MACHINE READABLE TRAVEL DOCUMENTS TECHNICAL REPORT

ICAO Datastructure for Barcode

Version – 1.10 | September 2023

ISO/IEC JTC1 SC17 WG3/TF5

FOR THE INTERNATIONAL CIVIL AVIATION ORGANIZATION

Release Control

Release	Date	Description
0.01	Jan 2023	Initial Draft setting parameters for ICAO Digital Barcode
0.02	Apr 2023	After Comment Resolution in WG3 meeting (Haarlem, Apr 4-5,2023)
0.03	Aug 2023	After Comment Resolution in TF5 meeting (Online, August 7-8,2023)
1.00	Aug 2023	After adding SMB worked example and NTWG approval
1.10	Sep 2023	Changes for Zlib, added barcode flag and created message types instead of SMB

Andy Hing	Singapore	Auctorizium
Kwan Wei Ren	Singapore	Auctorizium
R Rajeshkumar	Singapore	Auctorizium

Table of contents

1. Scope

ICAO specifications currently define a few types of barcode. Visible Digital Seal for Non-Electronic documents (VDS), Visible Digital Seal for Non-Constrained environments (VDS-NC) and Secure Messaging Barcode (SMB). Each of them has a different structure, payload and representation. This Technical Report defines a 2D barcode structure that allows to create a universal barcode structure for all ICAO barcodes.

1.1 Terminology

1.1.1 Technical report terminology

The key words “MUST”, “MUST NOT”, “SHALL”, “SHALL NOT”, “REQUIRED”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC 2119].

MUST	This word, or the terms “REQUIRED” or “SHALL”, means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase, or the phrase “SHALL NOT”, means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective “RECOMMENDED”, means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase “NOT RECOMMENDED” means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
MAY	This word, or the adjective “OPTIONAL”, means that an item is truly optional. One user may choose to include the item because a particular application requires it or because the user feels that it enhances the application while another user may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides).
CONDITIONAL	The usage of an item is dependent on the usage of other items. It is therefore further qualified under which conditions the item is REQUIRED or RECOMMENDED. This is an additional key word used in Doc 9303 (not part of RFC 2119).

In case OPTIONAL features are implemented, they MUST be implemented as described in this Technical Report.

1.1.2 Terms and Definitions

Term	Definition
CA	Certification Authority
CAN	Card Access Number
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
DER	Distinguished Encoding Rules
DOB	Date of Birth
DTA	Digital Travel Authorization
ECA	EF.CardAccess
ECC	Elliptic-curve cryptography
EKU	Extended Key Usage
ETD	Emergency Travel Document
IDB	ICAO Datastructure for Barcodes
MRZ	Machine Readable Zone
NAAT	Nucleic Acid Amplification Test
PoR	Proof of Recovery
PoT	Proof of Testing
PoV	Proof of Vaccination
TLV	Tag, Length, Value
URCI	Unique Recovery Certificate Identifier
UTCI	Unique Test Certificate Identifier
UVCI	Unique Vaccination Certificate Identifier
VDS	Visible Digital Seal
VDS-NC	Visible Digital Seal for Non Constrained environments

2. Digital Encoding of Document Features

The encoding of date, datetime and three letter country code MUST follow the process defined in this section. The encoding of other document features MUST follow the process defined in Doc 9303-13, section 2.3.1

2.1 Encoding of Date

A total of four bytes is used for encoding of date. The first byte of the encoded date is a date mask that is used to differentiate the known or unknown part of the date. The remaining three bytes will be formed by converting the date into a positive integer by concatenating the month (MM), the days (DD), the year (YYYY). Unknown part of the date is RECOMMENDED to use the integer 0. This positive integer is then concatenated into a sequence of one to three bytes, depending on the position of the unknown part of the date, using their unsigned integer representation. In the case where the sequence of bytes is less than three bytes, 0x00 MUST be prepended until it has three bytes. The date mask concatenated with the sequence of three bytes will formed the encoding of date.

Each bit of the date mask represents the known or unknown part of the date. Starting from the most significant bit to the least significant bit, a total of 8 bits, will represent the date MMDDYYYY in this order. A fully known date SHALL have a date mask of 0x00 and a fully unknown date SHALL have a date mask of 0xFF.

Example: Consider a date of birth, xx 1st, 19xx, where the month, the third and fourth digit of the year is unknown, the rest of the date is known. The date mask of 0xC3 (Binary: 1 1 0 0 0 0 1 1) is formed, which has the month, the third and fourth digit of the year masked. Concatenating the month, day and year yields the integer 00011900 resulting in the two bytes 0x2E 0x7C. 0x00 is appended to the front to make the sequence three bytes, 0x00 0x2E 0x7C. The encoded date will then be formed by concatenating the date mask and the date bytes, 0xC3 0x00 0x2E 0x7C.

2.2 Encoding of DateTime

The datetime MUST be in Coordinated Universal Time (UTC). A datetime is first converted into a positive integer by concatenating the month (MM), the days (DD), the year (YYYY), the hours (HH), the minutes (mm), the seconds(ss). This positive integer is then concatenated into a sequence of six bytes using their unsigned integer representation.

Example: Consider March 25th, 1957 08:15:22. Concatenating the month, day, year, hour, minute and second yields the integer 03251957081522, resulting in the six bytes 0x02 0xF5 0x27 0xBF 0x25 0xB2.

2.3 Encoding of three letter Country Code

If the three-letter code comprises less than three letters, the code MUST be padded with filler characters (‘<’), e.g. ‘D’ is padded to ‘D<<’. The code is encoded by C40.

3. ICAO Datastructure for Barcode Format – IDB

This document defines a generic barcode format that can be used for all ICAO barcode types. Only QR Code [ISO/IEC 18004], [ISO/IEC 23941] and DataMatrix [ISO/IEC 16022], [ISO/IEC 21471] SHALL be used for encoding IDB. QR Code is RECOMMENDED.

It is RECOMMENDED that the barcode is created with a minimum of 4 dots per module sidelength.

3.1 Barcode Structure

The barcode consists of a Barcode Identifier, Barcode Flag and a Barcode Payload shown below.

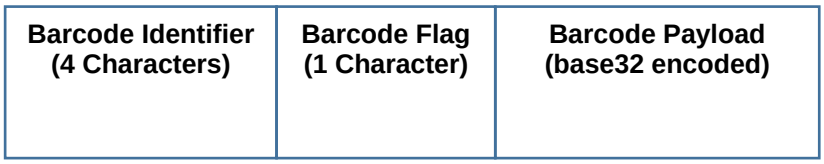

Figure 1

3.1.1 Barcode Identifier

The barcode Identifier MUST be in 4 characters by concatenating 'IDB' and version character of the barcode structure. The version of the barcode structure of this document is '1'. Therefore, the Barcode Identifier is 'IDB1'.

3.1.2 Barcode Flag

The Barcode Flag is a 1 byte value that is used for storing bit value (true or false) of the Barcode Payload.

The Barcode Flag is computed by getting the Barcode Bit Value and adding a constant value of 0x41 to it. The Barcode Bit Value is a 4 bit value, 2 bits are used in this document and 2 bits are reserved for future use.

The least significant bit is used for "IsSigned".

- "1" means message is signed
- "0" means message is not signed

The second least signification bit is used for "IsCompressed". (Refer to section 3.1.4 below)

- "1" means barcode is compressed
- "0" means barcode is not compressed

Barcode Bit Value	Constant	Result	ASCII Value	Description
0000	0100 0001(0x41)	0x41	A	Not Signed, Not Zipped
0001	0100 0001(0x41)	0x42	B	Is Signed, Not Zipped
0010	0100 0001(0x41)	0x43	C	Not Signed, Is Zipped
0011	0100 0001(0x41)	0x44	D	Is Signed, Is Zipped

Table 1

3.1.3 Base-32 Format

A 32-character subset of US-ASCII is used. The 32 characters that can be used in a QR or DataMatrix code. If we look at Base 64, it encodes 3 bytes into 4 characters. Base 32 encodes 5 bytes into 8 characters.

For encoding of base-32, refer to RFC 4648 section 6, table 3.

Padding characters increase the size of the barcode and add no significant value. Hence, it is REQUIRED that after doing the base-32 encoding, padding characters are removed.

During the process of decoding the payload, padding characters MUST be added to ensure that the length of the payload is a multiple of 8.

E.g.
Encoded Barcode Payload after base-32:
PDNLW6JU2GHMGZXL5VFQO5ZI6YXF42NTYOUDIRWYAYCQNOUFA4SWTRG4HTVJG27UE42N
Y64VTIDFZTXWT4QQAVTDC3PQ====

After removing padding characters (=):
PDNLW6JU2GHMGZXL5VFQO5ZI6YXF42NTYOUDIRWYAYCQNOUFA4SWTRG4HTVJG27UE42N
Y64VTIDFZTXWT4QQAVTDC3PQ

Length of the value after removing padding characters is 92. To decode this encoded value, padding MUST be appended at the end to make it multiple of 8. After appending the padding characters, the value will have the length of 96:

PDNLW6JU2GHMGZXL5VFQO5ZI6YXF42NTYOUDIRWYAYCQNOUFA4SWTRG4HTVJG27UE42N
Y64VTIDFZTXWT4QQAVTDC3PQ====

3.1.4 Encoded Barcode Payload

The following steps define the creation of the encoded barcode payload:

1) Form an encoded structure that consists of a header (see Section 3.4), message zone (see Section 3.5), signer certificate zone (see Section 3.6), and signature zone (see Section 3.7). An overview of the structure is given in Figure 2.

   Note: Multiple messages may be encoded in the message zone. For example, a Proof of Vaccination (PoV) and a Proof of Recovery (PoR) may be included under the barcode information group template using their appropriate tags.

2) Compress the encoded structure using ZLIB format. For ZLIB, refer to RFC 1950. This step is OPTIONAL, please refer to the recommendations below.
   - It is RECOMMENDED to use level 9 ZLIB DEFLATE compression. This gives the slowest speed but the best compression. For DEFLATE compression, refer to RFC 1951.
   - It is RECOMMENDED to skip this step for CAN only structure. A CAN only structure contains only the CAN message type in message zone. No other message type is in the message zone.
   - All structures except CAN only structure are RECOMMENDED to include this step for compression.

3) The output is then encoded using Base-32 format defined in this document. This Base-32 encoded output is the encoded barcode payload that will be used to form the final barcode structure.

Header

Country Identifier (2bytes)	**Signature Algorithm** (1bytes)	**Certificate Reference** (5bytes)	**Signature Creation Date** (3bytes)

Message

Tag	**L**	**Value**			
61	Var	Barcode Information Group Template			
		Tag	**L**	**Value**	
		0x01 (VDS - Visas)	Var	Refer to 3.3.1.1 below(OPTIONAL)	At least one of the Barcode structure MUST be present. Multiple messages can be encoded in the same barcode
		0x02 (VDS-Emergency Travel document)	Var	Refer to 3.3.1.2 below(OPTIONAL)	
		0x03 (PoT)	Var	Refer to3.3.1.3 below (OPTIONAL)	
		0x04 (PoV)	Var	Refer to 3.3.1.4 below (OPTIONAL)	
		0x05 (PoR)	Var	Refer to 3.3.1.5 below (OPTIONAL)	
		0x06 (DTA)	Var	Refer to 3.3.1.6 below (OPTIONAL)	
		0x07 (MRZ – TD1)	60	Refer to 3.3.1.7 below (OPTIONAL)	
		0x08 (MRZ – TD3)	60	Refer to 3.3.1.8 below (OPTIONAL)	
		0x09 (CAN)	4	Refer to 3.3.1.9 below (OPTIONAL)	
		0x0A (ECA)	Var	Refer to 3.3.1.10 below (OPTIONAL)	
		0x80-0xFF	Var	Defined by issuing state or organization (OPTIONAL)	
7E	Var	Signer Certificate (OPTIONAL)			
7F	Var	Signature Data			

Signer Certificate

Signature

Figure 2

3.2 Header

The header contains meta-data about the barcode and the encoding.

The overall length of the header is 11 bytes. A definition of the header is given in Table 2.

Start Position	Length(byte)	Content
0x00	2	Country Identifier (REQUIRED). A three-letter code identifying the issuing State or organization. The three-letter code is according to Doc 9303-3. The code is encoded in accordance with section 2.3.
0x02	1	Signature Algorithm (CONDITIONAL). The signature algorithm used to produce the signature.
0X03	5	Certificate Reference (CONDITIONAL). Last 5 bytes of the SHA1 Hash of the Signer Certificate.
0x08	3	Signature Creation Date (CONDITIONAL). The date the signature was created.

Table 2

3.2.1 Country Identifier

A three-letter code identifying the issuing State or organization. The three-letter code is according to Doc 9303-3

3.2.2 Signature Algorithm

The signature algorithm used to produce the signature. Signatures MUST be created using ECDSA. Elliptic Curve Signature Algorithm (ECDSA) with a key length of at least 256 bit in combination with SHA-256 is a MUST. This field MUST be present if IsSigned is “1” and MUST NOT be present if IsSigned is “0”. Refer to 3.1.2 above.

The Signature Algorithm MUST be only one of the following values:

Value	Description
0x01	ECDSA with SHA-256 hashing algorithm
0x02	ECDSA with SHA-384 hashing algorithm
0x03	ECDSA with SHA-512 hashing algorithm

Table 3

Note: Other algorithms may be added in future releases of the technical report

3.2.3 Certificate Reference

The Certificate reference value will be the last 5 bytes of the SHA1 Hash of the DER encoded Signer Certificate. This field MUST be present if IsSigned is “1”, and MUST be provided even if the Signer Certificate is included in the barcode. This field MUST NOT be present if IsSigned is “0”. Refer to 3.1.2 above.

3.2.4 Signature Creation Date

The date when the signature was created. Refer to section 2.1 for the encoding of this field. This field MUST be present if IsSigned is “1” and MUST NOT be present if IsSigned is “0”. Refer to 3.1.2 above.

3.3 Message Zone

Following the header is the message zone. The message zone MUST use the Barcode Information Group Template which allows the possibility to store different message types simultaneously. The Barcode Information Group Template MUST be encoded use DER-TLV.

The encoding of the message zone MUST follow the specifications of Doc 9303-13, Section 2.3.

3.3.1 Message Type

The message type is defined by a single byte value. Value 0x00, 0x7E and 0x7F are reserved. Values 0x01 to 0x7D are reserved for ICAO use. The remaining tags from 0x80 to 0xFF can be used for national use cases.

An Inspection System SHALL process the tags that it recognises and SHALL ignore any tags that it does not recognise. The presence of unrecognised tags SHALL NOT invalidate the barcode. An Inspection System SHALL ignore any barcode encodings it does not recognize.

Note: The signature is across the data specified in clause 3.5 and may contain elements (e.g. MRZ, CAN) which do not need to be signed. Signatures for individual messages within the structure are not catered for.

The following Table contains the type of message specified by ICAO.

List of Message Type	
TAG	**Description**
0x01	Visa
0x02	Emergency Travel Document
0x03	Proof of Testing
0x04	Proof of Vaccination
0x05	Proof of Recovery
0x06	Digital Travel Authorization
0x07	Machine Readable Zone (TD1)
0x08	Machine Readable Zone (TD3)
0x09	Card Access Number
0x0A	EF.CardAccess

Table 4

3.3.1.1 Visa (0x01)

The encoding of the message for a Visa SHALL follow Doc 9303-7, section 9.1.2

3.3.1.2 Emergency Travel Document (0x02)

The encoding of the message for an Emergency Travel Document SHALL follow Doc 9303-8, section 6.1.2

3.3.1.3 Proof of Testing (0x03)

This section describes the Data Elements that may be present in Proof of Testing Certificate(PoT).

Data Element	OPTIONAL (O) or MANDATORY (M) or CONDITIONAL (C)	Description	Max Number of Bytes (after encoding)	Fixed(F) or Variable(V)
UTCI (01)	C	Unique Test Certificate Identifier - REQUIRED if message is signed, OPTIONAL if message is not signed. (C40 Encoding)	12	V
Name (02)	M	Name of the holder (as specified in Doc 9303-3) (C40 Encoding)	26	V
DOB (03)	M	The DOB of the test subject. (Encoded according to section 2.1)	4	F
DocType (04)	M	The ID Document Type of the identity document MUST be used. Only these values MUST be used: P – Passport (Doc 9303-4) A – ID Card (Doc 9303-5) C – ID Card (Doc 9303-5) I – ID Card Doc 9303-5) AC - Crew Member Certificate (Doc 9303-5) V – Visa (Doc 9303-7) D – Driving License (ISO 18013-1)	2	F
DocNum (05)	M	The ID Document Number of the identity document MUST be used of the document used in DocType. The ID Document Number is the unique identifier of the test subject. (C40 Encoding)	16	V
Name of testing facility/service provider (06)	M	Name of testing facility or service provider MUST be used. (C40 Encoding)	14	V
Country of test (07)	M	Country of test MUST be used. (Three-letter code according to Doc 9303-3) (Encoded in accordance with section 2.3)	2	F
Testing Facility contact	M	Contact number of testing facility or service provider MUST be used. The maximum size of	12	F

number (08)		phone number is 19 characters (15 characters in accordance with [ITU-T E.123],3 characters for International Country Code. The symbol "+" to indicate that an international prefix is omitted). (C40 Encoding)		
Testing Facility email address (09)	M	Email address of testing facility or service provider MUST be used.		V
Testing Facility Address (10)	M	Address of testing facility or service provider MUST be used.		V
Specimen Collection DateTime (11)	M	Date and time of specimen collection MUST be used. (encoded according to Section 2.2)	6	F
Report Issuance DateTime (12)	M	Date and time of report issuance MUST be used. (encoded according to section 2.2)	6	F
Test Conducted (13)	M	Type of test conducted MUST be used. Only these values MUST be used: molecular(PCR) (0x01) molecular(other) (0x02) Antigen (0x03) Antibody (0x04)	1	F
Result (14)	M	Result of Test MUST be used. Only these values MUST be used: Normal (0x01) Abnormal (0x02) Positive (0x03) Negative (0x04)	1	F
Method Used (15)	O	Sampling method is OPTIONAL. Only these values MUST be used: nasopharyngeal (0x01) oropharyngeal (0x02) saliva (0x03) Blood (0x04) Other (0x05)	1	F
Optional Field (16)	O	Optional data issued at the discretion of the issuing authority (C40 Encoding)	14	V

Table 5

The table below shows the Proof of Testing(PoT) Encoding Tags.

Tag	**L**	**Value**		
61	Var	Barcode Information Group Template		
	Tag	**L**	**Value**	
	03	Var	Proof of Testing	
		Tag	**L**	**Value**
		01	12	UTCI
		02	26	Name
		03	4	Date of Birth

		04	2	Document Type
		05	16	Document Number
		06	14	Name of testing facility/service provider
		07	2	Country of Test
		08	19	Testing Facility Contact Number
		09	var	Testing Facility email address
		10	var	Testing Facility Address
		11	6	Specimen Collection DateTime
		12	6	Report Issuance DateTime
		13	1	Test Conducted
		14	1	Test Result
		15	1	Method Used
		16	14	Optional Field

Table 6

3.3.1.4 Proof of Vaccination (0x04)

This section describes the Data Elements that may be present Proof of Vaccination Certificate(PoV).

Data Group Element	Data Element	OPTIONAL (O) or MANDATORY (M) or CONDITIONAL (C) or RECOMMENDED (R)	Description	Max Number of Bytes (after encoding)	Fixed(F) or Variable(V)
	UVCI (01)	M	Unique Vaccination Certificate Identifier (C40 Encoding)	12	V
	Certificate valid from (02)	O	Date in which the certificate for a vaccination event became valid. (Encoded according to section 2.1)	4	F
	Certificate valid until (03)	O	Last date in which the certificate for a vaccination event is valid. (Encoded according to section 2.1)	4	F
	Name of holder (04)	M	Name of the holder (as specified in Doc 9303-3) (C40 Encoding)	26	V
	Date of Birth (05)	C	Vaccinated person's date of birth. REQUIRED if no *Unique identifier* is provided. (Encoded according to section 2.1)	4	F
	Sex (06)	R	Sex of the holder (as specified in Doc 9303-4 Section 4.1.1.1 – Visual	1	F

				Inspection Zone)		
	Unique Identifier (07)			Travel Document Number (C40 Encoding)	8	V
	Additional Identifier (08)		O	Any other document number at discretion of issuer (C40 Encoding)	16	V
***Vaccination Event (09)** (minimum dataset) * means that the whole section may be repeated	Vaccine or Prophylaxis (31)		M	Vaccine or vaccine sub-type (ICD-11 Extension codes (http://id.who.int/icd/entity/164949870)	6	F
	Vaccine brand (32)		M	Medicinal product name. (C40 Encoding)	As defined by Member State	F
	Vaccine manufacturer (33)		C	Name of the manufacturer of the vaccine received. If vaccine manufacturer is unknown, market authorization holder is REQUIRED. (C40 Encoding)	As defined by Member State	F
	Vaccine market authorization holder (34)		C	Name of the market authorization holder of the vaccine received. If market authorization holder is unknown, vaccine manufacturer is REQUIRED. (C40 Encoding)	As defined by Member State	F
	Disease or agent targeted (35)		R	Disease or agent that the vaccination provides protection against (ICD-11)	6	F
	***Vaccination Details(36)** (minimum dataset) * means that the whole section may be repeated	Date of vaccination (51)	M	Date on which the vaccine was administered.	4	F
		Dose Number (52)	M	Vaccine dose number	2	F
		Total Doses (53)	O	Total expected doses	2	F
		Country of vaccination (54)	M	The country in which the individual has been vaccinated. (Three-letter code according to Doc 9303-3) (C40 Encoding)	2	F
		Administering centre (55)	M	Name/code of administering centre or a health authority responsible for the vaccination event (C40 Encoding)	14	V
		Vaccine	M	A distinctive	14	V

		batch number (56)		combination of numbers and/or letters which specifically identifies a batch (C40 Encoding)		
		Due date of next dose (57)	O	Date on which the next vaccination should be administered. (Encoded according to section 2.1)	4	F
	Optional Data (10)		O	Issued at the discretion of the issuing authority (C40 Encoding)	14	V

Table 7

The table below shows the Proof of Vaccination(PoV) Encoding Tags.

Tag	**L**	**Value**				
61	Var	Barcode Information Group Template				
	Tag	**L**	**Value**			
	04	Var	Proof of Vaccination			
		Tag	**L**	**Value**		
		01	12	UTCI		
		02	4	Certificate Valid From		
		03	4	Certificate Valid Until		
		04	26	Name		
		05	4	Date of Birth		
		06	1	Sex		
		07	11	Unique Identifier		
		08	16	Additional Identifier		
		09	V	1st Vaccination Event		
			Tag	**L**	**Value**	
			31	6	Vaccine or Prophylaxis	
			32	As Defined by member states	Vaccine Brand	
			33		Vaccine Manufacturer	
			34		Vaccine market Authorization holder	
			35	6	Disease or agent targeted	
			36	V	1st Vaccination Details	
				Tag	**L**	**Value**
				51	4	Date of Vaccination
				52	2	Dose number
				53	2	Total Doses
				54	2	Country of Vaccination
				55	14	Administering Centre
				56	14	Vaccine batch Number
				57	4	Due date of next dose
			36	V	2nd Vaccination Details	
					.....	
			36	V	n Vaccination Details	
		09	V	Vaccination Event		
				c.....		
		09	V	Vaccination Event		

		10	14	Optional Field		

Table 8

3.3.1.5 Proof of Recovery (0x05)

This section describes the Data Elements that may be present Proof of Recovery Certificate(PoR).

Data Element	OPTIONAL (O) or MANDATORY(M)	Description	Max Number of Bytes (after encoding)	Fixed(F) or Variable(V)
URCI (01)	M	Unique Recovery Certificate Identifier (C40 Encoding)	12	V
Certificate Valid From (02)	O	Date in which the certificate for a test result became valid. (Encoded according to section 2.1)	4	F
Certificate Valid Until (03)	O	Last date in which the certificate for a test result is valid. (Encoded according to section 2.1)	4	F
Name (04)	M	Name of the holder (as specified in Doc 9303-3) MUST be used. (C40 Encoding)	26	V
DOB (05)	M	The DOB of the test subject. (Encoded according to section 2.1)	4	F
DocType (06) c	M	The ID Document Type of the identity document MUST be used. Only these values MUST be used: P – Passport (Doc 9303-4) A – ID Card (Doc 9303-5) C – ID Card (Doc 9303-5) I – ID Card Doc 9303-5) AC - Crew Member Certificate (Doc 9303-5) V – Visa (Doc 9303-7) D – Driving License (ISO 18013-1)	2	F
DocNum (07)	M	The ID Document Number of the identity	16	F

		document MUST be used of the document used in DocType. The ID Document Number is the unique identifier of the test subject. (C40 Encoding)		
Member state of test (08)	M	Three letter code identifying the country of test. (Three-letter code according to Doc 9303-3) (Encoded according to section 2.3)	2	F
Date of first positive NAAT test result (09)	M	The date when a sample for the NAAT test producing a positive result was collected. (Encoded according to section 2)	4	F
Optional Data Field (10)	O	Optional data issued at the discretion of the issuing authority (C40 Encoding)	14	V

Table 9

The table below shows the Proof of Recovery(PoR) Encoding Tags.

Tag	**L**	**Value**		
61	Var	Barcode Information Group Template		
	Tag	**L**	**Value**	
	05	Var	Proof of Recovery	
		Tag	**L**	**Value**
		01	12	URCI
		02	4	Certificate Valid From
		03	4	Certificate Valid Until
		04	26	Name
		05	4	Date of Birth
		06	2	Document Type
		07	16	Document Number
		08	2	Country of Test
		09	3	Date of first positive NAAT test result
		10	14	Optional Field

Table 10

3.3.1.6 Digital Travel Authorization (0x06)

This section describes the Data Elements that may be present in Digital Travel Authorization(DTA).

Data Element	OPTIONAL(O) or MANDATORY(m)	Description	Max Number of Bytes (after encoding)	Fixed(F) or Variable(V)
DTA Number (01)	M	The number given to the	10	V

		authorization by the issuing State. (C40 Encoding)		
Name (02)	M	Name of the holder (as specified in Doc 9303-3) MUST be used. (C40 Encoding)	26	V
Passport Number (03)	M	The 9 principal characters of the passport with which the travel authorization is linked. (C40 Encoding)	6	F
DOB (04)	M	Date of birth of holder.(Encoded according to section 2.1)	4	F
Nationality (05)	M	The nationality of the holder. (Three-letter code according to Doc 9303-3) (Encoded according to section 2.3)	2	F
Sex (06)	M	Sex of the holder	1	F
Place of Issue(07)	M	Post/location (usually a city) where the DTA is issued (C40 Encoding)	10	V
Valid from (08)	M	The date of issue of the DTA which indicates the first date from which the authorization can be used to seek entry. (Encoded according to section 2.1)	4	F
Valid Until (09)	M	The date of expiry of the authorization which indicates the last day on which the DTA can be used to seek entry. (Encoded according to section 2.1)	4	F
Duration of Stay (10)	M	The number of days, months or years during which the DTA holder may stay in the territory for which the DTA is valid. (encoded as DDMMYY, C40 encoding)	3	F
Number of Entries (11)	M	The number of allowed entries. • M denotes Multiple Entries • 1 – Single entry • 2 – 2 entries • …	1	F
Type-class-category (12)	M	This field shall include one or more of the following elements: • the issuing State's indication of the type	32	V

		and/or class of DTA granted in accordance with the law/practice of that State; • the broad categorization of the type of DTA granted, e.g. visitor/resident/ temporary resident/student/diplo mat, etc., in accordance with the law/practice of the issuing State; any limitations on the territorial validity of the travel authorization. (C40 Encoding)		
Additional Information (13)	O	This field may include necessary endorsements as to entitlements which attach to the DTA. (C40 Encoding)	67	V

Table 11

The table below shows the Digital Travel Authorization(DTA) Encoding Tags.

Tag	**L**	**Value**		
61	Var	Barcode Information Group Template		
	Tag	**L**	**Value**	
	06	Var	Digital Travel Authorization	
		Tag	**L**	**Value**
		01	10	DTA Number
		02	26	Name
		03	8	Passport Number
		04	4	Date of Birth
		05	2	Nationality
		06	1	Sex
		07	10	Place of Issue
		08	4	Valid from
		09	4	Valid Until
		10	3	Duration of Stay
		11	1	Number of entries
		12	32	Type-class-category
		13	67	Additional Information

Table 12

3.3.1.7 Machine Readable Zone (TD1) (0x07)

Refer to Doc9303-5 for Machine Readable Zone (MRZ) of TD1. MRZ (TD1) MUST be the concatenation of first, second and third line of the MRZ of TD1 and encoded by C40. The filler symbol < in the MRZ MUST be replaced by <SPACE> prior to encoding by C40.

The table below shows the MRZ of TD1 Encoding Tags.

Tag	**L**	**Value**	
61	Var	Barcode Information Group Template	
	Tag	**L**	**Value**

	07	60	MRZ (TD1)

Table 13

3.3.1.8 Machine Readable Zone (TD3) (0x08)

Refer to Doc9303-4 for Machine Readable Zone (MRZ) of TD3. MRZ (TD3) MUST be the concatenation of first and second line of the MRZ of TD3 and encoded by C40. The filler symbol < in the MRZ MUST be replaced by <SPACE> prior to encoding by C40.

The table below shows the MRZ of TD3 Encoding Tags.

Tag	**L**	**Value**	
61	Var	Barcode Information Group Template	
	Tag	**L**	**Value**
	08	60	MRZ (TD3)

Table 14

3.3.1.9 Card Access Number (0x09)

Card Access Number (CAN) MUST be encoded using C40 encoding.

The table below shows the CAN Encoding Tags.

Tag	**L**	**Value**	
61	Var	Barcode Information Group Template	
	Tag	**L**	**Value**
	09	4	CAN

Table 15

3.3.1.10 EF.CardAccess (0x0A)

EF.CardAccess (ECA) is a byte array.

The table below shows the ECA Encoding Tags.

Tag	**L**	**Value**	
61	Var	Barcode Information Group Template	
	Tag	**L**	**Value**
	0A	Var	ECA

Table 16

3.4 Signer Certificate Zone

If the Signer Certificate is included in the barcode, the beginning of the Signer Certificate is indicated by the tag 0x7E. This field will contain the full byte value of the signer certificate. The Signer Certificate Zone can only be present if IsSigned (Section 3.1.2) is “1” (Signed), and the Signer Certificate is included in the barcode. This field MUST NOT be part of the input for the signature algorithm to create the signature. This field MUST NOT be present if IsSigned is “0” (Not-Signed) or Signer Certificate is not included in this field. The Signer Certificate Zone MUST be encoded using DER-TLV.

3.5 Signature Zone

The beginning of the signature zone is indicated by the signature marker that has the value 0x7F, encoded as one byte, followed by one byte to five bytes denoting the length (the number of bytes) of the signature using the DER-TLV length fields encoding scheme.

The input of the signature algorithm MUST be the (hash of the) concatenation of the header and the complete message zone, excluding the tag that denotes the beginning of the signer certificate zone and everything after that. The signature zone contains the resulting signature.

Only hashing and signature algorithms defined in section 3.2.2 SHALL be used. Due to the resulting signature size, Elliptic Curve Digital Signature Algorithm (ECDSA) with a key length of at least 256 bit in combination with SHA-256 is a MUST.

The Signature Zone MUST be present if isSigned (Section 3.1.2) is “1” (signed) and MUST NOT be present if isSigned is “0” (not signed).

Refer to Doc 9303-13 Section 2.4 for more details.

3.6 Public Key Infrastructure (PKI) and Certificate Profiles

The signer certificate used for this specification will fall under the following OID branch:

id-icao OBJECT IDENTIFIER ::= {2.23.136}
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-idb OBJECT IDENTIFIER ::= {id-icao-mrtd-security 16}

3.6.1 Certificate Authorities (CAs) Hierarchy

The CA used for issuing IDB that contains travel document message MUST use the CSCA used for issuing document signers for travel documents.
A different CA may be used for issuing IDB that contains only health proof messages.

3.6.2 CA Profile

If a different root of trust is used for the issuance of the barcode signers which is only used for health proof messages, then the separate CA MUST comply with the CSCA specifications of Doc 9303-12 with the following restrictions:

- EKU extension MUST be included in the separate CA. The validation algorithm MUST ensure that the particular EKU as defined in this document is absent in the CSCA used for travel document. The OID for EKU for the separate CA is “2.23.136.1.1.16.1”. The EKU MUST be marked as Critical.
- Key-pair MUST be of ECC type.
- A namedCurve in the ECParameters of the Subject Public Key Information Field MAY be used. If a namedCurve is used, it MUST be one of the curves listed in clause 3.6.5

3.6.3 CRL Distribution Point

Refer to VDS-NC section 3.6.3.

3.6.4 Barcode Signer Certificate Profile

The barcode signer MUST comply with the barcode signer certificate profile defined in 9303-12, with the following restriction:

- The IDB signer key-pair MUST be of ECC type

- The EKU OID for IDB signer is “2.23.136.1.1.16.2”.

- `documentTypeList` extension MUST be present. It indicates the list of `DocumentType`, which the IDB signer is allowed to produce. More than one `DocumentType` may be added in the list.

- The `DocumentType` for ICAO use cases as defined currently will start with “N” and be followed by another letter denoting the message types the signer is allowed to produce. IDB signer MUST only add `DocumentType` defined in this section below.

The `DocumentType` value for health proof messages is “NH”. Health proof messages includes:
- PoV
- PoT
- PoR

The `DocumentType` value for travel document messages is “NA”. Travel document messages includes:
- Visa
- ETD
- DTA
- MRZ (TD1)
- MRZ (TD3)
- CAN
- ECA

3.6.5 ECParameters
Refer to VDS-NC section 3.6.5.

3.6.6 Barcode Signer Public Key Validity
Refer to VDS-NC section 3.6.6.

3.6.7 Trust List
Refer to VDS-NC section 3.6.7.

3.6.8 Distribution Mechanism
Refer to VDS-NC section 3.6.8.

4. Reference Documentation
The following documentation served as reference for this Technical Report:

[RFC 2119]	RFC 2119, S. Bradner, “Key Words for Use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997
[RFC 4648]	RFC 4648, S. Josefsson, “The Base16, Base32, and Base64 Data Encodings”, October 2006

[ISO/IEC 16022]	ISO/IEC 16022 Information technology — Automatic identification and data capture techniques — Data Matrix bar code symbology specification
[ISO/IEC 18004]	ISO/IEC 18004 Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification
[ISO/IEC 21471]	ISO/IEC 21471 Information technology — Automatic identification and data capture techniques — Extended rectangular data matrix (DMRE) bar code symbology specification
[ISO/IEC 23941]	ISO/IEC 23941 Information technology — Automatic identification and data capture techniques — Rectangular Micro QR Code (rMQR) bar code symbology specification
[ICD-11]	International Classification of Diseases 11th Revision - https://icd.who.int/en (retrieved April 23,2021)
[Doc 9303]	ICAO Doc 9303, 8th Edition, “Machine Readable Travel Documents”
[VDS-NC]	Visible Digital Seal for non-constrained environments V1.4 Technical Report
[RFC 1951]	RFC 1951, DEFLATE Compressed Data Format Specification
[RFC 1950]	RFC 1950, ZLIB Compressed Data Format Specification

Annex A Worked Examples

Worked examples will be added as the specification becomes stable. These will be available at the SC17/WG3 github page: https://github.com/ICAO-TRIP-ISO-WG3/IDB

A.1 Secure Messaging Barcode

This section contains examples for encoding the MRZ and CAN as detailed in section 3.3.1.7 and 3.3.1.9.

Raw Values:

Barcode Identifier
IDB1

Barcode Flag
A – Not signed, Not compressed
B – Signed, Not compressed
C – Not signed, Compressed
D – Signed, Compressed

Country Header
UTO

MRZ

P<UTOSPECIMEN<<PETER<<<<<<<<<<<<<<<<<<<<<<K7629352E7UTO8504279M2805203<<<<<<<<<<<<00

Value of MRZ after replacing "<" with space –

P UTOSPECIMEN PETER K7629352E7UTO8504279M2805203 00

CAN
156782

Barcode 1 (MRZ only)

- Barcode Payload
  - After C40 (In hexadecimal string) (Length = 66)
    - D9C5613E083CB5DBD2C1B8218DA3A93CB832755C133C133C133C133C133C133C135146575262285CD9C54C6D32FC55574BAA2628133C133C133C133C133DFE31
  - After ZLIB (In hexadecimal string) (Length = 57)
    - 78DABB7934D18EC366EBED4B077728F62E5E69B3C3A83446D8060506BA85072569C4DC3CEA936BF42734DC7B959A065CCEF69F2100566316DF
  - After Base32 encoding (Length = 96)
    - PDNLW6JU2GHMGZXL5VFQO5ZI6YXF42NTYOUDIRWYAYCQNOUFA4SWTRG4HTVJG27UE42NY64VTIDFZTXWT4QQAVTDC3PQ====
  - After removing Base-32 padding (Length = 92)

        - PDNLW6JU2GHMGZXL5VFQO5ZI6YXF42NTYOUDIRWYAYC QNOUFA4SWTRG4HTVJG27UE42NY64VTIDFZTXWT4QQAV TDC3PQ
- Barcode Value (Length = 97)
    - IDB1CPDNLW6JU2GHMGZXL5VFQO5ZI6YXF42NTYOUDIRWYAYC QNOUFA4SWTRG4HTVJG27UE42NY64VTIDFZTXWT4QQAVTDC3P Q
- Barcode

QR (Size 37x37) Data Matrix (Size 36x36)

Barcode 2 (CAN only – Not compressed)

- Barcode Payload
    - After C40 encoding (In hexadecimal string) (Length = 10)
        - D9C56106090420B346A7
    - After Base32 encoding (Length = 16)
        - 3HCWCBQJAQQLGRVH
- Barcode Value (Length = 21)
    - IDB1A3HCWCBQJAQQLGRVH
- Barcode

QR module size 25x25 Data Matrix (Size 18x18)

Barcode 3 (CAN only – Is compressed)

- Barcode Payload
    - After C40 encoding (In hexadecimal string) (Length = 10)
        - D9C56106090420B346A7
    - After ZLIB (In hexadecimal string) (Length = 18)
        - 78DABB7934918D934561B3DB720016B903D3
    - After Base32 encoding (Length = 32)
        - PDNLW6JUSGGZGRLBWPNXEAAWXEB5G===
    - After removing Base-32 padding (Length = 29)
        - PDNLW6JUSGGZGRLBWPNXEAAWXEB5G
- Barcode Value (Length = 34)
    - IDB1CPDNLW6JUSGGZGRLBWPNXEAAWXEB5G

- Barcode

QR (Size 29x29)

Data Matrix (Size 22x22)

Barcode 4 (MRZ and CAN)

- Barcode Payload
  - After C40 encoding (In hexadecimal string) (Length = 72)
    - D9C56144083CB5DBD2C1B8218DA3A93CB832755C133C133C133C133C133C133C133C135146575262285CD9C54C6D32FC55574BAA2628133C133C133C133C133DFE31090420B346A7
  - After ZLIB (In hexadecimal string) (Length = 63)
    - 78DABB7934D185C366EBED4B077728F62E5E69B3C3A83446D8060506BA85072569C4DC3CEA936BF42734DC7B959A065CCEF69F21278BC266B7E500E55118B2
  - After Base32 encoding (Length = 104)
    - PDNLW6JU2GC4GZXL5VFQO5ZI6YXF42NTYOUDIRWYAYCQNOUFA4SWTRG4HTVJG27UE42NY64VTIDFZTXWT4QSPC6CM236KAHFKEMLE===
  - After removing Base-32 padding (Length = 101)
    - PDNLW6JU2GC4GZXL5VFQO5ZI6YXF42NTYOUDIRWYAYCQNOUFA4SWTRG4HTVJG27UE42NY64VTIDFZTXWT4QSPC6CM236KAHFKEMLE
- Barcode Value (Length = 106)
  - IDB1CPDNLW6JU2GC4GZXL5VFQO5ZI6YXF42NTYOUDIRWYAYCQNOUFA4SWTRG4HTVJG27UE42NY64VTIDFZTXWT4QSPC6CM236KAHFKEMLE
- Barcode

QR (Size 37x37)

Data Matrix (Size 36x36)