

1st edition, August 2006

*Original*

# R

## **Technical security standards for electronic sales and distribution systems**

*This Leaflet is to be published in English only*



UNION INTERNATIONALE DES CHEMINS DE FER  
INTERNATIONALER EISENBAHNVERBAND  
INTERNATIONAL UNION OF RAILWAYS

## Leaflet to be classified in Volume:

IX - Information Technology, Miscellaneous

## Application:

With effect from 1st August 2006

All members of the International Union of Railways

## Record of updates

**1st edition, August 2006**

First issue

*The person responsible for this leaflet is named in the UIC Code*

# Contents

## List of figures

|                                               |           |
|-----------------------------------------------|-----------|
| <b>Summary .....</b>                          | <b>1</b>  |
| <b>1 - Definition of players.....</b>         | <b>2</b>  |
| 1.1 - Carrier.....                            | 2         |
| 1.2 - Ticket Control Organisation (TCO) ..... | 2         |
| 1.3 - Distributor .....                       | 2         |
| 1.4 - Issuer .....                            | 3         |
| 1.5 - Agent .....                             | 3         |
| 1.6 - Travel Agent .....                      | 3         |
| 1.7 - Contributor .....                       | 3         |
| 1.8 - Customer .....                          | 3         |
| 1.9 - Examples .....                          | 4         |
| <b>2 - Sales types .....</b>                  | <b>5</b>  |
| 2.1 - Direct in Station Use Case.....         | 5         |
| 2.2 - Direct in Travel Agency.....            | 7         |
| 2.3 - Call centre, mail delivery.....         | 9         |
| 2.4 - Call centre, electronic delivery.....   | 11        |
| 2.5 - Call centre, Device Delivery.....       | 13        |
| 2.6 - Call centre, paperless .....            | 15        |
| 2.7 - Internet, A4 Ticket.....                | 17        |
| 2.8 - Internet, chip card .....               | 18        |
| 2.9 - Internet, paperless .....               | 20        |
| <b>3 - Basic processes.....</b>               | <b>21</b> |
| 3.1 - Stock Management.....                   | 23        |
| 3.2 - Printing on Stock.....                  | 24        |
| 3.3 - Printing on A4 .....                    | 25        |
| 3.4 - Self-Retrieval .....                    | 26        |

|                                                                 |           |
|-----------------------------------------------------------------|-----------|
| 3.5 - Information to On-board Staff .....                       | 27        |
| 3.6 - Chip Card.....                                            | 27        |
| 3.7 - Proof of Purchase .....                                   | 28        |
| 3.7.1 - Issuing paperless or home printed tickets.....          | 28        |
| 3.7.2 - Avoiding the modification of home printed tickets.....  | 28        |
| 3.7.3 - Payment of paperless or home printed tickets.....       | 28        |
| 3.7.4 - Cancellation of paperless or home printed tickets ..... | 28        |
| 3.7.5 - Use of home printed tickets .....                       | 29        |
| 3.7.6 - Control processes .....                                 | 29        |
| 3.8 - Electronic Payment.....                                   | 29        |
| 3.8.1 - Obligatory measures and tests .....                     | 30        |
| 3.8.2 - Additional recommendations.....                         | 30        |
| 3.9 - Internet Transactions .....                               | 31        |
| 3.9.1 - Options for Secure eBusiness Environment .....          | 31        |
| 3.9.2 - Digital Certificates .....                              | 32        |
| 3.9.3 - Secure Sockets Layer (SSL).....                         | 33        |
| 3.9.4 - Secure File Transport Protocol (FTPS).....              | 33        |
| 3.9.5 - Public Key Infrastructure (PKI).....                    | 34        |
| 3.10 -Sales Data - Pricing and Transfer conditions.....         | 35        |
| 3.10.1 - General .....                                          | 35        |
| 3.10.2 - Transfer via on-line systems .....                     | 35        |
| 3.10.3 - Data transfer with off-line systems .....              | 36        |
| 3.11 -Change Management .....                                   | 37        |
| 3.11.1 - General .....                                          | 37        |
| 3.11.2 - Test system.....                                       | 37        |
| 3.11.3 - Production system .....                                | 37        |
| 3.11.4 - Change management .....                                | 37        |
| <b>Bibliography .....</b>                                       | <b>38</b> |

# List of figures

|                                                                  |    |
|------------------------------------------------------------------|----|
| Fig. 1 - Players .....                                           | 2  |
| Fig. 2 - Direct in Station Use Case .....                        | 5  |
| Fig. 3 - Direct in Station Activity Diagram .....                | 6  |
| Fig. 4 - Direct in Travel Agency Use Case .....                  | 7  |
| Fig. 5 - Direct Distribution Activity Diagram .....              | 8  |
| Fig. 6 - Call Centre, Mail Delivery Use Case .....               | 9  |
| Fig. 7 - Call Centre, Mail Delivery Activity Diagram .....       | 10 |
| Fig. 8 - Call centre, Electronic Delivery Use Case .....         | 11 |
| Fig. 9 - Call Centre, Electronic Delivery Activity Diagram ..... | 12 |
| Fig. 10 - Call Centre Device Delivery Use Case .....             | 13 |
| Fig. 11 - Call Centre, Device Delivery Activity Diagram .....    | 14 |
| Fig. 12 - Call Centre, Paperless Use Case .....                  | 15 |
| Fig. 13 - Call Centre, Paperless Activity Diagram .....          | 16 |
| Fig. 14 - Internet, A4 Ticket Use Case .....                     | 17 |
| Fig. 15 - Internet, Chip Card Use Case .....                     | 18 |
| Fig. 16 - Internet, Chip Card Activity Diagram .....             | 19 |
| Fig. 17 - Internet, Paperless Use Case .....                     | 20 |

## Summary

The purpose of *UIC Leaflet 914* is to identify security recommendations for on-line and off-line sales processes considering the complete chain from stock control to accounting. The Leaflet specifically addresses the sales of international tickets/passes (transport by at least two different carriers) or of foreign tickets/passes (transport by a single carrier, different from the issuer).

The Leaflet does not address domestic tickets (transport by a single carrier, which is also an issuer).

This leaflet will not address security requirements for Revenue Sharing, as that subject is treated in *UIC Leaflet 301*.

For a comprehensive framework, the leaflet lists the current and expected primary sales types, and analyses of the single component processes, focusing on the technical security aspects. Security problems already defined in other UIC documents, e.g. those concerning the security elements for blank coupons, will only be referred to in the document.

Further sales types may be added in the subsequent versions of this leaflet, as soon as technological development or commercial innovation make them realistic.

# 1 - Definition of players

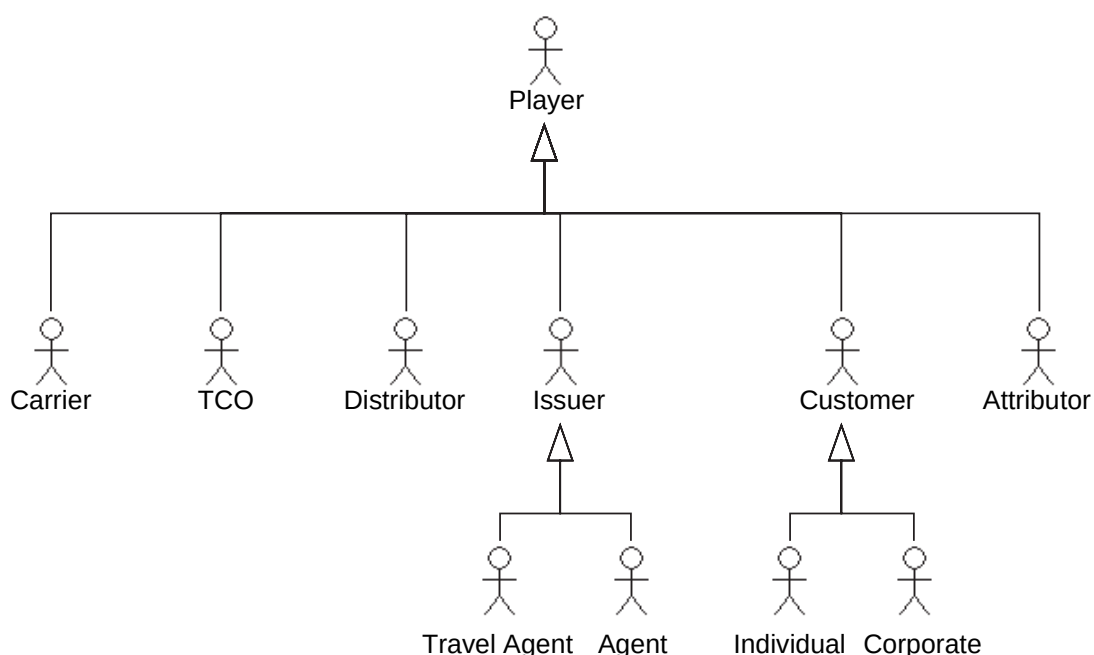


Fig. 1 - Players

## 1.1 - Carrier

An undertaking providing railway or sea transportation or a service connected to it and which, in return, directly receives part of the sales price. The carrier may be:

- a UIC transport company identified by a UIC code, or
- a non-UIC transport company, which therefore has no UIC code (e.g. a private railway),
- a grouping (e.g. EEIG) acting on behalf of carriers.

A rail product may also include sea and road transportation products linked to rail traffic.

## 1.2 - Ticket Control Organisation (TCO)

Any organisation which can verify a passenger's ticket before, during or after a given journey or any part of it. In most cases this organisation will be a carrier. For some types of sales (home printing, etc) the TCOs can provide the distributor with the Certificate data necessary for validating the ticket.

## 1.3 - Distributor

An undertaking providing to an issuer the legal and technical capacity to sell rail products to a customer, or providing directly to the customer the legal and technical capacity to buy rail products. This capacity is granted by both the Carriers and the TCOs.

## **1.4 - Issuer**

An undertaking (or single agent) receiving from the customer the payment for a rail product and delivering to him/her the ticket or proof of purchase.

An issuer can be:

- a Direct Issuer (Agent),
- an Accredited Issuer (Travel Agent).

## **1.5 - Agent**

A carrier's point of sale for products to customers via its own distribution channels.

## **1.6 - Travel Agent**

A point of sale for products to customers accredited by the carrier.

## **1.7 - Attributor**

A company managing a record of available seats/accommodations and corresponding prices in an IT system (attributing system) for its own services or those of other RUs and which can transmit in real time to an issuer (eventually through a distributor) the seating/accommodation details and price.

It makes no difference to the issuer if the attributor's product is stored in a GDS or another company's system. They can still access the product as if it were present in the attributor's system and the latter accepts fully its incumbent responsibilities (in particular, as regards accounting).

The attributor must be a UIC company identified by a UIC code.

The UIC attributor may, while retaining responsibility, contract out part of its accounting work to a third-party.

## **1.8 - Customer**

The Customer is the purchaser and user of a railway transportation or service. The customer can be classified into two categories: an individual, who is personally responsible for the payment of the service purchased or a corporate customer who has a contractual billing relationship with the issuer for payment of the service.

## 1.9 - Examples

The actors described above may play different roles depending on the use case. Some examples are found below:

- The Eurail EEIG is a grouping of carriers, acting on behalf of 29 carriers (rail carriers, such as SNCF, DB, ... and sea carriers such as Attica, etc).
- ÖBB is attributor for seats on its own trains. The attributing system is EPA, belonging to DB.
- REG is a distributor allowing several issuer travel agencies to sell products of different carriers.
- Thalys International is a TCO controlling the tickets for its own trains, where the carriers are SNCF, SNCB, NS, DB...

The functions of carriers, distributors, issuers and attributors, or a part of them, may be carried out by one and the same company.

## 2 - Sales types

### 2.1 - Direct in Station Use Case

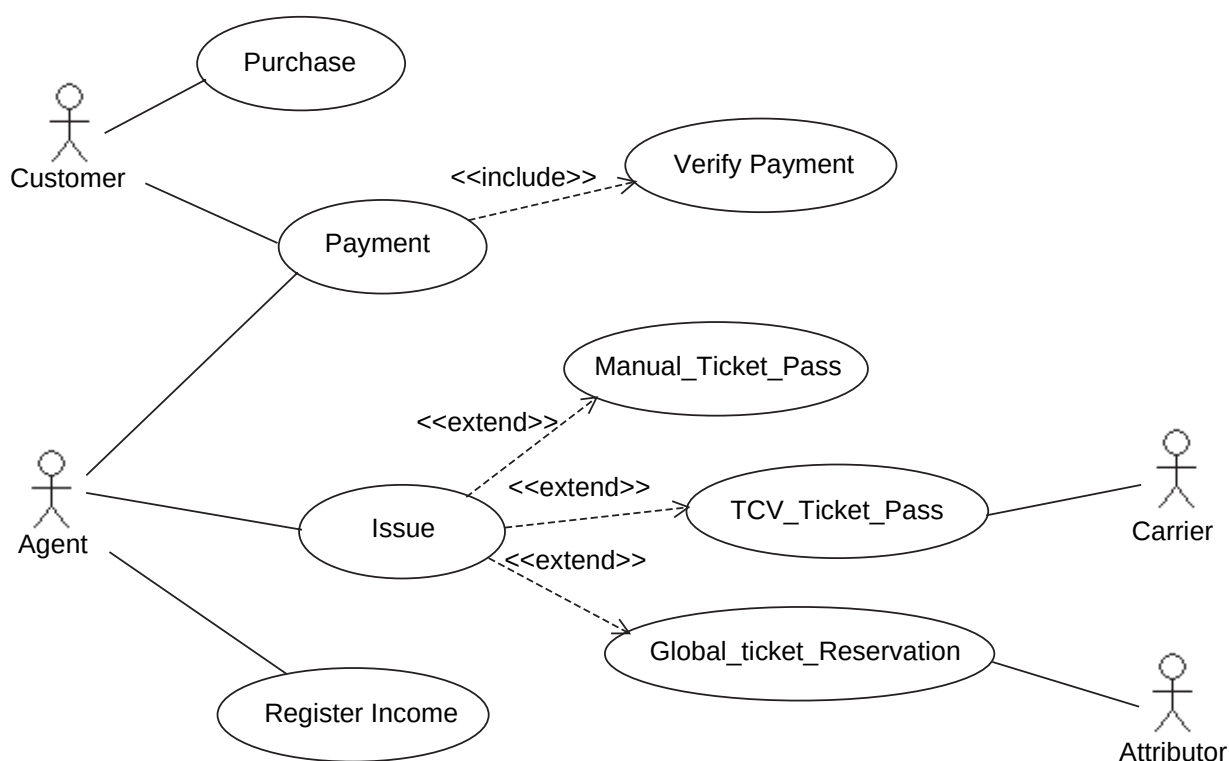


Fig. 2 - Direct in Station Use Case

The customer comes to a counter in a railway station or office. The issuer is a railway agent, who issues one of the following:

- a Global Ticket/reservation calling an attributing system,
- a TCV ticket/pass using an electronic system belonging to his/her undertaking,
- a manual ticket/pass (in this case, only TCV open tickets, no reservation or GT).

The customer pays on the spot (cash, cheque, credit card). The issuer verifies the payment and delivers the coupon(s) or ticket(s).

The sale amount is registered in the undertaking's income.

Monthly settlement amongst railways must be done according to *UIC Leaflet 301* (see Bibliography - page 38):

- For TCV tickets/passes, the agent credits the carriers involved in the transport for their revenue share ("allocated parts").
- For Global Tickets/reservations the agent waits for the debiting from the attributing undertaking ("attributed parts").

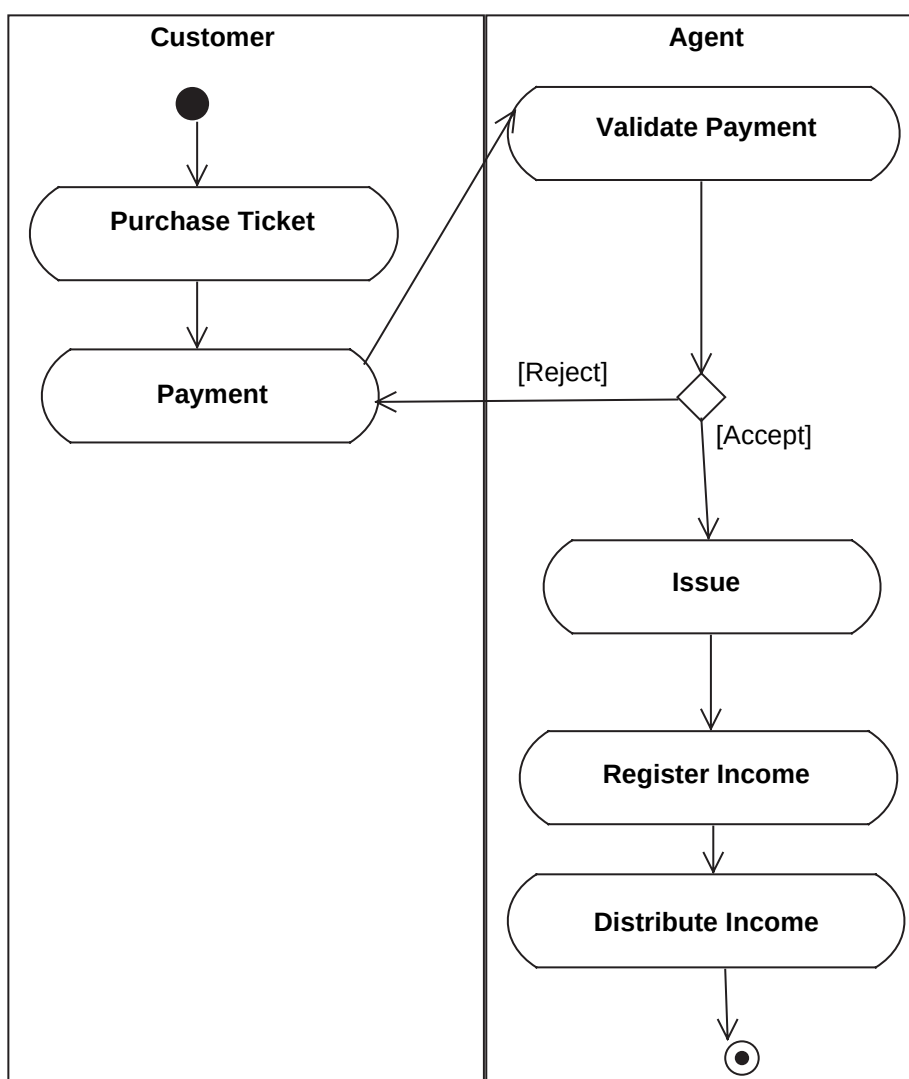


*Fig. 3 - Direct in Station Activity Diagram*

## 2.2 - Direct in Travel Agency

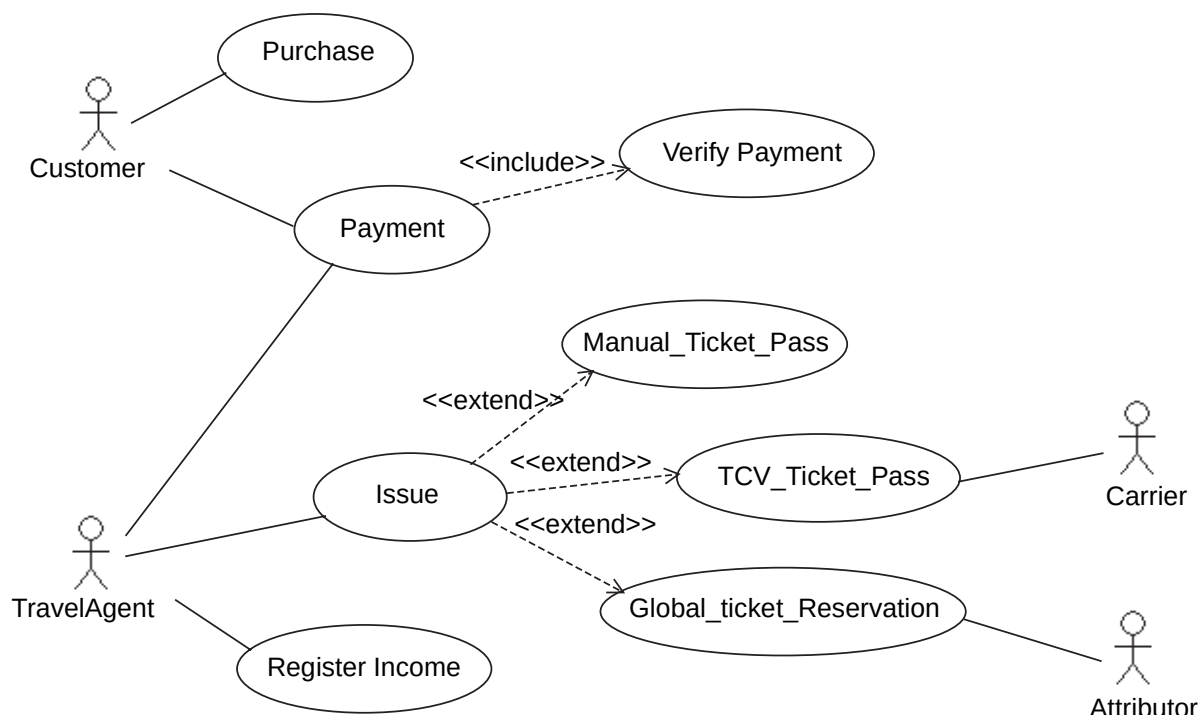


Fig. 4 - Direct in Travel Agency Use Case

The customer comes to a counter in a travel agency. The issuer is a travel agent, who issues one of the following:

- a Global Ticket/reservation calling an attributing system,
- a TCV ticket/pass using an electronic system belonging to his/her undertaking,
- a manual ticket/pass (in this case, only TCV open tickets, no reservation or GT).

The customer pays on the spot (cash, cheque, credit card). The issuer verifies the payment and delivers the coupon(s).

The sale amount is registered in the travel agency's income. The travel agency periodically reports sales to the accrediting RU and credits it with the corresponding amount, less the provision.

Monthly settlement amongst railways must be done by the accrediting carrier according to *UIC Leaflet 301*.

- For TCV tickets/passes, the accrediting carrier credits the carriers involved in the transport for their revenue share ("allocated parts").
- For Global Tickets/reservations the accrediting carrier waits for the debiting from the attributing undertaking ("attributed parts").
- For all types of tickets, the travel agent waits for the debit from the distributor.

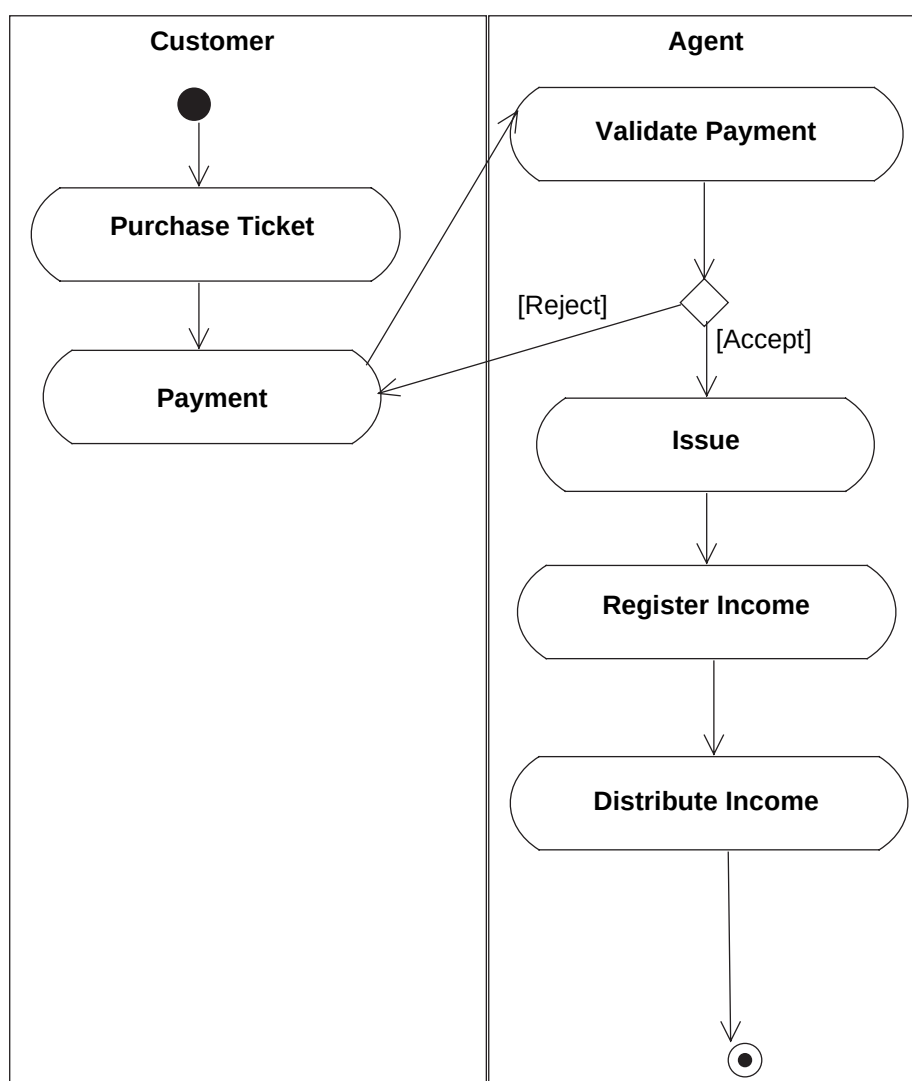


*Fig. 5 - Direct Distribution Activity Diagram*

## 2.3 - Call centre, mail delivery

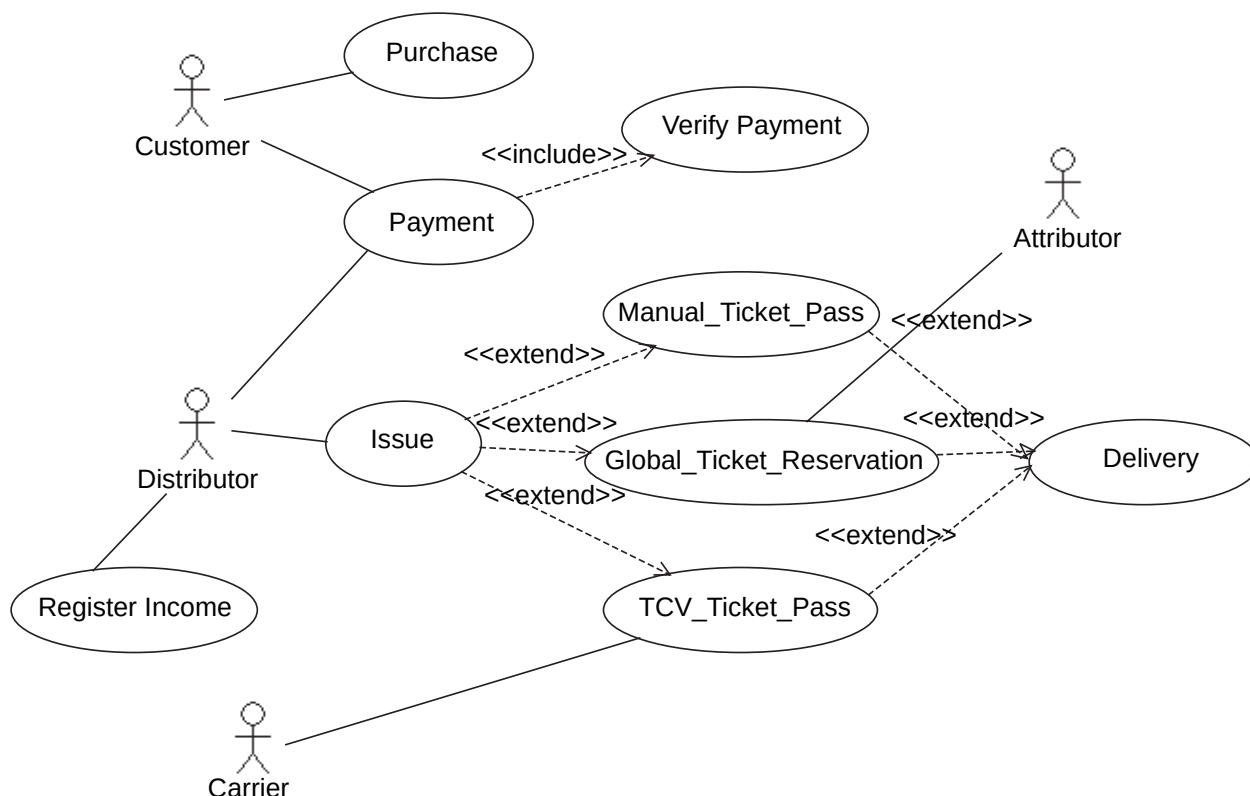


Fig. 6 - Call Centre, Mail Delivery Use Case

The customer contacts the call centre of a distributor, by available methods, to request the issuance of a ticket. The issuer is the distributor/agent who issues one of the following:

- a Global Ticket/reservation calling an attributing system,
- a TCV ticket/pass using an electronic system belonging to his/her undertaking,
- a manual ticket/pass (in this case, only TCV open tickets, no reservation or GT).

The customer pays remotely by credit card or on account. The issuer verifies the payment and prints the coupon and delivers by mail.

The sale amount is registered in the distributor's income. If the distributor is an RU, *UIC Leaflet 301* accounting rules apply for monthly settlement amongst railways:

- For TCV tickets/passes, the distributor credits the other carriers involved in the transport for their revenue share ("allocated parts").
- For Global Tickets/reservations the distributor waits for the debiting from the attributing undertaking ("attributed parts").