business data, defined as Resources (timetable, fares…), between RUs and third parties e.g. other RUs, Ticket Vendors, Public Authorities.

The architecture also describes possibilities for the Governance Entity to facilitate data provisioning and quality.

The architecture provides support to but does not cover:

* Production of the data, including reference data
* Assembling complete train schedule from different timetable resources
* Internal processes for the resource producers to fulfil the EU rail legislation requirements in TAP TSI on data provisioning (12-months history (TAP TSI chapter 4.2.1), NRT data to publish 3 months before they are applicable (TAP TSI Annex IV)
* Settlement (not part of TAP TSI)
* Intellectual Property Rights issues of data provided by the resource producers
* Software development cycles
* TAP TSI Governance process definition

## Actors and Landscape

* 1. **Actors definitions, goals and roles**

|  |  |  |
| --- | --- | --- |
| **Actor** | **Description** | **Goals** |
| **AC1** | **Resource Producer**  TAP TSI Actor that makes Resource available to Resource Consumers by registering Resource together with one or more Access Methods, in the Registry.  Resource Producers include;   * Schedule “Information” Providers * Fares and Tariff data providers * Reservation system Providers * PRM assistance service Providers * Ticket Controlling Organisations providing Control Certificates * Distributors providing Public Keys to Ticket Controlling Organisations * Providers of Reference Data | * Makes a Resource available to those Resource Consumers who are entitled to it under bilateral agreements and/or the TAP TSI Regulation * Register a Resource * Request quality validation report on a Resource from Data Quality Manager |
| **AC2** | **Resource Consumer**  TAP TSI Actor that consumes data produced by Resource Producers.  They can do so by:   * Receiving notifications of Resources being made available or updated when subscribed to their updates * Retrieving a Registry entry to obtain the location and Access Methods to use in order to know where said Resources are made available by Resource Producers   Resource Consumers include:   * Public Authorities * Railway Operators * Ticket Vendors | * Subscribe to availability and updates to Resources whether they are entitled or not to receive under bilateral agreements with Resource Producers and TAP-TSI Regulation * Retrieve Registry entries to determine Access Method to Resources * Use retrieved Access Method to access Resources from a chosen Resource Producer * ask quality validation report on a Resource from Data Quality Manager |
| **AC3** | **Data Quality Manager**  A specialised Resource Producer that provides an interface and/or service (a type of Resource) to perform quality checks and generate quality reports and logs on Resources. It can be used by both Resource Consumers and Resource Producers. | * As a Resource Producer, register interface to Data Quality validation and reporting procedure * Produce data quality report on Resources submitted to it for quality validation. |
| **AC4** | **Governance Entity**  It is a facilitator assisting all actors in the TAP TSI ecosystem to be compliant with the TAP TSI Regulation | * As a Resource Producer, register and make available Resources it controls, such as Code Lists and Reference Location Data. * As an entitled Resource Consumer under the TAP TSI Regulation, subscribe to Resource updates, obtain Registry entries and access Resources |
| **AC5** | **Registrar**  person in the Registry Service Provider organisation appointed by the Governance Entity to supervise the working of the Registry | * As an entitled Actor, providing operational day to day support with registered actors, and helping new actors to be registered |

* 1. **Actors landscape**

The landscape describing Actors is illustrated below.

There is a direct relationship between Resource Producers and Resource Consumers based on commercial agreements and the TAP TSI Regulation.

All Actors needs to subscribe to the Registry in order to at least get the Reference Data and other Services.

Resource Producers e.g. RUs register their Resources.

Resource Consumers subscribe to the Resource Registry entries.

Both Resource Producers and Consumers can submit their Resources to the DQM for a report on data quality.

Both Resource Producers and Consumers get Reference data from the RRD

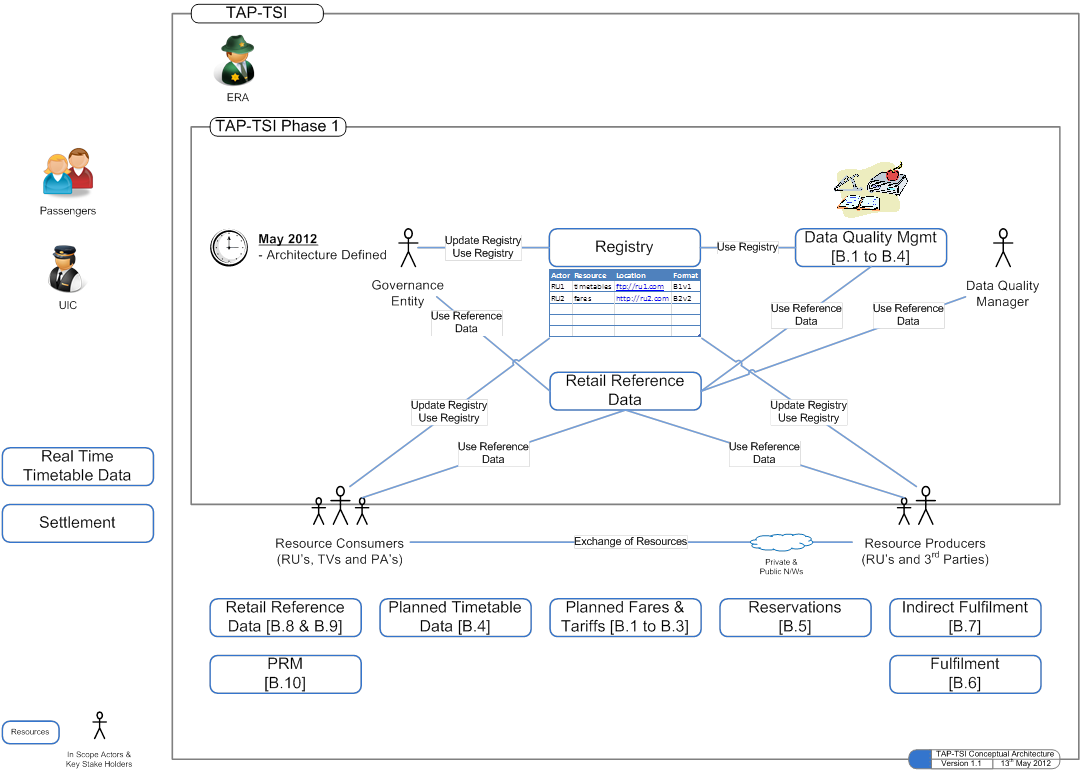
Governance Entity/ Registrar administers the Registry:

* Registrar provisions Membership credentials
* Governance Entity monitors activity (Registry, DQM, RRD)
* Governance Entity maintains RRD and DQM



* 1. **Interaction overview**

The following drawing shows the perimeter of the current proposed Architecture that matches the requirements of the Regulation (inside the TAP-TSI frame) and subjects that are not part of the Regulation (outside the TAP-TSI frame). Data to be exchanged between Resource Producers and Resource Consumers have a reference to the Technical Documents and the type of data mentioned in Basic Parameters**.**



Resource Producers produce resources and make them available in the format described in Technical Documents defined in the Regulation. They register their resources in a central registry, so that resource consumers know where and how to fetch them.

The quality of the data can be verified by the use of the Data Quality Management tool procured by the Governance Entity.

The resource consumers consult the registry to know how to get the resources. Alternately, they can subscribe to resources in order to receive a notification from the registry on resource update.

They can in turn retrieve the resources using the access method given by the registry.

Subscription to a resource is optional. Once subscription is made, the notification is automatic.

* 1. **Resources**
     1. List of resources

The table below lists the available resources and their functionality, as well as the message formats which must be indicated in the Registry and respected by the resource producers. The architecture should be designed so that it can expand and contract as needed.

|  |  |  |  |
| --- | --- | --- | --- |
| **Theme** | **Resource** | **Functionality** | **Format** |
| **Timetable** | Timetable | Planned timetable, made available by Producers on a regular basis or when needed. Applicable for information. | B4 |
| **Tariffs and fares** | NRT | NRT tariffs and fares; suitable for sales. Made available on a regular basis or when needed. | B1 |
|  | IRT | IRT tariffs and planned fares; applicable for information only. Made available at any time. | B2 |
|  | Special offers | Special tariffs and planned fares, applicable for information only made available at any time. | B3 |
| **Retail Reference data** | Passenger code lists | List of values for data used in Technical Documents  Required to read timetable and tariffs, perform reservation and ticketing | TD\_PassengerCodeList |
|  | Country codes | Required to read timetable and tariffs, perform reservation and ticketing | ISO Codes |
|  | Location codes | Required to read timetable and tariffs, perform reservation and ticketing | B9 or TAP TSI Common Reference Database (CRD) |
|  | Company codes | Required to read timetable and tariffs, perform booking and ticketing | B8 or TAP TSI Common Reference Database (CRD) |
| **e-Fulfilment data** | Public keys for print@home | Public keys that allow the Ticket Controlling Organisation (TCO) to read a P@H ticket for DST method.  Availability: depends on bilateral agreements. | Depends on bilateral agreement  B7 |
|  | Other print@home data | Interactive, on-demand transactions with the inventory systems | B7 |
| **Booking** | Inventory system | Interactive, on-demand transactions with the inventory systems, for IRTs and Reservation only | B5 |
| **PRM assistance** | PRM systems | Interactive, on-demand transactions between systems according to the standard recommended by the Regulation | B10 |
| **Data Quality**  **Management tool** | Data Quality | Resource procured by the Governance |  |

The above message formats and their appropriate use and implementation are described in the following TAP TSI IT Specifications:

|  |  |
| --- | --- |
| **Format** | **Implementation Guides (title, year, version)** |
| **Timetables** | *List to be maintained* |
| **Tariffs** | *List to be maintained* |
| **Direct Fulfilment** | *List to be maintained* |
| **Indirect Fulfilment** | *List to be maintained* |
| **Reservation** | *List to be maintained* |
| **PRM assistance** | *List to be maintained* |

* + 1. Register Resource

Resources listed in the previous chapters are delivered by Resource Producers according to the specification of the IT Specifications applicable for the specific Resource, which determine the Delivery contents for each type of Resource (i.e. whether a Resource such as a Timetable is a complete Timetable for a particular Resource Provider, or an incremental update).

Registration of a Resource consists of creating a Registry entry called a “Resource Delivery” which is an association of a Resource Producer and a list of Resource entries, each representing a Resource being made available such as Timetables, Fares etc.

A Resource entry should be generic and should represent any type of Resource, and contain a “Resource Name” attribute indicating its name (e.g. “TIMETABLE”, “FARES” etc.)

A Resource Entry is uniquely identified by a Delivery Entry with the following attributes:

* “Delivery Number”
* TAP TD baseline (version)
* Valid from / Valid to (date)
* Delivery datetime stamp
* Resource status: added, removed or updated
* Access Method (see chapter 7.4.3)

In case, a Producer wishes to use another standard than B5, he will have the choice to either fill in the description of the solution or just signalling that it is a proprietary solution. (cf annex)

A “Resource Delivery” is a unique combination of Resource Producer’s identifier, the “Resource Name” and “Delivery number

Illustrative example:

|  |  |  |
| --- | --- | --- |
| **Resource Producer** | **Resource Name** | **Delivery Number** |
| 83 | TIMETABLE | 4-2012 |
| 83 | TIMETABLE | 5-2012 |
| 83 | FARES | 4-2012 |
| 83 | RESERVATION | 4-2012 |
| 87 | TIMETABLE | 4-2012 |

In the example above, Resource Producer ‘83’ has made available two Timetable Resources numbered 4-2012 and 5-2012, a Fares Resource numbered 4-2012 and a RESERVATION Resource numbered 4-2012. Resource Producer ‘87’ has made available a Timetable Resource numbered 4-2012

Thus, Resource Provider ‘83’ is the owner of Deliveries 4-2012 and 5-2012 of a Timetable, and Resource Provider ‘87’ is the owner of Delivery 4-2012 of a Timetable.

The relationship of a Resource Producer to its Resources is a composition: deletion of the Resource Producer from the Registry removes all Resources, and therefore Deliveries, associated with it. Conversely, there can be no Resource Delivery not associated with its owning Resource Producer.

A Resource Producer can add, remove, read or update a Resource as follows:

* It can add a Resource provided a Resource with the same “Resource Name” and “Delivery Number” does not exist already in the Registry
* It can update a Resource if it exists in the Registry with a specific “Resource Name” and “Delivery Number”
* It can delete a Resource if it exists in the Registry with a specific “Resource Name” and “Delivery Number” (Deletion is logical, not physical. Deleted information should be available for Audit purposes)
  + - 1. Timetable Resources

Timetable resources are represented in the Registry as specific types of Resource entry.

A Timetable Resource entry is associated with” Timetable Services” describing either a list of Service Brands and/or a list of Service Number (train number) included in the Timetable delivery.

Timetable Resource is a description on the location where that Resource can be found with its Access Method

A Resource Producer making a Resource Delivery of timetable which specifies “Service Brand” and/or “Service Numbers” is the Information Provider for those Service Brands and/or Service Numbers.

A Partial Schedule for a “Service Number” is required to indicate that the Timetable contains a partial schedule for that “Service Number” that needs to be integrated according to the specifications of the relevant IT Specification.

* + - 1. IRT Tariffs/Fares Resources

IRT Tariffs/Fares resources are represented in the Registry as a specific type of Resource entry.

IRT Tariffs/Fares Resource is a description on the location where that Resource can be found with its Access Method

An IRT Tariff/Fare Resource is associated with a list of “Entity Codes” and/ or “IRT Tariff Codes” from the relevant Passenger Code lists.

* + - 1. NRT Fares Resources

NRT Tariffs/Fares resources are represented in the Registry as a specific type of Resource entry.

NRT Tariffs/Fares Resource is a description on the location where that Resource can be found with its Access Method

An NRT Tariffs/Fare Resource is associated with a list of “Series number” and year/month/day.

* + - 1. Special Tariffs/Fares Resources

Special Tariffs/Fares resources are represented in the Registry as a specific type of Resource entry.

A Special Tariffs/Fares Resource is a description on the location where that Resource can be found with its Access Method

Special Tariffs/Fares are not exchanged between RUs as the standard is not appropriate to RU’s needs.

* + - 1. Reservation Resources

Reservation resources are represented in the Registry as a specific type of Resource entry.

Reservation Resource is an address and signature of the interface to a Reservation System in which an Resource Consumer can find a reservation (either alone or combined with the travel journey.

* + - 1. Public Key Resources

Public key resources are represented in the Registry as a specific type of Resource entry.

Public Key Resource is a description on the location where that Resource can be found with its Access Method

It contains key strings with validity and expiration dates.

* + - 1. Retail Reference Data Resource

Retail Reference Data resource is represented in the Registry as a specific type of Resource entry.

Retail Reference Data t Resource is an address and signature of the interface to reference data. The RRD is an entry point where Consumers and Producers will be able to get retail reference data such as Code List, Station codes, retail specific codes.

* + - 1. Data Quality Management Resources

Data quality Management resource is represented in the Registry as a specific type of Resource entry.

Data Quality Management Resource is an address and signature of the interface to the DQM.

* + 1. Access Methods

Access Methods represent the specification of interfaces used by Resource Consumers to gain access to “Resource Deliveries” made available by a Resource Producer, or by the Registry to send notifications to Resource Consumers about Resources they subscribed to.

Resource Access specific methods are specified by:

* A Resource Producer in a Resource Delivery
* The Registry towards the specific Resource Consumer:
  + As a default notification method for all Resources it subscribes to
  + As a specific tailor-made notification method for a specific Resource it subscribes to.

An Access Method specifies an endpoint and an indicator that authentication by the Resource Consumer is required (where appropriate) at the endpoint (cf. Annex 12.2.).

* + - 1. File Transfer Access Method

A File Transfer access method is a specific Access Method with additional description pertaining to file transfer:

It can specify either a script to be run at the endpoint (such as a server side script on a web or ftp server), or a list of “Resource Files” entries, each consisting of a Filename with a CheckSum.

* + - 1. Web Service Access Method

A web service access method is a specific Access Method with additional description pertaining to a web services interface.

It specifies the name of a web service definition language (WSDL) file and an operation name to invoke the call.

* + - 1. E-mail Access Method

An e-mail access method is a specific Access Method with additional description pertaining to an e-mail interface.

It specifies a list of e-mail addresses and optional header and footer text to be included in the e-mail.

* + 1. Resource Subscriptions

Resource Consumers can subscribe in the Registry to notifications about specific Resources. The notifications are sent by the Registry automatically when a Resource Delivery is added, updated or removed by a Resource Producer to all Resource Consumers that subscribe to that specific Resource, indicated by its “Resource Name”.

A Resource Consumer is associated with one or more Resource Subscriptions entries, each consisting of the “Resource Name” and, optionally a list of selected Resource Producers of that Resource.

A “Resource Subscription” is a unique combination of Resource Consumer’s identifier, the “Resource Name” and Resource Provider.

Illustrative examples

|  |  |  |
| --- | --- | --- |
| **Resource Consumer** | **Resource Name** | **Resource Producer** |
| 83 | TIMETABLE | all |
| 83 | FARES | 87 |
| DRTY | TIMETABLE | 83 |

In the above example, the first entry specifies that Resource Consumer ‘83’ subscribes to notifications about Resource TIMETABLE from any Resource Producer, the second that it subscribes to notifications about Resource FARES delivered by Resource Producer ‘87 ’, and the third that Resource Consumer ‘DRTY’ subscribes to notifications about Resource TIMETABLE delivered by Resource Producer ‘83’.

The relationship of a Resource Consumer to Resources it subscribes to is a composition: deletion of the Resource Consumer from the Registry removes all “Resource Subscriptions” associated with it. Conversely, there can be no “Resource Subscriptions” not associated with its owning Resource Consumer.

The notifications from the Registry to the Resource Consumer will contain the Resource Delivery and the linked Delivery Entry (see chapter 7.4.2) of the appropriate Resource Producer.

## Business Rules

* 1. **Resource registration, subscription and access**

These are the business process rules for the operation of the Registry.

These rules must be implemented in the Registry.

|  |  |
| --- | --- |
| **##** | **Business Rule** |
| **BR1** | Resources are owned by Resource Producers who make them available under the TAP TSI Regulation. |
| **BR2** | Resource Producers can only register Resources they own or are delegated to register. A successful registration records the Resource Producer's ownership of the registered Resource (or alternatively above delegation) |
| **BR3** | Resources can only be registered by their owner Resource Producer unless the latter delegates officially the registration to another Resource Producer. |
| **BR4** | As a consequence of BR2 and BR3 above, the same Resource cannot be registered by more than one Resource Producer |
| **BR5** | If a Resource is to be registered by a different Resource Producer then the previous owner Resource Producer must first delete its registration in the Registry. |
| **BR6** | Resource Producers can restrict access to Resources they register to particular Resource Consumers, subject to the provision of the TAP TSI Regulation. In this case the Resource is a Restricted Resource. |
| **BR7** | Resource Producer can play the role of Resource Consumer when accessing Resources owned and registered by a different Resource Producer |
| **BR8** | Resource Producers are responsible for the authenticity checks to access their data repositories in Restricted Resources and maintain the access list in the system where they make Resources available:   * Identity check * Access rights check |
| **BR9** | A Resource Consumer can subscribe to notifications about any Resource. Subscription does not grant access to the Restricted Resource , access being controlled by Access List maintained by the Resource Producer in its own system. |
| **BR10** | A Resource Consumer can access any Resource it has a right to under the Regulation, or any Restricted Resource to which the owner Resource Producer has granted access to. |
| **BR11** | Other than playing the role of a Resource Consumer to subscribe to updates and access Resources, or, possibly, Resource Producer for certain resources such as Code Lists or Reference Location Data, the Governance Entity may have rights under the TAP TSI Regulation and the TAP TSI Governance Process to read the Registry contents, including its logs and audit trails and reports. The Governance Entity will have full access to the aforementioned logs and audit trails and reports in order to monitor the fair and transparent implementation of European rail interoperability.  Additional rights are subject to the TAP TSI Governance Process. |
| **BR12** | Versioning of Resources |

## Functional Requirements and Use Cases

* 1. **Functional requirements**

The TAP-TSI Retail Architecture is an ICT environment designed to realize the interaction between Actors as described in chapter 7.2, “Actors Landscape”, for the purpose of making available and accessing resources as described in chapter 7.4, “Resources”, subject to the rules described in chapter 8, “Business Rules”.

Chapters 9.1 through 9.4 document functions that must be provided by the Architecture in order for Actors to obtain results, such as “registering a resource”, or “subscribing to notifications”, that concretely implement the interactions necessary to obtain interoperability. They provide therefore a behavioural view of the Architecture.

Chapter 9.5 groups functions and allocates them to “Common Components”, i.e. structural components of the Architecture, which are a high level partition of deployable concrete implementations of the functional requirements.

Chapter 9.5.1, in particular, describes overall interoperable scenarios realized by Actors using the functions provided by the Common Components, including the coordination and communications between these components.

|  |  |
| --- | --- |
| **##** | **Functionality** |
| **FR1** | Profile support per user with access and control mechanism, for example role, rights, standard parameters. These functions are used by the Registrar to setup the Registry for use by Actors in the landscape |
| **FR2** | The registry provides the following services to Actors :   * Provide membership * Register a resource by creating “Resource Delivery” entries (cf chapter 9.2.1.2) * Update a “Resource Delivery” entry * Unregister a resource by deleting the “Resource Delivery” entry * List available “Resources Deliveries” * Read a particular Registry entry (Resource Delivery, Resource Subscription) * Subscribe to a resource by creating a Resource Subscription entry (cf chapter 9.2.1.3) * List current subscriptions * Logging * Audit |
| **FR3** | A Registrar has the following capabilities::   * FR2 and * Create, update and delete members * Provide all necessary functions to provision an actor |
| **FR4** | The registry provides the following Access Methods to services listed in FR2   * Website manual access (direct access by internet page)   + User web Interface   + Administrator’s wweb interface * Web services call (machine access to Registry services) |
| **FR5** | Registry notifies Resource Consumers that have subscribed to resources when “Resource Deliveries” have been created, deleted or changed .  Example of possible protocols for the notification method:   * Email * Web services ( a request to a Resource Consumer web service call) |
| **FR6** | Each time an existing “Resource Delivery” changes or is deleted, the Registry will trigger a component that will then perform the following actions:   * Retrieve the “Resource Subscription” entries to find resource Consumers that have subscribed to the resource * Notify Resource Consumers using notification method in the Resource Subscription |
| **FR8** | **The Registry user web interface** will use the underlying registry services listed in FR2  The user web interface is able to provide users with additional information about :   * The person to contact for each of the resource listed, in order to set up a business agreement to get access to the resource * Statistics of usage of the registry   The Registry user web interface application shall implement access security mechanisms, managed by the Registry Administrator's user interface. |
| **FR9** | **The Registry Administrators‘ user interface** will use the underlying registry services in FR2  The Administraror’s web interface allows the Registrar to perform the following tasks on behalf of the Governance Entity   * Same tasks as an ordinary user * Perform member credential provisioning * Access logs * Generate registry activity audit trails and reports * Perform backup / restore actions * Setup and monitor security mechanisms |

* 1. Use cases

List of use cases:

* Membership Registration (CRUD)
  + - Producers
    - Consumers
    - DQM
* Register a resource (CRUD)
  + - Timetables
    - Tariffs/fares
    - Public keys DST print@home
* Subscribe to a resource (CRUD)
  + - Timetables
    - Tariffs/fares
    - Public keys DST print@home
* Notify subscribers (CRUD)
* Retrieve a resource
* Submit data quality Checks

The following additional Use Cases are industry best practices and they will not be described in the reminder of this document:

* Logging
* Auditing
* Reporting
* Administrative function
* Security
  + 1. Membership Registration

Pre-condition: Candidate member has been validated by the Governance Entity, and Registrar has been cleared to grant Membership

Main success scenario:

1. Connect to Registration website
2. Complete Registration form
3. Submit

End

Extension:

2a- Create

2b- Read

2c- Update

2d- Delete

3a – success

3b – failure

4a – success

4a – failure

Post Conditions: awaiting approval

* + 1. Register a resource

A Resource Producer makes a Resource Available

Pre-condition: - actor is a registered user

- Resource has passed Data QualityManagement checks (whatever tool is used)

Main success scenario:

1. Resource Producer provides identification credentials to the Registry
2. Resource Producer creates Resource Delivery entry in the Registry

End

Extensions: ref Chapter 8 Business Rules

NOTE: Step 2 Use Case can be performed by Resource Producer Human operators using Registry web User Interface

* + 1. Subscribe to a resource

Pre-condition: - actor is a registered user

- The resource has been registered

Main Success Scenario

1. Resource Consumer Provides identification credentials to the Registry
2. Resource Consumer creates Resource Subscription entry in the Registry

End

* + 1. Notify subscribers

Upon reception of an Update Signal on a Resource, send notification messages to Resource Consumers subscribing to Resource

Precondition: Notifier receives signal from the Registry

Main Success Scenario

1. Notifier retrieves “Resource Subscription” entries from Registry
2. Notifier reads Resource Consumers and Notification methods from Resources Subscription entries
3. Notifier sends notifications to Resource Consumers using notification methods

End

* + 1. Retrieve a resource

A Resource Consumer retrieves a Resource made available by a Resource Producer

Preconditions: Resource Consumer has credentials to access Resource as specified by Resource Producer on Access method’s interface

Success Guarantee: Resource Consumer successfully retrieves Resource

Main Success scenario

1. Resource Consumer gets “Resource Delivery” entry from Registry to obtain Resource information and Access Method to the Resource
2. Resource Consumer uses Access Method to determine location and interface to Resource
3. Resource Consumer submit request of Resource using specified Interface
4. Resource Consumer stores Resource
5. Resource Consumer may optionally execute "Submit Resource to Quality Checks"

End

NOTE: Steps 1, 2 and 3 of Use Case can be performed by Resource Consumer Human operators using Registry web User Interface

* 1. **Data Quality Management**
     1. Functional Requirements

Functional Requirements listed in chapter 9.1 describe functions that must be available to Actors to realize interoperable exchange of Resources. In the interest of *effective* interoperability, however, the TAP-TSI Retail Architecture must provide functions to check that Resources exchanged meet certain quality standards in terms of the data content and consistency, as described in this chapter. Data Quality Management functions are allocated to a “Data Quality Management” (or DQM tool) component.

|  |  |
| --- | --- |
| **##** | **Functionality** |
| **DR1** | The Data Quality Management (DQM) tool will be able to access the following reference data in order to perform data quality checks:   * Reference Location Data * Code Lists * Retail Reference Data (RRD) |
| **DR2** | Data Quality Management checks vary depending on the Resource whose quality is requested to be checked (e.g. Timetables, Fares).  The checks will be done according to the mandatory data quality chapters of the individual TAP TSI implementation guidelines. |
| **DR3** | The DQM tool will carry out the following activities :   * Perform quality check on a resource * Produce a report on the resource * Produce audit logs * Produce standard and ad hoc reports |
| **DR4** | The Data Quality Management component provides the following interfaces to its services:   * Website manual access (direct access by internet page) * Web services call |
| **DR5** | The DQM user web interface uses the underlying DQM web services calls  The user interface allows the users to perform the following tasks :   * Log in * submit a resource for data quality checking * Save the report of the quality checks * receive the report on the quality check process * notify the requester that the data quality checks has been completed * View historic reports   The DQM user interface application shall implement access security mechanisms, managed by the DQM Administrator's user interface.  The user interface is able to provide users with additional information about :   * The person to contact regarding the service * Statistics of usage of the DQM |
| **DR6** | The DQM Administrators ‘ web interface uses the underlying DQM web services calls  The DQM Administrator’s web interface allows the DQM administrator on behalf of the Governance Entity to perform the following tasks :   * Same tasks as an ordinary user * Perform user credential provisioning. * Access and store logs * Generate DQM activity audit trails and reports * Perform backup / restore actions |

* + 1. Use cases

List of use cases:

* Submit a resource (through machine or web user interface)
  + Timetables
  + Tariffs/fares
* The following additional Use Cases are industry best practices and they will not be described in the reminder of this document:
* Logging
* Auditing
* Reporting
* Administrative function
* Security
  + - 1. Submit resource to quality checks

Precondition: actor is a registered user

Main Success scenario:

1. Resource Producers or Consumers retrieve data Management Tool address from Registry (could be done only once)
2. Resource Producers or Consumers provides credentials to DQM tool
3. Resource Producers or Consumers submit the resource
4. DQM checks the content of the submitted resource against Reference Data stored in the Retail Reference Data
5. Resource Producers or Consumers get report on the resource (synchronously or asynchronously depending on the solution)

Extension:

4.1 execute Get Reference Data Use Case (see chapter 9.4.2.1)

End

* 1. **Retail** **Reference Data**

The Retail Reference Data provides a single access channel to multiple primary reference data sources insulating Actors from the actual storage location and managing on behalf of the Actor the access credentials to these sources.

Retail Reference Data includes:

* Reference Location data (TAF-TAP CRD)
* Code lists
* Retail specific data
  + 1. Functional Requirements

|  |  |
| --- | --- |
| **##** | **Functionality** |
| **DR1** | * Governance Entity will provide credentials to RRD so that it can access to the primary reference data sources. |
| **DR2** | * Only Authorised users can access RRD |
| **DR3** | RRD provides a User interface for accessing the Retail Reference data which could be possible via:   * Downloading from a website * Using File transport Protocol * Web services   : |
| **DR4** | The user interface also provides an administration console for the Governance Entity to handle the provisioning of user credentials. |

* + 1. Use cases

List of use cases

* Get reference data

The following additional Use Cases are industry best practices and they will not be described in the reminder of this document:

* Logging
* Auditing
* Reporting
* Administrative function
* Security
  + - 1. Get reference data

Precondition: actor is a registered user

Main success scenario:

1. Resource Producer or Resource Consumer provide credentials to RRD
2. Resource Producer or Resource Consumer identify the type of reference data
3. Resource Producer or Resource Consumer submit
4. Reference data is returned to Resource Producer or Resource Consumer

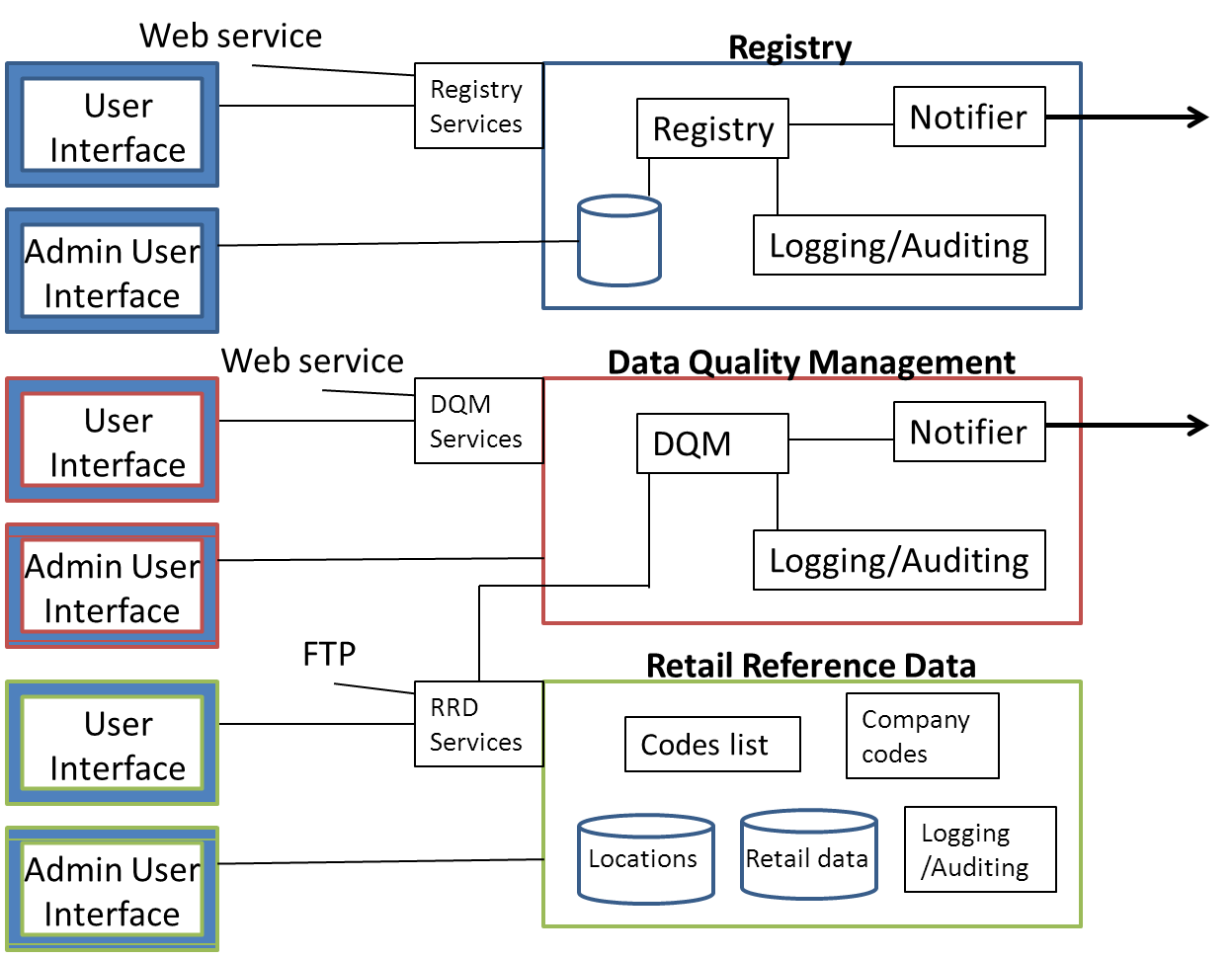
End

NOTE: Use case can be executed as extension of Submit Resource to Quality Checks Use case (see chapter 9.3.2.1) by Data Quality Management Tool.

**9.5 Common Components of the TAP-TSI Retail Architecture and their interaction**

The functional requirements described in chapters 9.1 through 9.4 are implemented by three structural, or “Common Components” of the TAP-TSI Retail Architecture described below.

The Common Components are deployable units providing logically coherent services, loosely coupled by web service consumer/producer relationships, and each support a User and an Administrator’s web interface for Human operators, including the Registrar.



The three common components of the TAP TSI retail architecture are:

* **TAP TSI Registry for Interoperability**. It provides:
  + Registry services
  + Notification services
  + Log/Audit services
  + User Interface
* **Data quality management** (DQM). It provides:
  + DQM services
  + Notification Services
  + Log/Audit services
  + User Interface
* **Retail Reference Data** (RRD). It provides:
  + Central Reference Data services
  + Code List
  + Retail data
  + TAP TSI-TAF TSI common reference data
  + User Interface
  + Log/Audit services

Retail Data is a database where the actors can find reference data specific to retail that cannot be found in the location Common Repository Domain of TAF (further details will be known at time of preparing the tender). The RRD is the interface the Actors needs to log in to be able to access different kinds of reference data (Code list, station Locations, specific retail locations data, company codes).

**DQM** and **RRD** are registered as Resource Producers.

* + 1. Overall interaction
       1. Actors ask for membership in the Registry

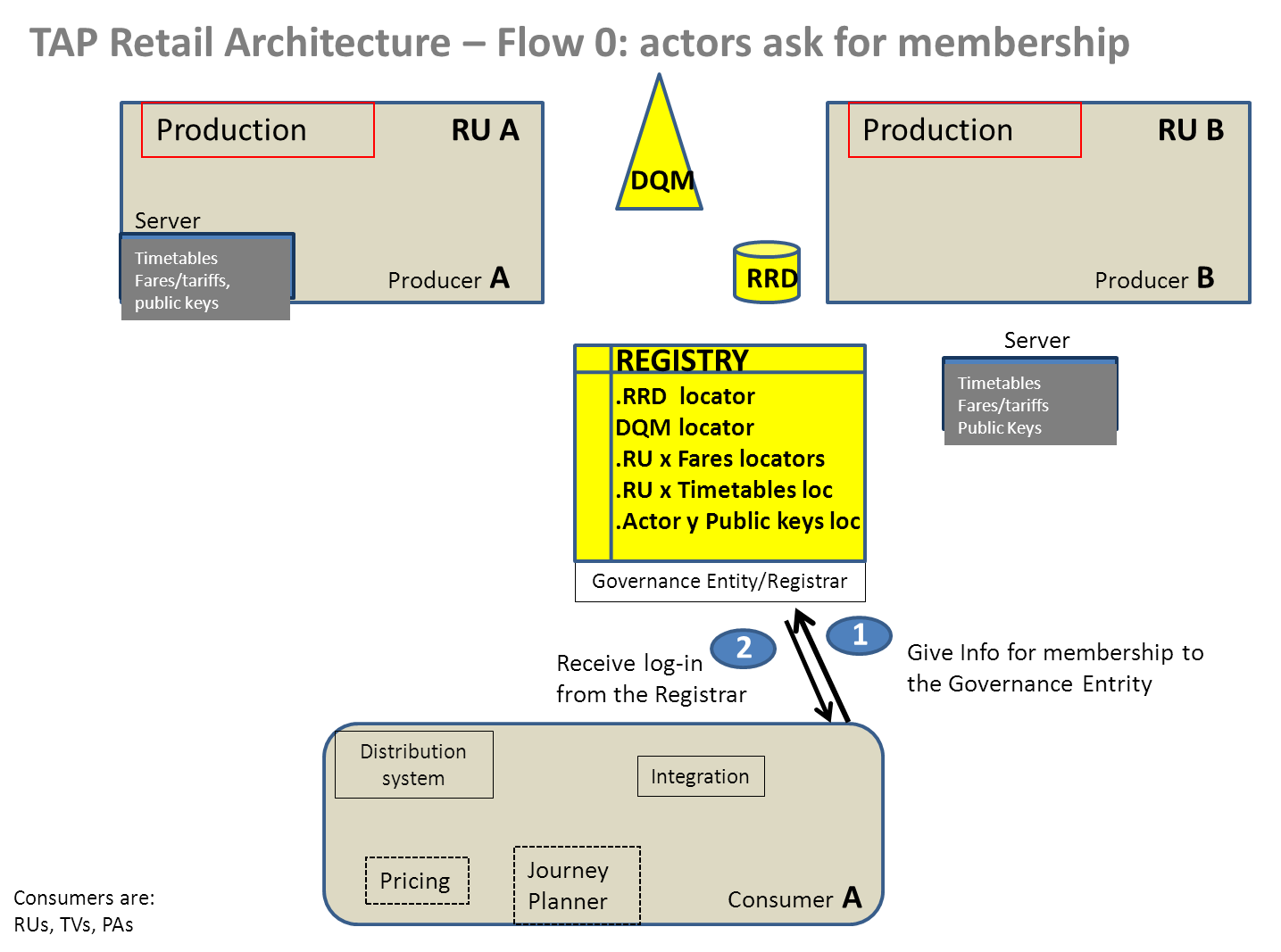
1- **P**roducer or **C**onsumer contact **G**overnance Entity to get membership

a- P or C are informed of all pre-requisite to be member of the TAP TSI community

b- P or C give commercial contact details in order to be contacted by **C**onsumers

2- G acknowledges the registration to P or C (if pre-conditions are fulfilled)

a- gives credentials details for the Registry (same login for Registry, DQM and RRD)



See activity diagram in Annex 2

* + - 1. Actors request information from the Registry

**1- Actor** accesses the Registry to request one of the following info:

a- Address where the DQM is located and related user guide

b- Address where the Retail Reference Data is located

c- Address where all official documents are situated (ERA web site)

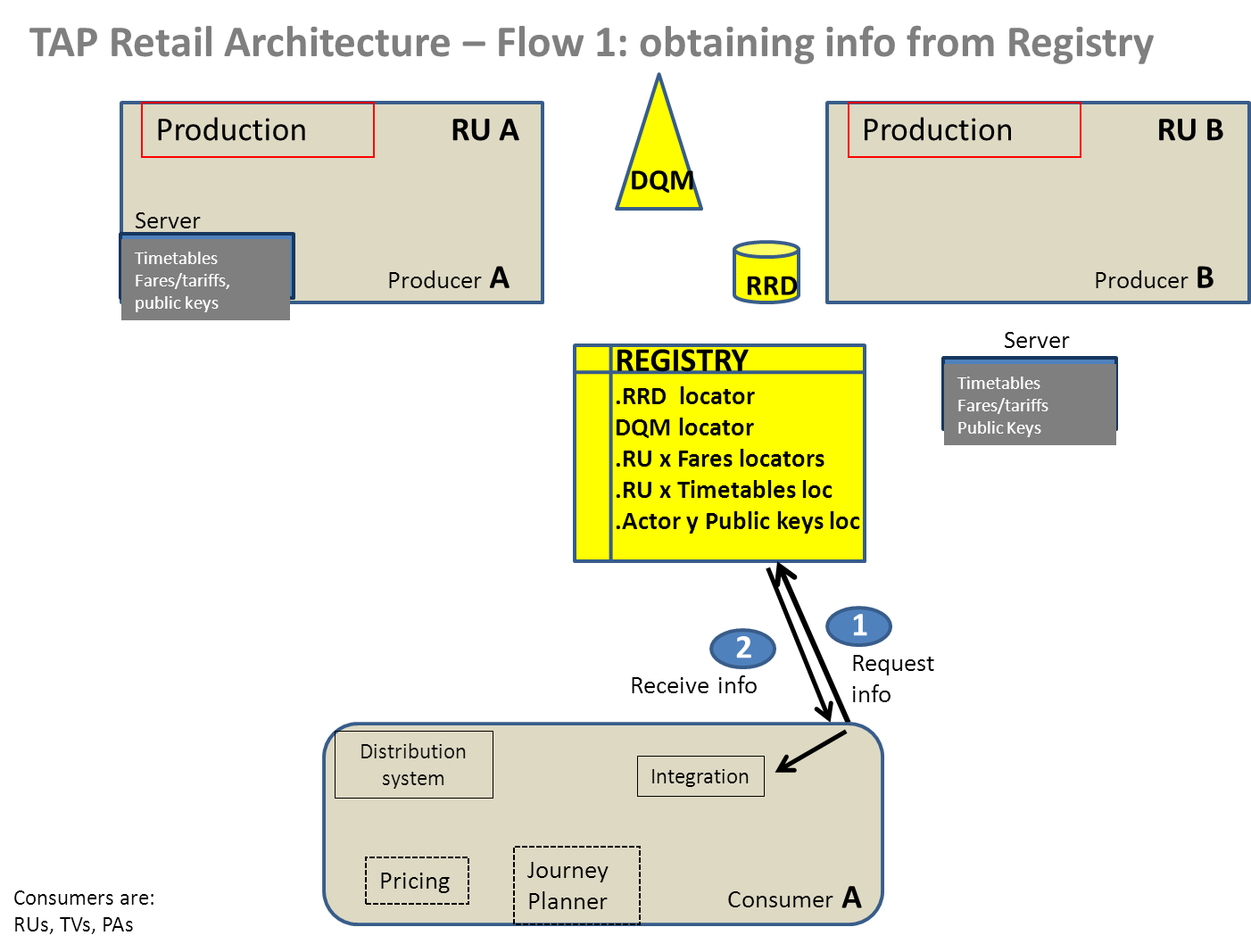
d- Address where all TAP documentation is located

- Technical Documents

- Retail Implementation Guides

- Retail Architecture guidelines to build a File Exchange Server

2- Actor receives the requested info.

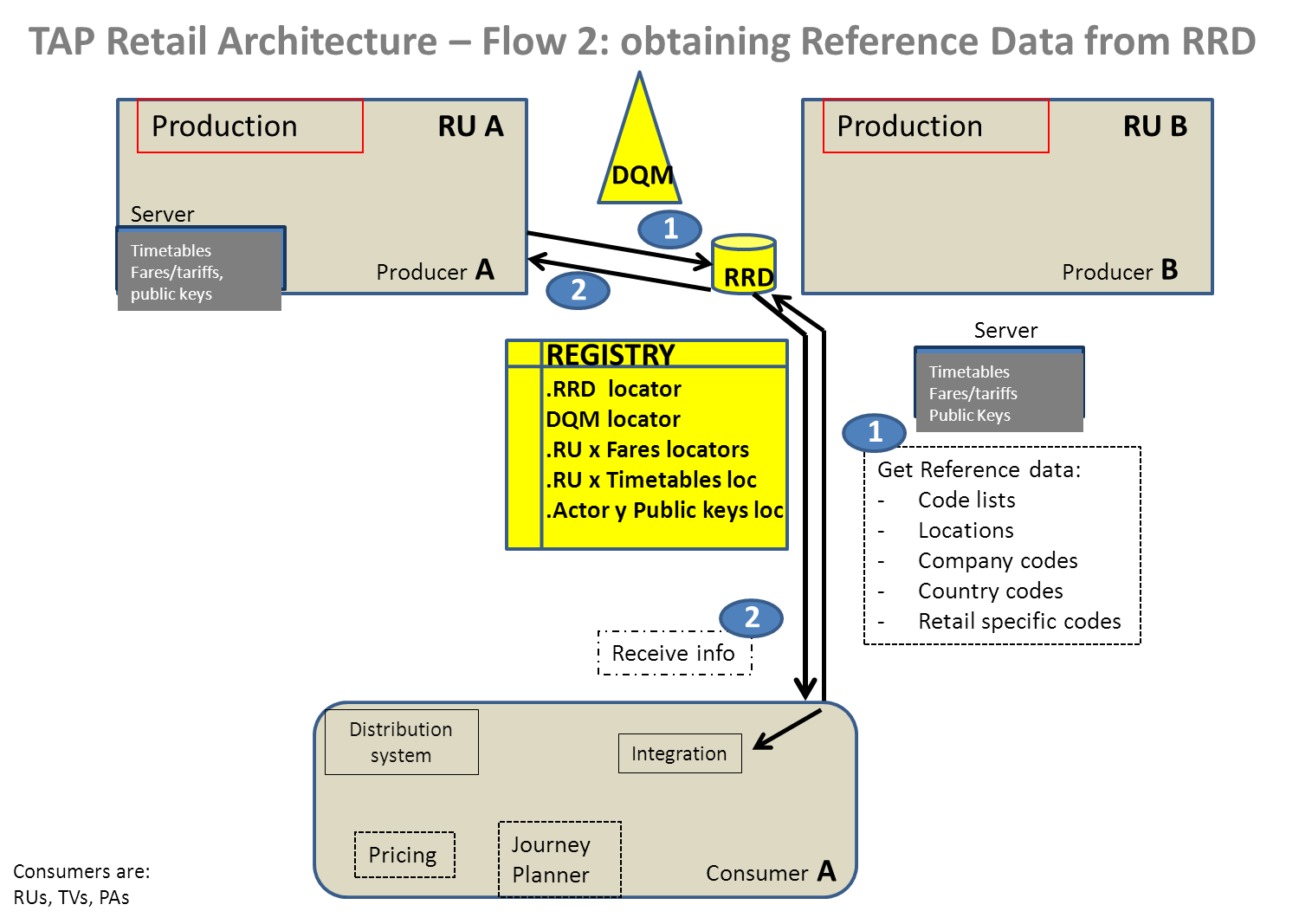


See activity diagram in Annex 2

* + - 1. Actors get reference data from the RRD

Producers and Consumers get the Locations, Code List, Company codes and retail data from the RRD.

1. All actors can request the reference data needed to exercise their rights or fulfil their obligations from the RRD, an interface able to access diferent types of reference data.
   1. They can request code lists (the RRD will get them from from updated files handled by the Governance Entity)
   2. They can request location code (the RRD will determine which source to get those data from whether it’s station codes used in common by TAF or it is retail specific codes)
   3. They can request Company codes and Country codes (the RRD will determine which source is the most relevant one)
2. Actors receive the requested info



See activity diagram in Annex 2

* + - 1. Actors check quality of Resources (Timetables and Tariffs/Fares)

Producers need to make available resources with the TAP expected quality.

The DQM tool is here to help producers to get insurance of the right quality and to help Consumers to have the insurance the data is of expected quality. This tool is available to any Producer or Consumer who wishes to use it .

Timetables data are checked with a tool, Tariffs/Fares with another one.

Consumers can use the DQM provided they didn’t alter the original data they got from the Producer.

1- Producers or Consumers need to send the complete set of data to the DQM

2- The DQM checks rules but also ensures Data are relevant in the RRD

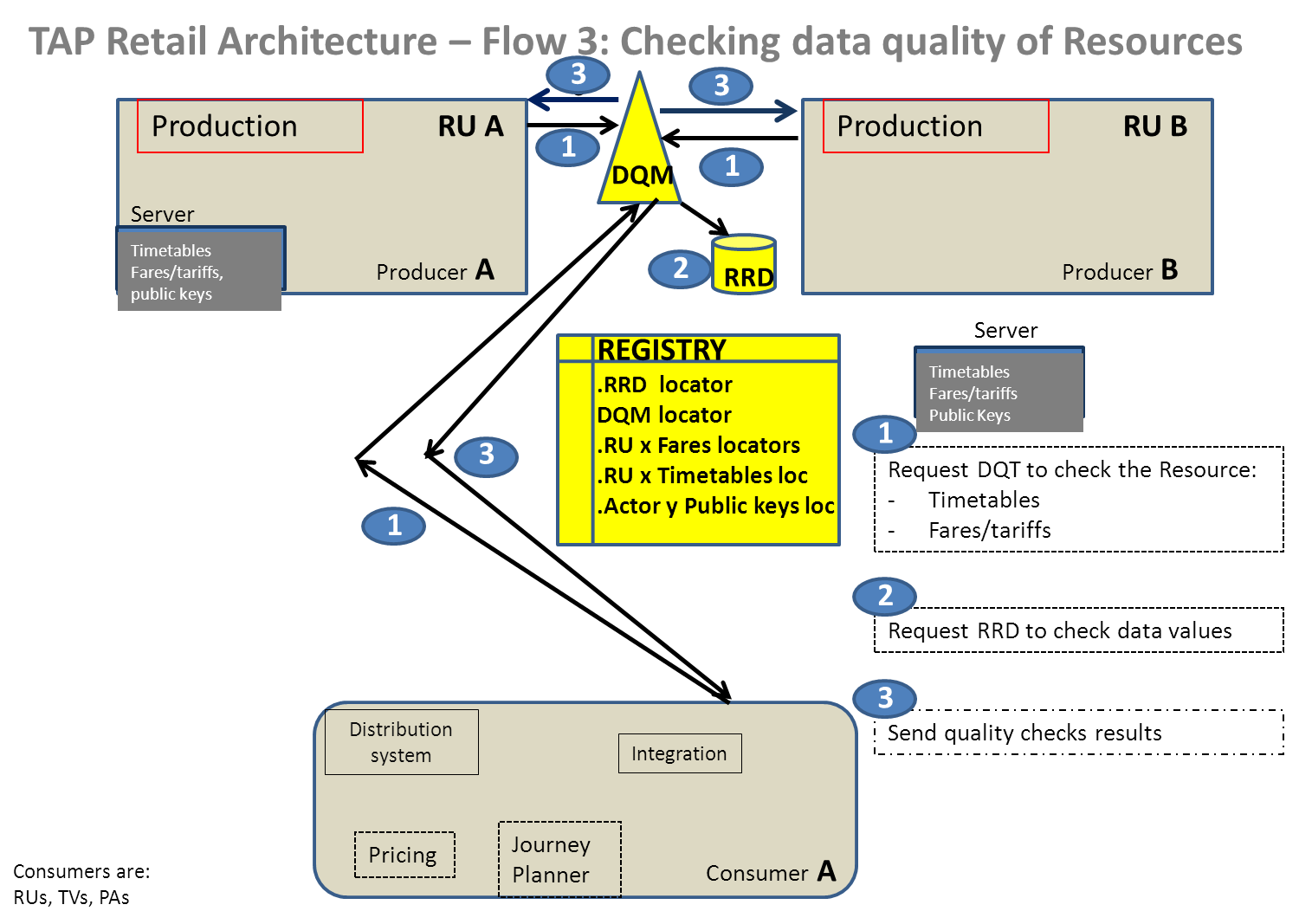
3- The DQM sends back a report.

If the DQM Report shows errors, then the Producer needs to correct them and re-send the whole set. In case the Consumer receives a report with errors, he can contact the concerned Producer and alert him of this situation.

If the DQM Report shows warnings, the Producer will decide whether it’s normal or not. If not, corrections should be brought and the whole set of data should be re-submitted, and this until the Producer decides the quality is correct.

Consumers may use the DQM to ensure the quality of data they got from a Producer.

The DQM perform syntax and logical checks that are listed in the appropriate Implementation Guides.



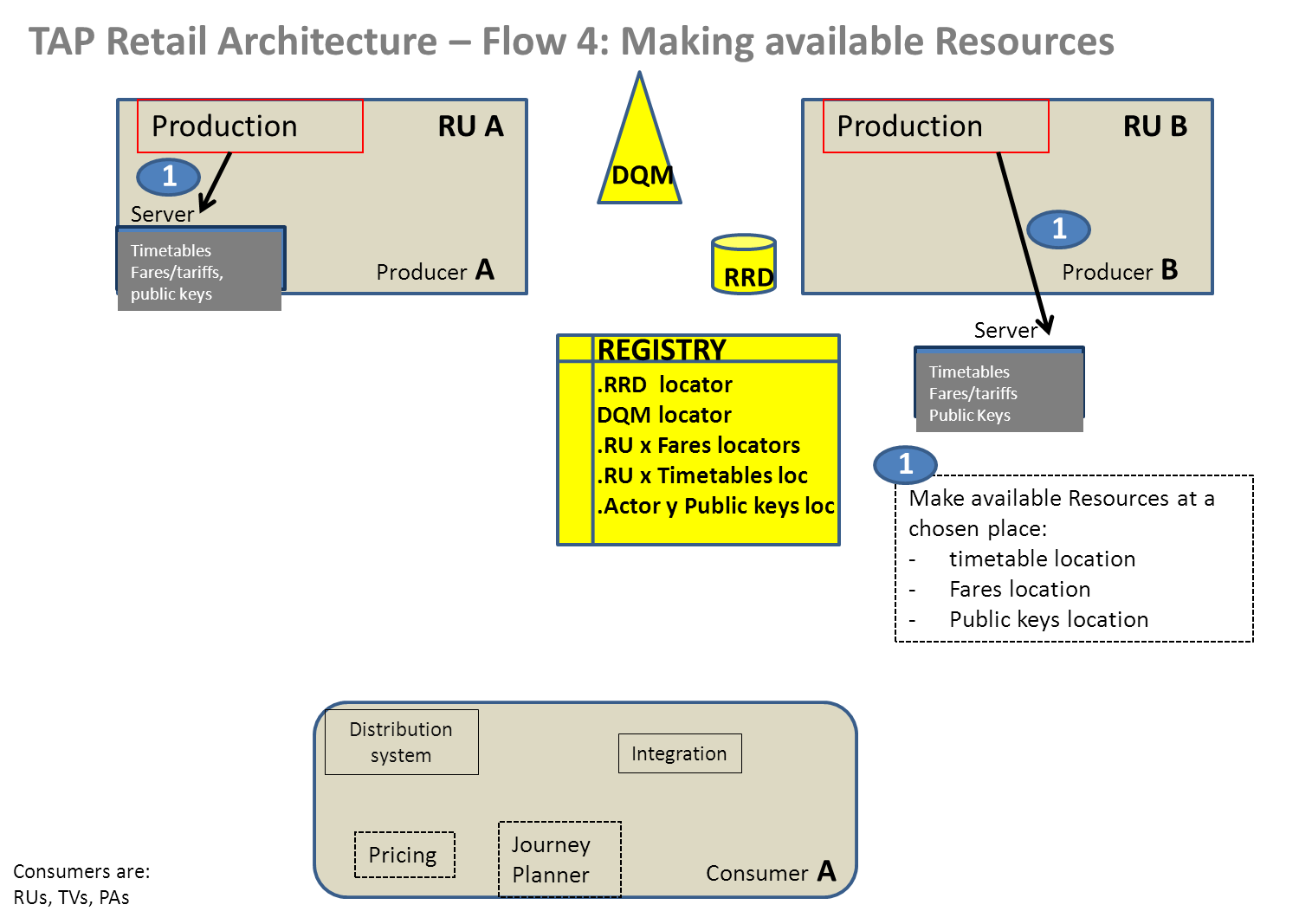
See activity diagram in Annex 2

* + - 1. Producers make available their resources on a data server

Once data quality is ensured, either by using the DQM or by another means, Producers makes their Resources available on the chosen data server.

In the drawing below, Producer A (RU A) has chosen to build its own data server and put its resources here.

Producer B (RU B) has chosen to use a third party owned date server where several other Producers may have their resources as well with a specific address.



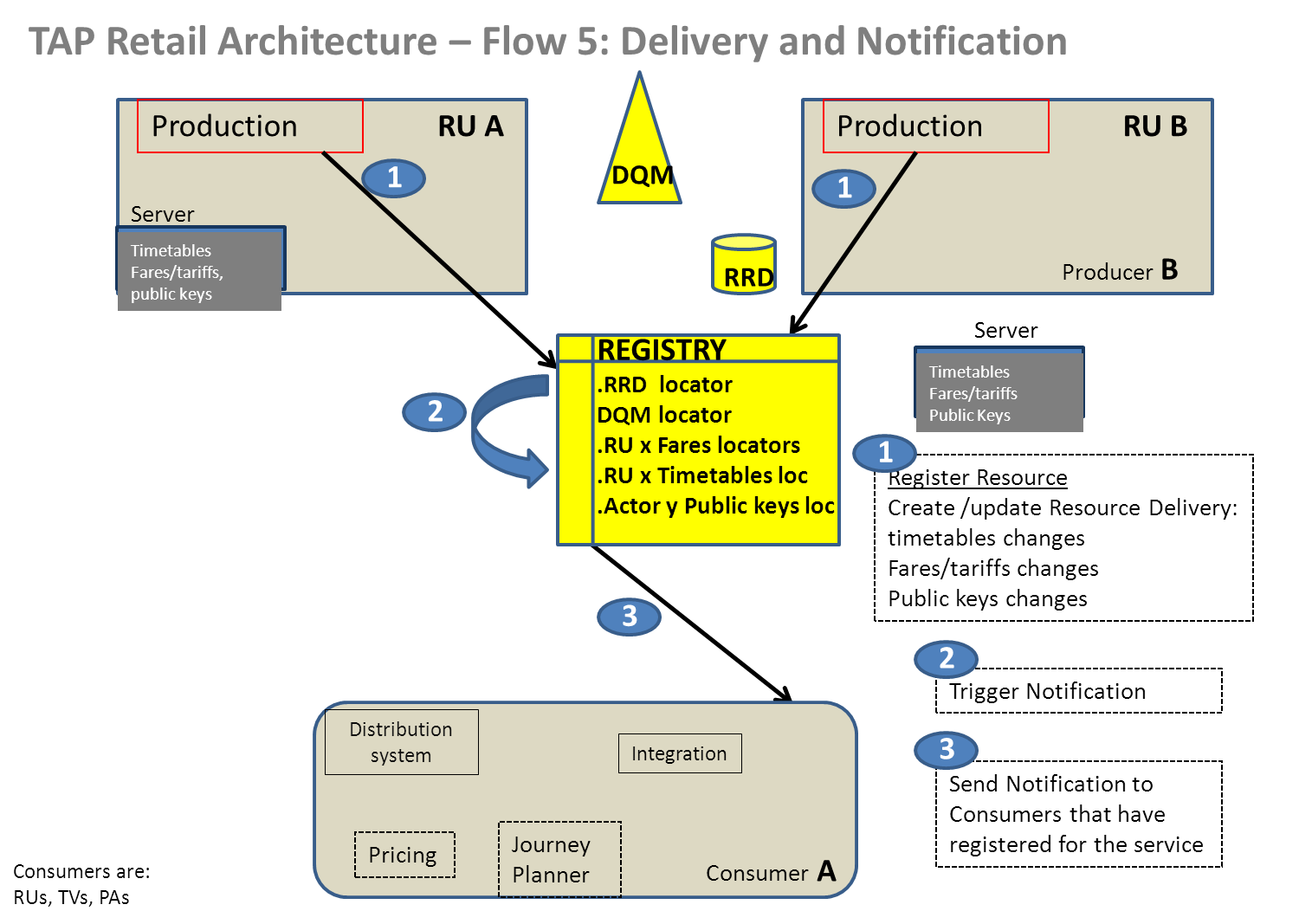
See activity diagram in Annex 2

* + - 1. Notification process for any changes in resources

Once a Producer is ready to make available a Resource, it registers it to the Registry.

Registry initiates the notification process by retrieving Resource Subscriptions

Registry notifies subscribed Resource Consumers.



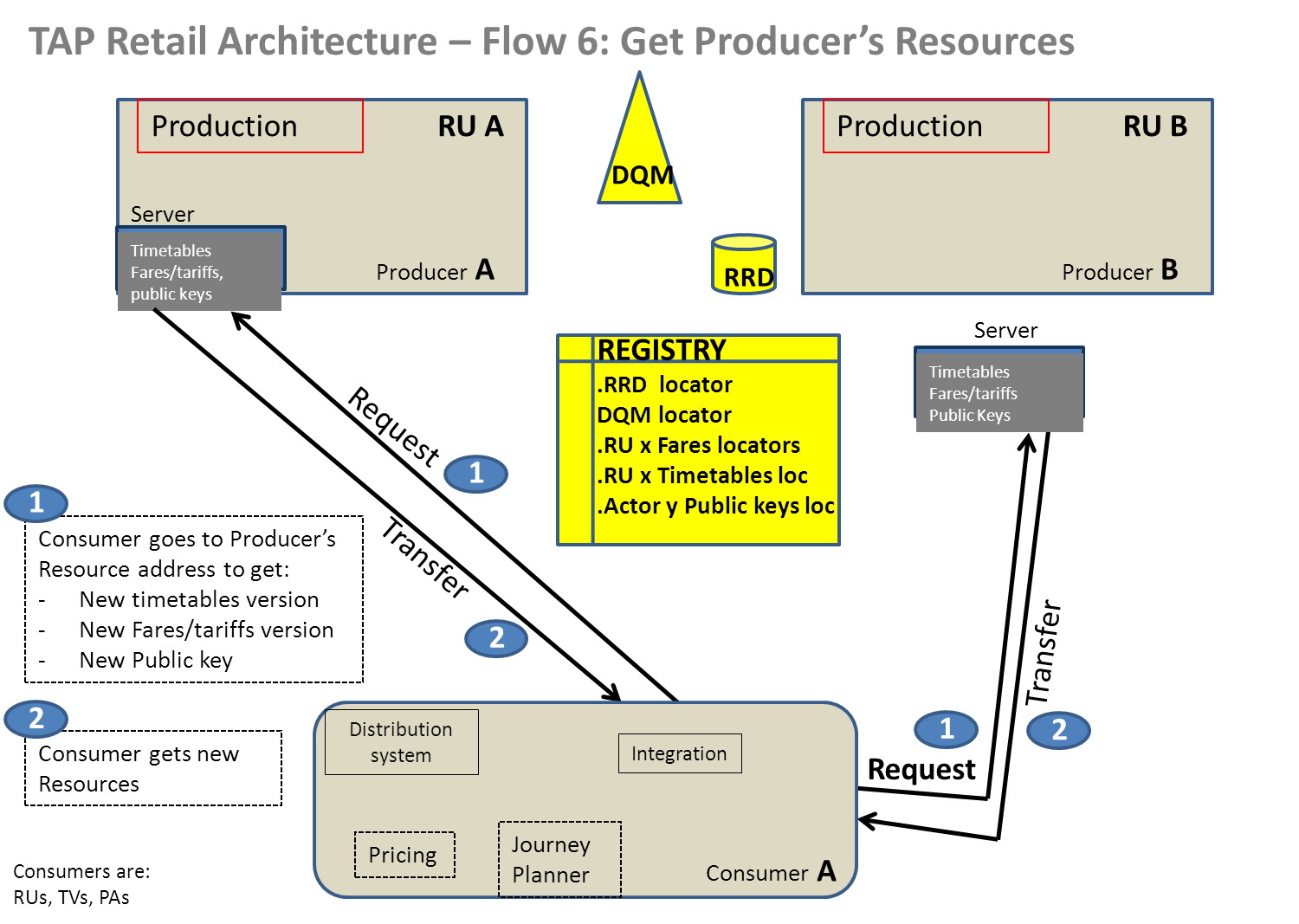
* + - 1. Consumers get Resources from Producers at the appropriate locations

Once notified, Consumers go and get the new Resource (the complete set) at the right place.

1- Consumer goes to the concerned system (thanks to the location he obtained from the Registry) to request the type of resource he wished to get

1. he identifies himself (security access controlled by the Producer)
2. he uses the access methods requested by the Producer

2- Consumer download the requested resource



See activity diagram in Annex 2

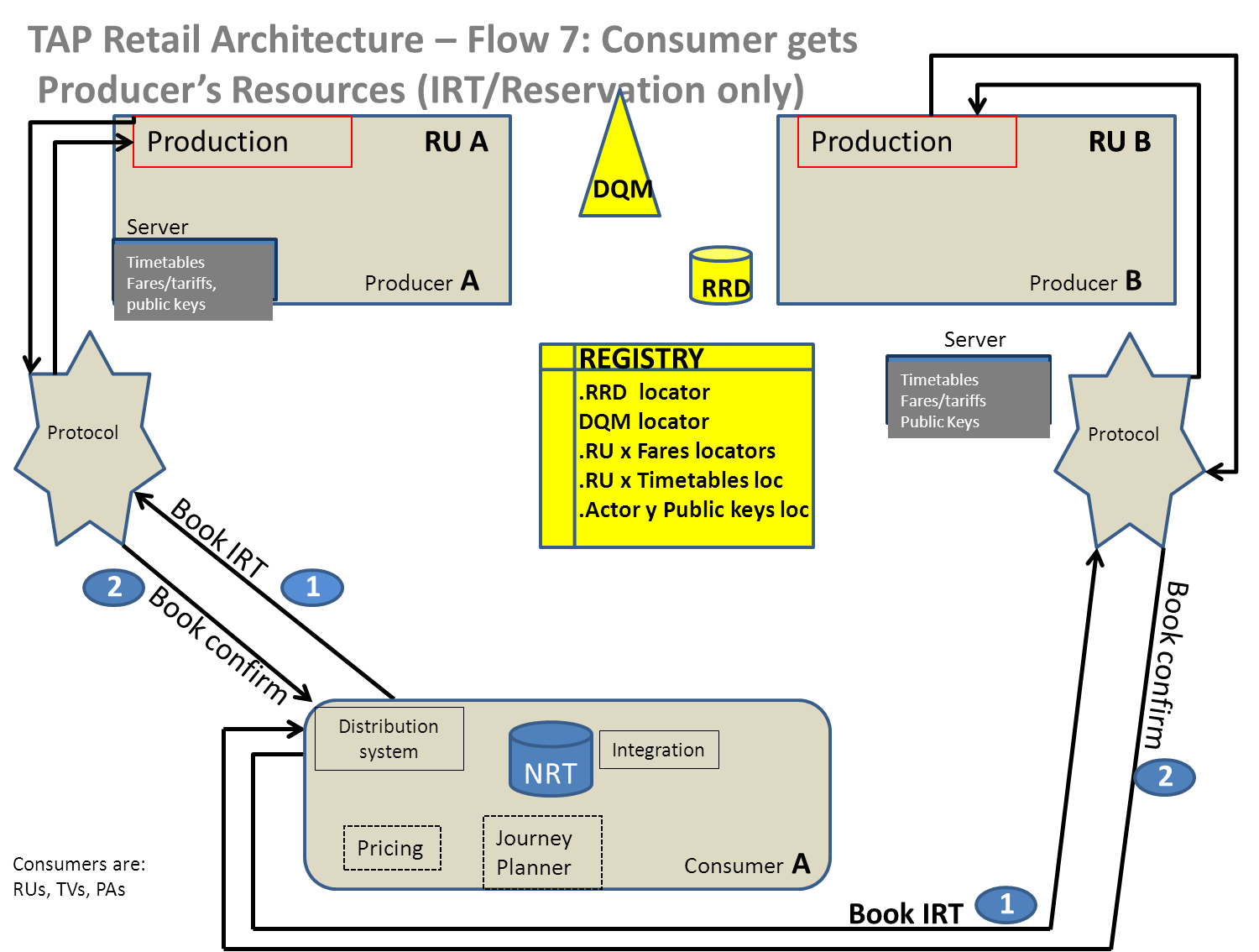
#### Consumers get a specific resource (Reservation and IRTs) via an interactive interface at an appropriate reservation system

Consumers can get IRTs or “Reservations only” by sending a message to the appropriate reservation systems, having previously located the address and interface of the target Reservation System in the Registry.For NRTs, as they represent open ticket, there is no need of reservation and sales are made within each own system thanks to the download done of that type of resource (see 9.5.2.7)).

That specific Resource does not need to go through a quality checker, it is assumed the quality is right. There is no notification for the update of that Resource

With such an interactive process through a specific protocol, Consumers are able to get a reservation on a designated train.

Architecture will not defined a specific protocol to exchange reservation even though it is needed. Actors need to agree between themselves in bilateral agreements the protocol they will use (MQ series?, other?) and they can register the protocol in the Registry



See activity diagram in Annex 2

#### 9.5.2.9 Printing ticket

Printing a ticket is the next step.

Using RCT2 ticketing solution does not require any specific architecture, the format is described in TD B6

Using the Print@home solution based on the Digital Signed Ticket security mechanism needs the Distributor to make available its public key to the Ticket Control Organisation (TCO) which will controls valid ticket onboard trains. The TCO is acting as a consumer and gets the Resource Public Key from the Producer (the distributor). This case is covered by Chapter 9.5.2.7 “Get Producer Resources”

## Non Functional Requirements for the TAP retail architecture

This chapter describes additional non-behavioural qualities of the TAP-TSI Retail Architecture implementation that are required to meet the provisions of the TAP Regulation in the actual operational Passenger interoperability environment, and to provide actionable governance operations to the Governance Body.

These requirements do not affect Functional requirements as described in chapters 9.1 through 9.4, or the structural composition in chapter 9.5, but they provide inputs in the selection of technologies, deployment options and infrastructure for implementation.

* 1. **Conditions for Access to the Registry**

|  |  |
| --- | --- |
| **##** | **Condition for Access** |
| **AR1** | The Registry must be accessible in a secure manner. |
| **AR2** | The Registry and the website will be available in English only |
| **AR3** | Access to the Registry for all users will be either through the internet or a private network. |
| **AR4** | Each user of the Registry will be responsible for making their own arrangements for access via the internet or a private network. The Registry extends only to the access point located at the Registrar’s hosting location. |
| **AR5** | The Registry shall be accessible 24 hours a day, 7 days a week, except if precluded by maintenance performed outside peak periods, or technical or security problems. Advance notice of any interruption in access, and expected resumption of service, shall, to the maximum practical extent, be provided via the website |

* 1. **Quality of Service requirements**

|  |  |
| --- | --- |
| **##** | **Requirement** |
| **NFR1** | The Service Desk and Operational support is delivered broadly in accordance with a Service Management model (using agreed process and agreed communication method) |
| **NFR2** | The Registry, the Data Quality Management Tool and the Central Reference Data components of the TAP TSI Retail Architecture will be deployed on a high availability and scalable industry standard infrastructure, not requiring specialised hardware or components. The design must be an independent of architecture, allowing choice to data centre providers for multiple strategies to achieve high performance and availability, including load balancing, provision of synchronised mirror sites, data centre virtualisation, cloud computing, etc., deployment. |
| **NFR3** | Documentation shall include, as a minimum:   1. Software Architecture Model 2. Use Case model 3. Domain Model 4. Service and Programming Model 5. Deployment Model 6. User Documentation and Manuals   All documentation must be in English, |
| **NFR4** | The Registry user interface, Registry Administrator's user interface, Data Quality Manager user interface, Data Quality Manager Administrators user interface should all be web based |
| **NFR5** | Registration Services, Subscription Services, Get Registry Entry Services, Registry Log/Audit services, Data Quality Management services, Data Quality Manager Log/Audit services and Central Reference Data services shall be protected against the following threats:   1. Coercive Parsing 2. Parameter Tampering 3. Recursive Payloads 4. Schema Poisoning 5. WSDL scanning 6. Routing Detours 7. External Entity Attack 8. SQL Injection 9. Reply Attack 10. Etc…   and be tested and certified against standard penetration tests.  All services will implement non-repudiation security mechanisms |
| **NFR6** | .  All Registry activity, including Registry Services and/or Registry User Interface security events, shall be logged at the TAP TSI Actor / Resource / Access Method level, whether initiated by remote computer or the User Interface web based applications, including notifications generated by the component in charge of notification to subscribed Resource Consumers.  Logs shall include signature of requestor, including referral IP address and/or User Interface application login credentials, and timestamp. |
| **NFR7** | Mechanisms shall be implemented to create full and incremental backups of the entire contents of the Registry, including logs, configuration files and user credentials, and for restoring the entire Registry to a specified consistent state |

* 1. **Volume of Exchanges**

Figures should be considered as indication

|  |  |
| --- | --- |
| Number of calls | Average : 6200 to 16100 / day (10 \* total amount of stakeholders) |
| Data volume per call | depends on the message formats specified in the registry solution |
| Access right and confidentiality | Authorised producers and consumers |

* 1. **Service capacity**

Figures should be considered as indication

|  |  |
| --- | --- |
| Availability | 99.8% minimum availability |
| Response / execution time | 500ms max response time |
| Integrity and security | Access authentication  SSL security |
| Limits | Maximum of 10 max concurrent calls for all stakeholders |

* 1. **Support level**

Figures should be considered as indication

|  |  |
| --- | --- |
| Support level | One: Basic support: restarting software application, network error, hardware malfunction…365 7/7  Two: Functional support: non working flow, halted software process…  Three: Advanced support: fixing data, bugs, … Working days / office hours 9-18 |
| Availability | Per annum and then per diem  Example : 365 7/7 |
| Maximum reaction time | 30 minutes |
| Maximum resolution time | 2 hours |

## Obligations of the Registry Service Provider

* 1. Definitions

|  |  |
| --- | --- |
| **(a)“Approval” means either:**  **or:**  **(b)“Confirmation” means**  **(c)“Website” means**  **(d) “Registrar” means** | (i) an electronic approval, by the Registrar, of an entity as a registry user entity and/or of an individual as that registry user entity’s administrator  (ii) an electronic approval, by the administrator, of an individual as a registry user of such registry user entity, and “approve” and “approved” shall be construed accordingly.  an electronic confirmation, automatically issued by the Registrar when a registration, amendment or discharge is searchable.  the website that provides the public interface of the International Registry and associated content provided by the Registrar under the Uniform Resource Locator (URL): [http ://www](http://www/).  that person appointed by the Governance Entity to supervise the working of the International Registry |

The registry service and its administrator must take reasonable care and a minimum set of formal checks to assure the integrity of the Register. This equally applies to all registry entry administrators.

Whilst the basic web service will be accessed through the open internet it is worthwhile considering that formal transactions would be safer via a secure VPN. This would significantly reduce the risks of service disruption through denial of service attacks.

* + 1. Sign-up and Approval – Registry User Entity and Administrator

1 The administrator of a proposed registry user entity shall complete and electronically submit to the Registrar, through the website, the form for approval of:

(a) a registry user entity; and

(b) an administrator of that entity.

Information designated as mandatory on the form shall be provided. Information designated as optional on the form may be provided. Names of organisations and persons must be their correct legal names. In exceptional cases (e.g. where the space on the form is insufficient), prior approval of the Registrar is needed for using a name other than the correct legal name must be sought by email. A proposed registry user entity shall also electronically submit to the Registrar, with proper signature, confirmation that a proposed administrator is entitled to act in that capacity. At the specific request of the Registrar, such confirmation shall be provided in hardcopy on the entity’s letterhead with proper signature. All applications for approval shall include acceptance of these Procedures and of the website terms and conditions governing the use of the International Registry.

2 All applications for approvals will be acknowledged to the electronic mail address provided on the submitted application form.

3 The proposed administrator shall promptly reply to requests for additional information from the Registrar in connection with the approval process. Such requests, made at the sole discretion of the Registrar, shall be consistent with applicable privacy laws.

4 After above information has been provided, the Registrar shall issue to the proposed administrator, in electronic form, the Registrar’s approval and a notification of the URL at which the administrator can access his/her digital certificate, together with appropriate instructions on its use.

5 The Registrar shall issue its approval (if given) as soon as is reasonably practicable and will complete the approval process within 48 hours of receipt of the application.

6 Once the Registrar has issued its approval, the administrator shall test his/her ability to access the website.

7 The Registrar shall not approve a registry user entity or an administrator where the Registrar believes that the requirements quality and care have not been met. In such a case, the Registrar, if requested in writing shall:

(a) specify in writing or via email, the reasons why such requirements have not been met; and

(b) provide the applicant with a reasonable opportunity to take corrective action.

If not corrected, at the sole discretion of the Registrar, the application shall be declined. Refusal of an application shall not prevent an applicant from making a subsequent application for approval, provided that the requirements of these Procedures are fully complied with in respect thereto, and payment of the appropriate fee for this subsequent application together with VAT (if applicable) is made.

8 The fee for issuing a replacement digital certificate shall be borne by the registry user entity. A person seeking a replacement digital certificate shall apply to the Registrar and follow the instructions specified on the website.

9. The Registrar may revoke the approval of a registry user entity and/or an administrator at any time where, in its view, there exists a material risk of fraudulent registrations or other misuse. In such a case, the Registrar and the registry user entity shall take all reasonable steps to cooperate to expeditiously take corrective action appropriate under the circumstances; the back-up contact may be used as required. In this case the Registrar may block and/or disable the user account of the registry user entity concerned.

* 1. Sign-up and Approval – Registry User

1 A proposed registry user seeking to act on behalf of an approved registry user entity shall apply through the website, requesting electronic approval from the administrator of that entity.

2 An administrator has the sole right to approve one or more registry users employed by a registry user entity to act on his/her behalf. If the administrator elects to approve such registry users, the administrator shall take that action through the “approved registry user” page on the website, specifying the period of validity of a proposed registry user’s access to the International Registry and directing that the associated payment be made.

3 Upon receiving the approval of his/her administrator and following successful testing of his/her ability to access the website, a registry user will be issued a digital certificate by the administrator via an email containing a link to the website. The registry user should then download from the website the digital certificate, providing him/her with a private key.

* 1. Effecting, Amending and Discharging Registrations – Registry User

1 To effect, amend or discharge a registration, a registering person shall:

(a) follow the relevant process and instructions specified on the website; and

(b) complete the electronic forms contained on the website, with the relevant information required by the Governance Entity.

Registration information electronically provided on the website shall be used by a registering person, as required by the Governance Entity. To the extent such information is not provided, registration information shall be inserted by a registering person following the instructions specified on the website.

2 An administrator may, at his/her sole discretion, authorise one or more of his/her approved registry users or professional users to effect, amend or discharge a registration. The authorisation may cover one or more items of railway rolling stock, including a group registration. Several users may be authorised to work on the same railway rolling stock, but not simultaneously during the same registration session. An administrator may, at any time, revoke an authorisation he/she has given and grant further authorisations to qualifying registry users.

3 Upon receipt of a confirmation pursuant to Section 12.2, any named party wishing to ensure that the respective entry has been correctly made may undertake a priority search.

4 Rectification of any error or inaccuracy in a registration, once searchable, may only be effected through an amended registration.

5 Initiated, but not completed, registrations, amendments or discharges shall not appear on any search results.

6 For the purposes of this Section 11, a group registration or amendment or discharge thereof shall be considered as one registration, amendment or discharge as appropriate save that the Registrar shall allocate a group file number to such group registration in addition to the file number for each item of railway rolling stock referenced in such group registration.

1. Sizing assessment

Figures should be considered as indication

* 1. Stakeholders

|  |  |  |
| --- | --- | --- |
| **Item** | **Description** | **Volume** |
| **Producers** | Railway Undertakings | 50 to 500 |
|  | Governance Entity | 1 |
| **Consumers** | Producers | See Railway Undertakings |
|  | GDS, data aggregators, … | 10 to 100 |
|  | Public authorities | Estimated 500 |
|  | Upcoming third parties | ~10 |

Total amount of stakeholders: 51 to 500 producers, 570 to 1110 consumers, 621 to 1610 total

* 1. Number of resources to be handled

|  |  |  |
| --- | --- | --- |
| **Data type** | **Resource** | **Number** |
| **Timetable** | Full timetable data | = Number of producers |
|  | Delta timetable | = Number of producers |
| **Fares and prices** | NRT | = Number of producers |
|  | IRT | = Half the number of producers |
|  | Special fares | = 0 (unused) |
| **Reference data** | Passenger code lists | 1 |
|  | Country codes | 1 |
|  | Location codes | 1 |
|  | Company codes | 1 |
| **e-Fulfilment data** | Public keys | = potential of distributors: RUs + travel distribution providers = 60 to 600 |
|  | Other fulfilment data | = Potential of producers supporting P@H => 50 up to 500 |
| **Booking** | Reservation only for NRT  IRT | = 2/3 producers |
| **PRM assistance** | PRM support services | = potential of all RUs: 50 to 500 |

1. Provisions for administrators and Consumers of Registry services
   1. Service to Consumers

1 No individual other than an administrator may effect, amend, discharge or consent to registrations with the International Registry until the individual has been approved as a registry user by the administrator of the registry user entity that such person represents.

2 No registry user may transmit information to the International Registry to effect, amend or discharge a registration in respect of railway passenger services data unless such registry user has first received authorisation to do so in relation to such railway passenger services data either:

(a) in the case of a transacting user, from the administrator of the transacting user entity that represents it; or

(b) in the case of a professional user, from the administrator of the transacting user entity being such professional user’s client.

3 Each registry user:

(a) shall keep his/her password and digital certificate secure;

(b) shall not transfer his/her digital certificate from the computer on which it was first installed, except to a replacement computer under his/her control, in which case he/she shall first apply to the Registrar for that purpose; and

(c) is permitted to make a secure back-up copy of his/her digital certificate.

4 Each registry user shall notify his/her respective administrator of any security breach, of which he/she is aware, that is expected to result in unauthorised registrations, including unauthorised use, disclosure or compromise of his/her password or private keys.

5 Each registry user acknowledges that his/her respective admin­istrator may make such identity checks as the Registrar considers necessary in connection with such registry user’s access to the International Registry.

* 1. Service Administrators

1 An administrator, who is an employee of a registry user entity, shall be duly appointed by each registry user entity, with authority to act on its behalf for the purposes of the International Registry, and such authority shall be represented during the approval process.

2 An administrator should hold appropriate formal professional qualifications commensurate with the requirements of the functions of administrator.

3 Each registry user entity may have only one administrator at any given time.

4 The administrator of a transacting user entity, who has been approved by the Registrar, is automatically authorised to effect, amend, discharge or consent to registrations in which that entity is a named party.

5 An administrator:

(a) shall keep his/her password and digital certificate secure;

(b) shall not transfer his/her digital certificate from the computer on which it was first installed, except to a replacement computer under his/her control, in which case he/she shall first apply to the Registrar for that purpose; and

(c) is permitted to make a secure back-up copy of his/her digital certificate subject to the requirements of the security standards as amended from time to time.

6 Where an administrator electronically delegates his/her powers to an acting administrator, that acting administrator shall be deemed to be the administrator for the purposes of these Procedures.

7 Where an administrator electronically approves a registry user to act on behalf of a registry user entity, the Registrar shall issue an email to that registry user containing a link to a digital certificate in accordance with these Procedures.

8 An administrator shall, through the website:

(a) keep up to date the email address and other details of the administrator and each registry user representing such registry user entity held by the International Registry;

(b) promptly revoke the approval of a registry user representing such registry user entity in the event that such registry user leaves the employment of, or otherwise ceases to be associated with, such registry user entity; and

(c) promptly revoke the authorisation of a registry user representing such registry user entity in the event that such registry user is no longer authorised to effect, amend, discharge or consent to one or more registrations in which that entity is a named party.

9 In the event that an administrator is to leave the employment of the registry user entity on whose behalf he/she is authorised to act or if there is to be a change of administrator, the administrator shall electronically notify the Registrar thereof in a timely fashion. Should the registry user entity wish to appoint a replacement administrator, such appointment shall be subject to a sign-up fee applicable to a new administrator.

10 The administrator of a registry user entity shall have the authority, through the website, to block and/or disable the user account of any registry user representing his/her registry user entity. It is the administrator’s responsibility to take such action promptly in the event of a security breach relating to any such registry user’s user account, of which he/she has actual knowledge, including but not limited to compromise of such registry user’s private key.

11 The administrator of a registry user entity shall notify the Registrar of any security breach (for example, a breach compromising a private key), of which he/she has actual knowledge that is expected to result in unauthorised registrations. If the security breach relates to a registry user account, the administrator may block and/or disable the account.

12 If the account of an administrator is subject to a security breach that could reasonably be expected to result in unauthorised access to and use of the International Registry, the Registrar and the registry user entity shall cooperate to expeditiously take corrective action appropriate under the circumstances. A registry user entity shall designate a “back-up contact” for these purposes.

13 On notification of a security breach, the Registrar may block and/or disable any user account.

14 The Registrar may make such reasonable identity checks of a proposed administrator as the Registrar considers necessary in relation to that person undertaking such function. The Registrar may make similar checks of a registry user, where deemed necessary by the Registrar.

15 Each administrator may electronically approve further registry users to act on behalf of the registry user entity which that administrator represents (when authorised to do so) and may approve the issue of a digital certificate to each of those registry users.

16 The administrator has sole responsibility for the selection of his/her registry user entity’s registry users and for ensuring that only individuals who are duly authorised to act on behalf of his/her registry user entity are appointed as registry users from time to time.

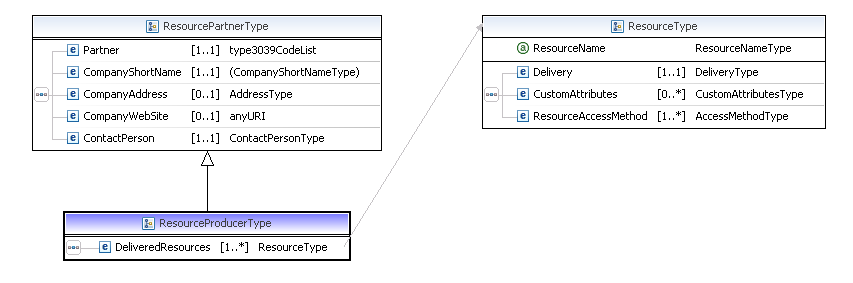
## ANNEX 1

This Annex provides a description of the Registry’s main persisted objects representing a high level model of Registry entries declaring Resource Deliveries, i.e. resource made available by Resource Producers, and Resource Subscriptions, i.e. subscriptions to Resource Delivery updates requested by Resource Consumers.

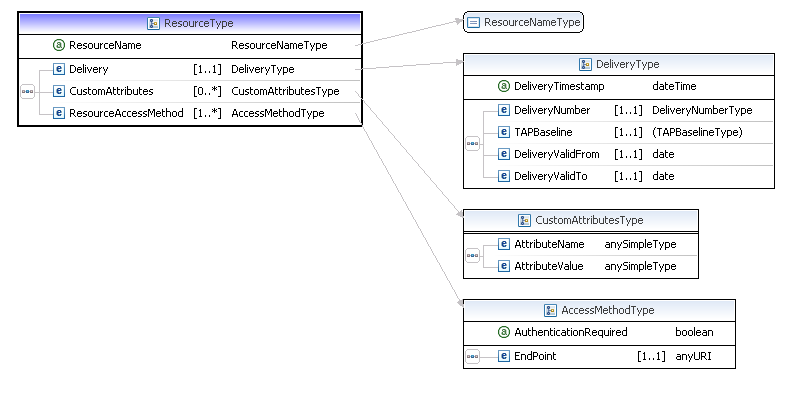
The model is intended solely for the purpose of illustration of the Landscape detailed in chapter 7 and does not constitute a specification for implementation. It can be used however as a guideline for such detailed specification.

* 1. **Resource Deliveries**

Resource Deliveries may be declared in the Registry with entries of the following format:



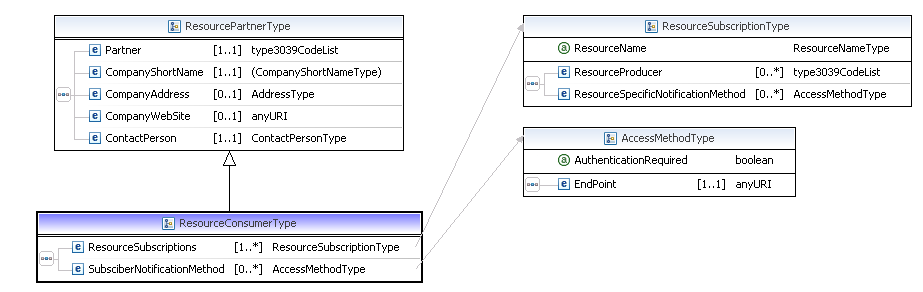
A delivering Resource Producer is therefore associated in the Registry with a minimum of one and an unbounded maximum of Resources, each described by a Resource Name indicating its time (e.g. “TIMETABLE”, “FARES”, etc) and a Delivery object, as follows:



A Resource Delivery is further described by additional attributes specifying the baseline number of the TAP TSI document under which the Resource is created and start and end validity dates, and custom attributes.

* 1. Resource Subscriptions

Resource Consumers can subscribe to notifications about specific Resources. The notifications are sent by the Registry automatically when a Resource Delivery is added, updated or removed by a Resource Producer to all Resource Consumers that subscribe to that specific Resource, indicated by its ResourceName.



As illustrated in the diagram above, a Resource Consumer is associated with a minimum of one and an unbounded maximum of ResourceSubscriptions, each consisting of the mandatory ResourceName and, optionally, specifying that ResourceNames from a specific Resource Provider are being subscribed.

A *unique combination* of the Resource Consumer’s “Partner” attribute, and of the Resource Name attribute exists in the Registry, such as:

|  |  |  |
| --- | --- | --- |
| **Partner** | **ResourceName** | **ResourceProvider** |
| 83 | TIMETABLE | ALL |
| 83 | FARES | 87 |
| 87 | TIMETABLE | 83 |

The first entry specifies that Resource Consumer ‘83’ subscribes to notifications about Resource TIMETABLE from any Resource Provider, the second that it subscribes to notifications about Resource FARES delivered by Resource Provider ‘87’, and the third that Resource Consumer subscribes to notifications about Resource FARES delivered by Resource Provider ‘83’.

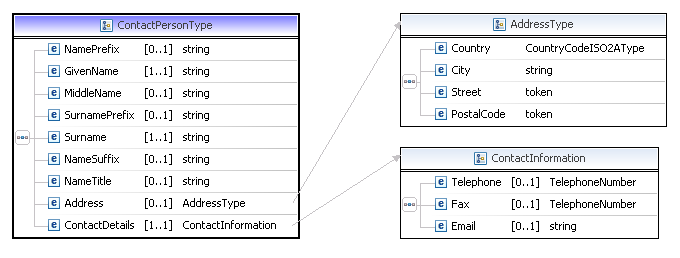
The relationship of a Resource Consumer to Resources it subscribes to is a *composition*: deletion of the Resource Consumer from the Registry removes all ResourceSubscriptions associated with it. Conversely, there can be no ResourceSubscriptions *not* associated with its owning Resource Consumer.

* 1. Resource Producers and Consumers

ResourceConsumers and ResourcePartners have attributes in common: this is modelled as Producers and Consumers being specialisations of a “ResourcePartner” entity, whereby a Resource Producer is a Resource Partner associated with one or more DeliveredResources, and a Resource Consumer is a Resource Partner associated with one or more Resource Subscriptions.

A ResourcePartner such as a Data Quality Tool does not have a street address but it *must* have a ContactPerson

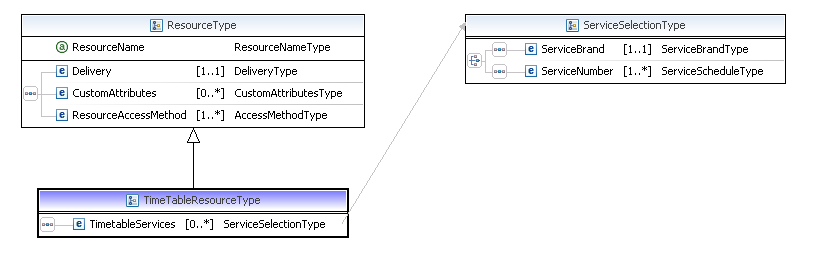
A ContactPerson entity is described below::



ResourcePartner (therefore both Producers and Consumers) have at least one ContactPerson, who must have at least one ContactDetail consisting of either phone, fax or email.

* 1. Timetable Resources

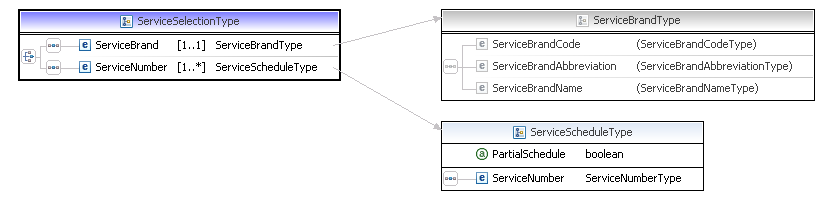
Timetable resources are represented in the Registry as extensions of the Resource entity, as follows:



A Timetable Resource is associated with an unbounded number of TimetableServices describing either a list of Service Brands and/or a list of Service Numbers included in the Timetable delivery.

A Resource Producer making a Resource Delivery of Timetable which specifies Service Brand and/or Service Numbers is the Information Provider for those Service Brands and/or Service Numbers.

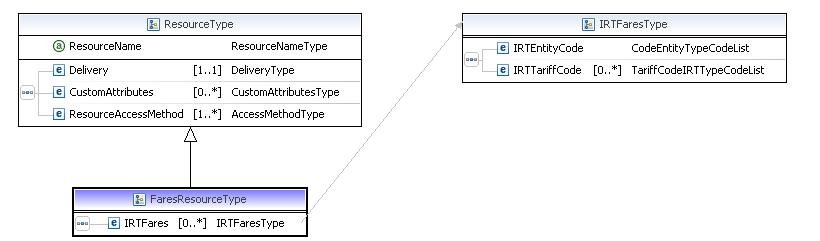
A Service Number declared in the list of TimetableServices is furthermore associated with a PartialSchedule attribute:



A PartialSchedule attribute set to ‘true’ for a Service Number indicated that the Timetable contains a partial schedule for that Service Number that needs to be integrated according to the specifications of the relevant Implementation Guide.

* 1. IRT Tariffs/Fares Resources

IRT Fares resources are represented in the Registry as extensions of the Resource entity, as follows:



A Fares Resource is associated with an unbounded number of IRTFares describing a list of EntityCodes and/or IRT TariffCodes from the relevant TAP TSI Codelists

* + 1. NRT Tariffs/Fares Resources

Same principles as above

* + 1. Special Tariffs/Fares Resources

Same principles as above

* + 1. Reservation Resources

Same principles as above

* + 1. Public Key Resources

Same principles as above

* + 1. Code List Resources

Same principles as above

* + 1. Data Quality Tool Resources

Same principles as above

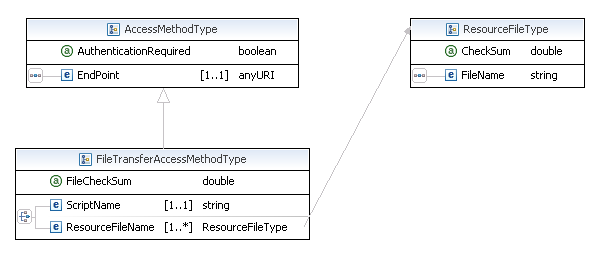
* 1. **Access Methods**

An Access Method specifies an endpoint and an AuthenticationRequired attribute to indicate that authentication by the Resource Consumer is requested at the endpoint:



* + 1. File Transfer Access Method

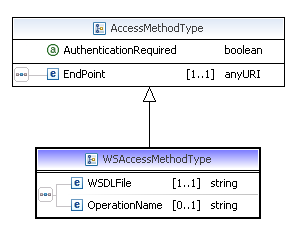
A File Transfer access method extends the Access Method with specific attributes pertaining to file transfer:



It can specify either a script to be run at the endpoint (such as a server side script on a web or ftp server), or an unbounded list of ResourceFiles, each consisting of a Filename with a CheckSum.

* + 1. Web Service Access Method

A File Transfer access method extends the Access Method with specific attributes pertaining to a web services interface:

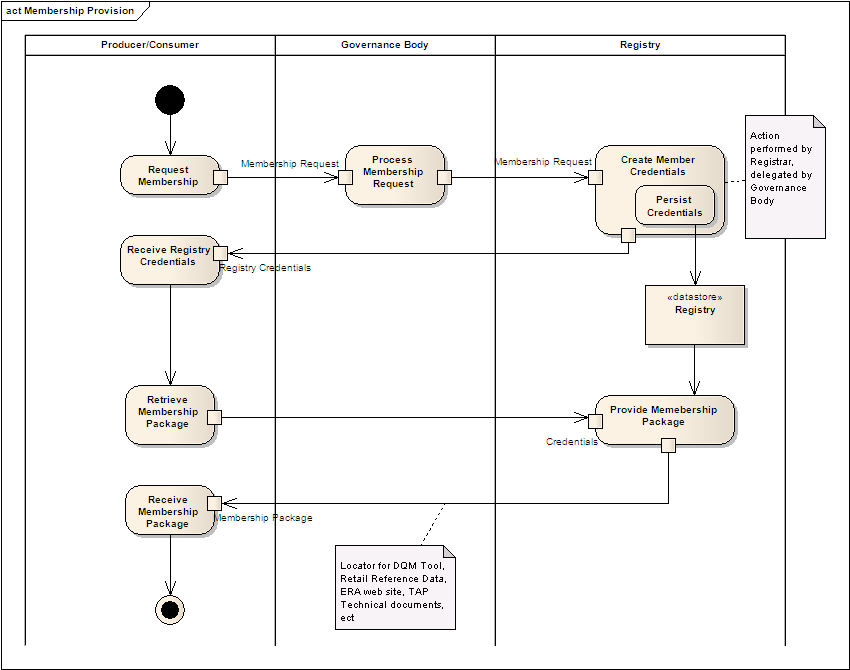


It specified the name of a web services definition language (WSDL) file and an operation name to invoke in the call.

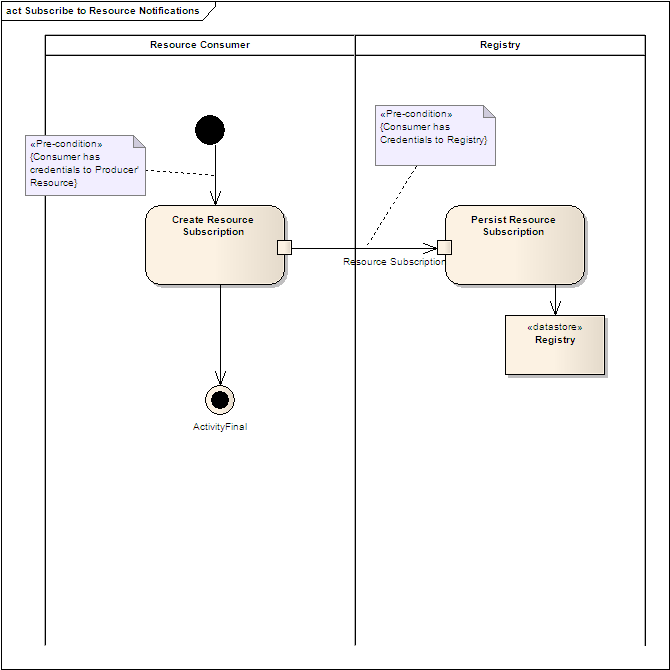
## ANNEX 2

This Annex 2 provides a High level UML description of the overall interaction complementing the drawings of chapter 9.4.3.

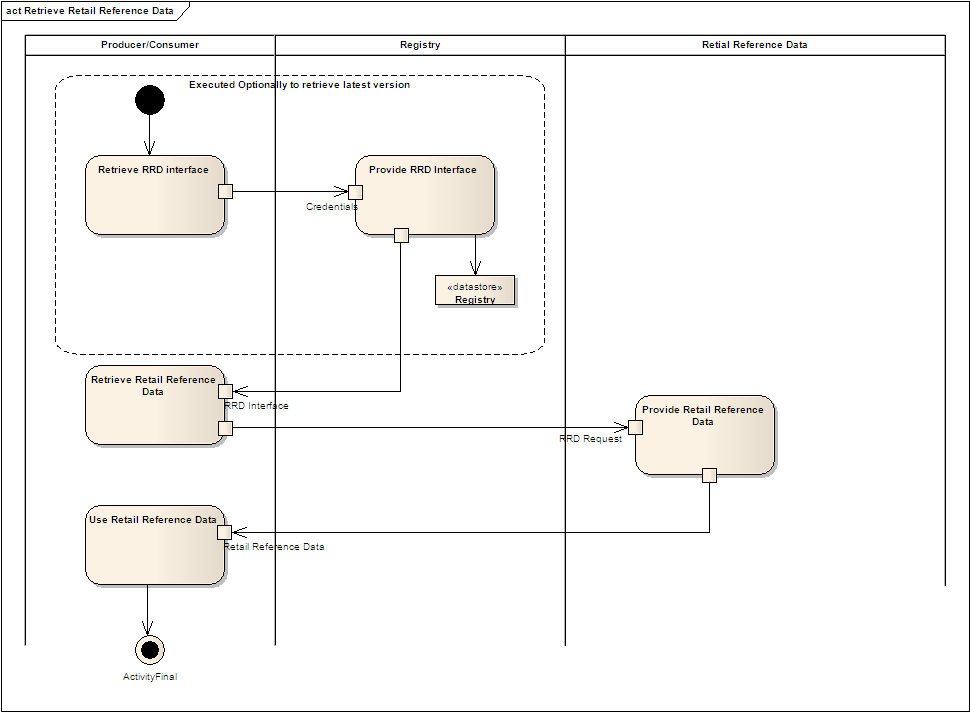
Membership Provision (corresponding to Chapter 9.4.3.1 drawing):



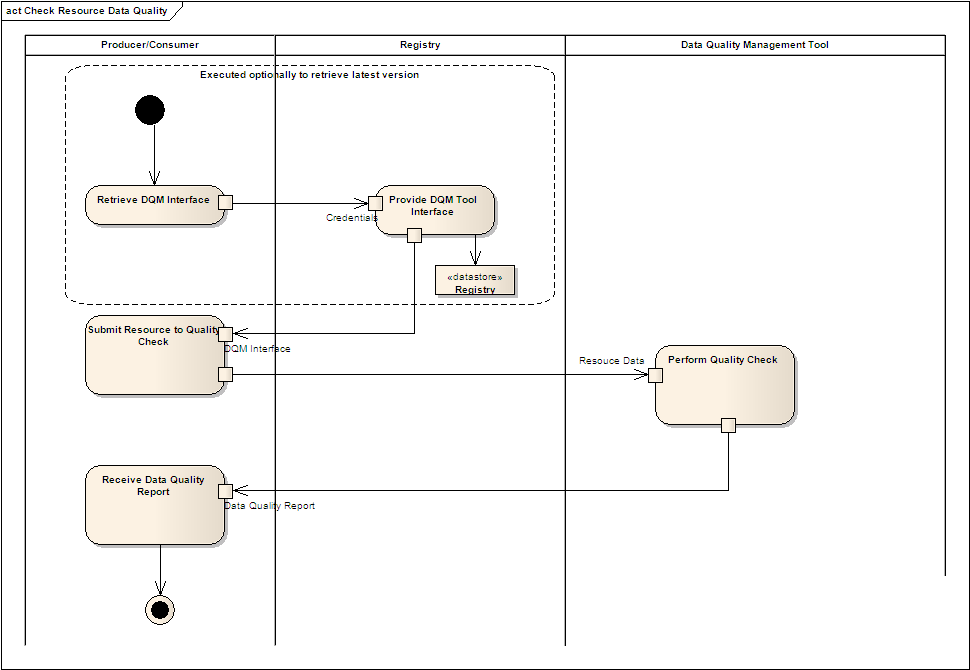
Subscribe to Resource Notifications (action that is complementary to the registration 9.4.3.1 if Consumer is interested to be notified on selected Resource changes)



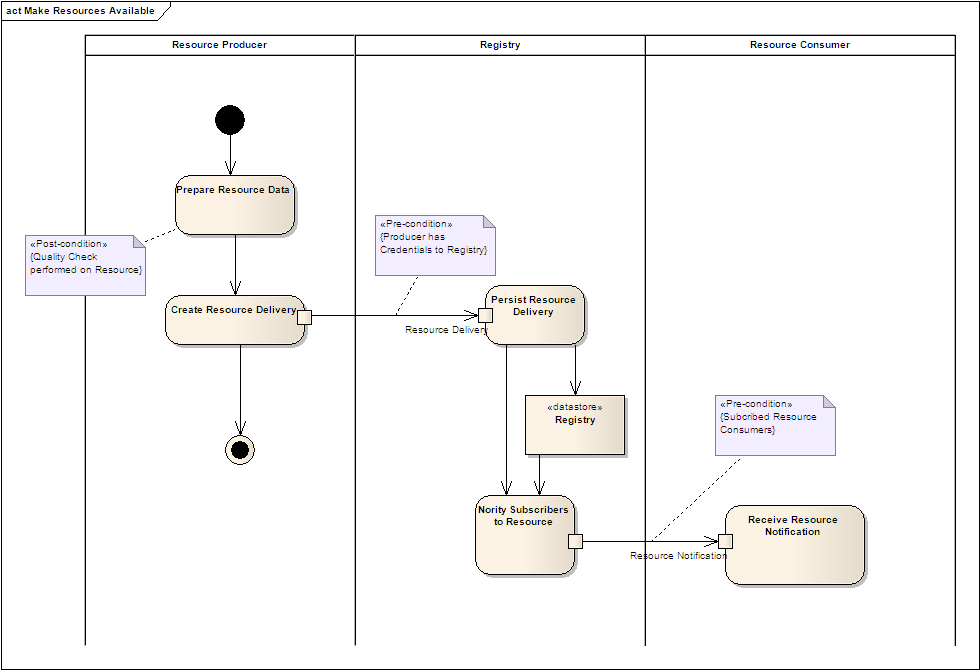
Retrieve reference data (see Ch 9.4.3.3)



Check Resource data quality (see Ch 9.4.3.4)



Make Resources available (see Ch 9.4.3.5)



Retrieve Resources (see Ch 9.4.3.7 and 9.4.3.8)

