UIC DIGITAL DAY
Paris, 7 October 2016

I'M A DIGITAL RAILWAY

“The new UIC paperless standards and solutions: Barcodes, Rail Ticket on Screen, Control App and Public Key website”

- Digitalisation of railways will enhance customer experience by offering a better and added value and by meeting their expectations.

Overview

- To allow the passenger to travel seamlessly in Europe, most B to B processes should be unseen, made simple and standardized.
- UIC Technical Groups, composed of IT rail experts from all European railways, meet several times a year in UIC Paris.

Overview

- In 2013, domestic mobile ticketing is booming in Europe
- In September 2013, UIC offered a first mobile ticketing Technical Report for international rail journeys
- In 2014, URT specifies the requirements, actors and roles definition, Uses Cases, sequence diagrams and the related messages specifications
- In 2015, UIC Ticketing group (TAG) defines new standards: the flexible barcode (FCB) and the layout on screen (RTS)
- In 2016, PRISM project is UIC Proof of Concept

Overview

- UIC defines standards for international tickets, for journeys between different countries and for journey in a foreign country.
- UIC TAG group defines Ticket layout standards in UIC leaflet 918-2 and 918-3.
- CIT defines the paper quality and the legal aspects of the contract of transportation.

Summary

- Definitions
  - IRT, NRT, RPT, GRT, RES,…
  - SiP, SiD and SiS
- Paperless Standards
  - URT: Universal Rail Ticket
  - RTS: Rail Ticket on Screen
  - FCB: Flexible Content Barcode
- Existing UIC IT Solutions
  - UIC Public Key Management Website
  - UIC Control App
- Proof of Concept
  - PRISM Project

UIC Classification of Tickets

- according to type of transportation contract

  - if T is used at the end of the acronym, the ticket is a transportation contract.
    - Non included Reservation Ticket (NRT or Transport only)
    - Included Reservation Ticket (IRT or Transport and Reservation)
    - Group ticket (GRT)
    - Rail Pass (RPT)
    - Vehicle Ticket (VET)

  - If no T at the end of the acronym, the document is not valid without a ticket.
    - Reservation only (RES), Supplement (SUP), Change of Itinerary (COI), Upgrade (UPG), Boarding pass (BOA), Transport Voucher (TRV)

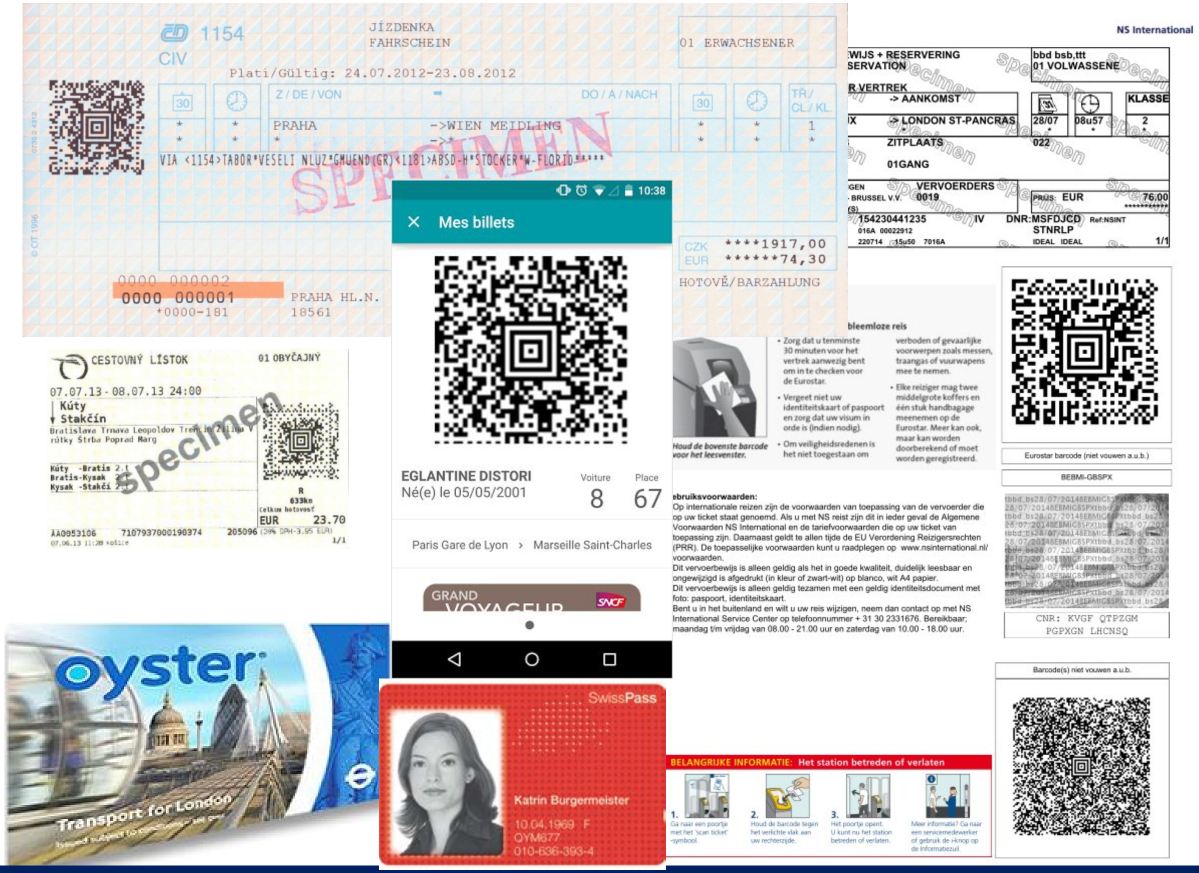
- Classification of Tickets is usually divided per sales channel and/or media

> RCT2 or RCCST (with or without barcode)
SiP: Security in Paper

> Home-print
SiD: Security in Data

> Paperless
SiS: Security in System

> Chipcard
SiD or **SiS**



UIC DIGITAL DAY
Paris, 7 October 2016

- UIC Classification of Tickets is according to type of security ("security elements")
  - SiP : 'Security in Paper' thickness, color, U.V. light, microtext, hologram
  - SiD 'Security in Data' Barcode with encrypted Seal, checksum, certificate, Visual security element
  - SiS 'Security in System' ticket is stored on a server

Or a combination

URT (Universal Rail Ticket)

> URT Technical Report agreed upon a set of messages to ensure interoperability between Railways, rail ticket types (IRT, NRT, RPT,…) and all ticket supports (paper, home printed, paperless,…).

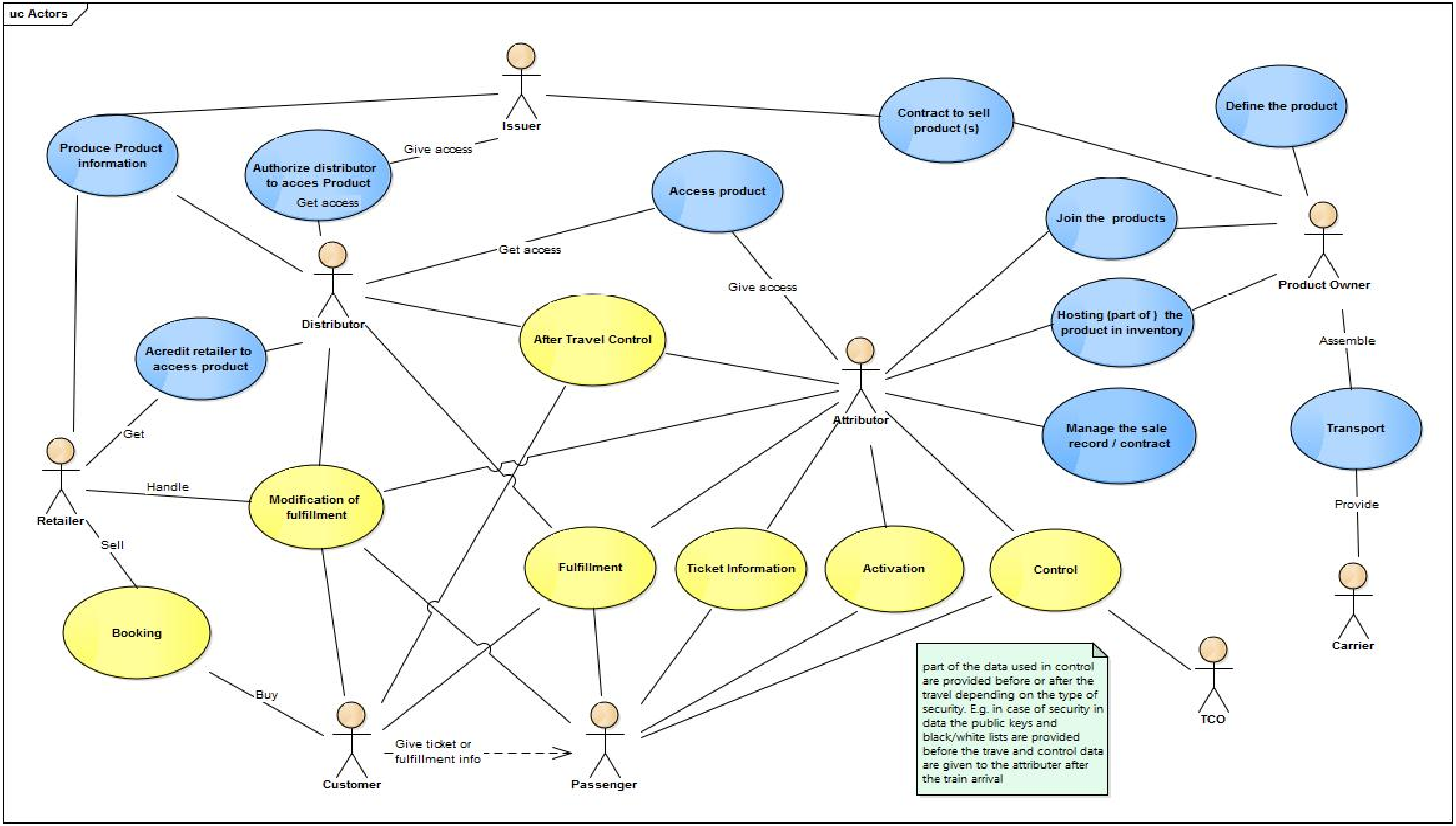
> From October 2013 to July 2015 :

- workshops took place to define “Opportunities for mobile Ticketing URT Part 1&2 Technical Report V1.1 18.08.2015
- 21 working groups experts from 13 Railways contributed.
- ÖBB, TCDD, DB, JR, NSB, BeNeRail, Masabi, CFR, TCDD, RZD, Linkon and CFF-SBB presented their mobile ticketing solutions.

> Part 1&2, 30 pages specification defines :

- **Seven** main business processes needed for interoperable ticketing
- **Thirteen** ticketing messages are defined

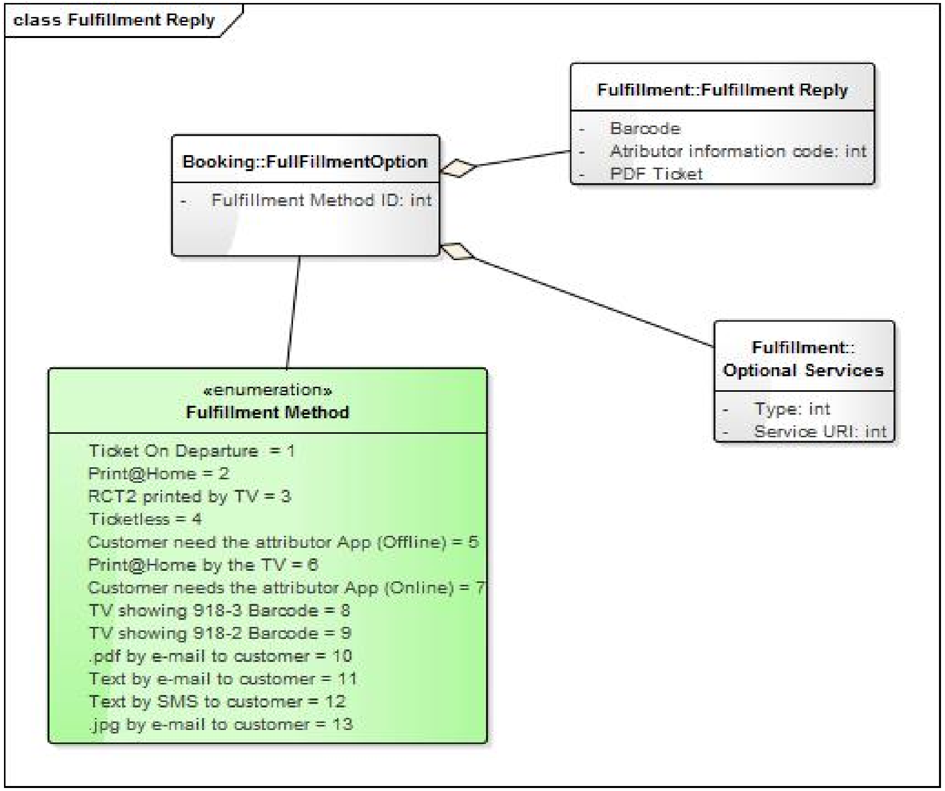
URT (Universal Rail Ticket)



part of the data used in control are provided before or after the travel depending on the type of security. E.g. in case of security in data the public keys and black/white lists are provided before the trave and control data are given to the attributer after the train arrival

URT (Universal Rail Ticket)

- Example: the fulfillment reply message



class Fulfillment Reply

Fulfillment::Fulfillment Reply

- Barcode
- Atributor information code: int
- PDF Ticket

Booking::FullFillmentOption

- Fulfillment Method ID: int

Fulfillment::
Optional Services

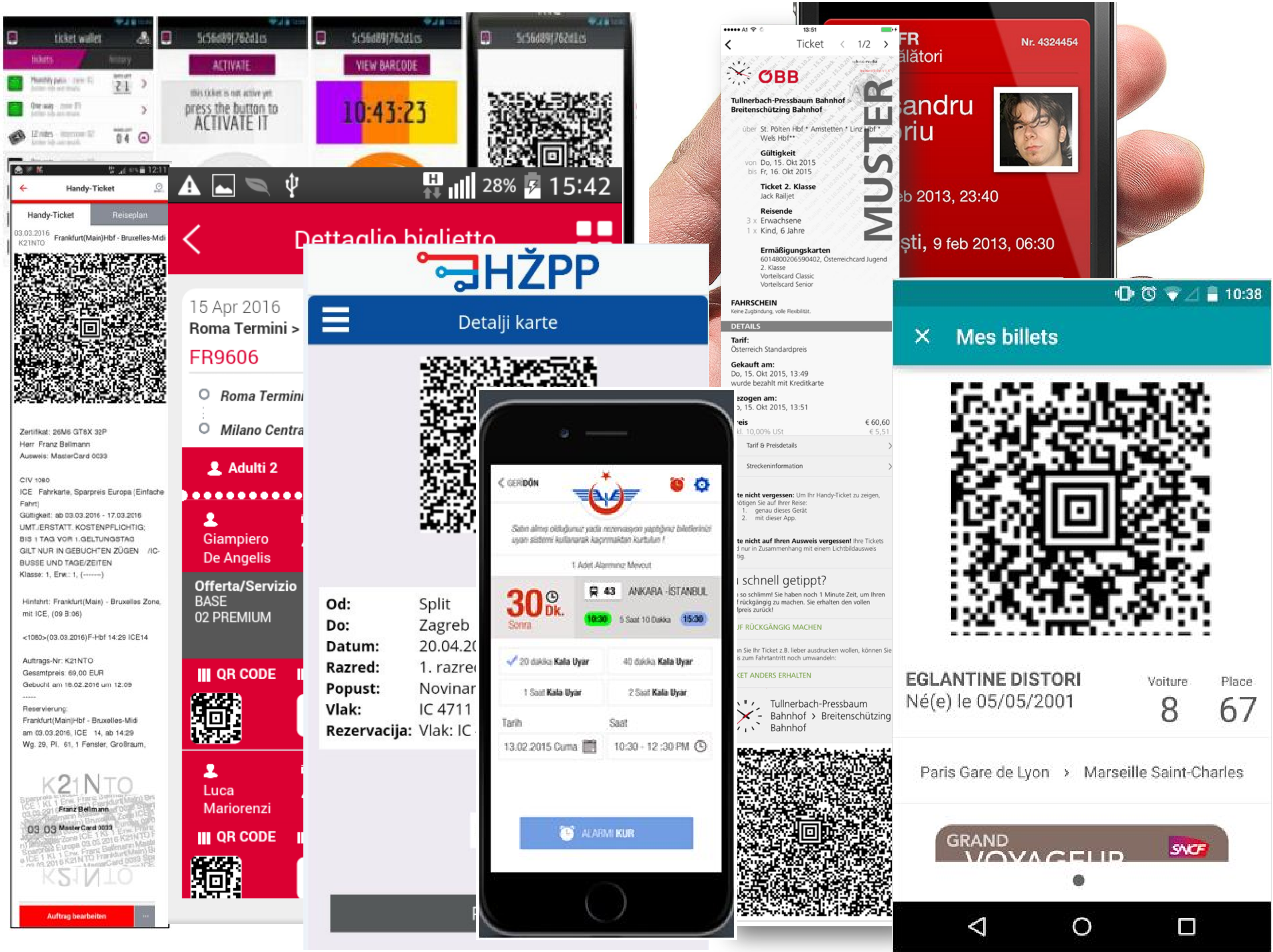
- Type: int
- Service URI: int

«enumeration»
Fulfillment Method

Ticket On Departure = 1
Print@Home = 2
RCT2 printed by TV = 3
Ticketless = 4
Customer need the attributor App (Offline) = 5
Print@Home by the TV = 6
Customer needs the attributor App (Online) = 7
TV showing 918-3 Barcode = 8
TV showing 918-2 Barcode = 9
.pdf by e-mail to customer = 10
Text by e-mail to customer = 11
Text by SMS to customer = 12
.jpg by e-mail to customer = 13

RTS (Rail Ticket on Screen)

- Eight meetings took place from November 2015 to August 2016. The RTS layout is defined based on 12 existing Railways App.



ticket wallet

tickets history

ACTIVATE

this ticket is not active yet
press the button to
ACTIVATE IT

VIEW BARCODE

10:43:23

Handy-Ticket

Handy-Ticket | Reiseplan

03.03.2016
K21NTO
Frankfurt(Main)Hbf - Bruxelles-Midi

Zertifikat: 26M6 GT8X 32P
Herr Franz Bellmann
Ausweis: MasterCard 0033

CIV 1080
ICE Fahrkarte, Sparpreis Europa (Einfache Fahrt)
Gültigkeit: ab 03.03.2016 - 17.03.2016
UMT./ERSTATT. KOSTENPFLICHTIG;
BIS 1 TAG VOR 1.GELTUNGSTAG
GILT NUR IN GEBUCHTEN ZÜGEN /IC-BUSSE UND TAGE/ZEITEN
Klasse: 1, Erw.: 1, (-------)

Hinfahrt: Frankfurt(Main) - Bruxelles Zone, mit ICE, (09 B 06)

<1080>(03.03.2016)F-Hbf 14:29 ICE14

Auftrags-Nr: K21NTO
Gesamtpreis: 69,00 EUR
Gebucht am 18.02.2016 um 12:09

Reservierung:
Frankfurt(Main)Hbf - Bruxelles-Midi
am 03.03.2016, ICE 14, ab 14:29
Wg. 29, Pl. 61, 1 Fenster, Großraum,

K21NTO
Franz Bellmann
03 03 MasterCard 0033

Auftrag bearbeiten

28% 15:42

Dettaglio biglietto

15 Apr 2016
Roma Termini >
FR9606

○ Roma Termini
○ Milano Centra

Adulti 2

Giampiero
De Angelis

Offerta/Servizio
BASE
02 PREMIUM

QR CODE

Luca
Mariorenzi

QR CODE

HŽPP

Detalji karte

Od: Split
Do: Zagreb
Datum: 20.04.20
Razred: 1. razre
Popust: Novinar
Vlak: IC 4711
Rezervacija: Vlak: IC

GERİDÖN

Satın almış olduğunuz yada rezervasyon yaptığınız biletlerinizi uyarı sistemi kullanarak kaçırmaktan kurtulun !

1 Adet Alarmınız Mevcut

30 Dk.
Sonra

43 ANKARA -İSTANBUL

10:30 5 Saat 10 Dakika 15:30

✓ 20 dakika Kala Uyar
40 dakika Kala Uyar
1 Saat Kala Uyar
2 Saat Kala Uyar

Tarih
13.02.2015 Cuma

Saat
10:30 - 12 :30 PM

ALARMI KUR

13:51

Ticket 1/2

ÖBB

MUSTER

Tullnerbach-Pressbaum Bahnhof > Breitenschützing Bahnhof

über St. Pölten Hbf * Amstetten * Linz Hbf * Wels Hbf**

Gültigkeit
von Do, 15. Okt 2015
bis Fr, 16. Okt 2015

Ticket 2. Klasse
Jack Railjet

Reisende
3 x Erwachsene
1 x Kind, 6 Jahre

Ermäßigungskarten
6014800206590402, Österreichcard Jugend 2. Klasse
Vorteilscard Classic
Vorteilscard Senior

FAHRSCHEIN
Keine Zugbindung, volle Flexibilität.

DETAILS

Tarif:
Österreich Standardpreis

Gekauft am:
Do, 15. Okt 2015, 13:49
wurde bezahlt mit Kreditkarte

ezogen am:
, 15. Okt 2015, 13:51

reis € 60,60
kl. 10,00% USt € 5,51

Tarif & Preisdetails

Streckeninformation

te nicht vergessen: Um Ihr Handy-Ticket zu zeigen, nötigen Sie auf Ihrer Reise:
1. genau dieses Gerät
2. mit dieser App.

te nicht auf Ihren Ausweis vergessen! Ihre Tickets d nur in Zusammenhang mit einem Lichtbildausweis tig.

schnell getippt?
so schlimm! Sie haben noch 1 Minute Zeit, um Ihren f rückgängig zu machen. Sie erhalten den vollen fpreis zurück!

JF RÜCKGÄNGIG MACHEN

n Sie Ihr Ticket z.B. lieber ausdrucken wollen, können Sie is zum Fahrtantritt noch umwandeln:

KET ANDERS ERHALTEN

Tullnerbach-Pressbaum Bahnhof > Breitenschützing Bahnhof

FR
ălători

Nr. 4324454

sandru
riu

eb 2013, 23:40

ști, 9 feb 2013, 06:30

10:38

Mes billets

EGLANTINE DISTORI
Né(e) le 05/05/2001

Voiture
8

Place
67

Paris Gare de Lyon > Marseille Saint-Charles

GRAND VOYAGEUR

SNCF

RTS (Rail Ticket on Screen)

Part 1: The Barcode

The RTS security relies on the barcode, The barcodes are defined in UIC leaflet 918.9.

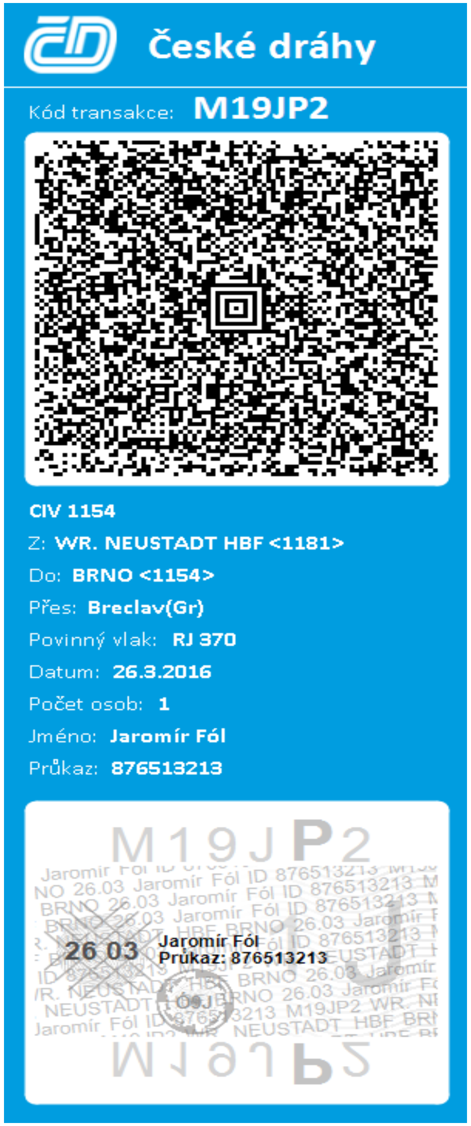
Part 2: The ticket information labels

These data are intended as information for the client. These information are defined in UIC leaflet 918.8.

	Field Name
Main information	Basic trip Information for the client to select the right ticket
Passenger Information	The passenger identification
Ticket ID	Ticket identification
Detail Information	Detail trip information on the route or trains to take.
Administrative Information	Activation, tariff, legal information

Part 3: The visual security element

This is a free open zone to be used by the RU for security.



České dráhy

Kód transakce: M19JP2

CIV 1154

Z: WR. NEUSTADT HBF <1181>

Do: BRNO <1154>

Přes: Breclav(Gr)

Povinný vlak: RJ 370

Datum: 26.3.2016

Počet osob: 1

Jméno: Jaromír Fól

Průkaz: 876513213

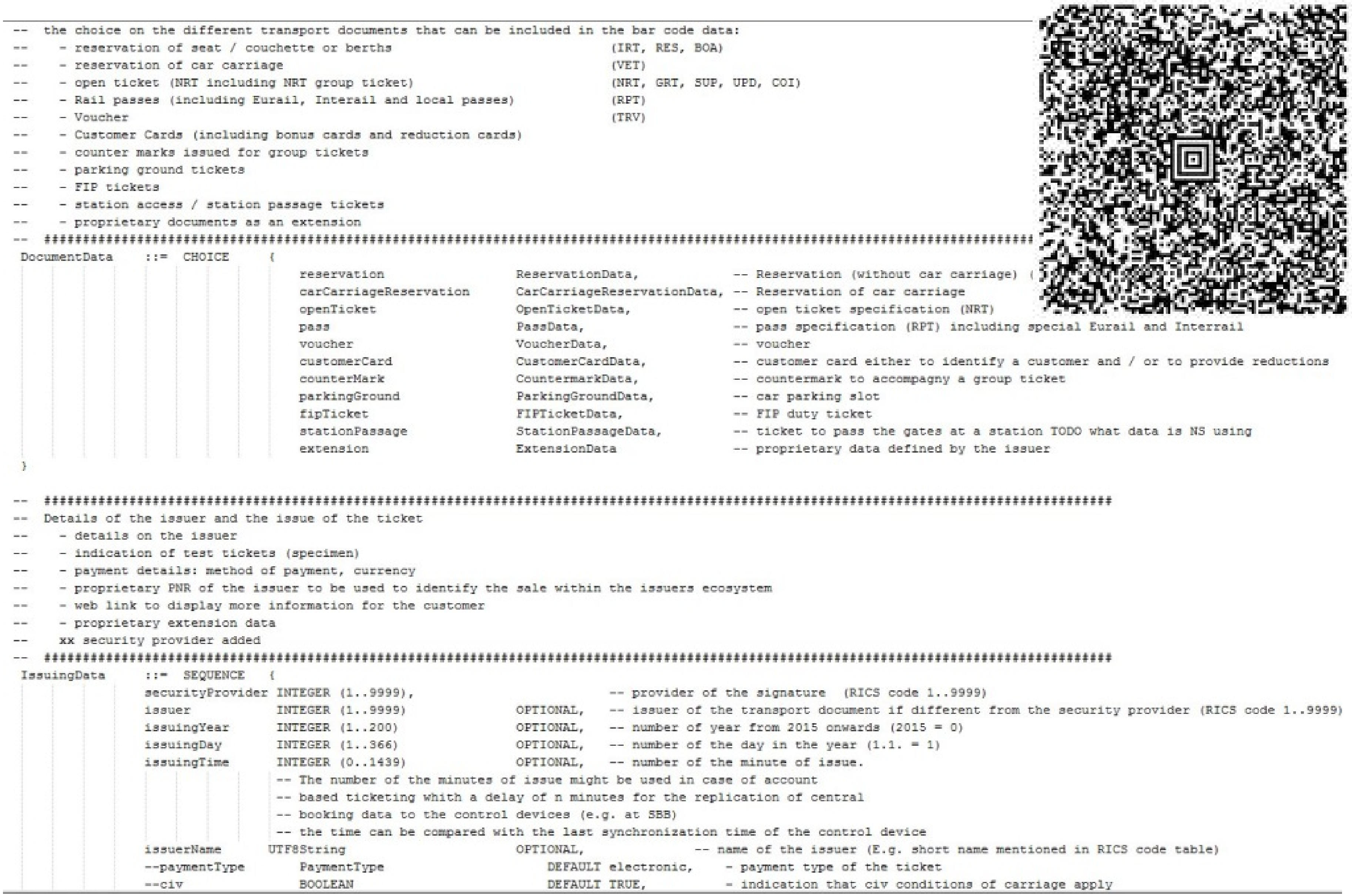
FCB (Flexible Content Barcode)

- All rail tickets types are possible
- Ticket type combination is possible in the same barcode (IRT + Parking access or NRT + IRT)
- The barcode security relies in the seal
- The limitation is the Barcode size to display

FCB (Flexible Content Barcode)

- Hundreds of fields are possible so most data are "optional“. The solution is to "tag" the info itself: each element has a tag, like in XML.
- The FCB is machine readable/interpretable.
- The FCB is encoded in ISO 8824 (ASN.1 / PER)

FCB (Flexible Content Barcode)



```
--  the choice on the different transport documents that can be included in the bar code data:
--    - reservation of seat / couchette or berths                             (IRT, RES, BOA)
--    - reservation of car carriage                                           (VET)
--    - open ticket (NRT including NRT group ticket)                          (NRT, GRT, SUP, UPD, COI)
--    - Rail passes (including Eurail, Interail and local passes)             (RPT)
--    - Voucher                                                               (TRV)
--    - Customer Cards (including bonus cards and reduction cards)
--    - counter marks issued for group tickets
--    - parking ground tickets
--    - FIP tickets
--    - station access / station passage tickets
--    - proprietary documents as an extension
--  ############################################################################################################################################
 DocumentData    ::=  CHOICE     {
                                    reservation                 ReservationData,            -- Reservation (without car carriage) (
                                    carCarriageReservation      CarCarriageReservationData, -- Reservation of car carriage
                                    openTicket                  OpenTicketData,             -- open ticket specification (NRT)
                                    pass                        PassData,                   -- pass specification (RPT) including special Eurail and Interrail
                                    voucher                     VoucherData,                -- voucher
                                    customerCard                CustomerCardData,           -- customer card either to identify a customer and / or to provide reductions
                                    counterMark                 CountermarkData,            -- countermark to accompagny a group ticket
                                    parkingGround               ParkingGroundData,          -- car parking slot
                                    fipTicket                   FIPTicketData,              -- FIP duty ticket
                                    stationPassage              StationPassageData,         -- ticket to pass the gates at a station TODO what data is NS using
                                    extension                   ExtensionData               -- proprietary data defined by the issuer
 }

--  ############################################################################################################################################
--  Details of the issuer and the issue of the ticket
--    - details on the issuer
--    - indication of test tickets (specimen)
--    - payment details: method of payment, currency
--    - proprietary PNR of the issuer to be used to identify the sale within the issuers ecosystem
--    - web link to display more information for the customer
--    - proprietary extension data
--    xx security provider added
--  ############################################################################################################################################
 IssuingData     ::=  SEQUENCE   {
                 securityProvider INTEGER (1..9999),                         -- provider of the signature  (RICS code 1..9999)
                 issuer           INTEGER (1..9999)             OPTIONAL,    -- issuer of the transport document if different from the security provider (RICS code 1..9999)
                 issuingYear      INTEGER (1..200)              OPTIONAL,    -- number of year from 2015 onwards (2015 = 0)
                 issuingDay       INTEGER (1..366)              OPTIONAL,    -- number of the day in the year (1.1. = 1)
                 issuingTime      INTEGER (0..1439)             OPTIONAL,    -- number of the minute of issue.
                                  -- The number of the minutes of issue might be used in case of account
                                  -- based ticketing whith a delay of n minutes for the replication of central
                                  -- booking data to the control devices (e.g. at SBB)
                                  -- the time can be compared with the last synchronization time of the control device
                 issuerName      UTF8String                     OPTIONAL,             -- name of the issuer (E.g. short name mentioned in RICS code table)
                 --paymentType        PaymentType                    DEFAULT electronic,    - payment type of the ticket
                 --civ                BOOLEAN                        DEFAULT TRUE,          - indication that civ conditions of carriage apply
```

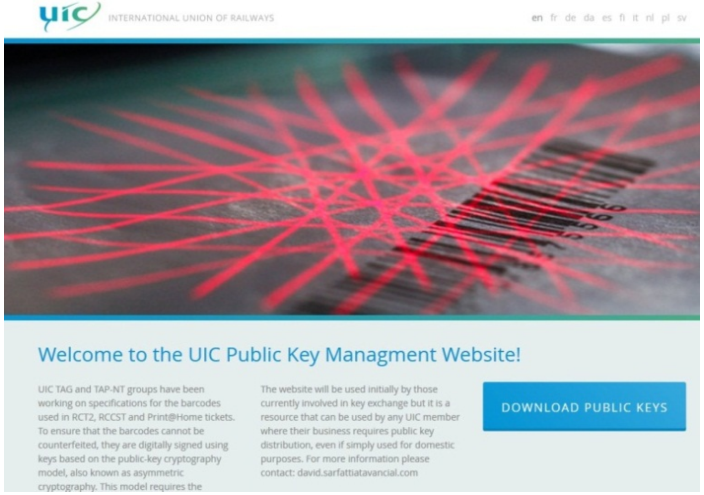
Barcode Seal

- The first step is the generation of the two keys (private/public). This process takes place once every 18 months, in the distribution system.
- To generate the encrypted seal :
  - All data in the Header and Open Data fields are hashed with the (SHA-2, 224) Algorithm
  - the result is encrypted with the private key of the DSA 2048 asymmetric cryptosystem (private-public key).
- To decrypt the seal :
  - The reading device need the barcode structure and the public key.

Private key is a cryptographic key that is uniquely associated with a public key and is not made public. The private key is used to compute the corresponding public key and to compute a digital signature that may be verified by the corresponding public key. The private key is only known and generated by computer. No railway personal can access the private key.
Public key is a cryptographic key that is uniquely associated with a private key. It may be made public. The public key may be known by anyone and may be used to verify a digital signature that is signed by the corresponding private key.

UIC Public Key Management Website

- The website to download public keys is in production since April 2014
- UIC upload the Rail Distributor public keys following a secured procedure
- Today available public keys are: SNCB, NS, CFL, SNCF, OBB and ZSSK
- http://railpublickey.uic.org


INTERNATIONAL UNION OF RAILWAYS
en fr de da es fi it nl pl sv
DOWNLOAD PUBLIC KEYS

Welcome to the UIC Public Key Managment Website!

UIC TAG and TAP-NT groups have been working on specifications for the barcodes used in RCT2, RCCST and Print@Home tickets. To ensure that the barcodes cannot be counterfeited, they are digitally signed using keys based on the public-key cryptography model, also known as asymmetric cryptography. This model requires the

The website will be used initially by those currently involved in key exchange but it is a resource that can be used by any UIC member where their business requires public key distribution, even if simply used for domestic purposes. For more information please contact: david.sarfattiatavancial.com

UIC Control APP

- It is an Android implementation in open source code to control Barcodes.

  Code should be free of access. The app would download the public keys and control all UIC barcodes.
- In March 2016, NS implements the App to be available to UIC in December 2016.

UIC PRISM

- Today most of European railways have already implemented high tech mobile e-tickets. But each railways system is not compatible with its neighbour.

UIC PRISM

- PRISM is the UIC Proof of Concept (PoC) for all standards stated in this presentation.

- The objective is to make sure there are efficient tested and proven versions of the following interoperable specifications:
  - mobile ticket display format and behaviour
  - mobile ticket barcode and security model
  - fulfilment data in the booking message
  - validation data exchange formats
  - interoperable service level requirements

UIC PRISM

- Three pilots are in progress:
  - LINKON/SJ/DSB pilot, the work is waiting for the launch of the new DSB booking system before further moves can be made.
  - THALYS/NS/SNCB pilot, the draft pilot plan is ready.
  - HZPP/OBB/SZ pilot, since 1 July SZ and HZPP have been using the ÖBB Aztec-Code-Reader app for checking international NRT barcodes on the Vienna-Zagreb route.

Thank you for your kind attention

David SARFATTI, UIC TAG Chairman
david.sarfatti@avancial.com

Summary

- Definitions
  - IRT, NRT, RPT, GRT, RES,…
  - SiP, SiD and SiS
- Paperless Standards
  - URT: Universal Rail Ticket
  - RTS: Rail Ticket on Screen
  - FCB: Flexible Content Barcode
- Existing UIC IT Solutions
  - UIC Public Key Management Website
  - UIC Control App
- Proof of Concept
  - PRISM Project