UIC CODE 914

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

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

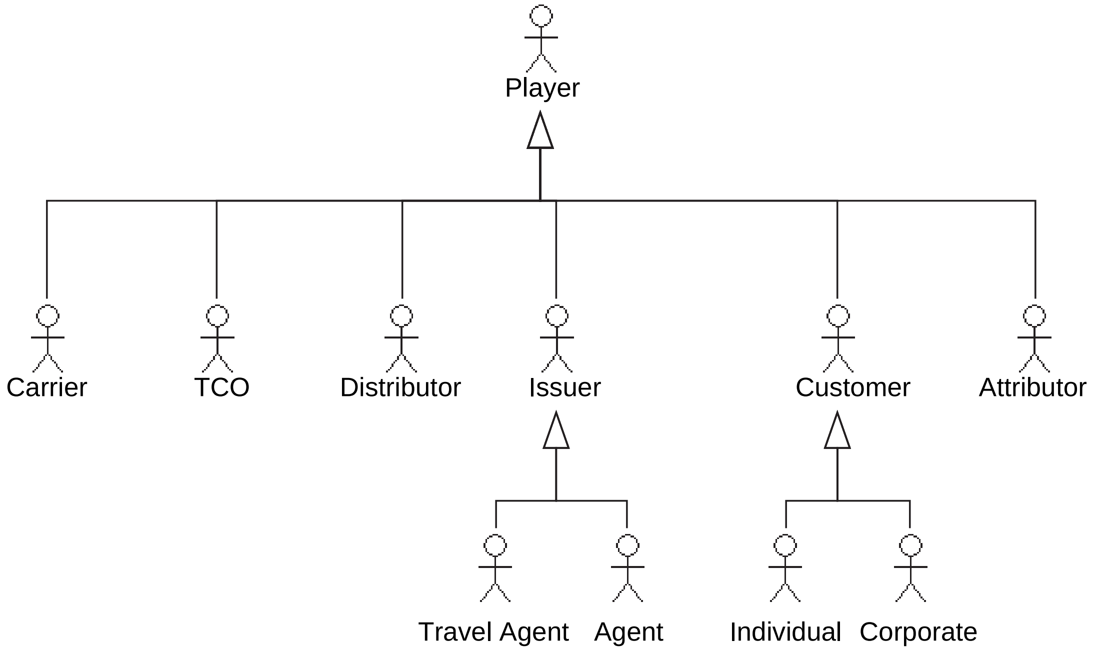


Fig. 1 - Players

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

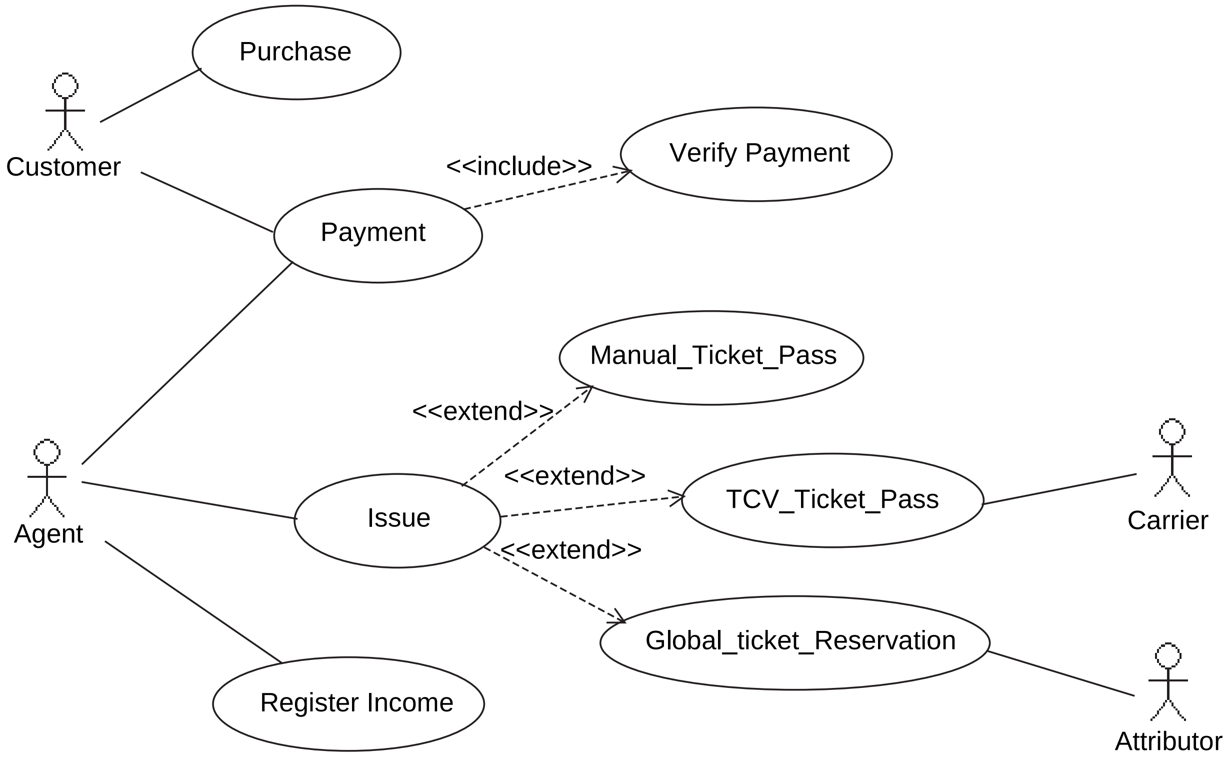


Fig. 2 - Direct in Station Use Case

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").

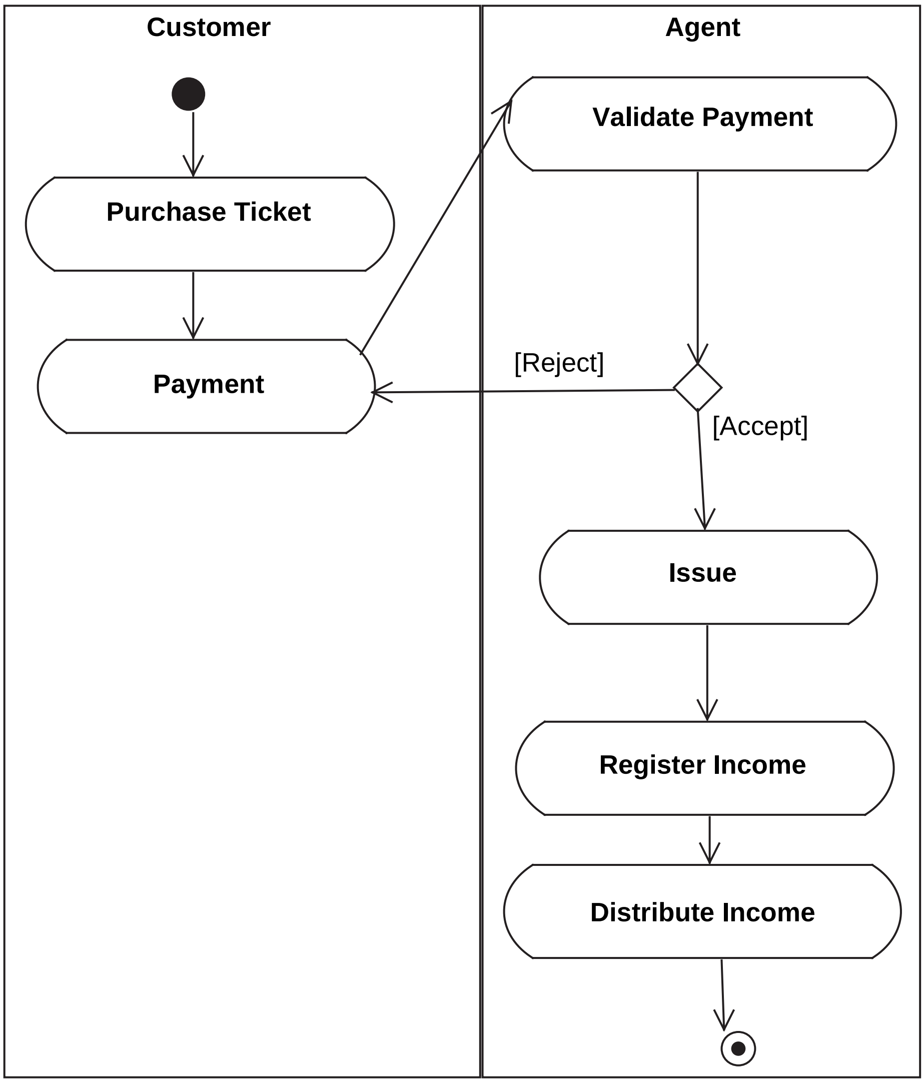


Fig. 3 - Direct in Station Activity Diagram

2.2 - Direct in Travel Agency

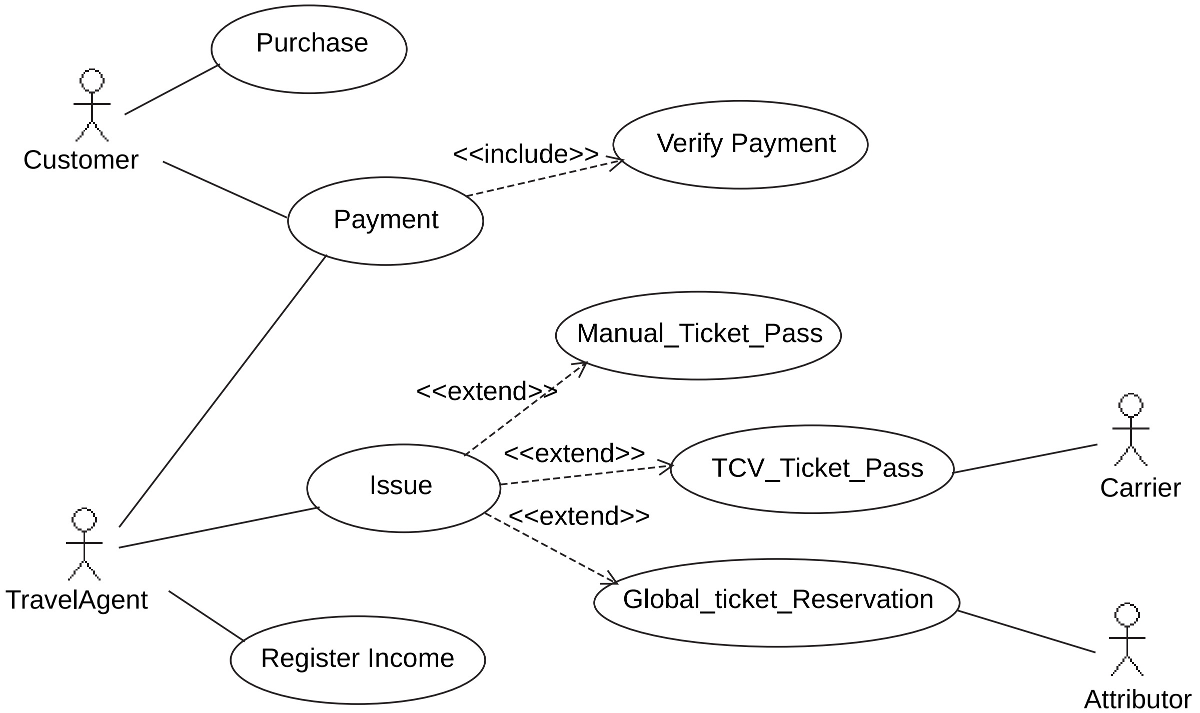


Fig. 4 - Direct in Travel Agency Use Case

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.

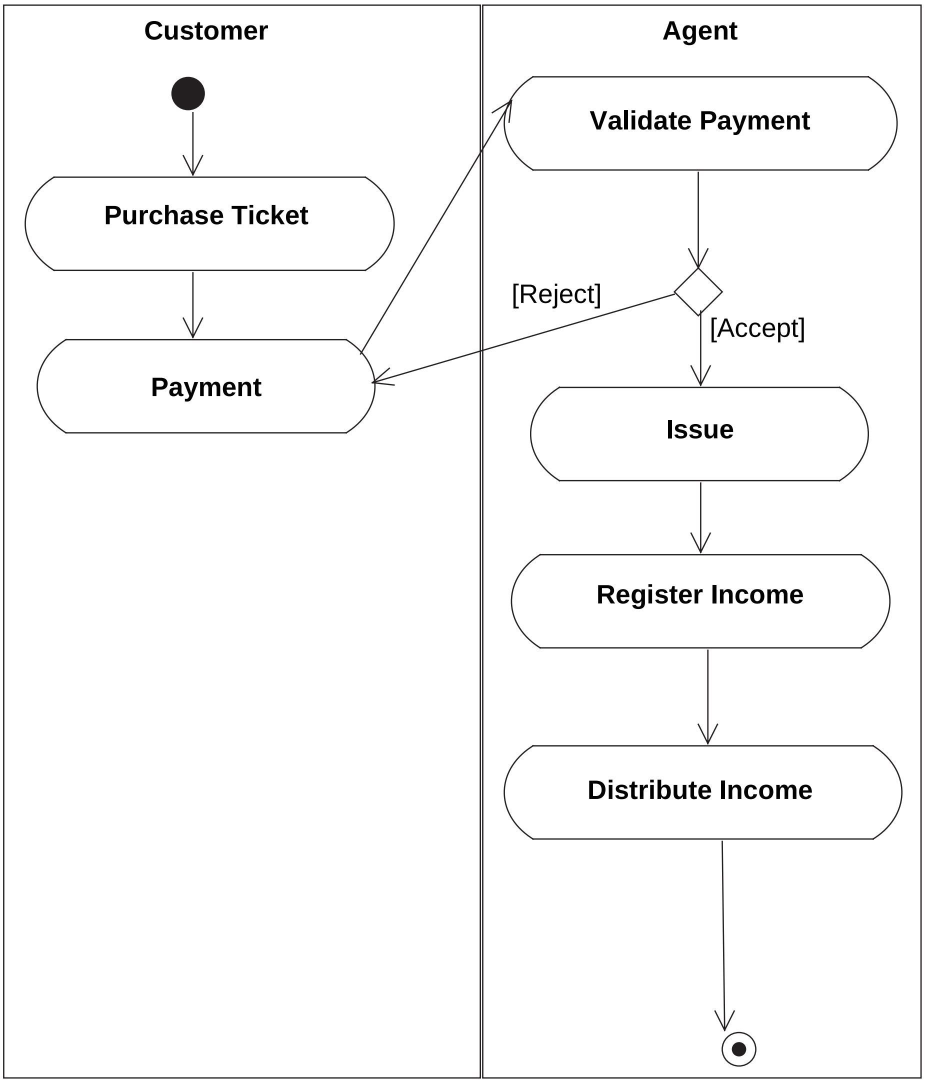


Fig. 5 - Direct Distribution Activity Diagram

2.3 - Call centre, mail delivery

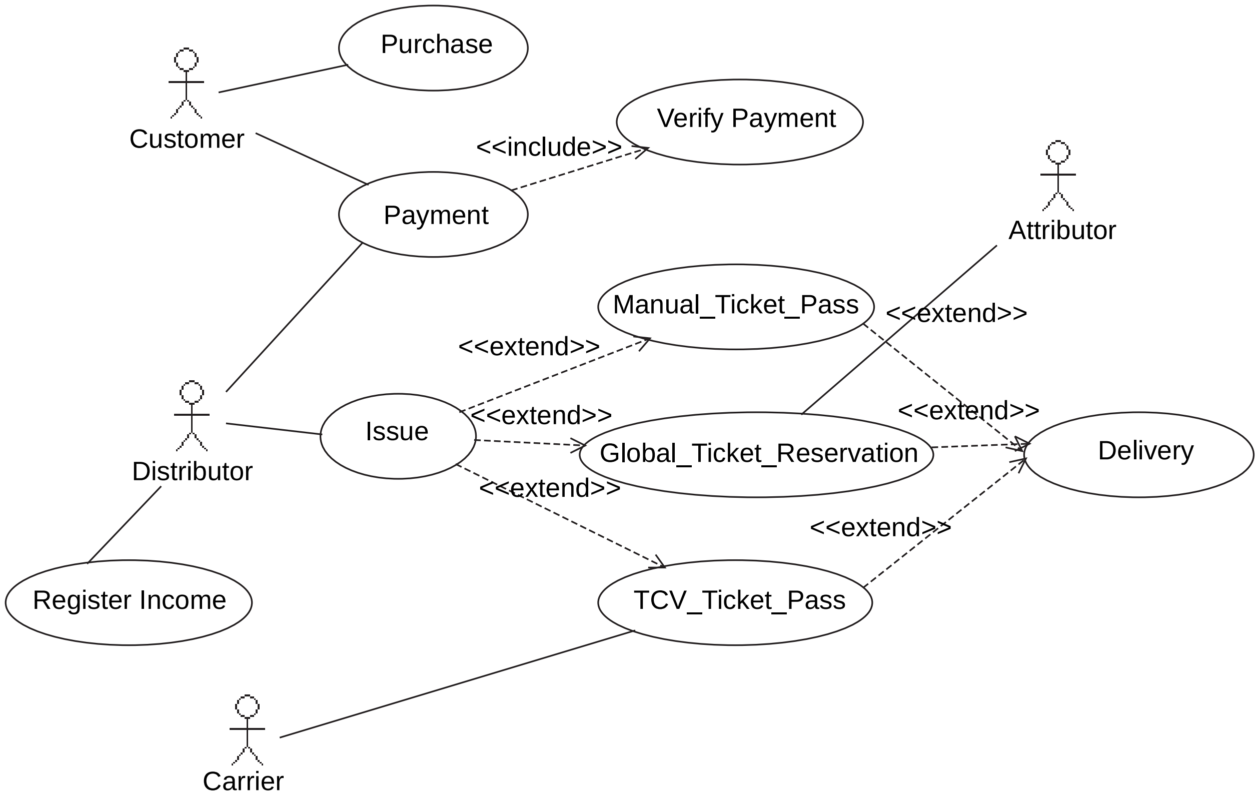


Fig. 6 - Call Centre, Mail Delivery Use Case

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").

If the distributor is not an RU, it will credit the revenue share to the concerned RUs according to established commercial agreements.

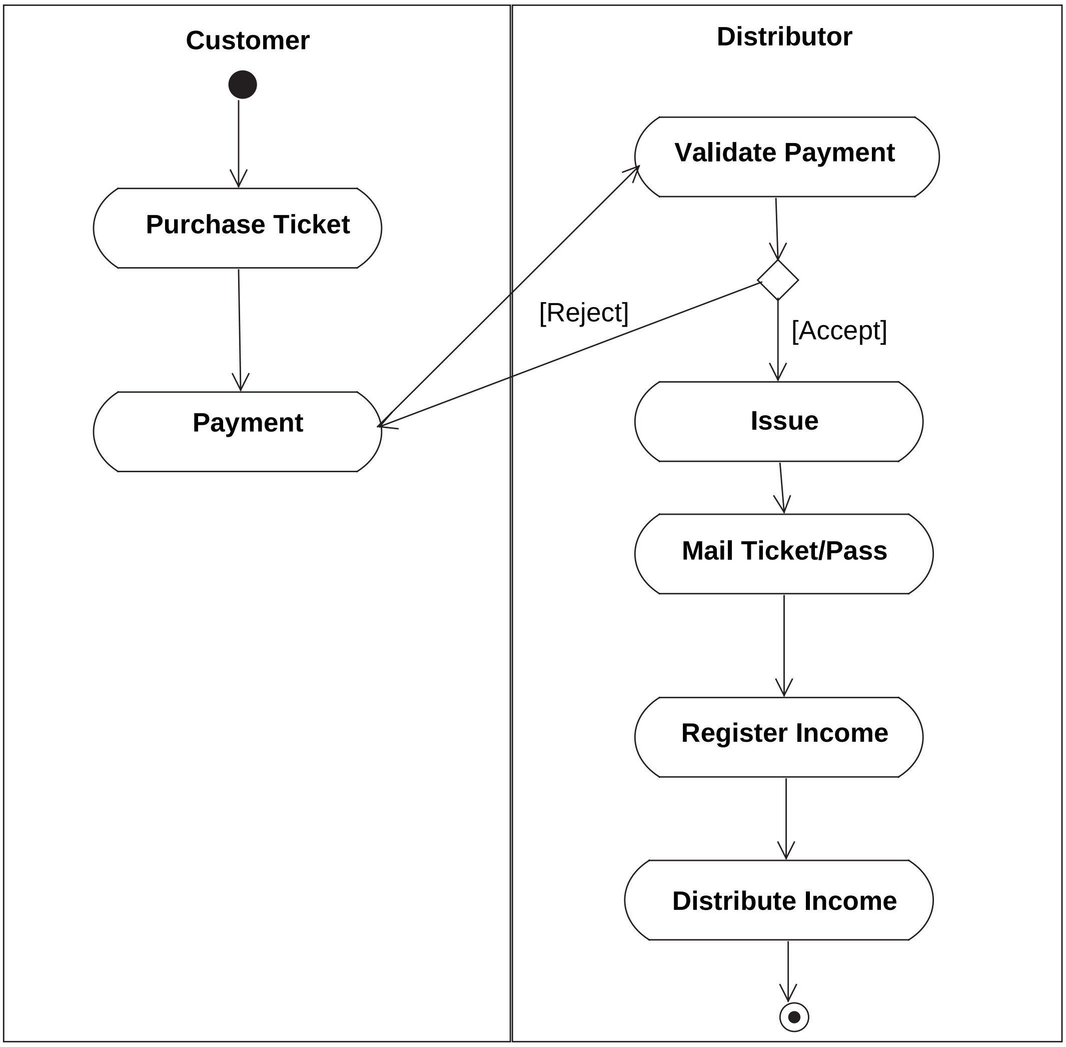


Fig. 7 - Call Centre, Mail Delivery Activity Diagram

2.4 - Call centre, electronic delivery

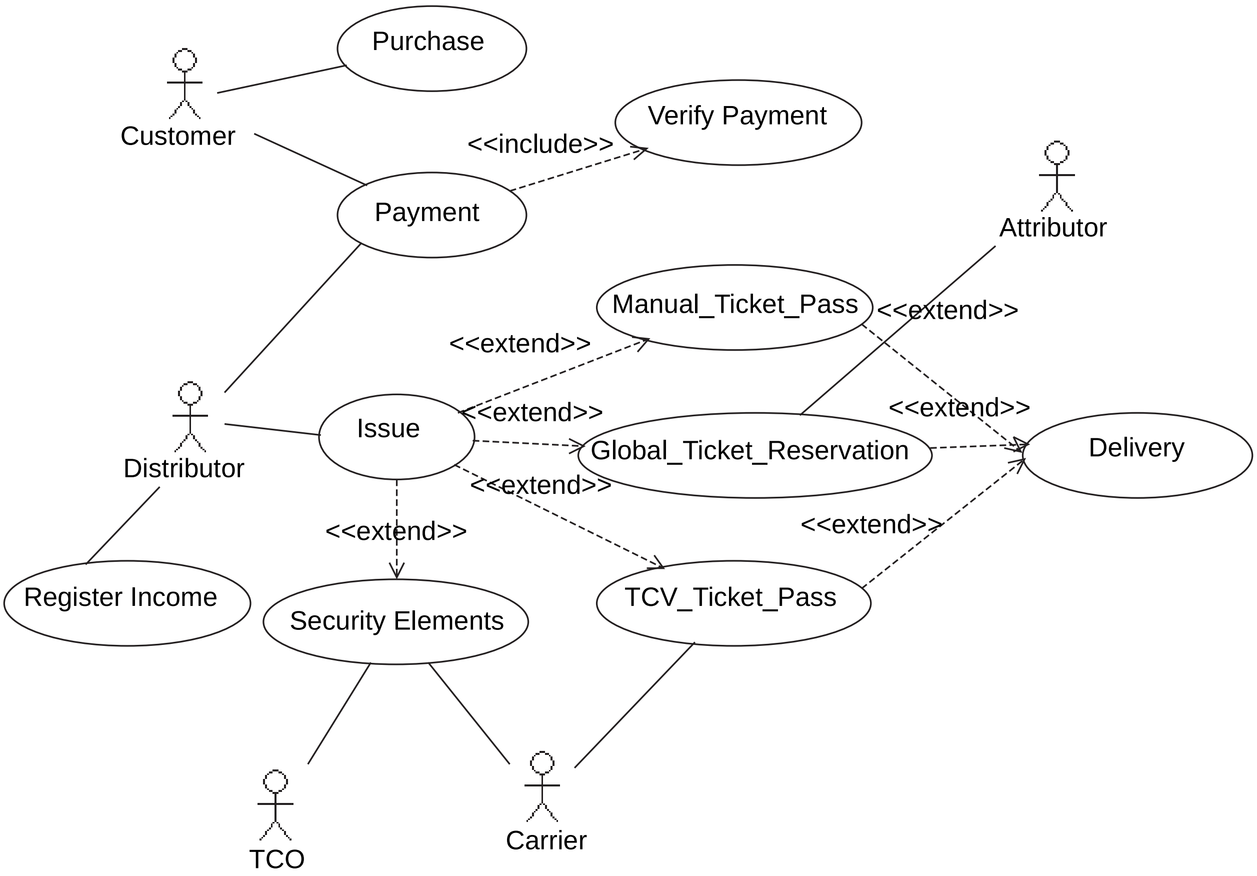


Fig. 8 - Call centre, Electronic Delivery Use Case

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 TCV ticket/pass using the distributor's electronic system,

- a Global Ticket/reservation calling an attributing system.

The customer pays remotely by credit card or on account.The issuer verifies the payment and contacts the carriers involved in the transport to request the security elements to be inserted in the printable document. The issuer produces a printable document that serves as a ticket instead of a standard coupon and sends to the customer electronically.

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").

If the distributor is not an RU, it will credit the revenue share to the concerned RUs according to established commercial agreements.

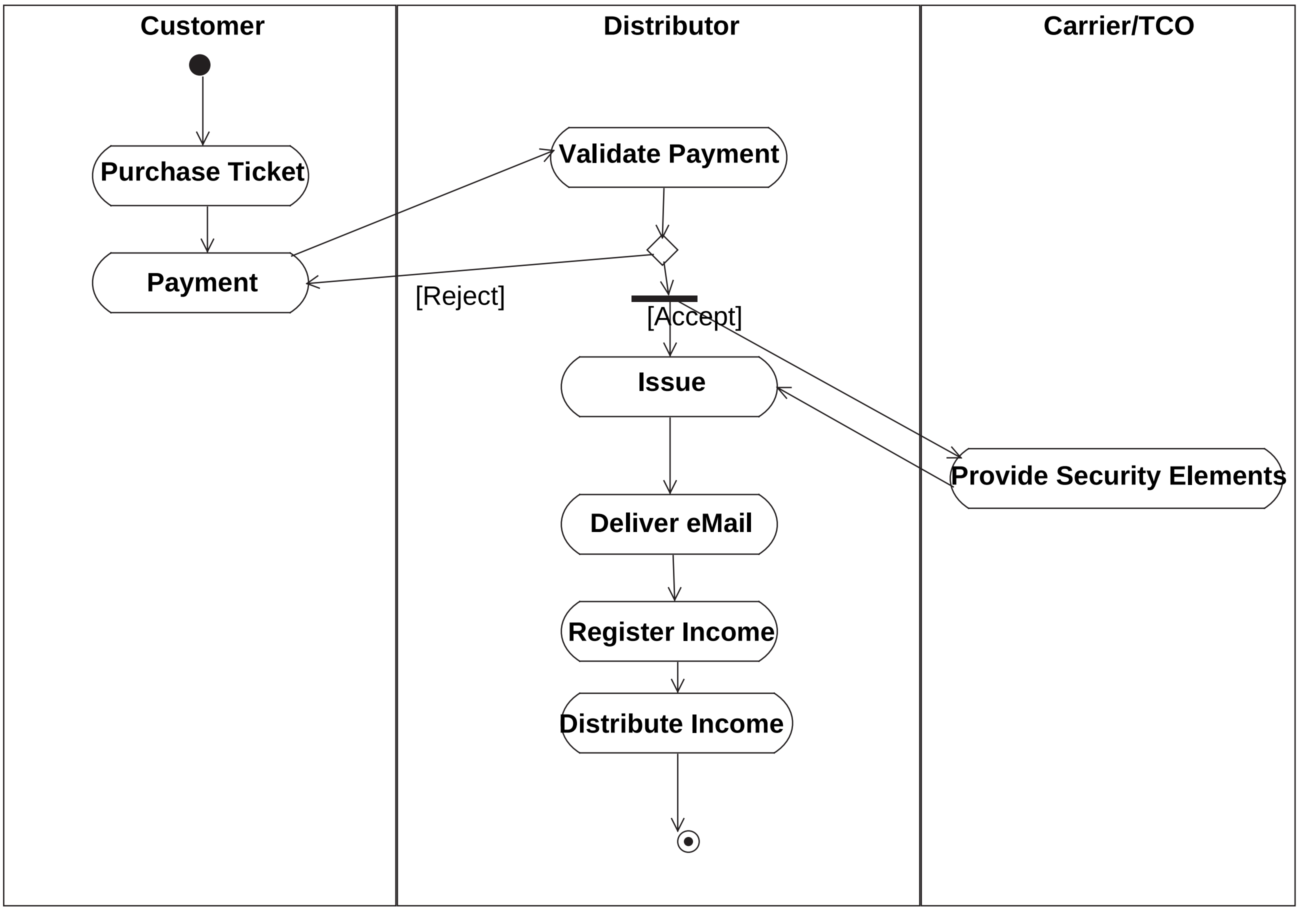


Fig. 9 - Call Centre, Electronic Delivery Activity Diagram

2.5 - Call centre, Device Delivery

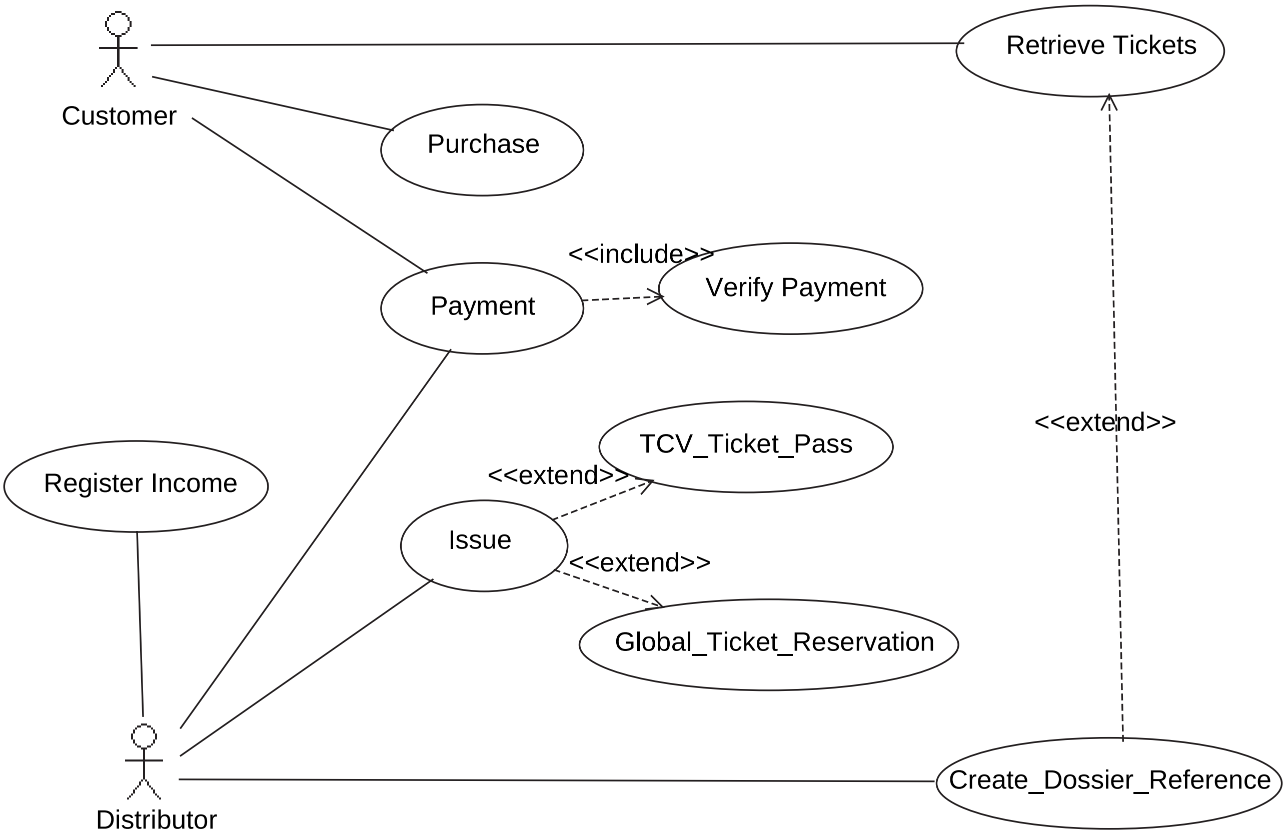


Fig. 10 - Call Centre Device Delivery Use Case

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 TCV ticket/pass using the distributor's electronic system,

- a Global Ticket/reservation calling an attributing system.

The customer pays remotely by credit card or on account. The issuer verifies the payment and produces a dossier reference to retrieve the ticket/reservation. The issuer sends this dossier reference to the customer and enters all information concerning the ticket into the electronic distribution system. The customer may then retrieve the ticket at from a device (such as a self-service ticketing machine) or at the counter.

The sale amount is registered in the distributor's income. *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").

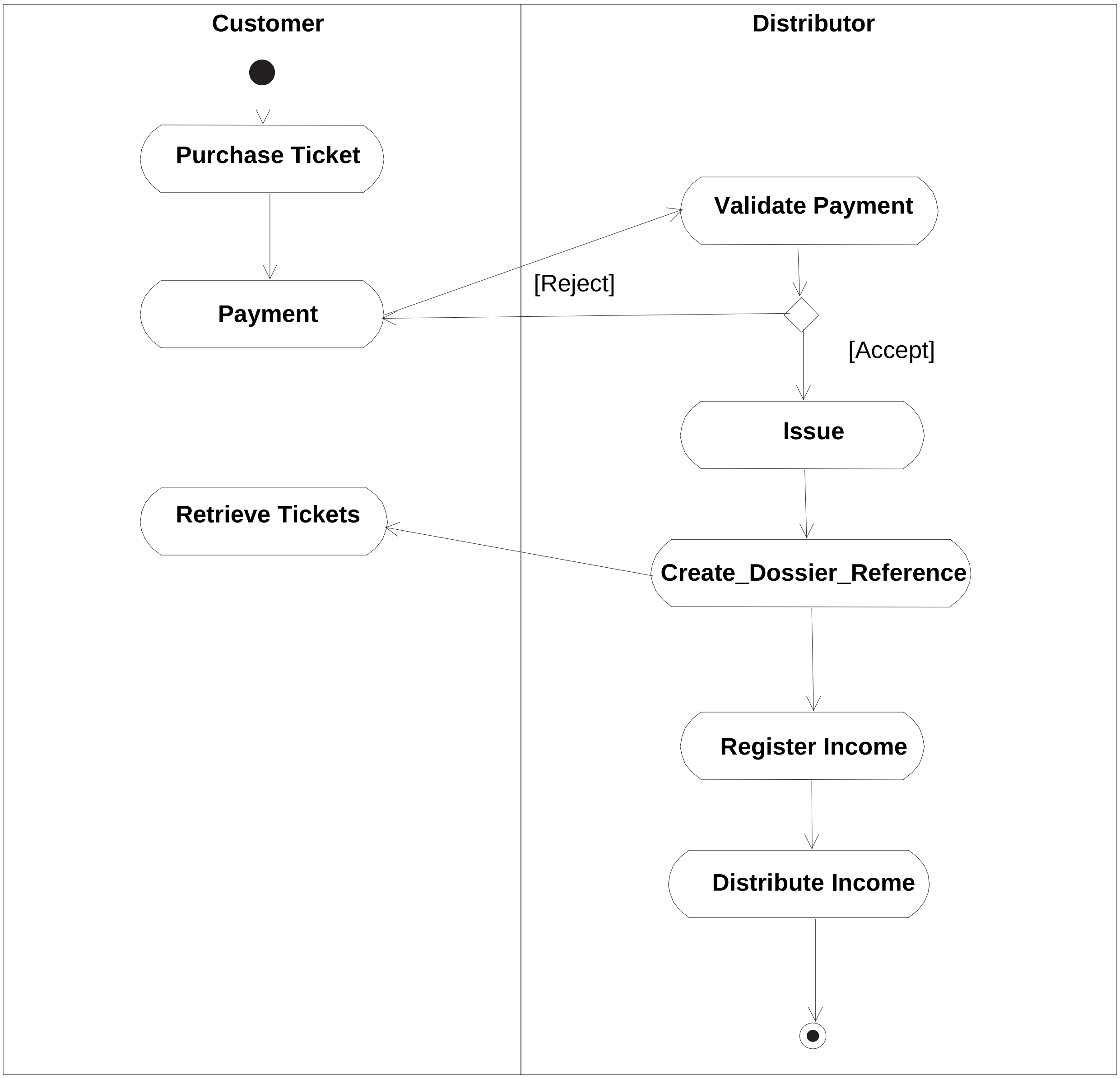


Fig. 11 - Call Centre, Device Delivery Activity Diagram

2.6 - Call centre, paperless

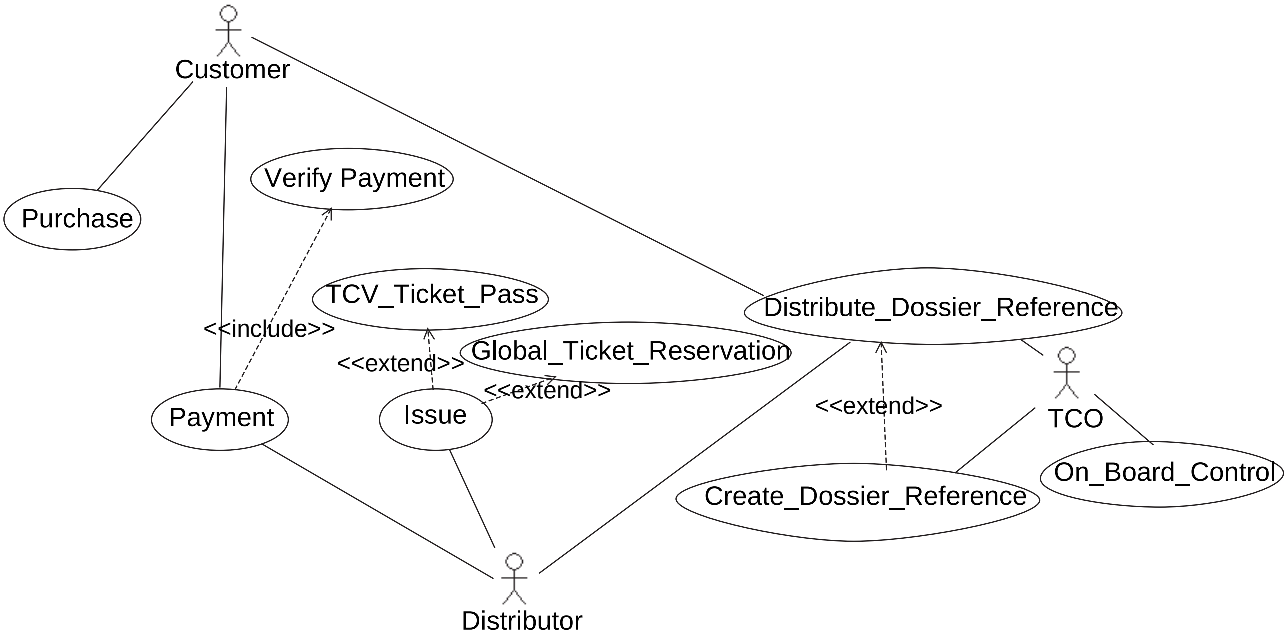


Fig. 12 - Call Centre, Paperless Use Case

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 TCV ticket/pass using the distributor's electronic system,

- a Global Ticket/reservation calling an attributing system.

The customer pays remotely by credit card or on account. The issuer verifies the payment, requests the certificates from the involved TCOs and produces a dossier reference to identify the passenger and travel data. The issuer sends this dossier reference to the customer and provides this information to all TCOs. The customer may then board the train without a printed ticket and the on-board personnel may verify the dossier reference.

The sale amount is registered in the distributor's income. *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").

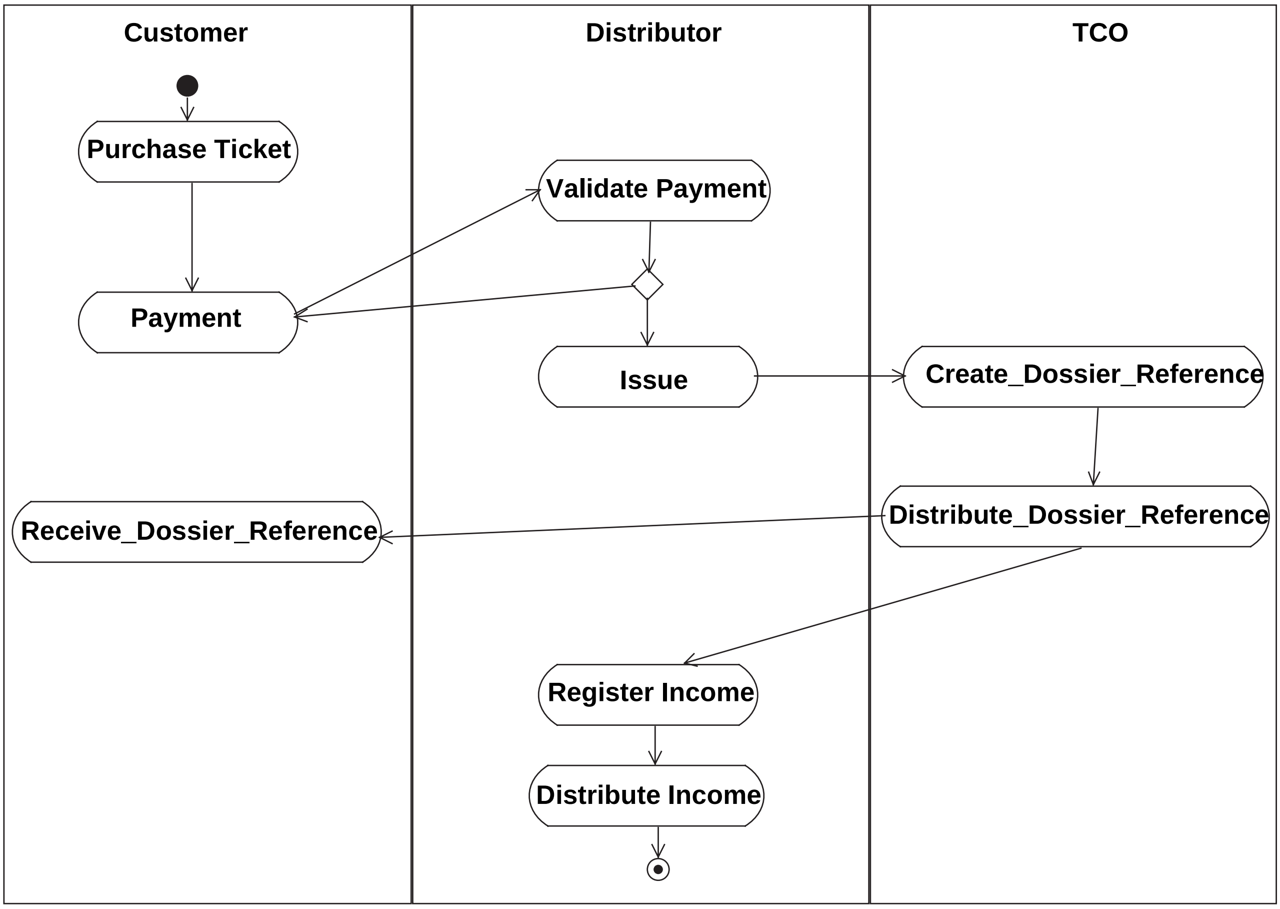


Fig. 13 - Call Centre, Paperless Activity Diagram

2.7 - Internet, A4 Ticket

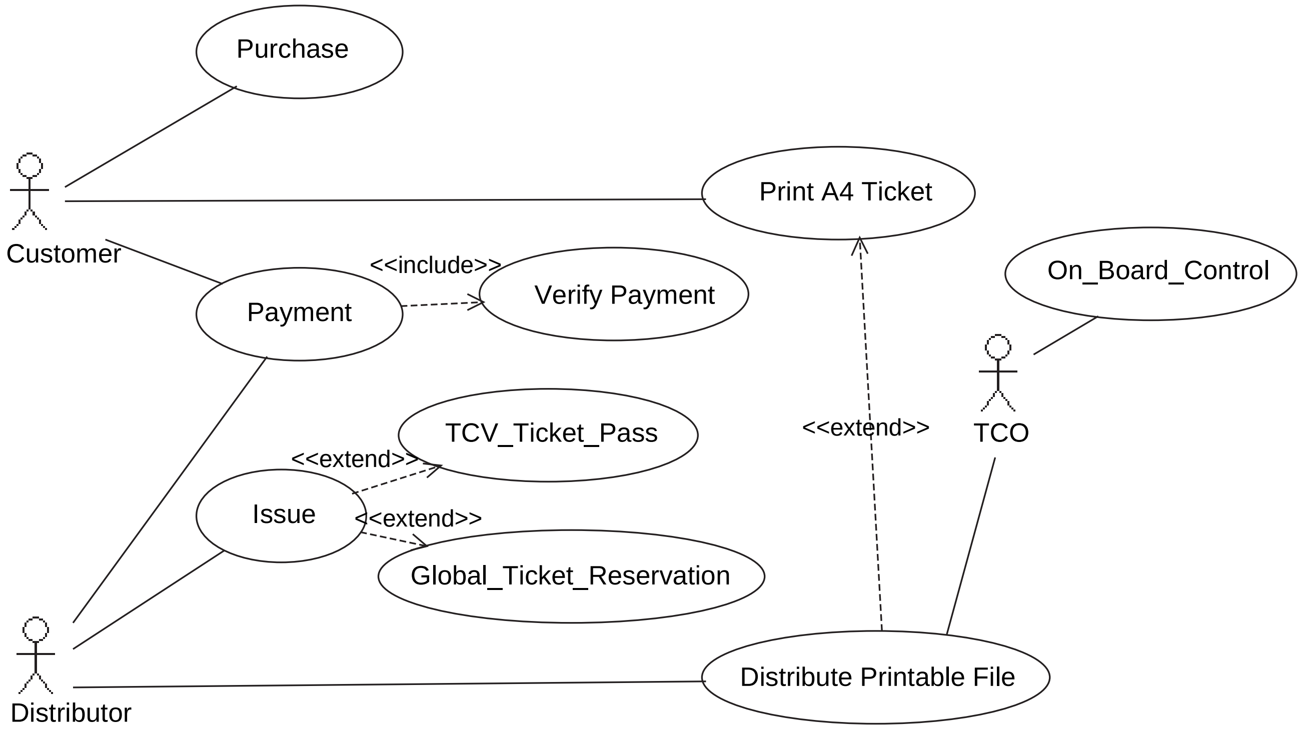


Fig. 14 - Internet, A4 Ticket Use Case

The customer contacts the website of a Distributor to request the issuance of a ticket. The site application issues one of the following:

- a TCV ticket/pass using the distributor's electronic system,
- a Global Ticket/reservation calling an attributing system.

The customer pays remotely by credit card or on account. The application verifies the payment and contacts the TCOs involved in the transport to request the security elements to be inserted in the printable document. The application then produces a printable document that serves as a ticket instead of a standard coupon and sends electronically to the customer or provides a printable file.

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").

If the distributor is not an RU, it will credit the revenue share to the concerned RUs according to established commercial agreements.

2.8 - Internet, chip card

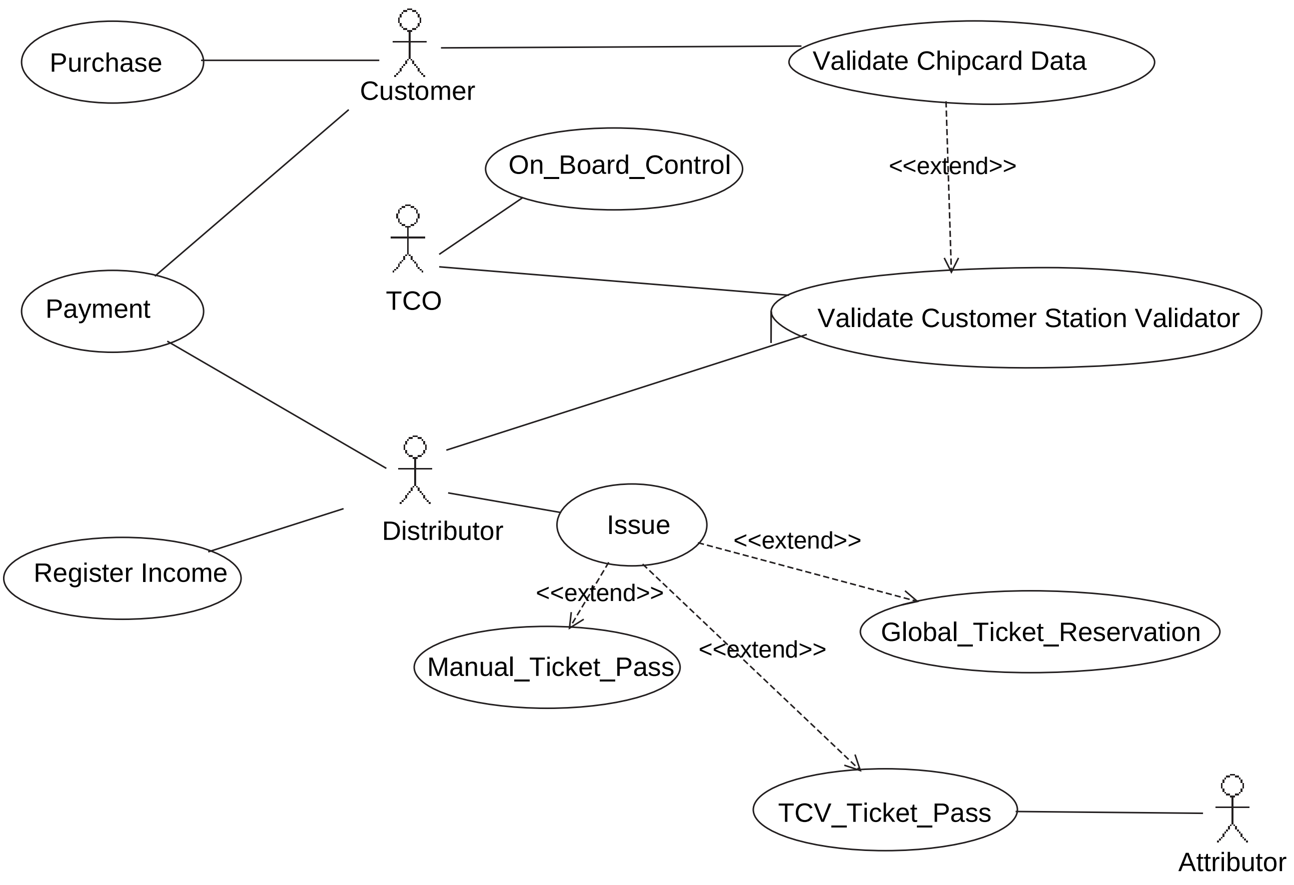


Fig. 15 - Internet, Chip Card Use Case

The customer contacts the website of a distributor to request the issuance of a ticket. The site application issues one of the following:

- a TCV ticket/pass using the distributor's electronic system,

- a Global Ticket/reservation calling an attributing system.

The customer pays remotely by credit card or on account. The customer also provides the personal data of the traveller (can be himself or another person), the chipcard type and its number. The application verifies the payment and sends the concerned TCOs the traveller and journey data. The TCO then generates the certificate which is stored on his server.

At the moment of starting his travel the traveller has to validate the journey by means of a "Station Validator": the TCO writes the Certificate on the chipcard in a dedicated zone, available for the on-board control staff.

The customer may then board the train with the chipcard "enabled" and the staff may verify the right to travel on that train/date/seat,… .

The sale amount is registered in the distributor's income. *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").

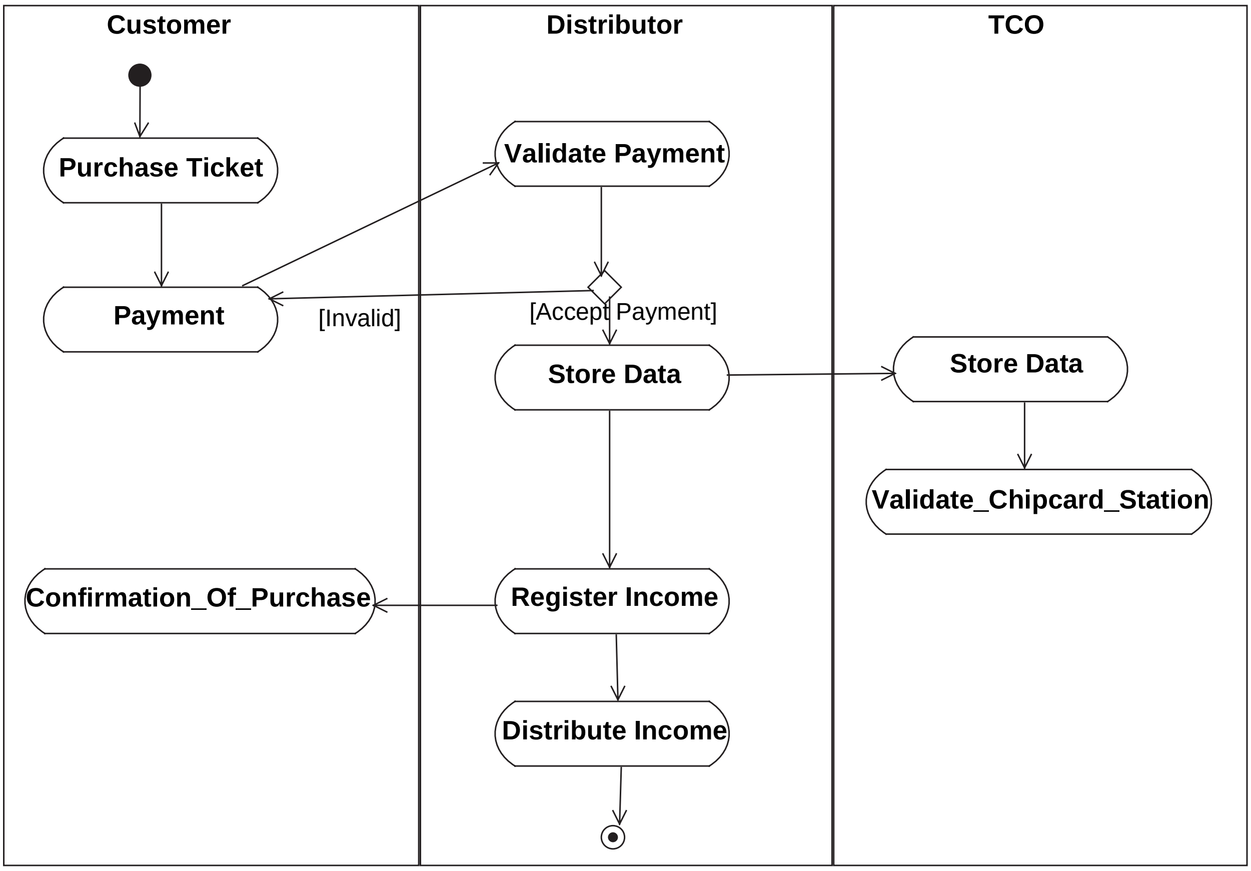


Fig. 16 - Internet, Chip Card Activity Diagram

2.9 - Internet, paperless

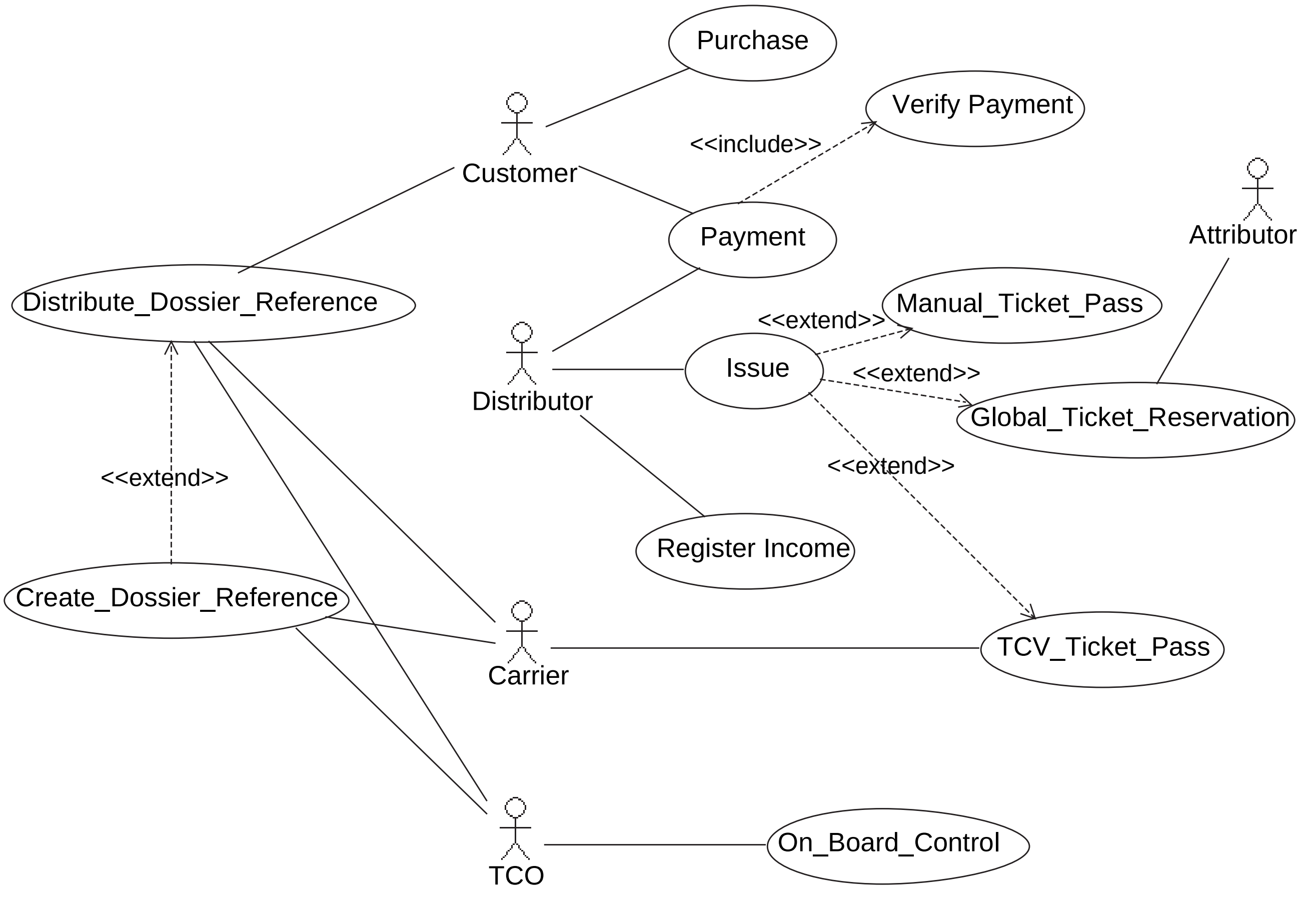


Fig. 17 - Internet, Paperless Use Case

The customer contacts the website of a distributor to request the issuance of a ticket. The site application issues one of the following:

- a TCV ticket/pass using the distributor's electronic system,
- a Global Ticket/reservation calling an attributing system.

The customer pays remotely by credit card or on account. The application verifies the payment and produces a dossier reference to identify the passenger and travel data. The application sends this dossier reference to the customer. The distributor then sends the concerned TCOs the dossier reference and the traveller and journey data. The TCO stores this data on his server and provides this information to its entire staff. The customer may then board the train without a printed ticket and the on-board personnel may verify the dossier reference.

The sale amount is registered in the distributor's income. *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").

3 - Basic processes

All the described sales types are composed of a certain number of basic processes. A full list of processes addressed is as follows:

- Specific Operational Processes

  - Stock Management - point 3.1 - page 23
  - Printing on Stock - point 3.2 - page 24
  - Printing on A4 - point 3.3 - page 25
  - Self-Retrieval - point 3.4 - page 26
  - Information to On-board staff - point 3.5 - page 27
  - Chip Card - point 3.6 - page 27
  - Proof of Purchase - point 3.7 - page 28
  - Electronic Payment - point 3.8 - page 29
  - Internet Transaction - point 3.9 - page 31

- General Framework Processes (apply to all sales types)

  - Sales Data Pricing, Transfer and Conditions - point 3.10 - page 35
  - Change Management - point 3.11 - page 37

The correspondence between specific operational processes and sales types is illustrated in the table 1 - page 22.

Table 1 : Corresponding Processes to Sales Types

	Stock Management	Printing on Stock	Printing on A4	Self-Retrieval	Info to onboard staff	Chip Card	Proof of Purchase	Electronic Payment	Internet Trans-action	Sales Data, Pricing, Transfer and Conditions	Change Management
Direct in Station	X	X								X	X
Direct in Travel Agency	X	X								X	X
Call Centre, Mail delivery	X	X						X	X	X	X
Call Centre, Electronic del.			X					X	X	X	X
Call Centre, device del.	X	X		X				X		X	X
Call Centre, paperless					X		X	X	X	X	X
Internet, A4 ticket			X					X	X	X	X
Internet, Chipcard						X	X	X	X	X	X
Internet, Paperless					X		X	X	X	X	X

Security Requirements and Recommendations are listed hereunder for each process:

3.1 - Stock Management

This process concerns the sales types 1, 2 and 3.

The coupons to be used have to comply with the GTT-CIV (formerly MDI) specifications by the CIT.

The undertaking provides its coupons to its own counter staff, or appointed travel agents, or call centre staff. The undertaking has to implement a security procedure, in order to be aware at any moment of which points of sale are holding the stock from number X to number Y.

It is recommended for the undertaking to also be able to trace for which sale any coupon number was used.

See *UIC Leaflets 130, 306, 361* (see Bibliography - page 38).

- Accrediting Carrier (entity giving the stock to the issuer) must keep record of all distributed blank coupons.
- Blank ticket stock must be stored and transported securely.
- Issuer receiving the stock must give formal acknowledgement to the distributor for receipt of stock
- If the issuer gives part of his stock to a subagent, he remains responsible for the distributed stock.
- The use of each coupon must be recorded.
- The distributor must define with the issuer which kind of products may be printed on the stock.
- Each coupon must be used for a sale (must be given to customer in exchange for payment), otherwise it must be sent back to the distributor.
- Coupons not used for sales and not sent back to the distributor are considered lost and must be repaid by the issuer.
- If the selling system prints two or more copies of each sale on a numbered coupon, all copies - except the one given to the customer - have to be sent back to the distributor.
- The distributor must agree with the issuer which procedures are to be followed when wrong content is printed on a coupon, when a coupon is damaged and in any other case of error.
- The distributor must keep files with evidence of the use of coupons for at least 3 years, unless local laws require a longer conservation.

3.2 - Printing on Stock

Distribution channels:

- Direct in Station,
- Direct in Travel Agency,
- Call Centre, Mail,
- Call Centre, Device,
- Ticket Issuing Machine.

Technical requirements:

Objective:

To prevent or identify fraud, especially misappropriation, by the use of automatic measures applied to electronic tickets (see also *UIC Leaflets 301 and 361*).

Description:

The seamless path followed by tickets from production to consumption at the point of sale and/or return/refund and destruction including any irregularities that arise shall be documented and monitored by technical means.

- acknowledgement of correct receipt of coupons,
- storage of coupons in a secure place,
- automatic monitoring of seamless use of coupons (where possible using machine-readable coupon numbers and storage on magnetic stripe, bar code, optically readable figures, chip, etc),
- gaps in the numbering sequence must be documented and/or justified,
- systematic check on coupon stock by means of a sequential numbering system,
- random checks on coupon stock.

Proof must be supplied for damaged, misprinted and invalid coupons and sent with the accountancy documents to revenue control.

3.3 - Printing on A4

Distribution channels:

- Call Centre, Electronic Delivery,

- Internet, A4 Ticket.

Technical requirements:

Objective:

To guarantee a procedure that is secured against misuse.

The security is based on an encryption procedure and an identification card or other means (e.g. customer card like RailPlus card, BahnCard, Privilege Card or credit card, etc to identify the customer).

Description:

Bookings over the Internet:

- Once the booking has been made in the distribution system over the Internet, the ticket parameters (departure station, destination station, class of accommodation, etc.) are encoded using a secret key and the ID card number to make a certificate.

- The ticket is assigned a sequential order number (optional).

- A benchmark data phrase must also be stored in a central database for subsequent comparison.

- The ticket is only valid in combination with the customer identification means used to make the booking.

Ticket inspection on board the train:

- During on-board inspections using a mobile terminal (or PDA) the certificate is typed in and decoded using the key stored in the device so it can be displayed on the mobile terminal.

- A control data phrase should also be saved.

- Afterwards the control data phrase and the benchmark data phrase can be checked against one another in the central system to prevent multiple use of tickets.

The procedure contains a kind of "double security": first of all the ticket can be checked as valid immediately by train crew using the certificate, and secondly a further verification can take place by offsetting the sale data phrase against the control data phrase to provide clear proof in cases of doubt.

NB : The security requirements will need to be adapted in line with PET solutions developed (PET working party in the DSSG).

3.4 - Self-Retrieval

Distribution channels:

- Call Centre, Internet.

Description of the process:

The Customer buys his ticket calling the Call Centre, or on the Web site, paying with his/her Credit Card; then he/she receives via email the confirmation of the purchase and a code (PIN, PNR, …). With this code the Customer has 2 possibilities to retrieve the ticket:

1. going to a Station counter, presenting the code and retrieving the ticket,

2. going to a Station, inserting the code in an ATM and retrieving the ticket.

Technical requirements:

Objective:

To guarantee a generation code procedure that is secured against disclosure.

The security is based on an encryption procedure/algorithm.

Description:

Bookings over the Call Centre/Internet:

- Once the booking has been made in the distribution system, the ticket parameters departure station, destination station, class of accommodation, etc. are encoded using a secret key and the Dossier Reference Number to make a certificate.

- The ticket is assigned a Dossier Reference Number.

- The ticket is combined with the physical stock at the moment of retrieval.

- The system must flag the Dossier Reference Number as "PRINTED" as soon as the ticket is retrieved, avoiding in this way the possibility to re-print it.

- In case of paper jam during the printing phase, the Customer will contact the Station Staff (a specific secured procedure, via a Help Desk, could enable the re-printing of the ticket, or a cancellation/new selling should be done) returning the damaged ticket.

- If allowed by the after sales conditions, a "no show" (i.e. the customer who doesn't go to a station counter or an ATM before the train departure) should be able to activate the procedure of refunds (through the Call Centre or the Web site).

3.5 - Information to On-board Staff

If a home printed ticket is used to travel, there are 2 possible solutions for verification by on-board staff: an open system where the client has all the information on his home-printed ticket (protected with certificates) or a closed system in which the on-board staff member has a 'list' with all ticket numbers that could travel on his train. This allows the staff to check if the client has "the right" to be on this train (usually for tickets WITH reservation).

Such a list must contain all E-Ticket passengers with their identification and some details (i.e. Class). This identification can also be an ID-Card number or even the code the client received when he bought the ticket. All staff must be informed, and as the on-board staff is a member of a TCO, this information is collected and the trip information is generated by the TCO at the moment of purchase. The TCO has to put in place a mechanism to send this information to the on-board staff. This can be a simple paper passenger list just before departure, an electronic version of a passenger list or a complex on-line consultation of this information on a centralised server.

3.6 - Chip Card

The chip card is used to identify the Traveller (who can be the Customer himself or another person) and to check the travel data on-board.

The system applies in a scenario where carriers have smart card systems for national distribution with installed dedicated equipment in stations able to read smart cards/chip cards and write information for its own customers.

1. At the moment of purchase the following data are stored in the central distributor system:
   - full name of the traveller, birth date,
   - chipcard type and number,
   - travel data.

2. The distributor system sends the information concerning the ticket sold on the carrier's system.

3. When starting the journey, following data are retrieved, matching the chip card data from the carrier central system and written on the chip card (Station Validation):
   - personal data of the traveller,
   - data travel.

4. The carrier marks the stored data as proof of ticket usage.

5. The staff on-board checks the personal and travel data reading the chip card, so they should be properly equipped:
   - if a TCV journey is included in the chip card the staff equipment has to flag the travel as consumed.

A specific standard zone of the chip card must be written/read, using a secure algorithm in order to prevent possible frauds (cryptography and security certificates can be adopted). If proprietary cryptography systems are used, data on chip card have to be repeated to comply with every segment/carrier involved in the journey.

On the contrary using asymmetric cryptography models or PKI certificates data can be written once and read for every carrier involved.

3.7 - Proof of Purchase

One of the most important topics concerning home printed tickets is to secure tickets against forgery. The processes and mechanisms to achieve this security are defined in *UIC Leaflet 361* concerning all tickets issued in the standard way for all currently defined tickets.

3.7.1 - Issuing paperless or home printed tickets

Considering paperless or home printed tickets new aspects arise. No security paper is used to print tickets and the customer uses his own personal computer and printer to print the ticket, or doesn't print anything at all. Therefore the issuing process has to be designed with additional safety features.

3.7.2 - Avoiding the modification of home printed tickets

It has to be secured, that the content of the printed ticket can not be manipulated. This concerns especially the main data, which would change the value of the ticket:

- class,
- origin,
- destination,
- description of the allowed routes,
- period of validity,
- number of passengers,
- passenger name (it is strongly recommended that all paperless or home printed tickets be issued nominatively).

3.7.3 - Payment of paperless or home printed tickets

Sales procedures have to ensure, that the customer receives the printing data only after the payment process has been completed.

3.7.4 - Cancellation of paperless or home printed tickets

Cancellation of a paperless or home printed ticket is permissible only, if the canceling system checks the validity of the cancellation by checking the unique central sales data. The central selling system has to cancel all possible reservations linked to the sale.

3.7.5 - Use of home printed tickets

To avoid a multiple use of the same ticket additional safety measures have to be taken:

It is not possible to avoid a multiple printing of tickets. The possibility of printing a ticket several times or to store it and print it at a later time is necessary for customer to handle printer problems.

It is also not possible to prevent copying of tickets.

To prevent frauds several procedures are possible:

- sale of offers, that are bound to an additional personal identification (passport, Bahncard, driver license etc..) and restricted to a train and travel date;

- control of the sales data during the utilization. The sales data have to be printed in an unchangeable way (i.e. using encryption) and be compared to sales data available on the train.

3.7.6 - Control processes

The sales systems have to implement appropriate procedures to ensure, that the frauds described above are not possible. Irregularities during the issuing process have to be documented, and processes to analyse the irregularities have to be in place.

The control staff on board has to be able to check a paperless or home printed ticket via at least one of two main procedures:

- the relevant data of the journey are encrypted in a text or image format and the on board staff is able to decrypt them via a portable device (where no sales are stored in advance);

- the relevant data are printed in plain writing, and the on board staff uses a portable device to verify all tickets sold for that train and date using a home printed format.

3.8 - Electronic Payment

Accountancy procedures for ticket sales with foreign RUs shall be independent of the payment process. The selling system shall be responsible for errors in the payment process. Payments that do not go through as a result can not be passed on to the service-providing carrier. This shall apply to payments on invoice as well as payments by card.

Charges for non-cash payments shall be payable by the sales and distribution system and **may not** be charged to the service-providing carrier (RU).

The possibilities for the payment process depend on the means of sale. Cash payments, for example, are not possible for sales made over the Internet or through a call centre.

Non-cash payments cannot be checked as effectively in each method of sale. When sales are made through a call centre or by Internet, cards cannot be subject to additional visual verification.

Call centres and most Internet terminals are not equipped to read the magnetic stripe or chip on the card. Checks can only extend to the information provided orally by the customer or input into the Internet terminal. It is not possible to check that a credit card is actually physically present.

3.8.1 - Obligatory measures and tests

3.8.1.1 - Measures

The following measures shall be mandatory:

- Encryption of transactions.
- Documentation of the payment process, to provide a substantiated answer to customer claims.
- Archiving of payment processes, at least until expiry of the claims validity period.
- Payment on invoice only once the customer's credit has been established as reliable.

3.8.1.2 - Tests

Irrespective of whether the card is presented or not, the sales system shall perform the following tests:

- Plausibility check on card number (test digit).
- Check on expiry date.
- Check on card against card issuers' blacklists.
- Checking of floor limit.

3.8.2 - Additional recommendations

The PIN number should be required wherever possible.

Request card security code. This is a means of checking whether the customer actually has the card in his possession.

Input of customer number to check credit reliability in customer database.

3.9 - Internet Transactions

3.9.1 - Options for Secure eBusiness Environment

Data transfer via on-line systems supporting the sales of international tickets/passes requires a high level of security. No matter what type of transport layer is used, the TCO needs to ensure that security policies are in place for:

- authentication and Authorisation of users,
- protection of confidentiality, and
- protection against interception and alteration of data.

Because of the diversity of implemented security systems and policies on the railways, it is not possible to dictate a standardised set of policies or tools to ensure the secure transport of data. However, this chapter will attempt to outline various technologies that may be employed to construct an over security environment for the exchange of data.

Specific requirements for secure data exchange are addressed in two other UIC Leaflets. *UIC Leaflet 910* (see Bibliography - page 38) addresses the minimum requirements for interoperability for managing Certificate Authorities for the industry. Additionally, *UIC Leaflet 918-3* (see Bibliography - page 38) outlines the certification and encryption procedures for International Rail Ticketing for Home Printing.

This section only addresses the transport layer for data exchange and does not address application-level security concerns. It is important to note that the options listed below are for illustrative purposes and do not imply any priority for implementation. It is up to each player to select the best solution to match the needs of its particular organisation in order to comply with the authentication, confidentiality and intrusion requirements.

3.9.2 - Digital Certificates

Most secure data exchanges depend on digital certificates. According to *ISO/IEC 9594-8* (see Bibliography - page 38), a certificate is "a data structure containing the public key of an entity, together with associated information, and rendered unforgeable by being digitally signed by the certification authority, which issued it." This option is commonly applied to secure servers and information.

3.9.2.1 - Transport Layer Certificates for Secure Communications

The most commonly used certificate is the *ITU-T X.509* (see Bibliography - page 38) and could contain just a public key and a name in its basic form. The use of the X.509 certificate assures interoperability in that they can be read by most commercial applications complying with the standard.

An *X.509* certificate consists of the following fields:

- version,
- serial number,
- signature algorithm ID,
- issuer name,
- validity period,
- subject (user) name,
- subject public key information,
- issuer unique identifier (version 2 and 3 only),
- subject unique identifier (version 2 and 3 only),
- extensions (version 3 only),
- signature on the above fields.

It is up to the trading partner community to define the content of the certificates used. They include the public keys for public key cryptography. Using such public key cryptography enables a secure key exchange to be made so that the symmetric keys used to encrypt and decrypt the data are not compromised.

Public keys must be delivered for certificate issuance in a way that binds the applicant subscriber's identification to the public key. When the key pairs are generated, secure mechanisms should be implemented to ensure that the token on which the key pair is held is securely sent to the proper Subscriber.

Certificates, once created, shall be checked to ensure that all fields and extensions are properly populated. This may be done through software, which scans the fields and extensions looking for any evidence that a certificate was improperly manufactured.

3.9.2.2 - Certificates for Home Printing of Tickets

In order to verify that Home Printed Tickets have not been altered, a certificate must be generated by the TCO and printed on the ticket. This certificate must be read and interpreted by all of the railways to verify the confidentiality of the information on the ticket. Although this is not applicable for the transport layer, the methodology described is similar to using a PKI.

The following instance is for the use of For Home Printing of Tickets, *UIC Leaflet 918-3* describes the asymmetrical algorithm to calculate the certificate found on the printed ticket, apart from the key pairs that need to be defined for each bi-lateral agreement. This method has the advantage that the algorithm works on every system and only needs to be programmed once. The trading partners must only then describe the key pairs and the mechanism and frequency for exchanging them.

In this instance, the key pairs are exchanged on a bi-lateral basis (by agreement) and will have a specified validity period.

3.9.3 - Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is perhaps the most widely used Internet security protocol for Business to Client Web-based transactions as it does not require the client to install any proprietary software to provide secure communications. It is based on digital certificates that provide Authentication and encryption to provide Confidentiality. This is an easy solution that is already in place on most systems.

Traditional SSL relies on server-based certificates while users identify themselves with a traditional User ID and Password to provide Authentication. The digital certificate also contains the public key providing the encryption for the transmission ensuring the necessary confidentiality of the data while passing through the public Internet.

The digital certificate stored on the server contains the Domain Name as well as the IP address of the server so that the user is able to verify that the site is actually the one requested. The user must verify the security information contained in the displayed certificate in case of a security warning.

The newer generation of SSL (Version 3) provides an even greater level of security by enabling "client side authentication", where clients store certificates locally. This allows the server to request a certificate from the client prior to opening a SSL session. The level of security for authenticating the user is higher than just using a User ID and Password.

3.9.4 - Secure File Transport Protocol (FTPS)

While SSL, as discussed above, provides for a sufficient level of security for Web-based transactions, it is not suitable for large data transfers of business information between partners. FTP allows trading partners to easily exchange large volumes of files and information between systems across the Internet, but it does not provide any inherent strong security components for authentication or confidentiality. To initiate a traditional FTP session, users are identified with a password and login - and the data is passed in clear text. Therefore, it is easy to intercept, read and modify files.

For these reasons, many users have abandoned the use of FTP as a means of data exchange and have replaced it with encrypted versions of FTP, or Secure FTP. Most Secure FTP exchanges use encryption and digital certificates to provide authentication and confidentiality.

Coupling FTP with the encryption features of SSL provides a good solution for transport layer security as well as FTP transfers within a Virtual Private Network. In any case, strong authentication and encryption capabilities should be implemented for FTP transfers, such as digital certificates and encryption algorithms.

This solution is not widely used in Europe and is difficult to manage with high volume data exchange and messaging.

3.9.5 - Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is the name given to all the components, functions and procedures specifically used to manage the cryptographic keys and certificates used by security systems based on public key cryptography. This infrastructure provides many functional and security services including a registration service of holders, a certificate generation service, a certificate distribution service, a time-stamping facility and a certificate revocation service.

UIC Leaflet 910 addresses the key points in building a PKI and how it may be applied to the railway industry. It specifically addresses the minimum specifications for building an interoperable PKI with specific guidelines for policy, governance and operational issues.

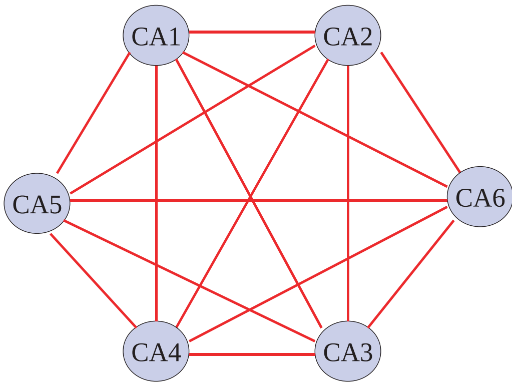
The specification supports interoperability for a large scale PKI that issues, revokes and manages digital signatures and key management for public key certificates. Digital signature certificates support the use of those signatures to replace hand-written signatures and to allow remote RUs or IMs, who have no previous relationship, to reliably authenticate each other and conduct business securely.

The Minimum Interoperability Specification Requirements (MISR) specifically addresses cross-certification between multiple Certificate Authorities (CAs). A CA could be an individual RU, TCO or national authority.

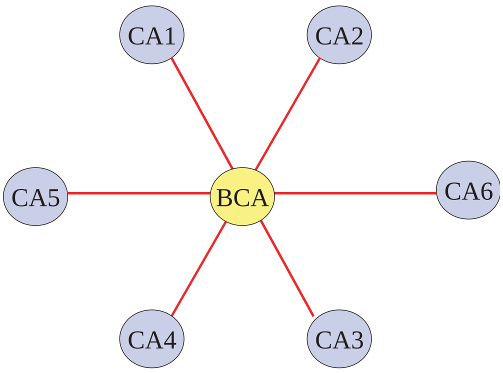
When RUs belonging to different trust domains need to communicate securely, they need first to ensure that they have established a trusted relationship. This trusted relationship is called a cross-certification. Basically there are two ways to create this cross certification, via a bilateral cross certification (two by two) or via a central hub, or Bridge CA (BCA).

The following example shows how certificates may be cross-certified.

- for n CAs that cross-certify each other, the number of cross-certifications is $\frac{n(n-1)}{2}$.



- for n CAs that can cross-certify with a BCA, the number of cross-certifications is only n.



The BCA is based on the idea that a central point is used to create a community of interests between companies. To enter this community of interest a company needs to be cross-certified with the Bridge CA.

This solution requires an industry-wide coordinated approach and is difficult to manage.

3.10 - Sales Data - Pricing and Transfer conditions

3.10.1 - General

Sales data phrases shall be compiled for each sale. The rules set out in this leaflet shall be mandatory for transactions carried out on behalf of other RUs.

The accountancy rules of *UIC Leaflet 301* lay down the settlement procedures applicable to sales between RUs. Irrespective of this, data must follow a secure path in the respective railway systems through to their transfer to the revenue accounting centre.

This requirement shall include all sales and the complete transfer of all the sales information necessary.

Information used by the system to calculate the price of Sale must also be used by the system for accounting and settlements.

Data should be archived and be retrievable by product type, place of purchase (or agent), date and time of sale, validity duration, amount and dossier number (transaction identifier). The archival period must conform to the individual railway policies and data must be archived for a sufficient period to perform financial settlements. This should also allow enough time for the receiving railways to accept or reject the transaction.

Documents shall be kept for as long as is necessary to provide detailed proof in the event of discrepancies in railways' statements of account.

UIC Leaflet 301 specifies the exact periods for account data.

3.10.2 - Transfer via on-line systems

3.10.2.1 - Normal procedure

Flows of sales data shall be displayed in an overview and shall be stored for the purposes of verification by UIC.

If the sales data are not directly transferred from the source to the accountancy procedure, intermediate stages must be shown.

Where sales data phrases are converted, there must be no losses in their number. Proof of data integrity (in/out) must be given in each case.

3.10.2.2 - Management of errors in on-line systems

Since problems can always arise during the execution of conversion operations, an indication of how errors were dealt with must be given. If the errors that arise cannot be dealt with, the cases in question must be stored in log files with all available information.

The further handling of the log files must be described. This also applies if the log files are processed manually by staff.

Sales data phrases that include errors that cannot be further processed by automatic means shall be transferred to lists and brought to account manually. *UIC Leaflet 301* gives further details as to the manual procedures.

3.10.2.3 - Archiving periods for on-line systems

Sales data (for conversions) once sent shall be archived until such time as the processing has taken place at the receiving centre.

3.10.3 - Data transfer with off-line systems

3.10.3.1 - Normal procedure

Flows of sales data shall be displayed in an overview and shall be stored for the purposes of verification by UIC.

Data transfer with off-line systems can take a variety of different forms (diskette, CD-ROM, memory stick, sporadic network connection).

The integrity of sales data must be guaranteed, as for transfer using on-line systems. Consequently, when transferring sales data the number of data phrases to be transferred must always be indicated first.

If the sales data are not directly transferred from the source to the accountancy procedure, intermediate stages must be shown.

Where sales data phrases are converted, there must be no losses in their number. Proof of data integrity (in/out) must be given in each case.

3.10.3.2 - Management of errors in off-line systems

If differences arise at the receiving centre, the reasons for this must be investigated.

The investigation processes must be described. Differences can be identified using the phrase counter transmitted.

If the errors that arise cannot be dealt with, the cases in question must be stored in log files with all available information.

The further handling of the log files must be described. This also applies if the log files are processed manually by staff.

Sales data that cannot be brought to account by automatic means because of errors in the phrase types shall be compiled in paper form and brought to account manually with the RUs concerned.

3.10.3.3 - Archiving periods for off-line systems

Sales data once sent shall be archived until such time as the processing has taken place at the receiving centre.

3.11 - Change Management

3.11.1 - General

Passenger distribution systems that carry out sales transactions for other RUs must perform sales and accountancy operations securely. For all general security requirements, the provisions of *UIC Leaflet 301, Appendix F* shall apply by analogy.

3.11.2 - Test system

In order to guarantee a clear separation between test and production modes, a separate test system shall be established. Test tickets shall be identified as such. Suitable measures shall be taken to ensure that test tickets cannot be fraudulently used for travel (by being marked "specimen", "not valid for travel", etc.).

Attention should also be paid to ensuring that data phrases from test sales do not find their way into the system for production accounts.

3.11.3 - Production system

Similarly to the stipulations for the test system, no test sales should be processed through the production system (with the exception of seat reservations identified as test items).

Changes to data and programs may only be implemented in the production system once they have been successfully deployed in the test system.

Once the authorisation has been given by the person responsible, no further changes may be made before implementation in the production system.

All sales must be brought to account.

3.11.4 - Change management

Before changes to data and programs are implemented in the production sales system, they must have been implemented and tested in the test system.

When the authorisation for the new release is given by the person responsible, this must be documented and must be made available for audits conducted by the UIC.

If data is input directly into the production system, this may only be done using data capture functions that have been through full testing and delivery acceptance.

Bibliography

1. UIC leaflets

International Union of Railways (UIC)
UIC Leaflet 130: Railway undertakings - Travel agencies - Services - Accreditation - Commission, 16th edition, December 2000 (reissue)

UIC Leaflet 301: Accountancy regulations for international "Passenger" traffic, 1st edition, December 2002

UIC Leaflet 306: Framework principles and conventions governing relationships between parties involved in passenger rail transport with respect to accounting and financial arrangements for international transport services and ancillary services, 2nd edition, December 2004

UIC Leaflet 361: Prevention of fraud on travel tickets in passsenger traffic, 4th edition, April 2001

UIC Leaflet 910: Railway Public Key Infrastructure Recommendations for Interoperability, 1st edition, May 2004

UIC Leaflet 918-3: International Rail Ticket for Home Printing (IRTHP), 1st edition under preparation

2. International standards

International Organization for Standardization (ISO)
ISO/IEC 9594-8:2001 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, 2001

International Telecommunication Union (ITU)
Telecommunication Standardization Sector (ITU-T)
X.509: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, March 2000

Warning

Printed by the International Union of Railways (UIC)
16, rue Jean Rey 75015 Paris - France, August 2006
Dépôt Légal August 2006

ISBN 2-7461-xxx (French version)
ISBN 2-7461-xxx (German version)
ISBN 2-7461-1117-9 (English version)