EUROPEAN UNION AGENCY FOR RAILWAYS

Making the railway system
work better for society.

Technical document

DIGITAL SECURITY ELEMENTS FOR RAIL PASSENGER TICKETING

In the Document History table, version are identified as x.n where
"x" is a correlative number assigned to an approved version when reaching a main milestones
"n" is a correlative number assigned to draft versions, starting by 1. "n"=0 means version approved
Information related to previous draft versions (i.e. 0.1, 0.2 etc.) shall be deleted from the table when a subsequent approved version is issued.

Document History

Version	*Date*	*Comments*
2.0	10.01.2020	Initial draft V 2.0
	26.06.2020	Correction of Record length for the U_FLEX data structure

Contents

Application:

With effect from 08 March 2012.

All actors of the European Union falling under the provisions of the TAP TSI.

1. Summary - relation with other leaflets

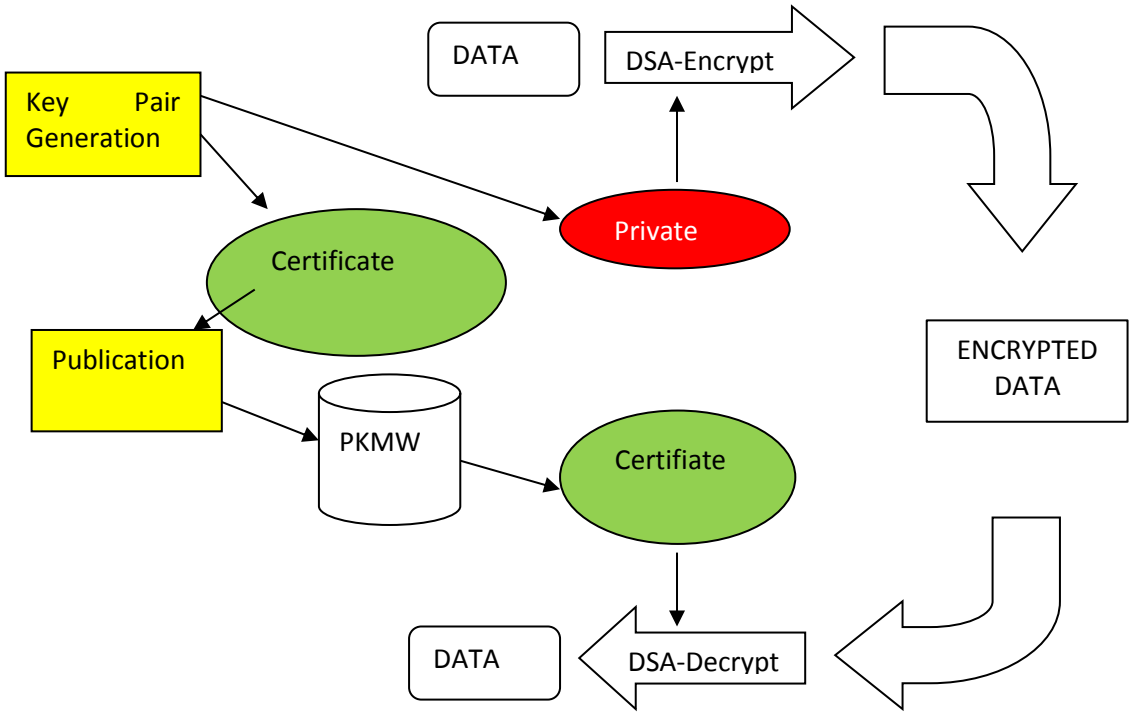
Railway ticketing used to be protected for years by SiP (Security in Paper) mechanisms. In this kind of ticketing, the security was organized by using specific paper, making it impossible for others than issuers to print tickets and for nobody to modify existing ones.

In international ticketing, the security background is - together with legal and functional specifications, the framework for checking, cancellation and after-sales sevices - defined by CIT and the layout of the tickets is defined by the Agency, both to make sure the tickets can be recognized by all railway companies involved.

Security in Paper has some limitations: tickets must be printed on specific printers with a stock of specific secured paper applying a ticket stock management control, making it not easy to sell tickets over the internet (fulfilment issues). Security in Paper has, on the other side, the advantage that the contract is unique and cannot be duplicated. All status changes of the ticket can be printed on the ticket itself, making these amendments on the original contract.

Modern ticketing systems using SiD (Security in Data), are not only defined by the layout (being recognized by all TCO's involved), but also by the security elements. These security elements allow TCO's to check that the content has not been created or modified by others than RU's. The reading/check must be possible without giving the party checking the ticket, rights to create the security elements. For this purpose, a so-called asymmetrical security algorithm is used.

In the figure below, a schematic description explains how it works:

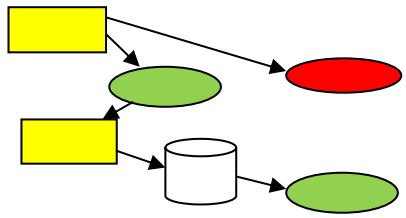


The whole security system is based on asymmetrical key pairs: Private and Public keys. To ensure the autenthicy of the public keys the keys shall be certified by a certification authority and the certificates exchanged for the ticket control precedures.

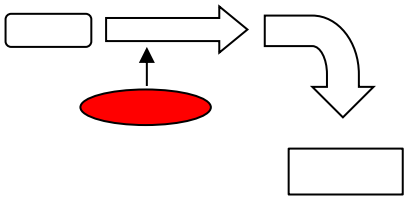
These keys are generated on a regular base (e.g. every 6 months) by the party that wants to encrypt data using such a key ("the security provider"). To enable decryption of the encoded data, the corresponding certificate should be made available to every TCO (Ticket Controlling Organisation). For the distribution of these certificates, the TAP TSI architecture has to be used.

In this part (see right) of the schematic above, the mechanism of key pair generation is shown.

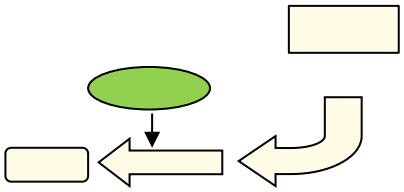
This action takes place on a regular base (e.g. once or twice a year). The security provider will use a specific key (the message header contains the reference of the key used). This key is published according to the TAP TSI architecture to be used by all TCO.



In this part (see right) of the scheme, the encryption mechanism using the private key generation is shown.



Finally, this part of the drawing (see right) shows the decryption, using the certificate.



From now on in this document, there will be "security provider" to indicate the ticket issuer (issuing undertaking), retailer, allocator, ticket vendor or any other party/company that is generating the barcode/security element to be checked by the TCO.

TAP TSI TD B.11 and TAP TSI TD B.12 together define both layout and security elements in (railway) ticketing.

This document (TAP TSI TD B.12) describes the different security elements, used in (international) ticketing.

The layout of the tickets and thus the place where the security-elements appear, is defined in the leaflet TAP TSI TD B.11.

Since some trains are run by one carrier, but the check on board is done by another carrier or more than one carrier, the “TCO” or "Ticket Controlling Organisation" is often used in this standard. A TCO is any organisation which can control a passenger's ticket before, during or after a given journey (or part of it). In most cases this organisation will be a carrier or a subcontractor of a carrier.

A company can only sell international tickets if there are agreements ensuring that every TCO can accept the security elements. For security-elements like barcodes this is the only way to make sure the TCO's are able to read and check the security-element (both because of technical limitations and because of electronic keys).

The TAP TSI technical documents B.6 (RCT-2 ticket layout) and B.7 (home-print tickets) are replaced by TAP TSI technical documents B.11 (ticket layouts) and B.12 (Digital Security Elements for Rail Passenger Ticketing), where the first one is dealing with layouts only and the second one with the security elements. The reason for this so-called "reshuffle" is that al lot of security elements can appear on multiple distribution channels and on multiple ticket modes (paper, screen, secured paper, ...). Since security elements are in constant evolution, upgrades can be done to the security element description without having to change it in multiple leaflets at the same moment.

Older security mechanisms that are no longer in use (magnetic stripe, TLB with Carrier Makes Certificate mechanism and TLB with Carrier Keeps Contract mechanism) are not integrated in this technical document B.12.

2. Generalities about Security Elements in Ticketing

The terms "Passenger" and "Customer" are used in this Document. They can be one and the same person but not necessarily. For example a passenger may take an international train journey using a ticket that was bought by his/her firm. In that case the firm is the customer. There definitions can also be found in the ticketing manual of CIT and in the URT document of UIC.

It is necessary to distinguish between the customer who buys the ticket and the passenger who is travelling. If several passengers are travelling together, either one passenger will be defined as "head of the group", holding the group ticket, or each passenger is defined as being an individual passenger, each with his/her own ticket (his/her own security elements). So either the personal data of the “head of the group” or the personal data of the passenger will be used to generate the security certificate(s) (in case personal data is used).

The security provider communicates with the customer in order to produce a ticket. For this purpose, they exchange the same information as when the client buys his/her ticket at a selling point. The security provider can compose a ticket autonomously or through a connection with the different distributors / different reservation systems necessary for creating the ticket.

A security element should be secured/protected against fraud. To achieve this, either encryption or sealing can be used. Since the data itself is not secret at all (in most cases it is even printed in clear text on the ticket), sealing is the mechanism used making all the ticket data readable (not encrypted).

"Sealing" means that the data itself is not encrypted, the data is expanded with a digital signature (which is an encrypted fingerprint of the data), unique for the set of data it "protects". As a result of this, the ticket data cannot be modified without invalidating the seal (the signature included in the security element will not be compliant with the modified data) – “authentication”. This mechanism makes it possible to check the ticket data already while the decryption calculation is conducted. This can speed up the procedure significantly.

The power of security in data depends heavily on the encryption used in the digital signature (The data elements of the ticket are translated in the signature, unique for this data. This signature is encrypted, using a powerful asymmetrical encryption mechanism: the key used to encrypt the data cannot be calculated out of the key for the decryption.

The procedure of selling SiD-tickets is identical to the procedure of selling a SiP-ticket and is therefore not a part of this standard. The standard deals only with the last phase of the procedure (the fulfilment, more in detail the protection of the representation of the contract).

Phase 1: The client books his/her ticket from the issuer via the Internet.

Phase 2: For this trip one or more security elements are generated. Each TCO must be able to check the validity of the part of the trip it is responsible for. To achieve this, multiple security elements can be combined in one ticket.

Since the total amount of data to be represented in the security element is like 100 bytes or more, 1D (one dimensional) barcodes are not possible. The solution is to use 2D barcodes (AZTEC or PDF 417 are both widely used in rail, QR-codes are not common in rail ticketing because of technical limitations).

AZTEC is the better one of both because of error-correction, readability in difficult conditions and the fact that it is more variable in size. The reason that the PDF417 barcode (a so called “Stacked linear

barcode") is still in the leaflet, is because there are a lot of applications in use in both airline and railway ticketing using these barcodes. The technology used, both for printing and reading these PDF417 barcodes is using older technology. Those printers and readers are often not able to print / read AZTEC barcodes. As mentioned above, the PDF417 is a "stacked linear" barcode, this means that the complete barcode is a composition of 1D barcodes; all stacked one on top of the other.

Aztec:

PDF417:

QR code:

(not used in international Rail Ticketing)

3. Transformation of data elements into barcodes

The functional steps to translate data (both ticket data and security elements in Alphanumerical, Numerical or Binary format) are the following ones (the UIC-document UIC SSB Implementation Guide explains in detail how a dataset has to transformed into an AZTEC SSB barcode, the transformation into TLB or FCB AZTEC barcodes is done following the same mechanism.)

Step 1: Collection of data elements defining the ticket (local representation of the data in the sales application) : Java, C++, ASCII, UTF-8, EBCDIC, …

Step 2: Translate this data collection in the data structures, as defined in this document, in the specific chapter about the barcode to be used (SSB, TLB, FCB) + create the seal as defined in the same chapter. Translation of Alphanumerical data is done differently in SSB (ASCII-6) than in TLB&FCB (ASCII-8) due to binary size limitation.

Step 3a: Encode the binary chain into the AZTEC binary content ("AZTEC encoding").

Step 3b: Translate this binary string in a graphical representation of the barcode (including error-correction data).

4. General Mechanism for creating security elements

4.1. Introduction: "asymmetric key cryptography"

The security provider generates a security element locally by using private/public key cryptography (“asymmetric key cryptography”). This will result in a certificate that is larger than the certificate obtained by using a symmetric key. A method with a symmetric key is never used in this context to avoid that encryption keys have to be distributed and might get stolen.

A stolen key still has to be used for months because of pre-sold tickets still using the old key.

An alphanumeric presentation will, because of the size of the seal, not be useful and for the same reason, neither a one-dimensional barcode can be used. The best possible solution to integrate these data in the paper ticket is a two-dimensional barcode.

The standard will describe the mechanism the different concerned companies will have to follow in creating and checking security elements.

The seal, used in the security element, is an encrypted hash code, calculated from the open data in the message (a so-called “encrypted fingerprint”).

This “encrypted fingerprint” mechanism, is a 2-step process. First step, a unique fingerprint is generated for the set of data to be protected (changing any data results in another fingerprint). The mechanism used for this is a public available algorithm (SHA-2), to be used by all railway ticketing related companies. In the second step, this fingerprint is encrypted, also using a public available algorithm with a private key (from the security provider). This result is the so-called “seal”. The use of the asymmetric algorithm makes it impossible to generate a new seal without the private key. The combination of the 2 public available algorithms and the use of the private key generates the necessary security against fraud.

4.2. Composition of the data

In the security element, generally a barcode, the data is often grouped in 3 logical groups: a header, the ticket data and a signature.

The ticket data is the data that has to be translated in a barcode. The different chapters define how the data has to be coded or represented. (Also called “open data”)

The header makes it possible for a reader to find out which encoding is used, thus how the barcode data should be interpreted and also which (public) keys should be used to check the key.

Finally, the seal is a digital signature, preventing non-recognized railway companies to generate or modify barcodes.

The different data in a security element can be grouped like this:

HEADER

- indicating:
  - which kind of barcode
  - which security provider (often "issuer")
  - which version
- (all of this for retrieving the right public key), and possibly which ticket type (for fixed-field barcodes - SSB, ELB).

OPEN DATA

- containing all the necessary ticket info.
- "Open" means that the info is not encrypted and can be interpreted directly, without any additional action.
- If data is structured, it can be by bit-position (SSB, ELB) or by (logical) tagging (FCB)
- data can be a translation of the layout of the ticket (TLB)

SIGNATURE / SEAL

- to detect fraud.

This is a generic way of presenting the data. In some cases, information can be combined in a bigger block (e.g. the signature can be part of the header).

5. Hash Code generation - "signature" / "encrypted seal"

5.1. General Mechanism

Encryption process is a 2 phases process:

- hash all data in the Header field and Open Data field with the SHA-2 xxx Algorithm.
- and then, to crypt the result with the DSA yyyy asymmetric cryptosystem (private-public key).

The output (called the "signature", "encrypted seal" or the "encrypted fingerprint of the data") is containing 2 (big) integer numbers, called "r" and "s" (so defined signature in the FIPS-186 standards, defining DSA).

5.2. Different versions + Size of the seal

This process is defined as (SHA-xxx, DSA-yyyy). The seal obtained is zz bytes long.

Mechanisms used in international railway ticketing are:

PROCESS	Xxx (bits)	Yyyy (bits)	Zz (bytes)	Zz (bytes, structured ASN-1)
SHA-160,DSA-512	160	512	(2x) 20	46
SHA-160,DSA-1024	160	1024	(2x) 20	46
SHA-224,DSA-2048	224	2048	(2x) 28	62
SHA-256,DSA-2048	256	2048	(2x) 32	70

NIST documents “FIPS PUB 180-4” and “FIPS 186-4” define that (SHA-160,DSA-512) and (SHA-160,DSA-1024) can be used for legacy purposes only and (SHA-224,DSA-2048) and (SHA-256,DSA-2048) can be used up to 2030.

The ASN-1 structure adds 6 bytes of data to the actual security elements (r,s). 1byte, indicating the message itself, 1 for the length, then for each of the 2 elements, 1 byte indicating that the number is an integer and 1 indicating the length of the integer (source: ITU X.509).

PROCESS	SSB	Size	TLB,FCB (V1)	Size	TLB,FCB (V2)	Size
SHA-160,DSA-512	S	46				
SHA-160,DSA-1024	S (*)	46	S (*)	46		
SHA-224,DSA-2048	2 (**)	2x28			2 (**)	2x28
SHA-256,DSA-2048					2 (**)	2x32

“S” means Structured, “2” means 2 different integers (r and s).
(*): commonly used today (Sep 2017); (**): Recommendation (up to 2030)

In TLB & FCB in the first version (header #UT version 1), SHA1 (1024,160) or SHA1 (512,160) are used. In TLB & FCB, in the second version (header #UT version 2), SHA2 (2048,224) or SHA2 (2048,256) are used. In SSB, SHA1 (512,160), SHA1 (1024,160) or SHA2 (2048,224) are used. In the case of the SHA2 (2048,224), there is not enough space in the barcode to put the signature in a structured format, but

there is a possibility to store the signature as 2 separate numbers (r and s), where r is the first number and s the second.

In case the seal is stored as 2 separate numbers, the total size (e.g. 56 for SSB) is split in 2 (thus 28 for SSB) second number

5.3. Generating the Seal - Step by step

The first step to make is the Key generation of the two keys (private / public). This process takes place at least once every 18 months, in the security provider distribution system.

The 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 a digital signature that can only be verified by the corresponding public key. The private key is only known and generated by the computer which generates the key pair (private – public key). No (railway) staff should have access to the private keys.

The 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 was signed by the corresponding private key.

To ensure the authenticity of the published public key, the key shall be approved by a certification authority, proving that the public key has been created by the railway undertaking indicated in the key.

Publishing the certificate (TAP TSI architecture) is needed (see the separate document "TAP TSI ANNEX B.60 TAP RETAIL ARCHITECTURE") and will not harm the security.

Then for every barcode ticket the following steps are conducted

5.3.1. Hashing the data (header and open data) in SHA - xxx

SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512) designed by the National Security Agency (NSA) and published in 2001.

A hash function is an algorithm that transforms (hashes) an arbitrary set of data elements into a single fixed length value (the hash). The computed hash value may then be used to verify the integrity of copies of the original data without providing any means to derive the source (irreversibly). A hash value therefore may be freely distributed or stored as it is only used for comparative purposes. SHA stands for Secure Hash Algorithm. SHA-2 includes a significant number of changes from its predecessor, SHA-1. SHA-2 consists of a set of four hash functions with digests that are 224, 256, 384 or 512 bits.

The security provided by a hashing algorithm is entirely dependent upon its ability to produce a unique value for any specific set of data. When a hash function produces the same hash value for two different sets of data then a collision is said to occur.

In 2005, security flaws were identified in SHA-1, namely that a mathematical weakness might exist, indicating that a stronger hash function would be desirable. Although SHA-2 bears some similarity to the SHA-1 algorithm, these attacks have not been successfully extended to SHA-2

5.3.2. Encryption of the Hash code with DSA yyyy (private key, hash value)

The Digital Signature Algorithm (DSA) is a Government standard (FIPS) for digital signatures. This patent is available from 1991 worldwide royalty-free.

The DSA algorithm is a cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that determining the private key from the public key is computationally infeasible.

5.3.3. The resulting seal - structured or not

The result is the seal (structured data, holding r (size zzz) and s (size zzz) or non-structured: 2 numbers r and s (both size zzz)) to be put in the dataset that will be translated in the Aztec (or PDF-417) barcode. Structure follows ASN.1 rules.

```
Dss-Sig-Value ::= SEQUENCE {
            r                                                   INTEGER,
            s       INTEGER  }
ASN.1                              DER                                encoding:

indication            Sequence                          1            Octet
length    of    sequence              1    Octet    up    to    128    byte
                               1  Octet  +  length  octets  in  case  of  more
content:
                                 first                                integer
                  indication        of        integer        1        Octet
               length      of      integer                    1..n      byte
                                                  content           octets
                                 second                               integer
                  indication        of        integer        1        Octet
              length     of     integer                  1..n     byte
                                content      octets
```

The growing computing power in new generation computers leads to the necessity to continuously increase security levels.

That's why it is recommended to use larger keys, i.e. 2048 bits instead of 1024 (next step after 1024 is 2048). This recommendation was already in the 918.2 ATBv2 specs in 2007.

However, developments went not as fast as expected, and DSA 2048 bits keys are not yet that common in the security environment. Some key generators support only creating key pairs up to 1024 bits for DSA.

In 2013, Microsoft (.Net) and Oracle (Java) standard software components do support DSA 2048 external provider security packages but these security packages could not have been yet agreed by railways undertakings.

The larger the keys are, the more computing power is needed both for the generation and the check of the keys.

It is therefore proposed to still allow DSA with 1024 bits keys (and SHA-224) in railway ticketing barcodes.

If, in due course, the Rail Undertakings will be capable to support 2048 bits keys, then the transition to these larger keys can be carried out smoothly.

The result of the whole operation is 2 numbers (r & s) that are stored in a structure (see last column) in the table. In some cases (limited space in the barcode) the structure can be skipped and the 2 numbers are stored the one after the other (first r, than s). This allows to win approximately 3 bytes. This is e.g. done in the SSB security elements.

5.4. Schematic representations of Seal Generation & Seal Verification

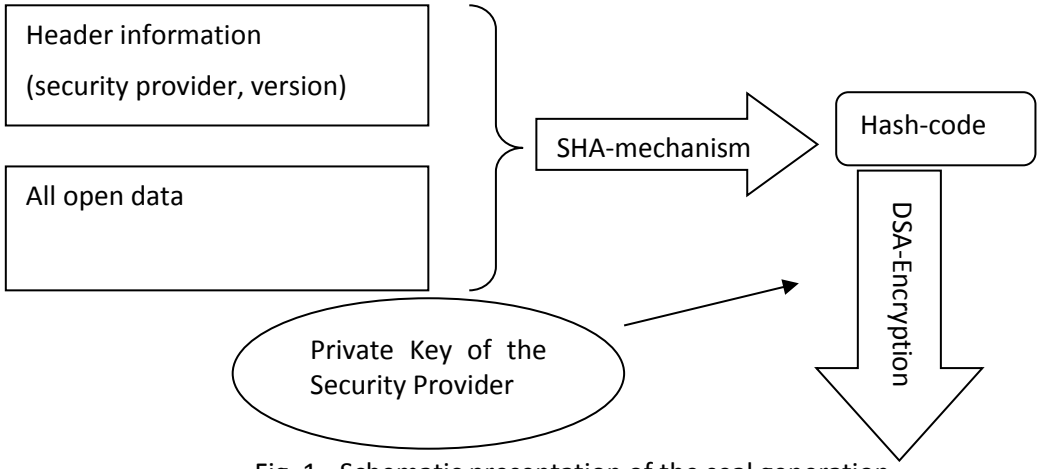


Fig. 1 - Schematic presentation of the seal generation

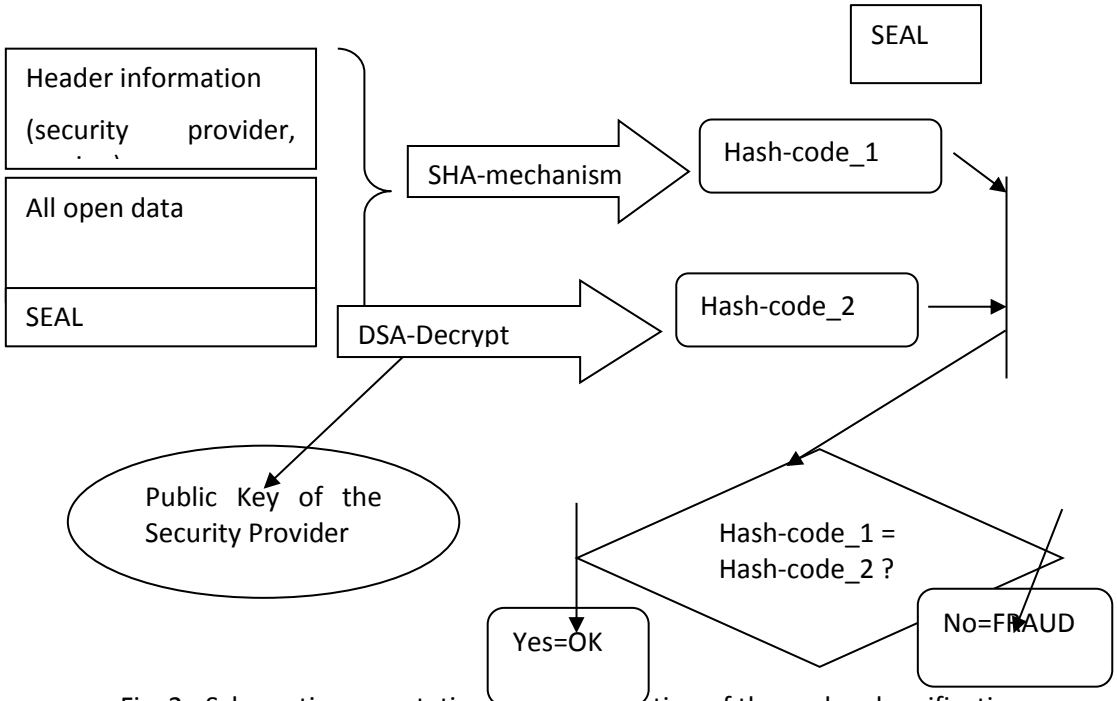


Fig. 2 - Schematic presentation of the decryption of the seal and verification

5.5. Public key exchange mechanism

The TCO must be able to receive in time the certificates of each security provider. Without this public key contained in the certificate, the ticket content of the barcode can be displayed, but it is impossible to check if the ticket is not a falsified one.

There is not necessary a fixed moment to change the keys (only a minimum frequency of changing is recommended: see below). A security provider can, in case of doubt, change the keys in between two regular changes. To inform all TCO's, a the TAP TSI retail architecture has to be used.

Issuing company should generate a private-public key at least every 18 month. The security provider should provide on the website its certificate at least 3 months before production, allowing the TCO to download them in advance.

“startDate” is the first possible day of travel.

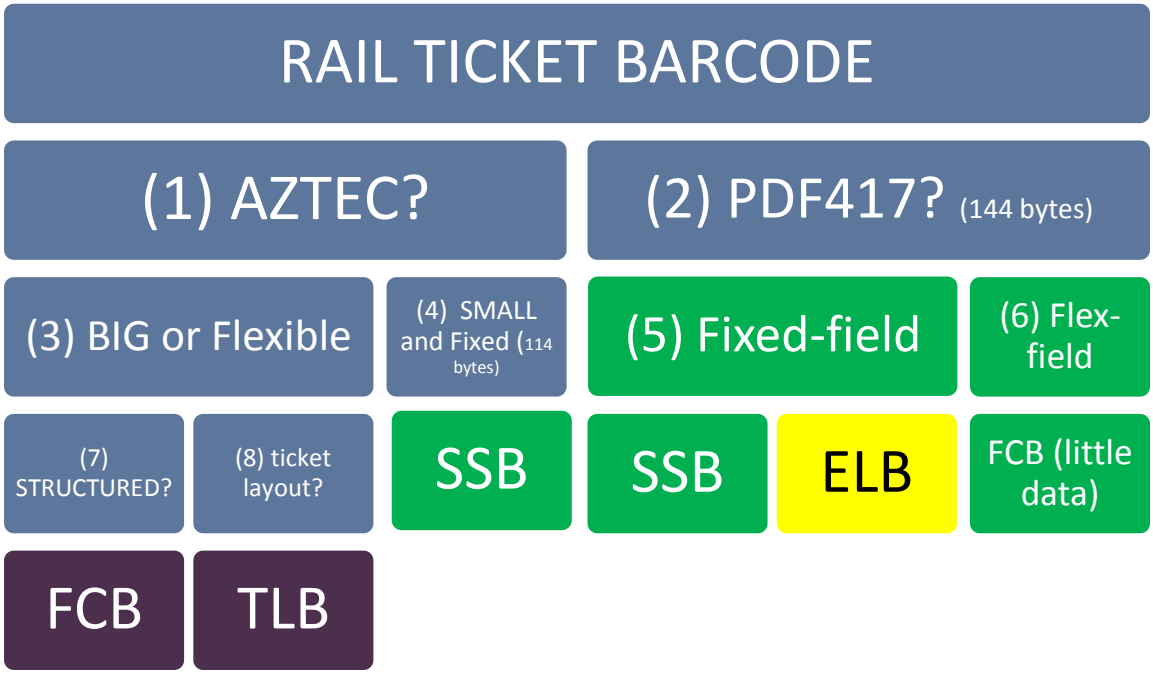
“endDate” , end date of the signature validity, is the last possible day of travel.

All details describing the processes to distribute the security provider's public keys to the ticket inspectors are defined in the application guide "TAP B 54 - Indirect Fulfilment Application Guide"

6. Different barcodes, used in international ticketing

Barcodes are always read by using a device (“machine readable”). The data, read by this device, can be either textual information (like ”Paris-Nord” or “28/02/2018”)called “human interpretable” or encoded (“8727100” or “59, 18”, holding the same info as above) called “machine interpretable” since code lists are needed.

SSB ***Small Structured Barcode*** (called “AZTEC V2” in the (old) 918-2V3 leaflet)
FCB ***Flexible Content Barcode*** (a recent developed 2D AZTEC barcode)
TLB ***Ticket Layout Barcode*** (called “DST barcode” in the (old) 918-3 leaflet)
ELB ***Element List Barcode*** (called “PDF 417” in the (old) 918-2V3 leaflet – used by SNCF)



SSB and ELB are made following a “fixed-field, fixed-size" data encoding mechanism
FCB and TLB are made following a “variable-field, variable-size” mechanism

Which barcode to be used by a security provider is depending on (external) parameters.

The above diagram should be read as follows: from top to bottom, and when in the level below there are 2 rectangles, a choice should be made. Parameters influencing the choices are described here:

(1), (2): The choice between AZTEC and PDF417 is made, based on the possibilities of the printers (older ATB printers are able to print PDF417, not AZTEC) in case the issuer should print barcodes too. If the barcode is only printed in a home-print situation (A4 laser- or inkjet printer e.g.) AZTEC is the better option.

(3), (4): AZTEC has 2 possibilities: Big or Small - depending on the area where the barcode should be printed and depending on the printing technology used. The small barcode is used on small tickets, or ATB tickets with limited space for security elements. Some RTS (Rail Tickets on (Smartphone-) Screen) have barcode sizing restrictions too. Sometimes, the barcode reader can be a limitation too in using the bigger one. To determine the choice BIG/SMALL, capabilities and limitations of all sales channels

and all systems to check the concerned tickets should be taken into account. These limitations a.o. determine which ticket layouts that can be used. For this, I refer to TAP TSI technical document B.11.

(4): The small AZTEC barcode with a fixed size, holding as much ticket info as possible is a SSB.

(7), (8): A big barcode can hold either structured ticket (and other) data (FCB) or hold the different elements used to compose the technical document B.11 layout of the ticket (TLB). The advantage of the first is to have more possibilities is which info to be added in the ticket as well as a better automated interpretation of the content of the ticket (FCB is machine readable / machine interpretable). The advantage of the ticket-layout based barcode is that the machine, used for reading the barcode can hold simpler software. No code lists, etc… have to be stored in the device since all the info comes directly, readable out of the barcode.

Disadvantage of this barcode is the fact that the barcode is machine readable / human interpretable. A (portable) device is only used to display the ticket info (as stored in a secured way in the barcode) on a screen. This info is real and cannot be counterfeit.

(5): Fixed field – the most common option – can be either SSB or ELB. In case of SSB, the same fields are used as in AZTEC SSB, just the last step (converting the data in a barcode) is done differently (PDF 417 instead of AZTEC). The ELB barcode standard was defined by SNCF (using specific character-based coding for data like stations).

(6): Flex field translated in a PDF 417 is only possible if the dataset which has to be included in the barcode is really small (the ASN.1 coding consumes data, meaning that less data can be stored than in the case of SSB).

Remark: The barcode, used in choice (7) can be, in some specific cases, very small too (e.g. a barcode holding only an identification (trip or passenger) to be used in a Sis application).

(↓) [TICKET TYPE][SECURITY ELEMENT] (→)		FCB	TLB	SSB	ELB
IRT	INTEGRATED RESERVATION TICKET	X	X	X	X
RES	RESERVATION	X	X	X	O(*)
NRT	NON-RESERVATION TICKET	X	X	X	O
GRT	GROUP TICKET (NRT)	X	X	X	O
RPT	RAIL PASS TICKET	X	X	X	O
VET	VEHICLE TICKET	X	X	O(*)	O
BOA	BOARDING PASS	X	X	X	O
COI	CHANGE OF ITENERARY	X	X	O	O
UPG	UPGRADE	X	X	O	O
SUP	SUPPLEMENT	X	X	X	O
TLT	TRAIN LINKED TICKET	X	X	O	O
ITT	LOCAL TRANSPORT TICKET	X	X	O	O
PARKING		X	O	O	O
ENDORSEMENT		X	O	O	O
ANNOTATION		X	O	O	O
DELAY CONFIRMATION		X	O	O	O
CUSTOMER CARD		X	O	O	O

X=possible, O=not possible,(*) technically possible, but not yet defined in detail

7. SSB – Small Structured Barcode

7.1. introduction

SSB (Small Structured Barcode) : Is used on ATB-tickets and in other environments where the physical space for the barcode is limited. The barcode technology used is AZTEC or PDF-417.

Because of the limited place of the area where the SSB should be printed / displayed, the barcode has to be small, thus the amount of data is limited too. As the total amount of information is limited, only the bare minimum of information is stored in the barcode, this has limitations (e.g. not the via stations in case of a specific route) that do not exist in FCB. So SSB should be used only is the necessary space for a FCB is not available. The best mechanism to save space in a data-set is by not tagging the data. Disadvantage of not-tagging is that there is no flexibility on the data-elements used in the data-set. Since different kind of tickets need different sets of data (e.g. seat number, coach number are only needed in an IRT ticket or a RES), different families of tickets are defined (so-called Ticket Types). In the standard 5 bits are reserved for this purpose, meaning there are 32 possibilities of which 31 can be used. 11 of them are defined for domestic purposes, the rest (20) is for international ticketing. Today 4 of them are defined.

As a result of this, the SSB is modular and covers the description of six different ticket types which define four different datasets used in SSB:

1. IRT, RES and BOA,
2. NRT
3. GRT (NRT)
4. RPT

The SSB is a fixed-field dataset barcode. The different fields (with a fixed size and encoding) are predefined, depending on the ticket type.

All fields in the barcodes are compulsory. All fields are readable (non-encrypted). Only the signature is encrypted (seal). The seal guarantees that the readable information is not modified. All data in the header and open data fields compose the seal.

Common fields to all sub barcode types are highlighted **in yellow**.
Variable fields, depending on Ticket Type and Sub Ticket Type code, are highlighted **in green**.
Fields with multiple data layout possibilities are written in RED text, when there is only one possibility, the text is BLACK. For fields with multiple options, the choice is part of bilateral/multilateral agreements between the security provider and the TCO(s).

The data in the SSB can be printed in a 6-layer AZTEC or a PDF417 Barcode.

7.1.1. AZTEC Barcode

Data is translated into a 6-layer AZTEC barcode (symbol size of 41x41) which provides a theoretical maximum data length of 114 bytes.

The surface of the barcode is 24mm x24mm - representing 41 dots x 41 dots.

Every pixel measures 0,59 mm x 0,59 mm

Printing resolution: minimum 150 dpi (average of 12 printer-pixels per barcode-dot).

Error correction must be at least 23 % using the standard AZTEC error correction mechanism.

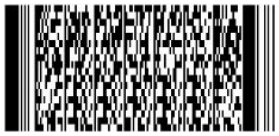
The technical header defined in the AZTEC Barcode encoding must be used and the data should be encoded in a 114 byte binary block.

7.1.2. PDF417 Barcode

Data is translated into a PDF 417 barcode according to the Association of European Airlines (AEA) 2002 standard which provides a theoretical maximum data length of 144 bytes.

The surface of the barcode is 30 mm x 17 mm - representing 72 rows x 18 columns.

ISO Reference is 15438.



7.2. Detailed description

The data in the SSB is composed of three parts:

- The header
- The open data
- The seal

The general description is:

Header	Version
	Issuer Code
	ID Code
	Ticket type Code
Open Data	Number of Adults
	Number of children
	First day of validity
	Sub-ID code
	…
	Information message
Encrypted Seal	Check Sum

See also extra explanation about the fields at the end of the chapter.

7.2.1. The header

The header is composed of 3 codes:

Header	Version	Num = 3	4,000	0.500
	Issuer Code	Num (< 9999)	14,000	1,750
	ID	Num (0..15)	4,000	0,500
	Ticket type Code	Num (0..31)	5,000	0,625

Version is the UIC Barcode version.
Ticket type values 0 to 20 are reserved for SSB international AZTEC Barcode definition.
Ticket types defined are:

Ticket Type	**Ticket type code value**
IRT, RES and BOA	1
NRT	2
GRT	3
RPT (InterRail Pass, Eurail Pass Overseas, Eurail Pass Europe)	4

Ticket type values 21 to 31 are for “bilateral” and domestic definition. Only the header and seal are mandatory and follow the specification. All open data fields are defined bilaterally.

7.2.2. The Open Data

7.2.2.1. Ticket type Barcode Ticket Type =1; IRT or RES or BOA

	Name	Type	Bit	Bytes	Remarks
Header	Version	Num = 3	4,000	0,500	
	Issuer Code	Num (< 9999)	14,000	1,750	
	ID	Num (0..15)	4,000	0,500	
	Ticket type Code	Num (0..31)	5,000	0,625	Value = 1
Open Data	Number of adult passengers	Num (<100)	7,000	0,875	If more than 100, 99 will be written in the barcode
	Number of child passengers	Num (<100)	7,000	0,875	If more than 100, 99 will be written in the barcode
	"specimen" code	Bit Flag	1,000	0,125	0=prod;1=specimen
	Class of travel	Lookup of 64 options	6,000	0,750	
	TCN: Issuing unique Ticket number	14 AlphaNum	84,000	10,500	PNR: Hermes Reference booking Number
	Year of issue	Num (0..9)	4,000	0,500	
	Issuing day, from first of January	Num (<512)	9,000	1,125	
	Sub-Ticket Type: IRT or RES or BOA Barcode	3 values	2,000	0,250	2=BOA; 1=IRT; 0=RES
	Station code Numeric or Alpha	Bit	1,000	0,125	0= Num; or 1=Bilateral AlphaNum
	Station code List type (NRT or Reservation HERMES) or Nothing	BitFlag or Nothing	4,000 or 0,000	0,500	1= NRT; 2=Reservation;
	Departure station Location or Bilateral AlphaNum	Num or Alpha	28,000 or 30,000	3,750	6 Char
	Arrival station Location or Bilateral AlphaNum	Num or Alpha	28,000 or 30,000	3,750	6 Char
	Departure date : First day of validity from the issuing date	Num (<367)	9,000	1,125	
	Departure Time	Num (<1440)	11,000	1,375	in minutes
	Train number	AlphaNum + 5 Car	30,000	3,750	
	Coach number	Num (< 999)	10,000	1,250	
	Seat/berth number	3 AlphaNum	18,000	2,250	Blank If AlphaNum or If several coach
	Overbooking indicator	Bit Flag	1,000	0,125	
	Information Messages	Num (< 9999)	14,000	1,750	
	Open Tekst	6 Bit ASCII (27 Car)	162,000	20,250	
	Padding	Bits	1,000	0,125	
Encrypted Seal	**DSA (2048, 224) part 1**		224,000	28,000	r value (*)
	DSA (2048, 224) part 2		224,000	28,000	s value (*)
TOTAL	**Total including seal**		**912,000**	**114,000**	

* Only the r and s values of the signature, not the structure around it.

7.2.2.2. Ticket type Barcode Ticket Type =2; NRT

	Name	Type	Bit	Bytes	Remarks
Header	Version	Num = 3	4,000	0,500	
	Issuer Code	Num (<9999)	14,000	1,750	
	ID	Num (0..15)	4,000	0,500	
	Ticket type Code	Num (0..31)	5,000	0,625	Value = 2
Open Data	Number of adult passengers	Num (<100)	7,000	0,875	
	Number of child passengers	Num (<100)	7,000	0,875	
	"specimen" code	Bit Flag	1,000	0,125	0=prod;1=specimen
	Class of travel	Lookup of 64 options	6,000	0,750	
	TCN: Issuing unique Ticket number	14 AlphaNum	84,000	10,500	
	Year of issue	Num (0..9)	4,000	0,500	
	Issuing day, from first of January	Num (<512)	9,000	1,125	
	Return journey flag	Return=1	1,000	0,125	
	First day of validity from the issuing date	Num (<512)	9,000	1,125	
	Last day of validity from the issuing date	Num (<512)	9,000	1,125	
	Station code Numeric or Alpha	Bit	1,000	0,125	0= Num; **or** 1=Bilateral AlphaNum
	Station code List type (NRT or Reservation HERMES) **or** Nothing	BitFlag **or** Nothing	4,000 **or** 0,000	0,500	1= NRT; 2=Reservation;
	Departure station Location **or** Bilateral AlphaNum	Num **or** Alpha	28,000 **or** 30,000	3,750	6 Char
	Arrival station Location **or** Bilateral AlphaNum	Num **or** Alpha	28,000 **or** 30,000	3,750	6 Char
	Information Messages	Num (< 9999)	14,000	1,750	
	Open Tekst	6 Bit ASCII (37 Car)	222,000	27,750	Advised space for Via codes and/or products codes
	Padding		3,000	0,375	
Encrypted Seal	**DSA (2048, 224) part 1**		224,000	28,000	
	DSA (2048, 224) part 2		224,000	28,000	
TOTAL	**Total including seal**		**912,000**	**114,000**	

7.2.2.3. Ticket type Barcode Ticket Type=3; GRT

	Name	Type	Bit	Bytes	Remarks
Header	Version	Num = 3	4,000	0,500	
	Issuer Code	Num (<9999)	14,000	1,750	
	ID	Num (0..15)	4,000	0,500	
	Ticket type Code	Num (0..31)	5,000	0,625	Value = 3
Open Data	Number of adult passengers	Num (<100)	7,000	0,875	
	Number of child passengers	Num (<100)	7,000	0,875	
	"specimen" code	Bit Flag	1,000	0,125	0=prod;1=specimen
	Class of travel	Lookup of 64 options	6,000	0,750	
	TCN: Issuing unique Ticket number	14 AlphaNum	84,000	10,500	
	Year of issue	Num (0..9)	4,000	0,500	
	Issuing day, from first of January	Num (<512)	9,000	1,125	
	Return journey flag	Return=1	1,000	0,125	
	First day of validity from the issuing date	Num (<512)	9,000	1,125	
	Last day of validity from the issuing date	Num (<512)	9,000	1,125	
	Station code Numeric or Alpha	Bit	1,000	0,125	0= Num; **or** 1=Bilateral AlphaNum
	Station code List type (NRT or Reservation HERMES) **or** Nothing	BitFlag **or** Nothing	4,000 **or** 0,000	0,500	1= NRT; 2=Reservation;
	Departure station Location **or** Bilateral AlphaNum	Num **or** Alpha	28,000 **or** 30,000	3,750	6 Char
	Arrival station Location **or** Bilateral AlphaNum	Num **or** Alpha	28,000 **or** 30,000	3,750	6 Char
	Name of the Group leader	12 Car	72,000	9,000	
	Countermark Number	Num (<247)	8,000	1,000	0 if Group leader, then 1 to max number of countermark
	Information Messages	Num (< 9999)	14,000	1,750	
	Open Tekst	6 Bit ASCII (24 Car)	144,000	18,000	
	Padding		1,000	0,125	
Encrypted Seal	**DSA (2048, 224) part 1**		224,000	28,000	
	DSA (2048, 224) part 2		224,000	28,000	
TOTAL	**Total including seal**		**912,000**	**114,000**	

7.2.2.4. Ticket type Barcode Ticket Type=4; RPT

	Name	Type	Bit	Bytes	Remarks
Header	Version	Num = 3	4,000	0,500	
	Issuer Code	Num (<9999)	14,000	1,750	
	ID	Num (0..15)	4,000	0,500	
	Ticket type Code	Num (0..31)	5,000	0,625	Value = 4
Open Data	Number of adult passengers	Num (<100)	7,000	0,875	
	Number of child passengers	Num (<100)	7,000	0,875	
	"specimen" code	Bit Flag	1,000	0,125	0=prod;1=specimen
	Class of travel	Lookup of 64 options	6,000	0,750	
	TCN: Issuing unique Ticket number	14 AlphaNum	84,000	10,500	
	Year of issue	*Num (0..9)*	4,000	0,500	
	Issuing day, from first of January	Num (<367)	9,000	1,125	
	RPT Sub Ticket Type	3 values	2,000	0,250	1=INTERAIL, 2=EURAIL EUROPE, 3=EURAIL OVERSEAS
	First day of validity from the issuing date	Num (<367)	9,000	1,125	000 = open date for regular Eurail pass to be activated
	Maximum duration from the issuing date for OVERSEAS otherwise last day of validity	Num (<278)	9,000	1,125	9 months max validity
	Number of days of travel allowed	Num(<93)	7,000	0,875	
	Country Code 1	Num (<100)	7,000	0,875	100 = all countries
	Country Code 2	Num (<99)	7,000	0,875	If Country code 1 is 100 then 00
	Country Code 3	Num (<99)	7,000	0,875	If Country code 1 is 100 then 00
	Country Code 4	Num (<99)	7,000	0,875	If Country code 1 is 100 then 00
	Country Code 5	Num (<99)	7,000	0,875	If Country code 1 is 100 then 00
	Second page	Bit Flag	1,000	0,125	If a two pages Pass
	Information Messages	*Num (< 9999)*	14,000	1,750	
	Open tekst	6 Bit ASCII (40 Car)	240,000	30,000	
	Padding		2,000	0,250	
Encrypted Seal	**DSA (2048, 224) part 1**		224,000	28,000	See also 6.2.3.2
	DSA (2048, 224) part 2		224,000	28,000	
	Total including seal		**912,000**	**114,000**	

Information messages Code Table

The new field “information message” is in the data fields of all different SSB Barcodes. The issuer could inform the controlling staff of special requirements according to the ticket or the sale conditions.

14 values could be defined and their combinations.

Information message	**Value**
Please check passport traveller	1
Please check customer railway card	2
…	3

The Station encoding

The station encoding can be provided as 6 character ASCII-6 codes or numerical codes in binary format.

The station data always consists of a one bit flag to indicate numerical or alphanumerical format

1: numerical format
0: alphanumerical format

The codes are contained in two 30 bit binary values (numerical format) or two30bit elements containing ASCII-6 codes.

Explanation about specific bar code elements and the way they are encoded

Barcode element	Description
Version	The version of the barcode. This element defines the way the following data are structured.
Issuer Code	Code of the provider of the signature
Id	Id of the private key used to create the signature. The signature must be checked with the public key related to this id.
Specimen code	The bit must be set if the barcode is issued for test purpose
Year of issue	The last position of the year when the barcode was issued (2015 → “5”)
Issuing day	Number of the day in the year at which the barcode was issued. The 1st of January corresponds to number 1.
Departure day	Number of days to be added to the issuing date to get the departure date.
Coach number	Binary encoding of the coach number. In case the coach number is not binary the value is 0.
First day of validity	Number of days to be added to the issuing date to get the first day of validity
Last day of validity	Number of days to be added to the issuing date to get the last day of validity

Return Journey Flag	Bit flag. If set to 1 this indicates a return journey.
Name of the group leader	Name of the group leader in 12 characters encoded as ASCII-6. Special letters not included in ASCII6 should be replaced by one corresponding ASCII letter.
Country code	Values below 100 are defined in the UIC country code table. Values above 99 are zone codes (see below:)

The Zone code list

If <99 then this corresponds with the country code
if >99 then this corresponds with a zone, the zone code list is:

Code	Counties or train products in the Zone Code
100	All countries participating in Eurail/InterRail Pass
101	Belgium, Luxembourg, Netherlands (Benelux)
102	Denmark, Finland, Norway, Sweden (Scandinavia)
103	Croatia, Slovenia
104	Montenegro, Serbia
105	Italy, Superfast (Italy Plus)
106	Greece, Superfast (Greece Plus)
107	Superfast (Italy, Greece)
108	Minoan Lines (Italy, Greece)

AlphaNumeric symbol translated into ASCII 6

Each alphanumerical sign is translated into a 6 bit decimal value (from 0 to 63). The translation is described below (also defined as: ASCII DEC SIXBIT)

Binary	Dec	Hex	Symbol		Binary	Dec	Hex	Symbol		Binary	Dec	Hex	Symbol
000000	0	0	SPACE		010110	22	16	6		101100	44	2C	L
000001	1	1	!		010111	23	17	7		101101	45	2D	M
000010	2	2	"		011000	24	18	8		101110	46	2E	N
000011	3	3	#		011001	25	19	9		101111	47	2F	O
000100	4	4	$		011010	26	1A	:		110000	48	30	P
000101	5	5	%		011011	27	1B	;		110001	49	31	Q
000110	6	6	&		011100	28	1C	<		110010	50	32	R
000111	7	7	'		011101	29	1D	=		110011	51	33	S
001000	8	8	(		011110	30	1E	>		110100	52	34	T
001001	9	9	)		011111	31	1F	?		110101	53	35	U
001010	10	A	*		100000	32	20	@		110110	54	36	V
001011	11	B	+		100001	33	21	A		110111	55	37	W
001100	12	C	,		100010	34	22	B		111000	56	38	X
001101	13	D	-		100011	35	23	C		111001	57	39	Y
001110	14	E	.		100100	36	24	D		111010	58	3A	Z
001111	15	F	/		100101	37	25	E		111011	59	3B	[

010000	16	10	0		100110	38	26	F		111100	60	3C	\
010001	17	11	1		100111	39	27	G		111101	61	3D	]
010010	18	12	2		101000	40	28	H		111110	62	3E	^
010011	19	13	3		101001	41	29	I		111111	63	3F	_
010100	20	14	4		101010	42	2A	J					
010101	21	15	5		101011	43	2B	K					

7.2.3. Generation of the Seal / Hash code

7.2.3.1. Hash Code generation-Encrypted seal: SHA-224, DSA, 2048

Encryption process:

- hash all data in the Header field and Open Data field with the SHA-2 224 Algorithm.
- and then, to crypt the result with the DSA 2048 asymmetric cryptosystem (private-public key).

This process is defined as (SHA-224, DSA, 2048). The seal obtained is 56 bytes long (non-structured).

1) **Hashing the header and open data in SHA-224**
2) **Encryption of the Hash code with DSA 2048 (private key, hash value)**
3) **The result is the seal (r size 224 bit, s size 224 bit) to be put at the end of the data to be translated into the SSB (Aztec barcode)**

7.2.3.2. Hash Code generation-Encrypted seal: SHA-160, DSA, 1024

Encryption process:

- hash all data in the Header field and Open Data field with the SHA-160 Algorithm.
- and then, to crypt the result with the DSA 1024 asymmetric cryptosystem (private-public key).

This process is defined as (SHA-160, DSA, 1024). The seal obtained is 47 bytes long (structured).

1) **Hashing the header and open data in SHA 160**
2) **Encryption of the Hash code with DSA 1024 (private key, hash value)**
3) **The result is the seal (r size 160, s size 160) to be put at the end of the data to be translated into the SSB (Aztec barcode).**

The signature issuing has a size of **46 bytes** in a structured layout. This fits in the field (indicated in the tables as “encrypted seal”) allocated for the signature (56 bytes). The remaining bytes will be filled with nulls at the end.

8. ELB - Element List Barcode

The ELB (Element List Barcode) is used in environments where the space for the barcode is limited and because of technical limitations, real 2D-barcode technology is not available. The barcode technology used is PDF-417, not a real 2D barcode, but a stack of 1D-barcodes, making it possible also to be printed by less sophisticated printers. The data-layout (content) of the barcode is an early developed standard, defined by SNCF. The data size of this PDF-417 is limited to max. 144 bytes.

Because of its limitations and the missing seal, ERA does not recommend the Element List Barcode for new developments or implementations.

8.1. Collecting the elements for the barcode (alphanumerical format)

A list of all the elements to be integrated in the PDF-417 barcode:
(All elements are in Alphanumerical format (A…Z, 0…9))

	Name	Size	Description
Decoding info	ID_format	1	Defines type of barcode/ticket/key etc... Default value="e"
	Code pectab	1	Code, used for ATB-printers - Default value="R"
	Ticket code	2	Code, indicating what kind of ticket is in the barcode
	PNR	6	Reference of the booking
	TCN-code	9	Issue booking number
	Specimen-flag	1	1=real ticket, 0=specimen
	Barcode Version		For decryption purposes - which elements can be found
	Number	1	where in which format
	Sequence number	2	xy: ticket x out of y tickets
	Non-used digits	10	for future use
Ticket Info	Traveler type	2	frequent traveler / ...
	Number of adults	2	00 – 99
	Number of children	2	00 – 99
	Year (last digit)	1	e.g. 2007 -> '7'
	Emission day	3	Sequence number (1/1=1, 2/1=2, ...)
	Begin validity day	3	Sequence number (1/1=1, 2/1=2, ...)
	End validity day	3	Sequence num3333ber (1/1=1, 2/1=2, ...)
Segment 1	Departure station	5	Alphanumerical encoding e.g. FRPNO
	Arrival station	5	Alphanumerical encoding
	Train number	6	(or 5 + 1 blank)
	Security code	4	Specific code for a train - antifraud
	Departure date	3	Sequence number (1/1=1, 2/1=2, ...)
	Coach number	3	Alphanumerical - 3 digits
	Seat/bed number	3	Alphanumerical - 3 digits
	Class of transport	1	1=first class, 2=second class
	Tariff code	4	4 blanks = full fare ticket
	Class of service	2	defining extra services or conditions (non exchangeable,...)
Segment 2	Departure station	5	Alphanumerical encoding e.g. FRPNO
	Arrival station	5	Alphanumerical encoding
	Train number	6	(or 5 + 1 blank)

	Security code	4	Specific code for a train – antifraud
	Departure date	3	Sequence number (1/1=1, 2/1=2, ...)
	Coach number	3	Alphanumerical
	Seat/bed number	3	Alphanumerical
	Class of transport	1	1 = first class, 2 = second class
	Tariff code	4	4 blanks = full fare ticket
	Class of service	2	defining extra services or conditions (non exchangeable,...)
	TOTAL SIZE	**85**	**(Characters) for a one-segment trip**
	TOTAL SIZE	**121**	**(Characters) for a two-segment trip**

8.2. Encoding in a PDF-417

The characters are put one next to the other to make one long word (85 or 121 characters long, depending on the fact if the ticket contains one or two segments).

This word is sent to the ATB printer, together with some commands, specific for printing the barcode (element of the PECTAB-file). For this, consult the manual of the printer to have the sizes as defined in the standard. The printer can be any printer able to print PDF-417 barcodes.

9. TLB (Ticket Layout Barcode) and FCB (Flexible Content Barcode) – common parts

9.1. Introduction

TLB and FCB are sharing the same high-level data lay-out. They can be combined in 1 barcode too, making it possible to read the ticket info both using FCB and TLB based TCO-systems. The barcode, holding both kind of ticket info (TLB, FCB) is even backwards compatible with an older TLB based TCO-system, developed before the introduction of FCB since the FCB data will be skipped by this system (if the TCO platform was developed as described in TAP TSI technical document B.7) - see generalities in chapter 11

The barcodes in international passenger traffic are composed as follows:

1. Message header with message ID and digital signature
2. Main record
3. Record containing the RCT2 ticket layout
4. Flexible content Data
5. Record(s) based on specific TCO standards.

1. is unique for UIC barcode security elements
2. and 3. have to appear together and define the TLB data in the barcode
4. holds FCB data
5. is for domestic ticketing.

For TAP TSI based ticketing, records 1,2,3 (TLB) or 1,4 (FCB) are the bare minimum to be used in the barcode. This structure makes it possible to make any combination of TLB, FCB and domestic ticket layout in 1 (big) AZTEC barcode.

All possibilities are:

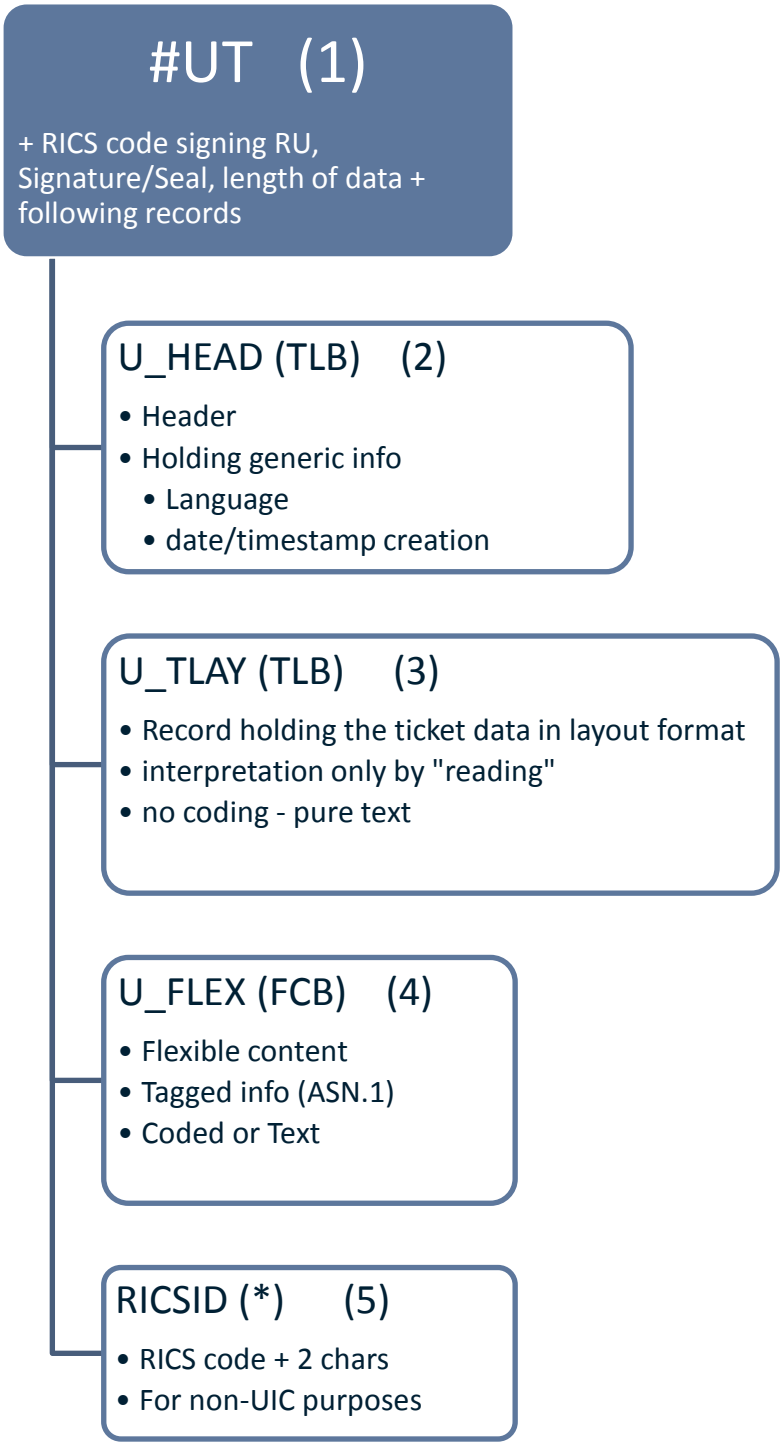
1+2+3	TLB
1+4	FCB
1+5	Domestic ticket - using UIC barcode
1+2+3+4	TLB + FCB (giving possibility to check "newer" FCB with "older" TLB-based devices.
1+2+3+5	TLB + Domestic ticket - using UIC barcode
1+4+5	FCB + Domestic ticket - using UIC barcode
1+2+3+4+5	TLB + FCB + Domestic ticket - using UIC barcode

Remark: multiple occurrences of 5 (Domestic) can co-exist in 1 barcode: e.g. 1+4+5+5 is possible.

In the next chapters (chapters 9, 10 and 11) detailed description about the generation of the specific barcodes can be found.

9.2. Composition of the data content of the TLB / FCB

(the numbers are reference to the numbers in the introduction above)



- (*) for domestic ticketing
- at least 1 of the record (combinations)(TLB), (FCB) or (*) should be used to have a valid barcode.
- the data in the white blocks is put together and compressed

9.3. 2D Barcode symbol

When translated into a 2D AZTEC barcode, the following specifications are mandatory:

Parameter	Value	Comments
Symbology used	Aztec	Specification see [AIMBC13].
Number of modules	87 (TLB only)	This means 17 Aztec layers (see Aztec standard)
Capacity	max. 621 Bytes (TLB only)	Binary data (8 bit). This limit may not be exceeded; otherwise the fault correction is jeopardized.
Physical size	50 x 50 mm (TLB only)	The size of the entire 2D barcode results from the recommended element size for the printout on the home printers (inkjet low-cost): Optimal recommendation: 25 mil / elem. Minimal recommendation: 15 mil / elem. (with 50 x 50 mm results in an element size of 23 mil) 1 mm = 40 mil
Share of fault correction data	23%	This value results from the previous values when using the full capacity. For Aztec 23% is the standard value for fault correction .

Figure: Example for 2D Barcode symbol in accordance with the specifications

10. TLB - Ticket Layout Barcode - detailed description

(See also chapter 9)

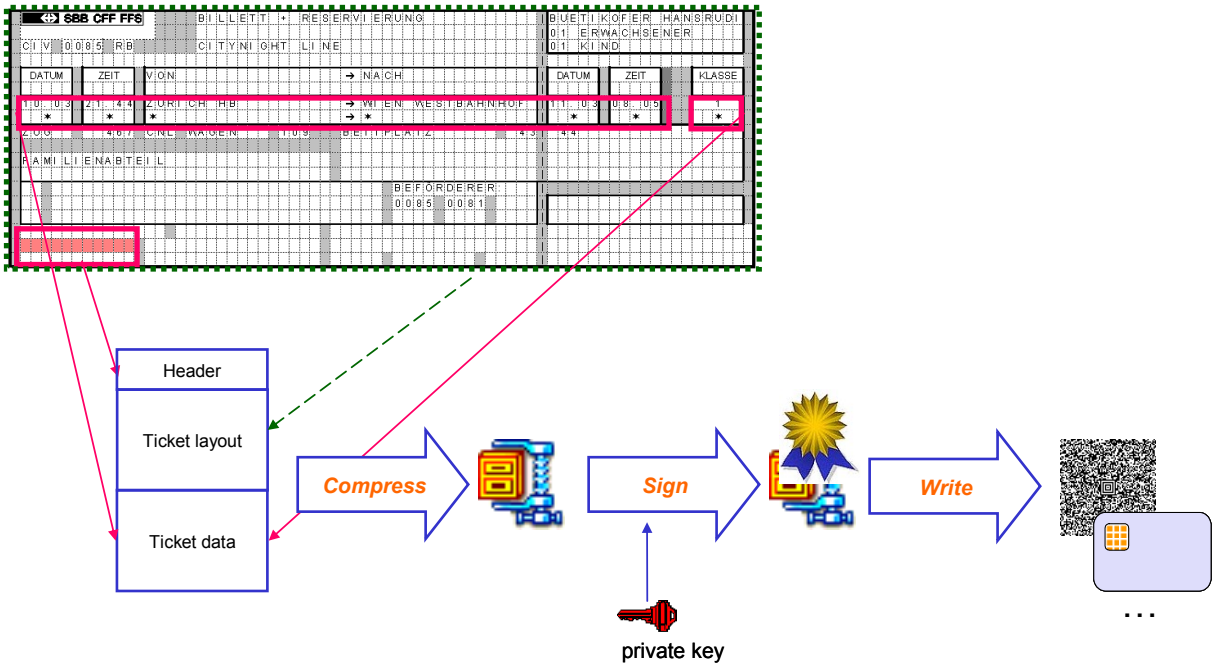
10.1. Generalities

The sequence of the records is seized by means of a compressing technique and then displayed on / stored in the support medium (2D Barcode, Smartcard, etc.).

All necessary ticket text, combined with the layout (as defined in the TAP TSI technical document B.11) is translated in a message. This message is compressed, signed (using a private key) and translated in the AZTEC-barcode.

During the ticket check, the barcode is read and translated back into the text fields that are displayed in the right position and with the right font on the screen of the control device (exactly in the way the security provider – the creator of the barcode - wanted it to be displayed to the train staff member).

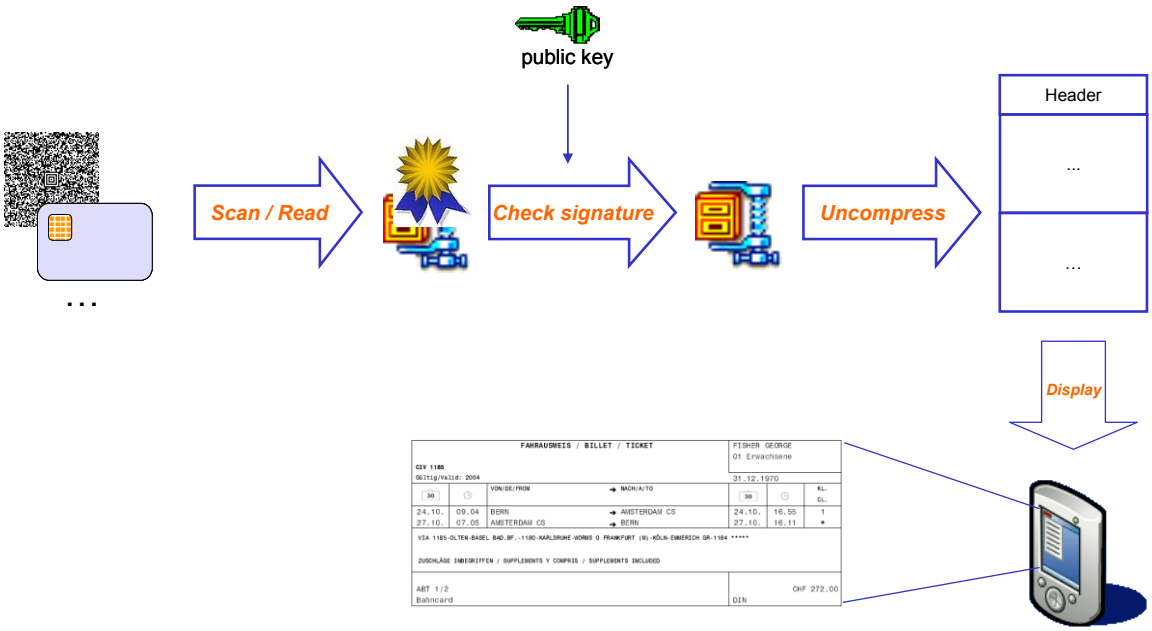
(the pink squares are just an example)



10.1.1. Controlling (checking) the TLB

The control process by means of an apparatus contains the following steps:

1. Reading the content of the TLB (2D Barcode)
2. Decompressing the content
3. Checking the signature by means of a public key, extracted from the certificate. If the result is negative, the train manager receives a corresponding notice
4. Output of the content of the ticket on the display (in the layout of the ticket printout)
5. Automatic check of some essential ticket attributes (trip date etc.)
6. Receiving the outcome of the control of the train manager



The process of checking the signature can be done in parallel with the process of uncompressing and displaying the content. In that case, the train staff member can already check the route, class, date etc... info before receiving confirmation the ticket / DST content was not falsified. This change in order to gain some time since the calculation which is needed to check the signature can take a lot of time.

10.1.2. Compressing procedure

For the compressing procedure the algorithm Deflate will be applied. The specification of Deflate can be found in [RFC1951] .

Comparing tests have shown that Deflate provides the best compression versus computing power rate (for the content of the open data in the barcode) among the procedures that were compared.

10.1.3. Character encoding

In text fields with fixed length, special characters are not permitted, only printable characters (U+0020 to U+007E) that are translated in one byte using the UTF-8 encoding, are allowed.

Text fields with a variable length may contain special characters. The strings must be encoded using UTF-8 transformation. The specification of UTF-8 can be found in [RFC3629]. Special characters will increase the length of the encoded string, since they are encoded using several octets.

Note: the value of the according length field must be determined *after* encoding the text, in order to allow decoding the entire text again when parsing the content.

10.2. Definition of the record structure

The different categories of content require a flexible structure. The structure must answer to the following demands:

- General record types, that are handed out and interpreted by all UIC members
- For specific ticket data, an UIC member can define its own record types. This way attributes that are not defined in the UIC standards can be used as ticket message content.

Each record type is composed according to the following pattern:

Number in sequence	***Element***	***Number of characters***	***Mandatory***	***Code***	***Comments***
1	Record ID	6A	X	X	Composition: • "Uxxxxx" for record types, standard in UIC. "xxxxx" is variable and determines the type • company Code of 4 characters + "xx" for record types defined by separate TCOs. "xx" is variable and can be filled in freely by the TCO for each type (2 characters)
2	Record version	2N	X		Allows different versions of one record type (having the same record ID)
3	Record length	4N	X		Number of characters starting from the record beginning (from the first character of the element “record ID”)
…	…	A			The actual fields of the records

10.3. Definitions of the record types

10.3.1. Main record (U_HEAD)

This record is mandatory for TLBs.

The main record contains information in common with all the transport documents (regardless the ticket layout standard, a domestic or international ticket).

Definition:

Number in sequence	Element	Number of characters	Mandatory	Code	Comments
1	Record ID	6A	X	X	ID is "U_HEAD" ("header")
2	Record version	2N	X		"01"
3	Record length	4N	X		
4	company code of the distributing RU	4N	X	X	Security provider, producing the tickets
5	Unambiguous key of the tickets	20A	X		The producer can complete this key freely; a specific key can only be used for one ticket. In combination with the company code this key provides a global unique key for each ticket within the TAP TSI.
6	Edition time	12N	X		Format "DDMMYYYYHHMM" This can be used to prevent fraud by buying a ticket after trip departure (only shortly before the conductor shows up).
7	Flags	1N	X	X	- International ticket: 1 - Edited by agent: 2 - Specimen: 4 The field is the decimal representation of the sum according to the flags set. E.g.: "6" means national ticket, edited by agent, specimen
8	Edition language of the tickets	2A	X	X	ISO 639 – 1 country code definitions and abbreviations
9	Second language of the contract of carriage (See 918-2)	2A	X	X	ISO 639 – 1 country code. If no second language is used, this field is filled with blanks.

10.4. Definition of the record types for the ticket data according to the UIC standard

In this chapter the record types containing the actual information of online tickets (print attributes) are defined. These contents allow the essential control of the ticket by means of a control apparatus.

10.4.1. Record of the ticket data "Ticket Layout" (U_TLAY)

This record is mandatory in TLBs and for international tickets it's mandatory that the layout standard used is "RCT2" (see element 4).

This record represents the entire information of the attribute fields on the printed ticket layout, so that a complete control of the ticket is possible without making an online connection to the vending system.

Note that only layout fields with variable content should be included in this record. Fields which have the same content for all tickets of a given layout standard (e.g. labels), will be completed by the control apparatus. In particular for "RCT 2" based layouts all labels on line 5 (E) may not be included.

To control offline, the entire content of the “ticket layout” field is extracted from the DST and shown on the display of the control apparatus. The layout must correspond exactly with the printed ticket.

This record only refers to the ticket content and not to a specific layout standard (for example "RCT 2"). As a consequence, also tickets that are not standardized in the UIC, can be depicted. In combination with the DST records specific for the TCO (chapter 7.5), DSTs can therefore be created for any carrier specific ticket. Nevertheless international tickets always must follow the "RCT2" layout standard.

Definition:

Number in sequence	Element	Number of characters	Mandatory	Code	Comments
1	Record ID	6A	X	X	ID is "U_TLAY" ("Ticket layout")
2	Record Version	2N	X		"01"
3	Record length	4N	X		
4	Layout Standard	4A	X		For example "RCT2"
5	Number of fields	4N	X		Number of following fields
The following elements define the individual text fields included on the ticket layout description formula. For each text field the elements are repeated (i= index of the text fields)					
6 + 6 i	Field line	2N	X		Line index of the first letter. Range: 0 till 14
7 + 6 i	Field column	2N	X		Column index of the first letter. Range: 0 till 71
8 + 6 i	Field height	2N	X		Number of lines reserved from the field
9 + 6 i	Field width	2N	X		Number of columns reserved from the field

10 + 6 i	Field formatting	1N	X	X	0: normal 1: bold 2: italic 3: bold & italic 4: small font (the “132-font” in RCT-2) 5: small + bold 6: small + italic 7: small + bold + italic
11 + 6 i	Field text length	4N	X		Length of the following text. Caution: the length must be determined using the already encoded text
12 + 6 i	Field text	nA	X		If “Field height” is bigger than 1, the text must be wrapped using the following rules: • The first word that doesn’t fit in the current field line, is printed at the beginning of the following line • If the field text contains the sign LF (ASCII "10"), the next word must be wrapped to the next line. The producer of the record must guarantee that the entire text, when applying these rules, fits within the indicated field sizes (height and width), can be entirely displayed.

Note:

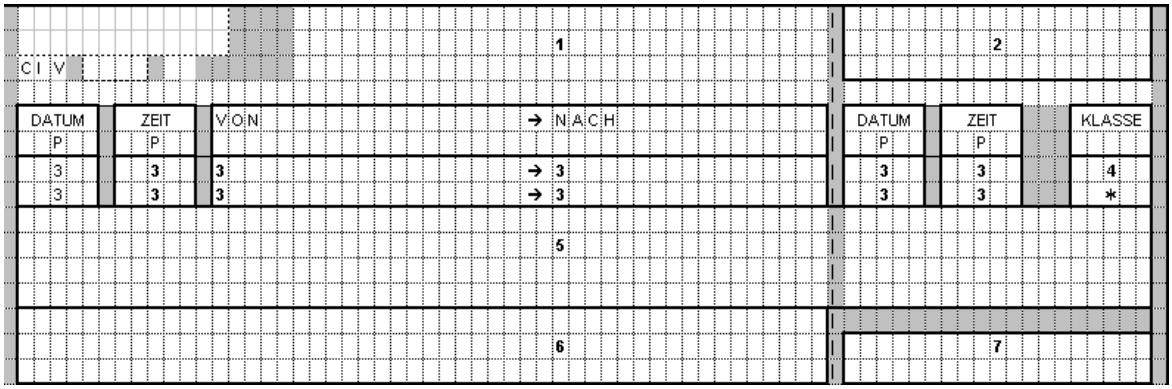
- When composing this record, one must pay attention to the fact that pictograms obviously can't be used in a field text. If the printed ticket contains pictograms, they must be replaced by a corresponding text. The language and content which are used to replace the pictograms must be set according to the standard that is used for the “Ticket layout” field (i.e. “RCT-2”).

- Using "small font" formatting has no impact on the number of characters possible for a certain field. E.g. a field using "small font" formatting still has a maximum width of 71 characters, even if there is space left on the form. The "small font" format is therefore a pure formatting option which can't be used to increase the textual capacity of the ticket fields.

10.4.1.1. Extraction of RCT 2 zones

If the element “Layout standard” in the “U_TLAY” record contains the value “RCT2”, it means that the content of the “U_TLAY” record is composed according to the layout defined by TAP TSI technical document B.11. This allows extracting directly specific ticket attributes from the “U_TLAY” record.

The layout of the ticket according to RCT2 is subdivided in different zones containing distinct attributes (s. [TAP TSI technical document B.11], chapter 1.2.3):



Zone	Content
1	Type of document
2	Names / first names of the travellers and the number of adults and children
3	Travel distance, departure date and – time, arrival date and - time
4	Class
5	Train, wagon, reserved seat (if not with compulsory reservation)
6	Used rates, used commercial conditions (from 1 till n carriers)
7	Currency (ISO code out of GIV) and total amount for each ticket

If the element “Layout standard” in the “U_TLAY” record contains the value “RCT2”, separate zones (1 till 7) can be extracted on the basis of the subdivision of the ticket layout (from the record “U_TLAY”). This allows subdividing the information included in the “U_TLAY” record into coherent parts.

The subdivision in separate zones makes it possible to show the content of the “U_TLAY” record on the display of a control apparatus that is too small for the entire layout. In this case, the separate RCT 2 zones can be displayed consecutively and or combined differently.

It is a recommendation to – for tickets holding this info – to include these fields at these exact locations for some basic machine interpretation (e.g. opening of station gates).

10.4.1.2. Extraction of RCT2 ticket attributes

Besides the subdivision of the zones, the TAP TSI technical document B.11 allows the extraction of separate ticket attributes (from the “U_TLAY” record). In the zones 3, 4 and 7 only one representation exists for all the different types of transport documents (see last column of the previous table). This means that the included ticket attributes are identical for all RCT 2 ticket types and these attributes can be extracted unambiguously.

10.5. Record types for ticket data in accordance with the standards of a specific TCO

The distributing RU can include attributes in the TLB that are not defined in the UIC standard. The TLB can also be used for national tickets that are not composed according to UIC layout standards.

For these cases the RU can define their own record types. As long as the base structure of the record is respected (part 7.2 “Definition of the record structure”), no other directives for the internal composition of this record exist.

Definition:

Number in sequence	Element	Number of characters	Mandatory	Code	Comments
1	Record ID	6A	x	x	RICS code of 4 characters + ID (2 characters) The company code is the number of the TCO defining the specific record type. The ID is composed by the TCO himself and contains 2 alphabetic signs that can freely be chosen.
2	Record version	2N	x		
3	Record length	4N	x		
…	…	A			Next there are the actual elements of the record in accordance to the standard specific for the TCO.

Example of an ID “1180XY” record:

Example of symbol	Meaning
"1180"	company code of the DB
"XY"	ID of 2 characters to distinct different record types of this TCO

10.6. Definition of the entire TLB message structure

The TLB message structure is defined below. Similar to the record definitions it contains header elements containing type id and version.

The entire content of the TLB is protected by means of a digital signature, that guarantees:

- Integrity:
  Even the smallest possible manipulation of the content (i.e. changing from 1st to 2nd class) leads to an invalid signature. Forged TLBs will be recognized immediately by verifying the signature.
- Authenticity:
  Since only the possessor of the private key is able to create the signature, the authorship of the TLB is proved.

Because the key necessary for the control of the signature cannot be fully protected against theft (due to its presence on each control apparatus), an asymmetric algorithm is used (public/private key). The

message header thus contains a signature generated from the algorithm DSA ("digital signature algorithm", see [FIPS186]).

Definition of the entire TLB message structure – VERSION 1:

(This version was used in the TAP TSI technical document B.7, but for future use - with the ability to hold bigger seals thus with improved security - version 2 is recommended)

Number in sequence	Element	Number of characters	Mandatory	Code	Comments
1	Unique Messagetype ID	3A	X	X	"#UT" for 'UIC Ticket'
2	Messagetype version	2N	X		"01" (Version of TAP TSI TD B.12)
3	company Code of the RU that is signing	4N	X	X	Allows the identification of the public key necessary for the verification in combination with the following element
4	ID of the signature key	5A	X		The ID must be managed by the RU issuing the signature key
5	Signature	50B	X		DSA signature for the message after compression (next element) in ASN.1 representation. If the actual ASN.1 representation is shorter than 50 bytes, it should be enlarged to the length of 50 by adding null bytes.
6	Length of compressed message	4N	X		
7	Compressed message	A	X		The entire record sequence compressed with DEFLATE.

Definition of the entire TLB message structure – VERSION 2 (NEW!):

Number in sequence	Element	Number of characters	Mandatory	Code	Comments
1	Unique Messagetype ID	3A	X	X	"#UT" for 'UIC Ticket'
2	Messagetype version	2N	X		"02" (Version of TAP TSI technical document B.12)
3	companyCode of the RU that is signing	4N	X	X	Allows the identification of the public key necessary for the verification in combination with the following element
4	ID of the signature key	5A	X		The ID must be managed by the RU issuing the signature key
5	Signature - r	32B	X		DSA signature, element “r”. If size is smaller than 32, it should be enlarged to the length of 32 by adding null bytes at the end.
6	Signature - s	32B	X		DSA signature, element “s”. If size is smaller than 32, it should be enlarged to the length of 32 by adding null bytes at the end.
7	Length of compressed message	4N	X		
8	Compressed message	A	X		The entire record sequence compressed with DEFLATE.

10.7. TLB on SiP tickets - extra information in the barcode to avoid copying

Barcodes (SiD) can be combined with SiP by printing the infomation (including the barcode) on CIT-paper. This allows all parties to threat the ticket (including stamps, annotations, ...) as unique. To avoid copying of these barcodes (e.g. to show it on a screen of a smartphone), printed on SiP-specific paper, extra information has to be added in the barcode. Using an extra bit for this purpose can cause existing systems to generate errors.

The solution to store this extra data is by "virtually" print it on the ticket, causing it to be handled by the standard mechanisms translating text in the barcode.

On ATB-tickets, the area's A2..A14 and B2..B14 are used to put the logo of a railway company. No text can be printed on the paper ticket. On the screen, when displaying the content of the barcode, translated in an ATB-ticket, there could figure "ON CIT PAPER", indicating the ticket can only exist in SiP context.

	2	3	4	5	6	7	8	9	10	11	12	13	14
A	**O**	**N**		**C**	**I**	**T**		**P**	**A**	**P**	**E**	**R**	

10.8.

10.9.

11. FCB - Flexible Content Barcode - detailed description

(See also chapter 9)

11.1. Generalities

If a ticket has to be read and checked by a computer (e.g. at an automated check-in device), the information in the ticket should be encoded, not alphanumerical (e.g. train station codes, reduction codes). This means that in a lot of cases, the alphanumerical version of the data elements are less suitable.

Thus there is a need for a barcode which is holding data in encoded format (to be machine-interpretable), which is holding different kind of data for different kind of contracts, with also the possibility to store some info in alphanumerical format (for companies, not having translation tables in their machines), and which can be used in more use cases than just for ticket check (e.g. parking contract, station passage, …).

For these needs, a flexible content, structured, encoded 2D barcode was developed.

The data in this barcode is structured and, since the content is variable (depending a.o. on the kind of contract), the size of the barcode will be variable too. Since the data content is variable, data should be labelled (the data is not found at fixed positions in the "message" as in the SSB).

The barcode can either hold all the contract details (SiD), hold no contract details at all (SiS), or hold some info and leave other data on the central server (combination of both). In SiD tickets, the commercial possibilities are limited. In SiS tickets, contracts can be modified in after sales operations, cancellations are possible, …

The barcode, described in this chapter is a flexible content barcode. This means that a lot of information in the barcode is optional, also the number of occurrences of some elements is variable (e.g. list of travellers) and the data format of some of the elements can be different (numerical / alphanumerical).

This is why the barcode of this standard is called the **"FLEXIBLE CONTENT BARCODE" (FCB).**

As a result of all this, RU's (and other companies – parking lots etc.) can choose about the content to be included in the barcode, which makes the barcode very flexible and as a result the size of the barcode will be variable.

The barcode itself will be created following the AZTEC standard (as in the TLB chapter of this document).

The barcode is made following these steps:

- (1) The right data is collected, depending on the use-case
- (2) The right format for the data is chosen (as defined in this leaflet and following ASN-1 standards)
- (3) All the data is translated in 1 "message" – a list of bits, using PER unaligned.
- (4) Other records (e.g. specific domestic or TLB layout) are added.
- (5) All this is compressed to save space
- (6) Next a header, holding the code of the security provider, a version number of the security key and a version number of the barcode is added (defining the key as well as the version). This header contains also the actual security element (the signature) as a proof that the data is not modified after being issued by a recognized security provider.

This data is translated in AZTEC. The number of layers (the physical size) of the AZTEC barcode is defined by the data size (the number of bits/bytes of the complete message).

The name of the record is : U_FLEX – This is compliant with the naming convention in the TLB barcode (element of 6 alphanumeric) : for the first 2 characters, “U_” is chosen, indicating it is a UIC record, not the record of a specific RU. For the last characters, we chose “FLEX” to indicate that this barcode is the flexible one, both in which elements to be included as well as their format.

Steps 1,2,3 are specific for the FCB barcode standard.

Steps 4,5,6 are general, they also exist for the TLB barcode. Even more, these steps are 100% compatible. This means that, when a 2D barcode, made following this description, holds both data as defined in the following chapters and as defined in the TLB, “old” software, able to read the TLB will read the barcode and decode the specific TLB-part of it. The software will skip, without generating errors, the data as defined in this standard.

This standardization can be compared with the standardization of colour-TV distribution. In the beginning of television, programs were distributed in black& white and televisions captured the Black and White signal on the specific frequencies of the different television channels. When the colour-TV’s were launched, the programs started to be distributed in colour, but the older black & white televisions were still able to capture the programs, without any adaptations – even using the existing frequencies. This was achieved by having the original B/W signal left unmodified and adding the colour information to this signal without modifying the original one. In this barcode, the same is done when (old) TLB data is combined with new data, as described in this leaflet. Existing barcode reading software, if developed following the older TLB definitions, can handle a combined barcode (holding TLB encoded info as well as Flexible Coded data) without problems: the software will find the necessary information and skip the data encoded following this FCB-standard. This “skipping” is already defined in the TLB part, where it is explained how to deal with headers, other than the ones defined in the TLB (and “U_FLEX” is a header of this kind).

The FCB description consists of 3 main parts:

- The Use Cases:
  - for which purposes these barcodes will be used
  - in each case, which elements are needed in the barcode
- The data elements:
  - every data element is explained in detail (format, size, coding)
  - elements are categorized into mandatory / optional / conditional
- The transformation into the barcode:
  - the list of data elements are transformed in a message
  - the message is compressed
  - a seal is calculated
  - the whole dataset is translated in a (variable size) AZTEC barcode

A complete list of data-elements will be defined (“the data elements”). Which data elements to be used from this list, depends on the use case. A list of use cases, together with the data elements to be used in each use case is part of this standard (“The use cases”).

The data is encoded using ASN.1 / PER encoding to reduce total data volume. (comparable with e.g. XML, but the result of the translation in ASN.1 will be much smaller (in bits) than in XML).

Some elements figure more than once in the leaflet, in different data formats (e.g. station code versus full name of a station) – the choice of the representation(s) is part of bi- and multilateral negotiations (between security provider(s) and TCO(‘s) e.g. is there a code list on the reading device?).

Optional elements consume 1 bit - even if not used (is because of the ASN.1 encoding).

Despite the fact that this leaflet is not dealing with on-line data communication, the result is quite similar (information going from a ticket issuer, via the client/passenger, to the TCO. The data to be

transferred is called the “message” as in on-line communication. In the rest of this document, when “message” is used, it means the string of binary data, created from the list of data-elements, in their right format.

11.2. “USE CASES” - "What can an FCB be used for?"

In this part of the leaflet, the different cases where Flexible Coded 2D barcodes can be used in a railway environment are described.

Generally there are 5 groups of so called “use cases”: (between brackets, the numbers of the use cases that are part of these groups):

Offline control of tickets (SiD) with/without reference data on the checking device (1,2,4)
Online control of tickets (SiS) (3)
Opening of station gates, platforms / entrance to parking (5,6,1,2)
Additional info for the client (7)
Back office reference data (8,9,10,11)

In the next section, the use cases are described, in the attached use-case table all mandatory, optional, conditional data can be found.

§ 11.3 shows the table of the elements per use case (mandatory, optional, ...)

§ 11.4 explains for some specific elements how this element should be interpreted

In attachment of this document, an .ASN file can be found with all data types that can be used in the FCB.

11.2.1. USE CASE 1: Offline control of tickets without reference data on a device (SiD)

In this use case, tickets can be checked without an on-line connection (all necessary data is in the barcode) and without a look-up table for reference data (ex. station names, tariff descriptions) in the ticket checking device. This is usually necessary for barcodes read by small companies or by companies checking only a limited number of tickets of this kind.

In the barcode all ticket info is included, in a non-coded (human-readable - alphanumeric) format.

Usually this use case is about a company, not involved in TAP TSI,checking (occasionally) a TAP TSI compliant-ticket/contract.

In this use case, the tickets are generally machine-readable, human-interpretable.

Tickets (NRT, IRT, RPT, FIP, Parking, GRT countermark)

Allowing these tickets to be read by a company, not involved in TAP TSI. E.g. partnership for local transport, ticket for connecting bus or metro of a corresponding city.

Customer card

In case a customer card of a railway company allows a client to travel with reduction on the network of the partner company (can be a non-railway company)

Station passage card

The barcode gives the right to enter in a building or in a certain area of a building. If this building is not a station, or a station of a company, not involved in TAP TSI, then this barcode can be interpreted without any specific TAP TSI compliant coding.

Voucher

The barcode can hold a voucher in a non-coded way (for a specific company, valid for a specific period, …)

11.2.2. USE CASE 2: Offline control of a ticket – reference data on the device (SiD)

These use cases are exactly the same as the ones mentioned above: tickets / contracts can be checked offline (security in data). All necessary info to check the contract(s) can be found in the barcode itself. The main difference with use case 1 above is that the info is coded using code lists used in the corresponding TAP TSI technical documents (e.g. station codes, tariff codes). This gives the possibility to reduce the data size significantly and makes it easier to have the barcode machine interpretable.

To make the contract info in the barcode human-interpretable, reference data should be on the checking device to translate the codes into the corresponding descriptions (e.g. station code / station name).

Usually this use case is about RU's checking tickets/contracts without an on-line connection (e.g. with a portable device on board of a train)

Tickets (NRT, IRT, RPT, FIP, Parking, GRT countermark)
Customer card
Station passage card
Voucher

11.2.3. USE CASE 3: Online control (SiS)

Tickets are checked by reading one or more identifiers, retrieve information from a central server and check this info to make sure the passenger is having the right contract (of carriage). This is the most secured system and allows the companies to develop the most flexible commercial formulas to be used in combination with (e.g. home printed) barcode ticketing. A customer can, e.g. change a existing contract on-line on the server, after printing or receiving the barcode.

For this use case, only a very limited amount of data is needed. The barcode is just for (secure) identification purposes.

11.2.4. USE CASE 4: Partially automated ticket check – (SiD)

First, all information in the barcode is read. Then, some checks are done automatically by the machine (e.g. check-in device, train staff device): location, time (machine knows both where it is: line, time, even GPS corrections can be implemented and the date/time the ticket is checked), class, ... Additional checks (like reduction, age, tariff code) can be checked by a human staff member by reading that info from the screen of the barcode reading device. For this, the portable device of the train staff member can e.g. show 3 different colour codes: Green: everything OK, no additional checks are needed (e.g. full fare ticket), Red: problem with O/D combination or date of validity, Orange: ticket seems OK, but additional checks are needed: e.g. passenger has to show Bahncard number XXXX or proof his/her age.

11.2.5. USE CASE 5: Opening of platform gates(SiD, SiS)

Platform gates will only open if the client can show a barcode, holding a valid "key" to open the gate (e.g. Eurostar Departure Control System). This key can have a limited validity period, and/or a limited number of times it can be used.

2 different cases exist:

NRT/IRT/RPT/group ticket countermark

Client is in possession of a valid ticket for the train leaving from that platform. Possibly in combination with date/time of departure. In that case a connection between the gate and central servers might be needed to deal with delays and last-minute platform changes. In case of a check-in gate (e.g. as used for Eurostar trains between Paris and London), the train number can be entered locally on the devices by a staff member when check-in opens.

Platform passage card

For staff members that need to enter specific areas of the station (e.g. specific platforms) without being in possession of a ticket (e.g. shop owners on a "closed" platform or station staff members). For security reasons, these barcodes should have a (very) limited validity since they can be copied and distributed.

11.2.6. USE CASE 6: Opening of station gates (SiD)

Station gates will only open for clients that are allowed to enter that station (e.g. the case of the NS stations). There can be a limitation in number of stations and/or a limited validity time (from-to). There can be a limited number of times the gates will open. Combinations are also possible (limitation in time and in number of passages).

NRT/IRT/RPT/GRT countermark

Client is in possession of a valid ticket for the train leaving from that station. Possibly in combination with date/time of departure. In that case a connection between the gate and central servers might be needed to deal with delays.

Station passage card

For staff members that need to enter the station without being in possession of a ticket (e.g. shop owners, train staff members). For security reasons, these barcodes should have a (very) limited validity since they can be copied and distributed.

Customer card

For clients holding a card giving him/her the possibility to enter a station.

11.2.7. USE CASE 7: Information function for routing in a station (SiS)

In some stations, different areas or different levels are used by different trains (local, high-speed, intercity,…). Specific information in the barcode can be used to guide the client to the right area of the station (using info point barcode readers or at check-in devices in the station).

11.2.8. USE CASE 8: Barcode to identify tickets for refund processes (SiS)

The minimum information that is needed to retrieve the contract on the server for refunding, depending on tariff conditions or legal regulations e.g.as defined in the EU / CIV regulation in case of train cancellations or certain delays. Occurs after the (theoretical) train departure.

11.2.9. USE CASE 9: Barcode to identify tickets for after sales processes (SiS)

In case of after sale operations, this info is the basic info to retrieve the ticket info on the server. This use case occurs typically before the train leaves and deals with typical after sales operations (refund, exchange).

11.2.10. USE CASE 10: Validation of settlements vs. control data (SiS)

Not in scope of the TAP TSI

11.2.11. USE CASE 11: Annotation, “digital stamp” (SiD)

(info from ticket sales, to be shared with train staff)

On a TAP TSI technical document B.11 based Security in Paper ticket, a train staff member, checking a ticket, can write information on the backside and "secure" it with a stamp. This information is data to be exchanged with colleagues, checking the ticket later on or performing after sales operations.

In case of a SiD ticket with a 2D barcode, the TCO will issue a new barcode (either an extra one or a new one, replacing the old one). This barcode holds the information to be exchanged between the different train staff members or between the train staff member and after sales. On a Smartphone, this could be part of a new barcode, replacing the old one.

Barcode type (→) USE CASE(↓)	Flexible Content **FCB**	Ticket Layout **TLB**	Small Structured **SSB**	Element List **ELB**
1	X	X	O	O
2	X	X	X	X
3	X	O(*)	X	X
4	X	O	X	O
5	X	O	X	O
6	X	O	X	O
7	X	O	X	X
8	X	O(*)	X	O
9	X	O(*)	X	O
10	X	O	X	O
11	X	O	O	O

X=possible, O=not possible,(*) technically possible, but not yet defined in detail

11.3. Table with Data Elements per Use Case

LEGEND:

	Columns: The specific use cases, as defined above
Rows: The data elements per use case (mandatory, optional, …)	

m	mandatory data
om	mandatory detail of an option
c	conditional data (mandatory depending on details of the use case)
o	optional data
na	data not applicable

Details about some specific data elements can be found in § 11.4

In attachment of this document, the .ASN file of all data elements that can be used in a FCB can be found.

Data Element (↓) / Use Case (→)		offline control of validity without reference data on the control device. Typical for check by companies, not involved in TAP TSI like local bus company (reference data: e.g. UIC-station code vs station name) - SID				offline control of validity with reference data on the control device. (reference data: e.g. TAP TSI-station code vs station name) - SID				online control of validity - Security in System - Ticket data in system	automatic control of some data (other controls still to be performed by train staff - e.g. reduction card)	opening of platform gates		opening of station gates (e.g. NS)			information function for routing at station (info point for "routing" the passenger to right platform etc ...)			barcode to identify tickets for refund processes (EG Regulation purposes)	barcode to identify tickets for after sales processes (cross validation of accounting - depends on commercial conditions)	validation of settlements vs. control data (to check if accounting info coming from other RU's is correct)
		tickets (NRT / IRT / RPT / FIP / Parking / countermark)	customer card	station passage card	voucher	tickets (NRT / IRT / RPT / FIP / Parking / countermark)	customer card	station passage card	voucher	all	tickets (NRT / IRT / RPT / countermark)	tickets (NRT / IRT / RPT / FIP / countermark)	station passage card	tickets (NRT / IRT / RPT / FIP / countermark)	station passage card	customer card	NRT ticket	IRT ticket	countermark	all	all	all
UICBarcode Structured Data	issuingDetail	m	m	m	m	m	m	m	m	m	na	na	na	na	na	na	na	na	na	m	m	m
	transportDocument	m	m	m	m	m	m	m	m	m	m	na	na	na	na	na	na	na	na	m	m	m
	controlDetail	m	na	m	m	m	m	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	travelerDetail	c	c	c	c	c	c	m	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	extension	o	o	o	o	o	o	o	o	na	na	na	na	na	na	na	na	na	na	na	na	na
Document Data	token	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
	reservation	c	na	na	na	c	na	na	na	c	c	na	na	na	na	na	na	na	na	c	c	c
	carCarriageReservation	c	na	na	na	c	na	na	na	c	c	na	na	na	na	na	na	na	na	c	c	c
	openTicket	c	na	na	na	c	na	na	na	c	c	na	na	na	na	na	na	na	na	c	c	c
	pass	c	na	na	na	c	na	na	na	c	c	na	na	na	na	na	na	na	na	c	c	c
	voucher	na	na	na	m	na	na	na	m	c	na	na	na	na	na	na	na	na	na	c	c	c
	customerCard	na	m	na	na	na	m	na	na	c	c	na	na	na	na	na	na	na	na	c	c	c
	counterMark	c	na	na	na	c	na	na	na	c	na	na	na	na	na	na	na	na	na	c	c	c
	parkingGround	c	na	na	na	c	na	na	na	c	c	na	na	na	na	na	na	na	na	c	c	c
	fipTicket	c	na	na	na	c	na	na	na	c	na	na	na	na	na	na	na	na	na	c	c	c
	stationPassage	na	na	m	na	na	na	m	na	c	na	na	na	na	na	na	na	na	na	c	c	c
	extension	o	o	o	o	o	o	o	o	c	na	na	na	na	na	na	na	na	na	c	c	c
IssuingData	issuer	m	m	m	m	m	m	m	m	m	na	na	na	na	na	na	na	na	na	m	m	m
	securityProvider	m	m	m	m	m	m	m	m	m	na	na	na	na	na	na	na	na	na	m	m	m
	issuingYear/Day/Time	m	m	m	m	m	m	m	m	m	m	na	na	na	na	na	na	na	na	m	m	m
	issuerName	m	m	m	m	m	m	m	m	na	na	na	na	na	na	na	na	na	na	na	na	na
	specimen	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m
	activated	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m
	currency	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	currencyFract	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	issuerPNR (IssuerTicketId)	o	o	o	o	o	o	o	o	na	na	na	na	na	na	na	na	na	na	na	na	na
	extension	o	o	o	o	o	o	o	o	na	na	na	na	na	na	na	na	na	na	na	na	na
	issuedOnTrainNum/ issuedOnTrain	c	c	c	c	c	c	c	c	na	c	na	na	na	na	na	na	na	na	na	na	na
	issuedOnLine	c	c	c	c	c	c	c	c	na	c	na	na	na	na	na	na	na	na	na	na	na
	SecurePaperTicket	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c	c
	pointOfSale	o	o	o	o	o	o	o	o	na	c	na	na	na	na	na	na	na	na	na	na	na
ControlData	identificationByCardReference	c	c	c	c	c	c	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	identificationByIdCard	c	c	c	c	c	c	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	identificationByPassportId	c	c	c	c	c	c	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	passportValidationRequired	c	c	c	c	c	c	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	IdentificationItem	c	c	c	c	c	c	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	onlineValidationRequired	c	c	c	c	c	c	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	randomOnlineValidationRequired	c	c	c	c	c	c	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na

	ageCheckRequired	c	na	c	c	c	na	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	reductionCardCheckRequired	c	na	c	c	c	na	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	includedTickets	o	na	na	o	o	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na
	infoText	o	na	na	o	o	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na
	extension	o	na	na	o	o	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na
TravelerData	traveler	c	o	c	c	c	o	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	groupName	c	na	na	na	c	na	na	na	m	na	na	na	na	na	na	na	na	na	m	m	m
	PreferedLanguage	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
ReservationData	train	m	na	na	na	m	na	na	na	m	m	na	na	na	na	na	na	m	na	m	m	m
	travelDate	m	na	na	na	m	na	na	na	m	m	m	na	m	na	na	na	m	na	m	m	m
	reference	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	service	m	na	na	na	m	na	na	na	na	m	na	na	na	na	na	na	m	na	na	na	na
	serviceBrandNb	na	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	serviceBrand/ serviceBrandUTF8	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	serviceBrandAbr/ serviceBrandAbrUTF8	m	na	na	na	na	na	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na
	stationCodeTable	na	na	na	na	m	na	na	na	na	m	m	na	m	na	na	na	na	na	na	na	na
	fromStationNb	na	na	na	na	m	na	na	na	na	m	m	na	m	na	na	na	na	na	na	na	na
	toStationNb	na	na	na	na	m	na	na	na	na	na	m	na	m	na	na	na	na	na	na	na	na
	fromStation/ fromStationUTF8	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	toStation/ toStationUTF8	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	departureTime	m	na	na	na	na	m	na	na	na	na	na	na	na	na	na	na	m	na	na	na	na
	arrivalTime	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	arrivalDate	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	carrier	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	classCode	c	na	na	na	c	na	na	na	na	m	na	na	na	na	na	na	m	na	na	na	na
	places	c	na	na	na	c	na	na	na	na	m	na	na	na	na	na	na	m	na	na	na	na
	bicyclePlaces	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	m	na	na	na	na
	compartmentDetails	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	numberOfOverbooked	c	na	na	na	c	na	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na
	berth	c	na	na	na	c	na	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na
	tariff	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	priceType	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	typeOfSupplement	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	numberOfSupplements	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	luggage	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	infoText	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	extension	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
CarCarriageReservationData	train	m	na	na	na	m	na	na	na	m	m	m	na	m	na	na	na	m	na	m	m	m
	travelDate	m	na	na	na	m	na	na	na	m	m	m	na	m	na	na	na	m	na	m	m	m
	reference	m	na	na	na	m	na	na	na	m	m	na	na	na	na	na	na	na	na	m	m	m
	serviceBrandNb	na	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	serviceBrand/ serviceBrandUTF8	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	serviceBrandUTF8/ serviceBrandAbrUTF8	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	stationCodeTable	na	na	na	na	m	na	na	na	na	na	m	na	m	na	na	na	m	na	na	na	na
	fromStationNb	na	na	na	na	m	na	na	na	na	na	m	na	m	na	na	na	m	na	na	na	na
	toStationNb	na	na	na	na	m	na	na	na	na	na	m	na	m	na	na	na	na	na	na	na	na
	fromStation/ fromStationUTF8	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	toStation/ toStationUTF8	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	coach	m	na	na	na	m	na	na	na	na	m	na	na	na	na	na	na	m	na	na	na	na
	place	m	na	na	na	m	na	na	na	na	m	na	na	na	na	na	na	m	na	na	na	na
	compartmentDetails	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	numberPlate	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	trailerPlate	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	carCategory	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	boatCategory	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	textileRoof	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	roofRackType	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	luggageRack	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	skiRack	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	boxRack	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	rackWithOneBox	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	rackWithTwoBoxes	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	bicycleRack	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	otherRack	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	roofRackHeight	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	attachedBoats	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	attachedBicycles	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	attachedSurfboards	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	beginLoadingTime	o	na	na	na	o	na	na	na	na	na	m	na	m	na	na	na	m	na	na	na	na
	endLoadingTime	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	m	na	na	na	na
	beginUnLoadingTime	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	endUnLoadingTime	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	loadingListEntry	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	loadingDeck	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	m	na	na	na	na
	tariff	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	priceType	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na

	infoText	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	extension	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
OpenTicketData	reference/ referenceNum	m	na	na	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	m	m	m
	productOwner	m	na	na	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	m	m	m
	extProductOwner	m	na	na	na	m	na	na	na	o	na	na	na	na	na	na	na	na	na	o	o	o
	productId	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	productCode	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	returnIncluded	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	stationCodeTable	na	na	na	na	m	na	na	na	na	m	m	na	m	na	na	m	na	na	na	na	na
	fromStationNb	na	na	na	na	m	na	na	na	na	m	m	na	m	na	na	m	na	na	na	na	na
	toStationNb	na	na	na	na	m	na	na	na	na	m	m	na	m	na	na	m	na	na	na	na	na
	fromStationNbReturn	na	na	na	na	c	na	na	na	na	c	c	na	c	na	na	c	na	na	na	na	na
	toStationNbReturn	na	na	na	na	c	na	na	na	na	c	c	na	c	na	na	c	na	na	na	na	na
	fromStation/ fromStationUTF8	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	toStation/ toStationUTF8	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	fromStationReturn/ fromStationReturnUTF8	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	toStationReturn/ toStationReturnUTF8	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validRegionDesc	m	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validRegion	o	na	na	na	m	na	na	na	na	m	m	na	na	na	na	m	na	na	na	na	na
	validReturnRegionDesc	c	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validReturnRegion	c	na	na	na	m	na	na	na	na	c	na	na	na	na	na	c	na	na	na	na	na
	validFromDay	m	na	na	na	m	na	na	na	na	m	m	na	m	na	na	m	na	na	na	na	na
	validFromTime	c	na	na	na	c	na	na	na	na	c	c	na	c	na	na	c	na	na	na	na	na
	validUntilDay	m	na	na	na	m	na	na	na	na	m	m	na	m	na	na	m	na	na	na	na	na
	validUntilTime	c	na	na	na	c	na	na	na	na	c	c	na	c	na	na	c	na	na	na	na	na
	activatedDay	c	na	na	na	c	na	na	na	na	c	c	na	c	na	na	c	na	na	na	na	na
	classCode	m	na	na	na	m	na	na	na	na	m	na	na	na	na	na	m	na	na	na	na	na
	serviceLevelCode	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	included/ excluded Carriers	m	na	na	na	m	na	na	na	na	m	na	na	na	na	na	m	na	na	na	na	na
	included / excluded ServiceBrands	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	m	na	na	na	na	na
	tariffs	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	luggage	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	infoText	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	includedAddOns	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	extension	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
PassData	reference/referenceNum	m	na	na	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	m	m	m
	productOwner	m	na	na	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	m	m	m
	extProductOwner	o	na	na	na	o	na	na	na	m	na	na	na	na	na	na	na	na	na	m	m	m
	passType	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	classCode	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validFromDay	m	na	na	na	m	na	na	na	na	m	m	na	m	na	na	na	na	na	na	na	na
	validFromTime	c	na	na	na	c	na	na	na	na	c	c	na	c	na	na	na	na	na	na	na	na
	validUntilDay	m	na	na	na	m	na	na	na	na	m	m	na	m	na	na	na	na	na	na	na	na
	validUntilTime	c	na	na	na	c	na	na	na	na	c	c	na	c	na	na	na	na	na	na	na	na
	numberOfValidityDays	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	numberOfDaysOfTravel	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	countries	m	na	na	na	m	na	na	na	na	m	m	na	m	na	na	na	na	na	na	na	na
	included / excluded carriers	m	na	na	na	m	na	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na
	tariffs	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	infoText	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	extension	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
VoucherData	reference/ referenceNum	na	na	na	m	na	na	na	m	m	na	na	na	na	na	na	na	na	na	m	m	m
	validFromYear/Day	na	na	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na
	validUntilYear/Day	na	na	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na
	value	na	na	na	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	productOwner	na	na	na	m	na	na	na	m	m	na	na	na	na	na	na	na	na	na	m	m	m
	type	na	na	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na
	infoText	na	na	na	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na
FIPTicket Data	reference/ referenceNum	m	na	na	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	m	m	m
	validFromDay	m	na	na	na	m	na	na	na	na	m	na	na	m	na	na	na	na	na	na	na	na
	validUntilDay	m	na	na	na	m	na	na	na	na	m	na	na	m	na	na	na	na	na	na	na	na
	carrier	m	na	na	na	m	na	na	na	na	m	na	na	m	na	na	na	na	na	na	na	na
	number Of TravelDays	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	includesSupplements	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	classCode	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
StationPassageData	reference/ referenceNum	na	na	o	na	na	na	o	na	m	na	na	m	na	m	na	na	na	na	m	m	m
	productType	na	na	o	na	na	na	o	na	na	na	na	m	na	m	na	na	na	na	na	na	na
	productCode	na	na	o	na	na	na	o	na	na	na	na	m	na	m	na	na	na	na	na	na	na
	stationCodeTable	na	na	na	na	na	na	na	na	na	m	na	m	na	m	na	na	na	na	na	na	na
	stationNb	na	na	na	na	na	na	na	na	na	m	na	m	na	m	na	na	na	na	na	na	na
	station/ stationUTF8	na	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	passageAllowed	na	na	c	na	na	na	c	na	na	m	na	c	na	c	na	na	na	na	na	na	na
	numberOfDaysValid	na	na	c	na	na	na	c	na	na	m	na	c	na	c	na	na	na	na	na	na	na
	validFromDay	na	na	m	na	na	na	m	na	na	m	na	m	na	m	na	na	na	na	na	na	na
	validFromTime	na	na	c	na	na	na	c	na	na	c	na	c	na	c	na	na	na	na	na	na	na
	validUntilDay	na	na	m	na	na	na	m	na	na	m	na	m	na	m	na	na	na	na	na	na	na
	validUntilTime	na	na	c	na	na	na	c	na	na	c	na	c	na	c	na	na	na	na	na	na	na
CustomerCardData	customer	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na

	cardId/ cardIdNum	na	m	na	na	na	m	na	na	m	na	na	na	na	na	na	na	na	na	m	m	m
	validFromYear	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validFromDay	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validUntilYear	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validUntilDay	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	classCode	na	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	issuingTime	na	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	cardType	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	cardTypeDescr	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	customerStatus	na	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	costomerStatusDescr	na	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	includedServices	na	c	na	na	na	c	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na
ParkingGroundData	parkingGroundId	m	na	na	na	m	na	na	na	m	m	na	na	na	na	na	na	na	na	m	m	m
	parkingDate	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	reference	m	na	na	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	m	m	m
	accessCode	m	na	na	na	m	na	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na
	location	m	na	na	na	m	na	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na
	stationNb	na	na	na	na	m	na	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na
	station	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	specialInformation	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	entryTrack	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	extension	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
CountermarkData	reference/referenceNum	m	na	na	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	m	m	m
	ticketReference/ticketReferenceNum	m	na	na	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	m	m	m
	productOwner	na	na	na	na	na	na	na	na	m	na	na	na	na	na	na	na	na	na	m	m	m
	extProductOwner	na	na	na	na	na	na	na	na	o	na	na	na	na	na	na	na	na	na	o	o	o
	productId	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	productCode	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	numberOfCountermark	m	na	na	na	m	na	na	na	m	na	na	na	na	na	na	na	na	na	m	m	m
	totalOfCountermarks	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	groupName	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	stationCodeTable	na	na	na	na	m	na	na	na	na	m	na	na	m	na	na	na	na	na	na	na	na
	fromStationNb	na	na	na	na	m	na	na	na	na	m	na	na	m	na	na	na	na	na	na	na	na
	toStationNb	na	na	na	na	m	na	na	na	na	m	na	na	m	na	na	na	na	na	na	na	na
	fromStation/ fromStationUTF8	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	toStation/toStationUTF8	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	fromStationReturnNb	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	toStationReturnNb	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	fromStationReturn/ fromStationReturnUTF8	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	toStationReturn/toStationReturnUTF8	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validRegionDesc	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validRegion	na	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validReturnRegionDesc	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validReturnRegion	na	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	validFromDay	m	na	na	na	m	na	na	na	na	m	na	na	m	na	na	na	na	na	na	na	na
	validFromTime	c	na	na	na	c	na	na	na	na	c	na	na	c	na	na	na	na	na	na	na	na
	validUntilDay	m	na	na	na	m	na	na	na	na	m	na	na	m	na	na	na	na	na	na	na	na
	validUntilTime	c	na	na	na	c	na	na	na	na	c	na	na	c	na	na	na	na	na	na	na	na
	classCode	m	na	na	na	m	na	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na
	includedCarriers	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	includedServiceBrands	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	excludedServiceBrands	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	infoText	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	extension	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
LayoutElement	colum	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	row	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	heigth	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	length	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	format	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	textLine	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
IncludedOpenTicketType	productOwner	om	na	na	na	om	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	extProductOwner	om	na	na	na	om	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	productId	om	na	na	na	om	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	productCode	om	na	na	na	om	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	stationCodeTable	om	na	na	na	om	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validRegion	om	na	na	na	om	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validFromDay	om	na	na	na	om	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validFromTime	om	na	na	na	om	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validUntilDay	om	na	na	na	om	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	validUntilTime	om	na	na	na	om	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	classCode	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	serviceLevelCode	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	includedCarriers	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	includedServiceBrands	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	excludedServiceBrands	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	tariffs	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	infoText	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	extension	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
TariffType	number	m	na	c	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na

	passengerType	m	na	c	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	addonPassengers	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	addonPassengerType	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	ageBelow	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	ageAbove	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	traverlerid	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	stationCodeTable	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	fromStationNb	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	toStationNb	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	supplyingCarrier	c	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	offerIdentification	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	series	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	tariffIdNum	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	tariffId	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	tariffDesc	m	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	reductionCard	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
CardReferenceType	railCardIssuer	om	na	om	om	om	na	om	om	na	na	na	na	na	na	na	na	na	na	na	na	na
	nonRailCardIssuer	c	na	c	c	c	na	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	cardName	om	na	om	om	om	na	om	om	na	na	na	na	na	na	na	na	na	na	na	na	na
	cardNumber	om	na	om	om	om	na	om	om	na	na	na	na	na	na	na	na	na	na	na	na	na
	cardType	om	na	om	om	om	na	om	om	na	na	na	na	na	na	na	na	na	na	na	na	na
	cardCode	om	na	om	om	om	na	om	om	na	na	na	na	na	na	na	na	na	na	na	na	na
	leadingCardNumber	c	na	c	c	c	na	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	trailingCardNumber	c	na	c	c	c	na	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	trailingCardCode	c	na	c	c	c	na	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
TravelerType	firstName	om	c	om	om	om	c	om	om	na	na	na	na	na	na	na	na	na	na	na	na	na
	secondName	c	c	c	c	c	c	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	lastName	om	c	om	om	om	c	om	om	na	na	na	na	na	na	na	na	na	na	na	na	na
	idCard	o	na	o	o	o	na	o	o	na	na	na	na	na	na	na	na	na	na	na	na	na
	passportId	o	na	o	o	o	na	o	o	na	na	na	na	na	na	na	na	na	na	na	na	na
	title	c	c	c	c	c	c	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	gender	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	customerId	o	c	o	o	o	c	o	o	na	na	na	na	na	na	na	na	na	na	na	na	na
	customerNum	o	c	o	o	o	c	o	o	na	na	na	na	na	na	na	na	na	na	na	na	na
	yearOfBirthYear	c	c	c	c	c	c	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	dayOfBirth	c	c	c	c	c	c	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	ticketHolder	c	na	na	c	c	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	passengerType	c	c	c	c	c	c	c	c	na	na	na	na	na	na	na	na	na	na	na	na	na
	status	o	c	o	o	o	c	o	o	na	na	na	na	na	na	na	na	na	na	na	na	na
CustomerStatusType	statusProvider	om	c	om	om	om	c	om	om	na	na	na	na	na	na	na	na	na	na	na	na	na
	extStatusProvider	om	c	om	om	om	c	om	om	na	na	na	na	na	na	na	na	na	na	na	na	na
	customerStatus	om	c	om	om	om	c	om	om	na	na	na	na	na	na	na	na	na	na	na	na	na
	customerstatusDescr	om	c	om	om	om	c	om	om	na	na	na	na	na	na	na	na	na	na	na	na	na
RegionalValidityType	trainLink	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	viaStations	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	zones	o	na	na	na	o	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	lines	o	na	na	na	o	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	polygone	o	na	na	na	o	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
TrainLinkType	train	om	na	na	na	om	na	na	na	na	c	c	na	na	na	na	na	na	na	na	na	na
	travelDate	om	na	na	na	om	na	na	na	na	c	c	na	na	na	na	na	na	na	na	na	na
	departureTime	om	na	na	na	om	na	na	na	na	c	c	na	na	na	na	na	na	na	na	na	na
	stationCodeTable	na	na	na	na	om	na	na	na	na	c	c	na	na	na	na	na	na	na	na	na	na
	fromStationNb	na	na	na	na	om	na	na	na	na	c	c	na	na	na	na	na	na	na	na	na	na
	toStationNb	na	na	na	na	om	na	na	na	na	c	c	na	na	na	na	na	na	na	na	na	na
	fromStation/ fromStationUtf8	om	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	toStation/ to StationUTF8	om	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
LineType	codeTable	om	na	na	na	om	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	entryStation	om	na	na	na	om	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	terminatingStation	om	na	na	na	om	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	city	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	carrierRICS	om	na	na	na	om	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	carrierCode	om	na	na	na	om	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	lineId	o	na	na	na	o	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	binaryZoneId	o	na	na	na	o	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
ZoneType	codeTable	om	na	na	na	om	na	na	na	na	na	na	na	na	na	na	c	na	na	na	na	na
	entryStation	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	c	na	na	na	na	na
	terminatingStation	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	c	na	na	na	na	na
	city	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	c	na	na	na	na	na
	carriercompany CODE	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	c	na	na	na	na	na
	carrierCode	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	c	na	na	na	na	na
	zoneId	om	na	na	na	om	na	na	na	na	na	na	na	na	na	na	c	na	na	na	na	na
	binaryZoneId	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	c	na	na	na	na	na
ViaStationType	stationCodeTable	na	na	na	na	m	na	na	na	na	m	na	na	na	na	na	c	na	na	na	na	na
	stationNb	na	na	na	na	m	na	na	na	na	m	na	na	na	na	na	c	na	na	na	na	na
	alternativeStations	na	na	na	na	c	na	na	na	na	c	na	na	na	na	na	c	na	na	na	na	na
	alternativeRoutes	na	na	na	na	c	na	na	na	na	c	na	na	na	na	na	c	na	na	na	na	na
	route	na	na	na	na	c	na	na	na	na	c	na	na	na	na	na	c	na	na	na	na	na
	border	na	na	na	na	c	na	na	na	na	c	na	na	na	na	na	c	na	na	na	na	na
	carrier	na	na	na	na	c	na	na	na	na	c	na	na	na	na	na	c	na	na	na	na	na
	seriesId	na	na	na	na	c	na	na	na	na	c	na	na	na	na	na	c	na	na	na	na	na
	routeId	na	na	na	na	c	na	na	na	na	c	na	na	na	na	na	c	na	na	na	na	na
PolygoneType	edges	na	na	na	na	na	na	na	na	na	c	na	na	na	na	na	c	na	na	na	na	na
TicketLinkType	reference/ referenceNum	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na

	issuerName	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	productOwner	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	extProductOwner	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	ticketType	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	linkMode	o	na	na	na	o	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
VatDetailData	country	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	vatAmount	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	vatPercentage	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
ResTariffType	code	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	number	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	description	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
PlacesType	coach	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	m	na	na	na	na
	placeString	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	placeDescription	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	place/ placeNum	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
BerthDetailData	berthType	c	na	na	na	c	na	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na
	number	c	na	na	na	c	na	na	na	na	m	na	na	na	na	na	na	na	na	na	na	na
	gender	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
CompartmentDetailsType	compartmentType	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	specialAllocation	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	coachTypeDescr	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	comparttmentTypeDescr	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	specialAllocationDescr	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
	position	c	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na	na
GeoCoordinateType	geoUnit	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	coordinateSystem	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	hemisphereLongitude	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	hemisphereLatitude	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	longitude	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	latitude	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na
	accuracy	c	na	na	na	c	na	na	na	na	c	na	na	na	na	na	na	na	na	na	na	na

11.4. "DATA ELEMENTS"

Brief description of the different data elements as they appear in the BARCODE.ASN document. To improve readability of the attached ASN.1 document, the names used in this chapter are the same as the ones used in the ASN.1 document.

Some elements do exist in multiple format types. Theoretically multiple format types could be used per element, but only 1 format type per element is allowed to be included. The reason why multiple format types exist is to make it possible, depending on the use case, to have the element machine interpretable or human interpretable, to have a need of a lookup table on the machine or not. The limited space in the 2D barcode does not allow to have different data format types co-existing in one single barcode.
As an example we take "station": 2 possibilities exist
-there is the code of the station, which gives a unique identification of every possible station.
-there is the name of the station (with language issues…)
Using the code has as advantage that different languages can be used, the ticket can be checked by a machine, the back office is easier to organize … . The main disadvantage of using the coded station name is that TCO's dealing with occasional checks of some specific

The choice of the code list is based on bilateral or multilateral agreements between issuers and TCO's. The content of the UicRailTicketData element allows the reading device to determine which code list is used by the issuer so which format type is used for each element in the barcode.

In different data elements, future extensions are allowed (indicated with a ",…"). This is not to be used by the railway undertakings for bilateral extensions of the standard. It is intended for future adaptations only. Barcode reading software, developed following this leaflet must support this to be "forward-compatible".

Bilateral agreements are possible in the leaflet, but only in the zones, defined for this purpose ("extensiondata").

The different groups of data-elements:

UicRailTicketData

- issuingDetail
  - Data specific on the issuer and the issuing itself (company, sales channel, timestamp, payment details, …)
- travelerDetail
  - Details about the type of travellers + their preferred language (e.g. to display the ticket information on a screen of an un-manned device in case a ticket is displayed on a screen of a check-in device or a ticket vending machine
- transportDocuments
  - The actual tickets/contracts. The different documents that can be included are (one or more): OpenTicket, Pass, Reservation, Carcarriagereservation,voucher, customercard, group ticket countermark, parking ticket, fipticket, stationpassage.
- controlDetail

How the ticket should be checked (e.g. if a passport identification is needed, but also of how many % of tickets randomly need online check (additional SiS), …), if an age check is needed (in case the ticket is only valid for a specific age (youngsters, child, …)
Infotext (to be used for annotation purposes), …

extension
Specific data of the issuer – defined bilateral

IssuingDetail

SecurityProvider / Issuer (if not same as SecurityProvider)
Which company issued the ticket? This is important to know which security data - private key - is used (to use the right public key)

IssuingYear/Day/Time
Moment the ticket was issued (e.g. to avoid last-minute or last-second buying when a train staff member shows up)

Currency (payment is electronically by default)

Specimen / secured paper
Binary elements indicating if the ticket was specimen ticket or not / if the ticket was printed on secured paper or not. The secured paper flag is important to avoid scanning of the barcode of a SiP ticket (with additional security) and printing the barcode on a fake non-SiP ticket.

Issued on board / on-line / @point of sales
Element indicating where the ticket has been issued.

Activated
Binary element indicating if the ticket was already activated.

TravelerDetail

List of travellers (travelerTypes)
Elements, holding – per traveller – details like name, identity card number, gender, birth date, passenger type, …

preferedLanguage
used e.g. if the passenger has to visualize info, this element can put the user-interface in his/her preferred language

groupname (in case of a group)
The name, defined by the group

TransportDocument

Token
The token is just an ID. This ID is composed of 2 elements: first, the identification of the ID issuer and second, the ID itself.
Since an issuer can use a lot of different devices (payment card number, frequent traveller number, …) it is better to use, as a first part of the ID, a so-called Issuer Identification Number.

+ one of the following:
by default, one barcode may only host 1 contract (“document”). If multiple documents have to be combined in one barcode, this is technically possible (ASN1:”SEQUENCE of ticket”), but it should be decided on a bilateral base between issuer and TCO. Reason: refund, after sales operations, partial usage of barcode …

Reservation

Train number, departure & arrival-date &-time, seats, berth, service level,…
Typical reservation data
Product owner, Product_id, service brand
Organisation, responsible for the definition of this product
The reference of the product, defined by the product owner
From-to stations
Origin/destination of the leg
Carriers
List of carriers on the reserved route
Bicycle places, luggage restriction info
Info text
Extra information to be exchanged
Extension data
Bilateral decided data to be exchanged

CarCarriageReservation
Trainnumber, BeginLoadingDate&-Time, EndLoadingTime
Licenseplate, carcategory, textileroof, roofrack, elements on roof,…
Typical car carriage reservation information, part of the contract
Productowner, Product_id, servicebrand
Organisation, responsible for the definition of this product
The reference of the product, defined by the product owner
From-to stations
Origin/destination of the leg
Trailerplate, trailertype
In case of an optional trailer, attached to the car.
Carriers: Carriers on the route
List of carriers on the reserved route
Infotext
Extra information to be exchanged
Extensiondata
Bilateral decided data to be exchanged

OpenTicket (for NRT tickets)
Productowner, Product_id
Organisation, responsible for the definition of this product
The reference of the product, defined by the product owner
Stationcodetable,From, To
List of Via stations
Origin / Destination of the open ticket
Valid Region
Used to indicate via stations in a route
Other options are : zones, lines (city transport e.g.), train links.
“zones” can be defined by a code or a geo-coordinate (GPS-) polygon
Valid from / until, class
Period of validity
Servicelevel
Specific extra service levels (premium, …)
Included carriers / included service brands
List of carriers on the route
Infotext

Extra information to be exchanged

Luggage

In some cases, luggage must be defined separately

Extensiondata

Bilateral decided data to be exchanged

Pass (Rail passes)

Productowner, Product_id

Organisation, responsible for the definition of this product

The reference of the product, defined by the product owner

Passtype

Type of pass, as defined in a lookup table or readable description

Valid from / until - Number of validity days

Defining validity period (time)

Number of possible trips / number of days of travel

Defining validity period (in number of trips / travel days)

Activated days / Included countries

Number of activated days / valid countries (pass specific info)

Infotext

Extra information to be exchanged

Extensiondata

Bilateral decided data to be exchanged

Voucher (For group tickets)

Productowner, Product_id

Organisation, responsible for the definition of this product

The reference of the product, defined by the product owner

Valid from / until

Defining validity period (time)

Type of voucher

Numerical – coding defined by the product owner

infotext

Extra information to be exchanged

Extensiondata

Bilateral decided data to be exchanged

CustomerCard (e.g. Bahncard)

Customer

Cardholder

Valid from / until

Validity period of the card

Class

Class where the card is valid for

Card type / status

Coding/description of the customer card + status (gold, silver, …)

Included services

List of services

Countermark (Group ticket add-on)

Productowner, Product_id

Organisation, responsible for the definition of this product

The reference of the product, defined by the product owner

Ticketreference

Link to the group ticket

Number of Countermark / total number of countermarks

Specific countermark data

Stationcodetable,From, To

List of Via stations

Origin / Destination of the ticket

Valid from/until

Begin/end of validity

Class

Default 2nd

Included carriers / included service brands

infotext

Extra information to be exchanged

Extensiondata

Bilateral decided data to be exchanged

ParkingGround

Productowner, Product_id

Organisation, responsible for the definition of this product

The reference of the product, defined by the product owner

parkingID , location, station code

Identification of the parking ground

from / until date

Validity period

Accesscode

“Password” to open the parking gate

License plate

ID of the car

Extensiondata

Bilateral decided data to be exchanged

FIPTicket (can be used for tickets for train staff members and their benefits)

Productowner, Product_id

Organisation, responsible for the definition of this product

The reference of the product, defined by the product owner

valid from / until

Validity period of the FIP ticket

Carriers

List of carriers for which the ticket is accepted

number of travel days

Number of travel days allowed

activated days

list of days on which the ticket can be used

StationPassage

Productowner, Product_id

Organisation, responsible for the definition of this product

The reference of the product, defined by the product owner

Station IDs

The stations where passage is allowed

Area IDs

The specific areas in the station where passage is allowed

Valid from / until / number of days valid

Validity period

Extension

Bilateral decided data to be exchanged

Controldata

Cards that can be used to identify client

IdentificationbyIdcard – identificationbypassportId

If the client has to show IDcard resp. Passport during ticket check

Reductioncardcheckrequired

If a reduction card must be shown by the passenger and checked while the TCO performs a ticket check

Number of random “deep” checks needed

Number (percentage of total) of tickets of this type that should be checked more in detail

infotext for the controller

annotationinfo to be exchanged between different issuers/controllers

includedTickets

Other tickets that should be checked together with this ticket

11.5. "ENCODING MECHANISM"

11.5.1. Introduction

The data as defined in the use cases and translated following the table above (ASN.1) has to be encoded following the ***PER unaligned*** encoding rule (see ITU-T Recommendation X.691 "OSI networking and system aspects – Abstract Syntax Notation One (ASN.1) Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)" file: X.691-0207.pdf).

11.5.2. Composition of the barcode content

The content of the barcode, holding the structured data, is composed of the following records:

- "Main record" ("U_HEAD" - optional – to be backwards compatible with TAP TSI technical document B.7 DST barcodes)
- Record with RCT2 ticket layout ("U_TLAY" - optional to be backwards compatible with TAP TSI technical document B.7 DST barcodes).
- **Record with variable size structured data ("U_FLEX").**
- Record(s) based on specific bilateral standards (optional)

The absolute minimum set of records to define a 2D barcode following this leaflet is a **header** and a record type **U_FLEX**.

The sequence of the records is seized by means of a compressing technique and then printed/displayed on the support medium (paper ticket, home-printed ticket, Smartphone screen, …).

11.5.3. Definition of the record structure

As in the TAP TSI technical document B.7, the different categories of content require a flexible structure. The structure must answer to the following demands:

- General record types, that are handed out and interpreted by all UIC members
- For specific ticket data, an UIC member can define its own record types. This way attributes that are not defined in the UIC standards can be used as ticket message content.

Each record type is composed according to the following pattern:

Number in sequence	***Element***	***Number of characters***	***Mandatory***	***Code***	***Comments***
1	Record ID	6A	X	X	Composition: • "Uxxxxx" for record types, standard in UIC. "xxxxx" is variable and determines the type • company Code of 4 characters + "xx" for record types defined by separate TCOs. "xx" is variable and can be filled

					in freely by the TCO for each type (2 characters)
2	Record version	2N	X		Allows different versions of one record type (having the same record ID)
3	Record length	4N	X		Number of bytes of the record data
4	Record data	Data Bytes			The actual record data

11.5.4. Definition of the "Structured Data"-record structure (U_FLEX)

Number in sequence	***Element***	***Number of characters***	***Mandatory***	***Code***	***Comments***
1	Record ID	6A	X	X	ID is "U_FLEX" (UIC flexible, structured data barcode message)
2	Record version	2N	X		Allows different versions to co-exist (important in case of pre-sales)
3	Record length	4N	X		Number of bytes in the record data, starting from the first character of the "Record ID" element
4	The ASN.1 data	NBytes	X		The actual data as defined in the data-definition chapter, keeping in mind the right use case. The data, in ASN.1 format is following the PER unaligned encoding rules

11.5.5. Record types for ticket data in accordance with the standards of a specific TCO

The distributing RU can include attributes in the barcode that are not defined in the UIC standard. The DST can also be used for domestic tickets that are not composed according to UIC layout standards.

There is also a possibility to integrate DST – layout based ticket info (as defined in the TAP TSI technical document B.7 "DST"). The messaging is fully backwards compatible with this barcode standard. Existing parsers, developed based on the TAP TSI technical document B.7, will be looking for the right info (as defined in the TAP TSI technical document B.7), skipping the data defined in this leaflet

RU can also define their own record types. As long as the base structure of the record is respected (see "Definition of the record structure"), no other directives for the internal composition of this record exist.

These records can be added to the U_flex records to define the whole message to be translated in the barcode.

RU's that defined their (domestic, bilateral, or international IRTHP) system following the old UIC 918-3 leaflet will be able to continue using it, their parser will be able to "skip" the U_flex record.

Definition of a RU specific record (e.g. in domestic ticketing):

Number in sequence	Element	Number of characters	Mandatory	Code	Comments
1	Record ID	6A	x	X	companycode of 4 characters + ID (2 characters) The companycode is the number of the TCO defining the specific record type. The ID is composed by the TCO himself and contains 2 alphabetic signs that can freely be chosen.
2	Record version	2N	x		
3	Record length	4N	x		
…	…	Bytes			Next there are the actual elements of the record in accordance to the standard specific for the TCO.

11.5.6. Definition of the entire DST message structure

The DST message structure is defined below. Similar to the record definitions it contains header elements containing type id and version.

The entire content of the DST is protected by means of a digital signature, that guarantees:

- Integrity:
  Even the smallest possible manipulation of the content (i.e. changing from 1st to 2nd class) leads to an invalid signature. Forged DSTs will be recognized immediately by verifying the signature.
- Authenticity:
  Since only the possessor of the private key is able to create the signature, the authorship of the DST is proved.

Because the key necessary for the control of the signature cannot be fully protected against theft (due to its presence on each control apparatus), an asymmetric algorithm is used (public/private key). The message header thus contains a signature generated from the algorithm DSA ("digital signature algorithm", see [FIPS186]).

Definition of the entire DST message structure:

Number in sequence	Element	Number of characters	Mandatory	Code	Comments
1	Unique ID	3A	X	X	"#UT" for 'UIC Ticket'
2	Messagetype version	2N	X		"01" (to be compatible with 918-3)
3	companyCode of the RU that is signing	4N	X	X	Allows the identification of the public key necessary for the verification in

					combination with the following element
4	ID of the signature key	5A	X		The ID must be managed by the RU issuing the signature key
5	Signature	50A	X		DSA signature for the message after compression (next element) in ASN.1 representation. If the actual ASN.1 representation is shorter than 50 bytes, it should be enlarged to the length of 50 by adding null bytes.
6	Length of compressed message	4N	X		
7	Compressed message	A	X		The entire record sequence compressed with DEFLATE.

This Compressed message can be composed of

- different layout based messages (see 918-3) (Record_ID: U_HEAD, U_TLAY)
- specific messages of RU's for domestic travel (Record_ID: company-code+2digits)
- the structured data message (as defined in this leaflet) (Record_ID: U_flex)

11.5.7. Compressing procedure

For the compressing procedure the algorithm Deflate will be applied. The specification of Deflate can be found in [RFC1951] (see RFC1951 DEFLATE Compressed Data Format – Specification version 1.3 May 1996 - Peter Deutsch).

11.5.8. The 2D Barcode symbol

When the message is translated in a 2D AZTEC barcode, the following specifications are mandatory:

Parameter	**Value**	**Comments**
Symbology used	Aztec	Specification see [AIMBC13].
Number of modules	Depends on size of message	see Aztec
Share of fault correction data	23%	For Aztec 23% is the standard value for fault correction. This is an absolute need for reading 2D barcodes in difficult conditions (on a train).

11.5.9. Control of the Barcode

The control process by means of an apparatus contains the following steps:

1. Reading the content of the 2D Barcode
2. Decompressing the content
3. Checking the signature by means of the corresponding public key, extracted from the certificate (defined by the header data). If the result is negative, the train manager receives a corresponding notice
4. Interpretation of the content in the structured data record – "machine interpretable" data
5. Output of the content of the contract(s) on the display – "human interpretable" data

11.5.10. Key management - Duration of validity of the signature key

Since the signature algorithm DSA is an asymmetric and robust cryptographic procedure, the key pairs must in general be rarely switched. A relative long duration of validity can be chosen.

Public keys can be published by means of the TAP TSI technical document B-.60 Retail architecture

The maximum duration (e.g. **12 months)** is defined in each bilateral agreement.

Tickets can be valid over longer periods (e.g. 2 months or more) and only one signature per ticket is possible, therefore the validity periods of subsequent keys must overlap. The overlap period must be at least as long as the maximum ticket validity time span (minus 1 day).

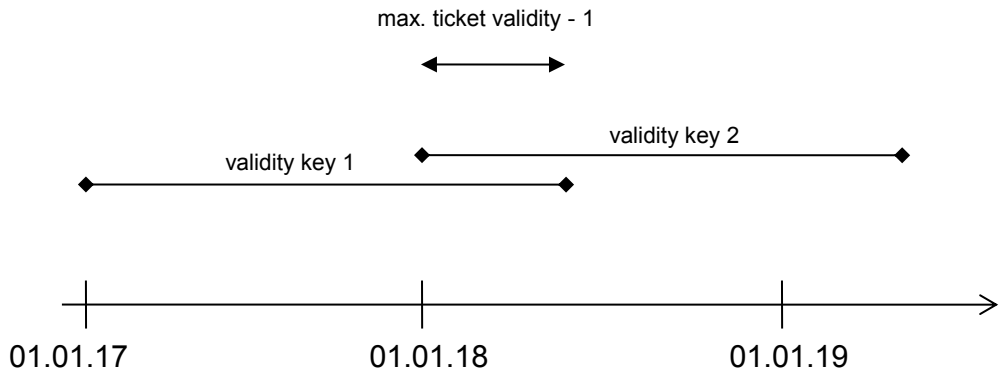


Figure: Example, showing minimum key validity overlap

11.5.11. Test Key Pairs

Some testing scenarios can require a special set of keys, which are used on pre productive system platforms. Since productive ("live") private keys usually can't be deployed to testing platforms for security reasons, special testing key pairs must be used in this context. Testing keys must have an ID beginning with "TT" (for details about the key ID see paragraph 10.6, element 4 "ID of the signature key"). Sample for a test key ID: "TT001".

The test key pairs are deployed on test environments, which usually can't guarantee a defined security level. Due to this situation it is very important to be aware that tickets signed using a test key can never be considered as valid, even if the specimen flag of the DST message is not set. It is the responsibility of each TCO to ensure that their controlling devices follow this policy and always display these tickets with the indication "Test" or "Specimen".

On the other hand the ticket security provider is fully responsible to guarantee the secrecy of its *productive* private keys. Any ticket signed with a non-test private key will be considered as authentic by a TCO.

11.5.12. Exchange of signature keys (public keys) with partner companies

The period of validity of a key pair is defined in each bilateral agreement. Since the certificates must be distributed on the control apparatus of the different RUs, the exchange of a certificate must take place in advance of its validity time span.

The public keys must be at the disposal of the different RUs at the dates defined in the bilateral agreements. Keys are distributed via the TAP TSI technical document B.60 TAP retail architecture.

11.5.13. Test Barcode

Not in scope of the TAP TSI

12. Glossary

1

1D barcode 1 dimensional barcode (uses vertical bars for data encoding, limited data capacity)

2D barcode 2 dimensional barcode (uses a 2 dimensional matrix for data encoding)

A

AEA Association of European Airlines

ASCII American Standard Code for Information Interchange: a character set and encoding

ASN.1 Abstract Syntax Notation one, see ISO/IEC 8824

Asymmetric key cryptography cryptography using symmetric key pairs: private and public keys. Safe since the decoding party don't possess the encoding key, making it possible to check security without the ability to create new security elements.

AZTEC is a type of 2D barcode invented by Andrew Longacre, Jr. and Robert Hussey in 1995.[1] The code was published by AIM, Inc. in 1997. Although the Aztec code was patented,[1] that patent was officially made public domain.[2] The Aztec code is also published as ISO/IEC 24778:2008 standard.

C

Carrier keeps contract(CKC) (Old) mechanism, defined in TAP TSI technical document B.7. Not in use anymore.

Carrier makes certificate (CMC) (Old) mechanism, defined in TAP TSI technical document B.7. Not in use anymore.

Certificate electronic document used to prove the ownership of a public key

CIT International Railway Transport Committee.

CIV Uniform rules concerning the contract of international carriage of passengers by rail

Customer person/company buying the ticket/contract

D

Domestic Ticket A domestic ticket is a ticket sold by a railway undertaking (or under licence of this railway undertaking) for use on this specific railway company. These tickets are not necessary defined by UIC standards.

DSA DSA is an encryption algorithm using asymmetric keys and is covered by U.S. Patent 5,231,688, filed July 26, 1991 and attributed to David W. Kravitz, a former NSA employee. This patent was given to "The United States of America as represented by the Secretary of Commerce, Washington, D.C.", and NIST has made this patent available worldwide royalty-free. see FIPS publication 186.

E

Encrypted fingerprint see Seal

ELB Element List Barcode

F

FCB Flexible Content Barcode

H

Hash function is a mathematical operation on a list of data, resulting in a so called hash-code that is unique for this list of data: if anything of the data set is changed, the corresponding hash will be different from the original one. A good hash function is able to detect simple and multiple changes in data. The hash is smaller is size than the original data and is sent together with the data in case of a data transfer. For detecting possible fraud, the hash has to be encrypted before it is added to the actual data.

Header – Open Data – Signature/Seal the 3 distinguished parts of a SiD dataset that can be translated in a barcode.

N

NSA National Security Agency

O

O/D Origin / Destination

P

Passenger person travelling with a ticket/contract

PDF417 is a so-called “stacked linear barcode symbol”.”PDF” stands for Portable Data File. The 417 signifies that each pattern in the code consists of 4 bars and spaces, and that each pattern is 17 units long. The PDF417 symbology was invented by Dr. Ynjiun P. Wang at Symbol Technologies in 1991. It is published as ISO standard 15438.

PER unaligned Packed encoding rules (PER) are ASN.1 encoding rules for producing a compact transfer syntax for data structures described in ASN.1. Unaligned encoding means that the bits are packed with no regard for octet (byte) boundaries. This guaranties maximum usage of every available bit in the data message.

PKI Public Key Infrastructure

PKMW Public Key Management Website. UIC website containing the public keys of the different security providers. The information has to be provided in a specific way and format. See publication “UIC Public Key distribution using PKMW”

Q

QR code Originally invented in 1994 by Denso (A Japanese automotive component manufacturer) for part numbering applications of the different parts in stock. Since February 2015 QR code is described in ISO/IEC 18004:2015

R

RCT-2 Rail Combined Ticket V2: European standard, describing the layout of a SiP based international rail ticket

companycode Railway Interchange Coding System - code to identify a (railway) company

RU Railway Undertaking

S

Security in Paper - see SiP

Security in Data - see SiD

Security in System - see SiS

SiP Security in Paper. A ticket (representing the contract of carriage) is unique and printed on secured paper to avoid modification or creation by other than a railway company.

SiD Security in Data. A ticket contains security elements. These are created/calculated based on the content of the ticket, resulting in a non-compliant security element in case of falsification or modification. SiD tickets are usually easy to regenerate or to copy.

SiS Security in System. The contract is on a server. Every operation (creation, check, modification, …) on the ticket is conducted on the record(s) on the server. Most secured system, but technically complex.

Security Background Background, defined by CIT, to be pre-printed on so-called secured paper (used in SiP). This background contains a number of elements making it very difficult to create this paper and impossible to just scan & print a ticket.

Security elements Elements allowing the TCO to check that a ticket has been created / modified by a company, allowed to do so. Used in SiD.

Seal/Sealing Security element as used in the barcodes in SiD

Structured Seal vs. Non-Structured Seal The seal in this leaflet consists of 2 numbers (integers). They can be translated in the barcode as 2 numbers (without metadata) or as a structured message (containing extra info).

SSB Small Structured Barcode

Symmetric key cryptography cryptography using symmetric keys: both sender and receiver use the same key. This results in smaller security elements, but the sender needs to trust the receiver for 100%, since the decoding key can be used for encoding purposes too.

SHA is a family of hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS).

T

TCN Ticket Control Number

TCO Ticket controlling organization, allowed to check tickets before, during or after the trip.

TLB Ticket Layout Barcode

U

URT Universal Rail Ticket, a document, written by UIC, defining the actions and the actors involved in ticketing before, during and after the trip.

UTF-8 Unicode Transformation Format: variable-length character encoding for Unicode data, see [RFC3629]

X

XML Extensible Markup Language is a markup language that defines a set of rules for encoding documents or data in a format that is both human-readable and machine-readable.

13. Bibliography

UIC Public Key distribution using PKMW

TAP TSI technical document B.1: Computer generation and exchange of tariff information

TAP TSI technical document B.2: Computer generation of global prices and exchange of fare information on computer medium

TAP TSI technical document B.5: Electronic reservation of seats/berths and electronic production of travel documents – Exchange of messages

TAP TSI technical document B.11: Layout for electronically issued rail passenger tickets

TAP TSI technical document B.8: Standard numerical coding for railway undertakings, infrastructure managers and others companies involved in rail-transport chains

TAP TSI technical document B.9: Standard numerical coding of locations

TAP TSI technical document Directory of code lists for the passenger domain

ISO 639-1: Codes for the representation of names of languages - Part 1: Alpha 2 code, 2002

PER Unaligned see ITU-T Recommendation X.691 "OSI networking and system aspects - Abstract Syntax Notation One (ASN.1) Information Technology - ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)" file: X.691-0207.pdf

RFC1951 - DEFLATE Compressed Data Format - Specification version 1.3, May 1996 - Peter Deutsch

RFC3629 - UTF-8, a transformation format of ISO 10646, November 2003 - François Yergeau

Federal Information Processing Standards Publications (FIPS PUBS) FIPS186 - Digital Signature Standard (DSS), version 1.0, 19 May 1994, version 4.0, 2013

Global trade association for automatic identification and mobility (AIM) ANSI/AIM BC13 ISS - Aztec Code/97/002, November 1997

ASN.1: ISO/IEC 8824

UTF-8: RFC3629

DSA: FIPS 186-4

SHA: FIPS180

AZTEC code: ISO/IEC 24778

PDF417: ISO 15438

obsolete leaflets, used for research purposes:

TAP TSI technical document B.6: Electronic seat/berth reservation and electronic production of transports documents -Transport documents (RCT2 Standard)

TAP TSI technical document B.7: International Rail Ticket for Home Printing

14. APPENDICES

Appendix A	BARCODE.ASN
Appendix B	(old) SSB, previously 918-2 V2

15. Appendix B – SSB – old version

15.1. 1 Collect elements

NEW	**Version number**
	Value = 2
	Up to 16 different versions of the standard can co-exist.
	Value 15 is reserved for domestic use.
	Suggested type-size: Numerical 0..15
	Suggested bit size: 4
	Actual value: 2 (0010 Bin)
177	**Issuing Railway code**
	This code is also used to retrieve the correct public key (for decryption)
	Actual type: Numerical
	Actual size: 4
	Suggested type-size: Numerical 0..9999
	Suggested bit size: 14
	Translation: Integer <> Binary
NEW	**Public key version**
	The signature keys for hashing should be changed frequently (e.g. twice per year) to prevent fraud.
	Up to 16 different versions of the signature can co-exist (enough for eight years).
	Suggested type-size: Numerical 0..15
	Suggested bit size: 4
242	**RCT type indicator**
	1= single segment, 2=bi-segment
	Actual type: Numerical
	Actual size: 1
	Suggested type-size: Numerical, only 2 values
	Suggested bit size: 1
	Translation: "1" <> Binary "0"; "2" <> Binary "1"
	Old value - 1, convert to binary Binary value, convert to decimal + 1
200	**Number of ticket (if multiple tickets)**
	Blank or total number of tickets. Ticket number for serial linkage + total number of tickets e.g. "12"= first ticket out of 2

Actual type: Numerical

Actual size: 2

Suggested type-size: Numerical 00..99, translated in numerical 1..45 (special encoding is used, as the first digit must always be less than or equal to the second one).

Suggested bit size: 6

Translation algorithm:

First, the following table is defined:

(1)	1	1
(2)	1	2
(3)	2	2
(4)	1	3
(5)	2	3
(6)	3	3
(7)	1	4
(8)	2	4
(9)	3	4
(10)	4	4
(11)	1	5
…	…	…
(42)	6	9
(43)	7	9
(44)	8	9
(45)	9	9

To find the sequence number (43), corresponding to e.g. 7 9, the following algorithm can be used: (a=7, b=9)

*num = b * (b-1) / 2 + a*

In this example: *num = 9*8/2+7 = 43*

Translation in the other direction can be done this way (the sequence number is given (43) and the corresponding numbers (7 and 9) have to be found:

num =43

b = 0

Do While (num - b) > 1

b = b + 1

num = num - b

Loop

a = num

b = b + 1

In this example, the values of b and num will be in the different sequences: 0/43, 1/42,2/40,3/37,4/33,5/28,6/22,7/15,8/7, so a=7, b=9.

137	**Number of adult passengers**
	Actual type: Numerical
	Actual size: 2
	Suggested type-size: Numerical 0…99
	Suggested bit size: 7
	Translation: Integer <> Binary
138	**Number of child passengers**
	Actual type: Numerical
	Actual size: 2
	Suggested type-size: Numerical 0...99
	Suggested bit size: 7
	Translation: Integer <> Binary
142	**First day of validity**
	Blank or Julian number (001 to 366) for first day of validity
	Actual type: Numerical
	Actual size: 3
	Suggested type-size: Numerical 0...366
	Suggested bit size: 9
	Translation: Integer <> Binary
143	**Last day of validity**
	Blank or Julian number (001 to 366) for last day of validity
	Actual type: Numerical
	Actual size: 3
	Suggested type-size: Numerical 0...366
	Suggested bit size: 9
	Translation: Integer <> Binary
243	**"Corporate" frequent**
	Blank or "customer number"
	Actual type: Numerical
	Actual size: 14
	Suggested type-size: 1 bit (see element 171) + Numerical 14 digits
	Suggested bit size: 48
	Translation: bit1 = 0 + Integer <> Binary
171	**"Individual" frequent**
	Blank or "customer number"

Actual type: Numerical

Actual size: 14

Suggested type-size: 1 bit (see element 243) + Numerical 14 digits

Suggested bit size: 48

Translation: bit1 = 1 + Integer <> Binary

145 **Departure station**

Actual type: Numerical or Alphanumerical

Actual size: 7(N) or 5(A)

Suggested type-size: 1 bit (A) + 5 chars (= 5 * 6 bit) -or- 1 bit (N) + 7 digits (0000000 .. 9999999) (= 20 bit)

(the first bit "0" indicates Alphanumerical, the first bit "1" indicates Numerical) Suggested bit size: 31 bit (the biggest = alphanumerical)

Translation: - Alphanumerical: bit1 = 0 + 5 * 6 bit + Translation from alphanumerical to 6 bit:

0	0
1	1
2	2
...	...
9	9
A	10
B	11
...	…
Z	35

- Numerical: bit1 = 1 + 20 bit, rest: "0"

146 **Arrival Station (see element 145)**

Suggested type-size: 1 bit (A) + 5 chars (= 5 * 6 bit) -or- 1 bit (N) + 7 digits (0000000…9999999) (= 20 bit)

Suggested bit size: 31 bit (the biggest = alphanumerical)

147 **Departure date**

Blank or Julian number (001 to 366) for departure date

Actual type: Numerical

Actual size: 3

Suggested type-size: Numerical 0...366

Suggested bit size: 0 - see element 142 which will be used for such a ticket

148 **Departure time (*)**

Blank or 4-digit numerical from 0000 to 2359

Actual type: Numerical

Actual size: 3

Suggested type-size: 48 slots of 30 minutes

Suggested bit size: 6

Translation: 00:00 to 00:29: timeslot 1 00:30 to 00:59: timeslot 2 01:00 to 01:29: timeslot 3...

If the timeslot-number is 0, than the departure date / departure time is not used, which means that element 142 is not used as a departure date, but as a "first date of validity" for an open ticket.

(*) This is a restriction: not the exact time is stored, but a "time slot".

149 **Train number**

Actual type: Alphanumerical

Actual size: 5

Suggested type: Numerical (*)

Suggested size: 5 (00000…99999)

Suggested bit size: 17

(*) This means that there is a restriction for the train numbers to encode only the numerical fields

206 **Reservation reference**

Blank or 12 num with no blank spaces

Actual type: Numerical

Actual size: 12

Suggested type-size: num (000000000000…999999999999)

Suggested bit size: 40

215 **Class of travel**

Blank or "1 ", "2", "P", "C" or "T"

Actual type: Alphanumerical

Actual size: 1

Suggested type: 64 possible options (a letter or a number)

Suggested bit size: 6

Translation:

0	0
1	1
2	2
...	...
9	9
A	10
B	11
...	…

	Z 35
151	**Coach number**
	Blank or from "001" to "999"
	Actual type: Alphanumerical
	Actual size: 3
	Suggested type: Numerical (000…999)
	Suggested bit size: 10
153	**Seat / berth number**
	Blank or 3 num or 2 num + 1 alpha
	Actual type: Alphanumerical
	Actual size: 3
	Suggested type: 2 Numerical (00...99) + 1 character (*)
	Suggested bit size: 7+ 6 = 13
	(*) limitation: seat/berth number is only 1 alpha and 2 num
154	**Overbooking indicator**
	"0"=not overbooked, "1 "=overbooked
	Actual type: Numerical
	Actual size: 1
	Suggested type: binary
	Suggested bit size: 1
219	**Issuer's Passenger Name Record (PNR)**
	Actual type: Alphanumerical
	Actual size: 7
	Suggested type: 7 character
	Suggested bit size: 42
196	**Ticket type**
	Can be IV,IR,BP,IQ,IM,IO,IP,IK or IT
	Actual type: Alphanumerical
	Actual size: 2
	Suggested type: lookup of 16 options
	Suggested bit size: 4
	Translation:
	IV 1
	IR 2
	BP 3

IQ	4
IM	5
IO	6
IP	7
IK	8
IT	9

198 **"Specimen" code**

"0"=test ticket, "1"=operational ticket

Actual type: Alphanumerical

Actual size: 1

Suggested type: binary

Suggested bit size: 1

VIA **Via Stations**

First letter of max. 6 via stations (if less via stations: Blanc (space)) Suggested type: Binary (5 bit per station)

Suggested total bit size: 30 bit

NEW **Carrier contract reference code**

Actual size: 4 num (railway code of carrier) + 8 alphanumerical (reference) Suggested type-size: num 0..9999 + 8 x 64 options

Bitsize: 14+8*6 = 62 bit + Translation from alphanumerical to 6 bit:

0	0
1	1
2	2
...	...
9	9
A	10
B	11
...	...
Z	35

15.2. 2 Hash Code generation

For security reasons the barcode should be signed with a digital signature. The digital signature is a hash of the ticket data which is encrypted with the private key of the distributor. A carrier can use the public key of the distributor to decrypt the digital signature and compare it to a hash of the ticket data. If the hash of the ticket data matches the decrypted digital signature, the carrier can identify the distributor and the carrier is sure the ticket data has not been tampered with.

It is suggested that both Homeprint and RCT2 (ATB) tickets use the same encryption standards. The UIC Homeprint contains an Aztec 2D barcode. The barcode also has a digital signature. The digital signature is created with SHA-1, DSA, 1024.

The SHA-1 mechanism is used to generate a hash-code. SHA-1 stands for "Secure Hash Algorithm, first family". SHA-1 is still secure today. The SHA-1 hash function can't be broken yet otherwise than by using vast computational resources.

A DSA-asymmetric encryption mechanism is used to encrypt the hash-code. To generate a seal from the hash-cod e (or: "to encrypt the hash-code"), a distributor uses his private (secret) key. The advantage of DSA over RSA is that DSA creates shorter signatures. This is important for the size-constrained barcode under consideration here. The DSA signatures are twice as long as the output of the hash function (i.e. the digest). For the particular (SHA-1, DSA, 1024) configuration this amounts to 2 x 160 bits = 40 bytes. In the current (6-layered, 114 bytes wide) Aztec barcode that UIC 918-2 defines, this would leave 114 - 40 = 74 bytes = 592 bits available for ticket information. This means an increase of 592 - 337 = 255 bits as compared to the current standard.

NB: If however one day SHA-1 can effectively be easily broken by fraudsters, then the UIC would need to move on to stronger signatures for both its Homeprint and ATB barcodes. One possibility would be (SHA-224, DSA, 2048), as prescribed by the forthcoming third revision of the Digital Signature Standard. These signatures would be 56 bytes long, i.e. 16 bytes longer than the signatures of (SHA-1, DSA, 1024), but still yielding 127 bits of extra barcode capacity when compared to the current 918-2 standard. A cautious implementation of (SHA-1, DSA, 1024) for the ATB 2D barcode should leave 16 bytes = 128 bits of capacity unused for this possible future stronger signature. The version number in the barcode (first element) can be used to identify the used standard.

For the verification, a railway undertaker, wanting to interpret the information in the digital signature, should know which public key to use. For this, the element 177 - "Issuing railway code" and a new element "Id of the signature key" are used.

The key pairs (private key for the encryption by the distributor, public key for the decryption by the TCO) are chosen by the distributor. The distributor gives the public key to the TCO in advance, so that he can check tickets with a hash-code that is encrypted with the corresponding private key. It is strongly recommended to change the key pairs frequently (e.g. twice a year). This requires the carrier to be able to identify the public key that should be used for decryption of the digital signature (id of the signature key should be stored in the barcode, just like for the Homeprint barcodes).

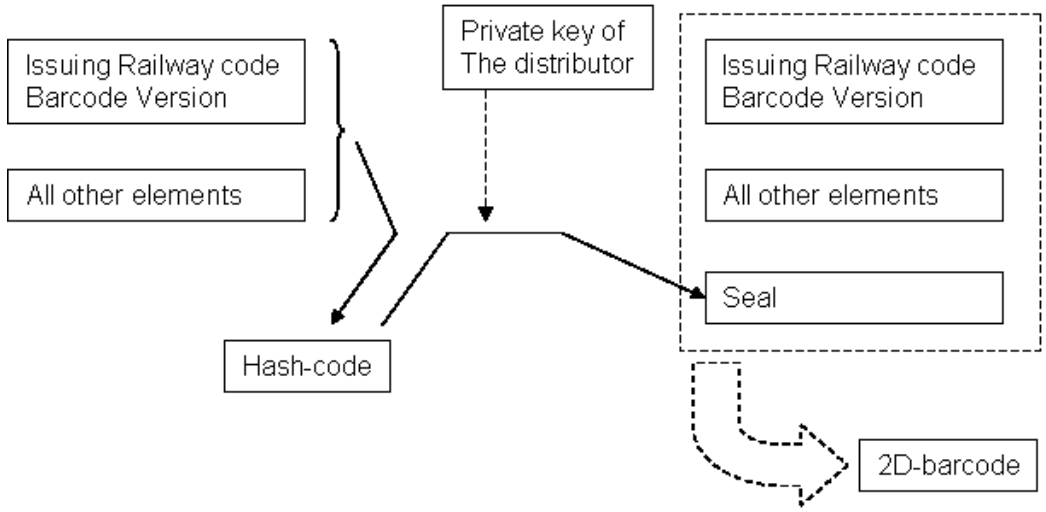


Fig. 1 - Schematic presentation seal generation encryption and barcode generation

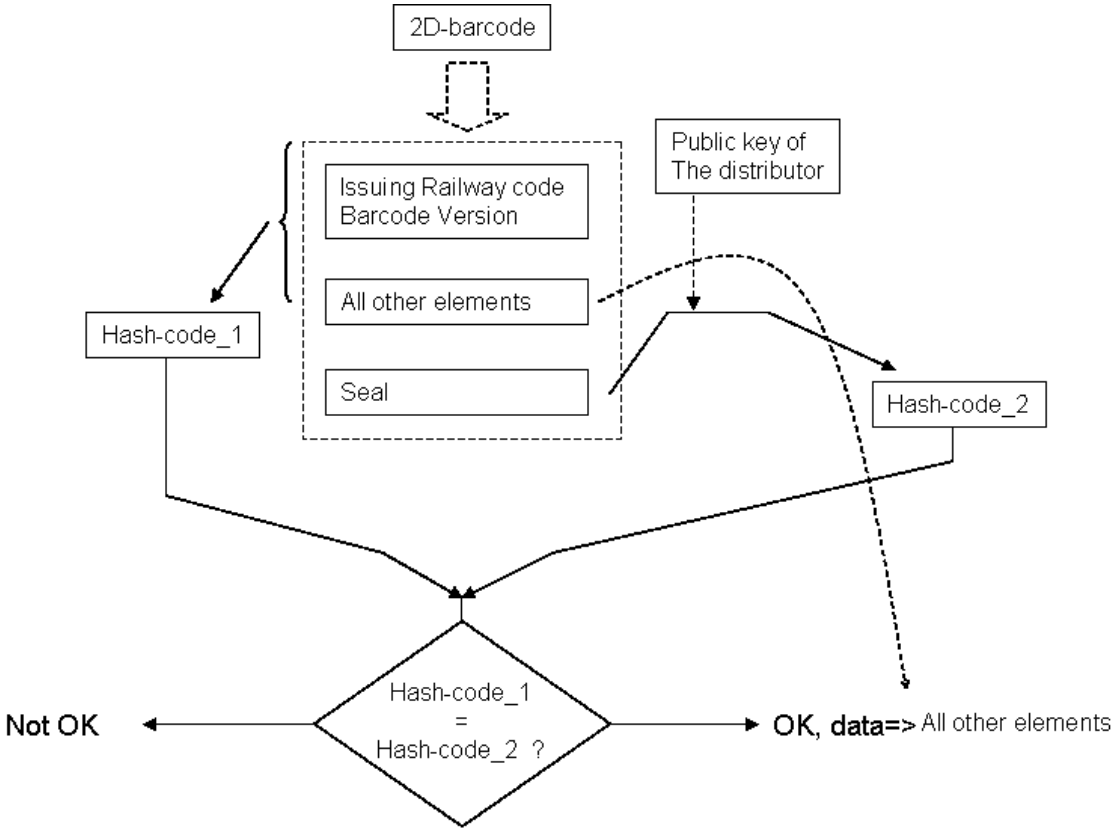


Fig. 2 - Schematic presentation of the decryption of the seal verification

Table 2: Bitsize after seal generation (based upon SHA-1, DSA, 1024)

Element	Element_description	Suggested Type	Bits	Bytes
Barcode Version	Version number cyclic (max 16)	Num (0.. 15)	4	0,5
177	Issuing railway code	Num (? 9999)	14	1,75
Public key	Version of the public key that should be version used to check the digital signature	Num (0..15)	4	0,5
242	RCT type indicator	Bit	1	0,125
200	Number of ticket (if multiple tickets)	Num<100	6	0,75
137	Number of adult passengers	Num (<100)	7	0,875
138	Number of child passengers	Num (<100)	7	0,875
142	First day of validity	Num (<367)	9	1,125
143	Last day of validity	Num (<367)	9	1,125
243	"Corporate" frequent	Bit Flag + 14 Num	48	6
171	Individual frequent	N/A	0	0
145	Departure station	Bit Flag for Alpha or Num + x Characters	31	3,875
146	Arrival station	Bit Flag for Alpha or Num + x Characters	31	3,875
147	Departure date			0
148	Departure Time	6 bits for 48 slots	6	0,75
149	Train number	5 alpha	25	3,25
206	Reservation reference	Num (<999999999999)	40	5
215	Class of travel	Lookup of 64 options	6	0,75
151	Coach number	Num (<999)	10	1,25
153	Seat/berth number	2 Num + 1 Character	13	1,625
154	Overbooking indicator	Bit Flag	1	0,125
219	Issuer's PNR number	7 Chars	42	5,25
196	Ticket type	Lookup of 16 options	4	0,5
198	"specimen" code	Bit Flag	1	0,125
VIA	VIA STATIONS - first letters (max 6 via)	6 alpha's	30	3,75
NEW	Carrier contract reference code	4 num + 8 alpha	62	7,75
	Total Data		**411**	**51,375**
	Digital Seal		**320**	**40**

Additional free space for SHA-224, DSA, 2048 ***(a)***	128	16
Total including seal	**859**	**107,375**
Total size of barcode (based on configuration 41x41)	912	114
Free space	53	6,625

(a) It is strongly recommended to reserve upfront the additional required bits (bytes) in case of SHA-224 implementation.

The total size of the barcode: 114 bytes of data (based on barcode configuration 41x41)