“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”)

  – 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 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)

> Example: the fulfillment reply message

```
+----------------+-------------------+
|     Booking    |   Fulfillment     |
|+----------------+-------------------+
|                |                   |
|    Option      |   Optional Services|
|+----------------+-------------------+
|   Fulfillment   |                   |
|Method ID: 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 S18-3 Barcode = 8
  TV showing S18-2 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.
# 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.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main information</strong></td>
<td>Basic trip Information for the client to select the right ticket</td>
</tr>
<tr>
<td><strong>Passenger Information</strong></td>
<td>The passenger identification</td>
</tr>
<tr>
<td><strong>Ticket ID</strong></td>
<td>Ticket identification</td>
</tr>
<tr>
<td><strong>Detail Information</strong></td>
<td>Detail trip information on the route or trains to take.</td>
</tr>
<tr>
<td><strong>Administrative Information</strong></td>
<td>Activation, tariff, legal information</td>
</tr>
</tbody>
</table>

## Part 3: The visual security element

This is a free open zone to be used by the RU for security.
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
  -- reservation of car carriage
  -- open ticket (NRT including NRT group ticket)
  -- Rail passes (including Eurail, Interail and local passes)
  -- Voucher
  -- 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, -- open ticket specification (RPT) including special Eurail and Interrail
  voucher VoucherData, -- voucher
  customerCard CustomerCardData, -- customer card either to identify a customer and / or to provide reductions
  counterCard CounterCardData, -- counter card to accompany 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 {
  issuingProvider 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 with 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 OPTIONAL, -- 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](http://railpublickey.uic.org)
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.
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