MRZ character positions (line 2)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
43		Check digit	See paragraph 12. When the personal number field is not used and filler characters (<) are used in positions 29 to 42, the check digit may be zero or the filler character (<) at the option of the issuing State or organization.	1	Notes b, c, d
44		Composite check digit	Check digit for all characters of machine readable data of the lower line in positions 1 to 10, 14 to 20 and 22 to 43. The composite check digit is calculated on the basis of all figures shown on the lower machine readable line, including values for letters that are a part of the number fields and their check digits.	1	Paragraph 12; Notes b, d

** Notes for 5.3, 6.5 and 6.6.*

a) Alphabetic characters (A to Z) as defined in Appendix 2 to Section III. In the MRZ, only those characters specified in Appendix 2 to Section III shall be used.

b) Numeric characters (0 to 9) as defined in Appendix 2 to Section III. In the MRZ, only those characters specified in Appendix 2 to Section III shall be used.

c) Punctuation or other special characters. In the MRZ, only those characters specified in Appendix 2 to Section III shall be used.

d) The field name is not printed on the document.

e) The use of a field name is at the option of the issuing State.

f) In the case of the United Nations Laissez-passer, Field 01 (Issuing State or organization) in the visual inspection zone shall be completed with the words "UNITED NATIONS — NATIONS UNIES". In keeping with the international character of United Nations officials, neither nationality nor place of birth shall be shown. The caption for Field 08 (Nationality) shall read instead: "Official of/Fonctionnaire des" and the words "UNITED NATIONS/NATIONS UNIES" entered instead of nationality. Field 12 (Place of birth) shall be left blank. The codes to be used in Field 04 (Code for issuing State or organization) in the visual inspection zone as well as in character positions 3 to 5 (Issuing State or organization) in the upper line of the machine readable zone and in character positions 11 to 13 (Nationality) in the lower line shall be as specified in Appendix 1 to Section III.

g) Space.

h) With respect to the maximum number of character positions and/or the width of the field for this data element, refer to the specifications given for Field 19, when it is necessary to move the holder's portrait 4 mm (0.16 in) to the right.

i) The method of writing dates is given in paragraph 10.

j) The space reserved for Field 15 may be expanded to include additionally the space for Field 18 when the option is taken of locating the holder's signature or usual mark on the adjacent page. In this instance, the Authority or issuing office may be expressed as two lines of variable numbers of character positions.

k) When the name cannot be accommodated in the space provided for it in the viz, a notation giving the full name may be written on another page of the MRP. Alternatively, a smaller type font may be selected for use in the visual inspection zone only.

6.7 *Examples of name of the holder in the MRZ*

Note.— In the following examples, the document is assumed to be a passport issued by the State of Utopia. The first five characters of the upper machine readable line are P<UTO.

a) Usual representation:

Name: Anna Maria Eriksson
VIZ: ERIKSSON, Anna Maria
MRZ: P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<<

b) Central primary identifier:

Name: Deborah Heng Ming Lo
VIZ: HENG, Deborah Ming Lo
MRZ: P<UTOHENG<<DEBORAH<MING<LO<<<<<<<<<<<<<<<<<<

c) Hyphen as part of the name:

Name: Susie Margaret Smith-Jones
VIZ: SMITH-JONES, Susie Margaret
MRZ: P<UTOSMITH<JONES<<SUSIE<MARGARET<<<<<<<<<<<<

d) Apostophe as part of the name:

Name: Enya Siobhan O'Connor
VIZ: O'CONNOR, Enya Siobhan
MRZ: P<UTOOCONNOR<<ENYA<SIOBHAN<<<<<<<<<<<<<<<<<<

e) Multiple name components:

Name: Martin Van Der Muellen
VIZ: VAN DER MUELLEN, Martin
MRZ: P<UTOVAN<DER<MUELLEN<<MARTIN<<<<<<<<<<<<<<<<

f) No secondary identifier:

Name: Arkfreith
VIZ: ARKFREITH
MRZ: P<UTOARKFREITH<<<<<<<<<<<<<<<<<<<<<<<<<<<<

6.7.1 *Truncated names — secondary identifier truncated*

a) One or more name components truncated to initials:

Name: Nilavadhanananda Chayapa Dejthamrong Krasuang
VIZ: NILAVADHANANANDA, Chayapa Dejthamrong Krasuang
MRZ: P<UTONILAVADHANANANDA<<CHAYAPA<DEJTHAMRONG<K

b) One or more name components truncated:

Name: Nilavadhanananda Arnpol Petch Charonguang
VIZ: NILAVADHANANANDA, Arnpol Petch Charonguang
MRZ: P<UTONILAVADHANANANDA<<ARNPOL<PETCH<CHARONGU

6.7.2 *Truncated names — primary identifier truncated*

a) One or more components truncated to initials:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, Dingo Potoroo
MRZ: P<UTOBENNELONG<WOOLOOMOOLOO<WARRANDYTE<W<<DI

b) One or more components truncated:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, Dingo Potoroo
MRZ: P<UTOBENNELONG<WOOLOOM<WARRAND<WARNAM<<DINGO

c) One or more components truncated to a fixed number of characters:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, Dingo Potoroo
MRZ: P<UTOBENNEL<WOOLOO<WARRAN<WARNAM<<DINGO<POTO

6.7.3 *Names that just fit, indicating possible truncation by letter in the last position of the name field, but which are not truncated*

Name: Jonathon Warren Trevor Papandropoulous
VIZ: PAPANDROPOULOUS, Jonathon Warren Trevor
MRZ: P<UTOPAPANDROPOULOUS<<JONATHON<WARREN<TREVOR

Note.— Even though there is an alpha character in the 44th position of this passport upper machine readable line, this name has not been truncated ***but it must be assumed that it has been truncated.***

Representation of issuing State or organization and nationality of holder

7. *Visual inspection zone (VIZ)*

7.1 Where the name of the issuing State and/or the place of issue or place of birth are in a national language that does not use Latin characters, the name shall appear in the national language and also shall be either transliterated into Latin characters or translated into one or more languages (at least one of which must be English, French or Spanish) in which the name may be more commonly known to the international community. The name in the different languages shall be separated by an oblique character (/) followed by at least one blank space.

7.2 Where the name of the issuing State or place of issue or place of birth is in a language that uses the Latin alphabet, but where the name is more familiar to the international community in its translation into another language or languages (particularly English, French or Spanish), the name in the national language should be accompanied by one or more translations of the name. The name in the different languages shall be separated by an oblique character (/) followed by at least one blank space.

7.3 The three-letter codes listed in Appendix 1 to Section III may also be used, at the discretion of the issuing State or organization, to complete the field for the place of birth in the VIZ.

8. *Machine readable zone (MRZ)*

8.1 The three-letter codes listed in Appendix 1 to Section III shall be used to complete the field for the issuing State or organization and the nationality in the MRZ.

9. *Three-letter code use*

9.1 Use of three-letter codes is mandatory in the MRZ and Field 04 in the VIZ. Specific locations are defined in the following table.

	Zone	*Field no.*	*Character position no.*	*Number of character positions*
Issuing State or organization	VIZ	04	—	3
	MRZ (upper line)		3-5	3
Holder's nationality	MRZ (lower line)		11-13	3

Representation of dates

10. Dates shall be written as set forth hereunder.

10.1 *Dates in the VIZ.* Such dates on the MRP data page shall be entered in accordance with the Gregorian calendar as follows.

10.1.1 Days shall be shown by a two-digit number, i.e. the dates from one to nine shall be preceded by a zero; this number shall be followed by a blank space.

10.1.2 The name of the month may be written out in full in the language of the issuing State or organization or abbreviated, using up to four character positions.

10.1.3 Where the language of the issuing State or organization is not English, French or Spanish, the name of the month as defined in 10.1.2 shall be followed by an oblique character (/) and the name of the month or the abbreviation of the month up to four character positions, in one of the three languages, as shown in the table below.

Abbreviations of months in English, French and Spanish

Month	*English*	*French*	*Spanish*
January	Jan	Jan	Ene
February	Feb	Fév	Feb
March	Mar	Mars	Mar
April	Apr	Avr	Abr
May	May	Mai	Mayo
June	Jun	Juin	Jun
July	Jul	Juil	Jul
August	Aug	Août	Ago
September	Sep	Sept	Sept
October	Oct	Oct	Oct
November	Nov	Nov	Nov
December	Dec	Déc	Dic

Note.— Where the language of the issuing State or organization is English, French or Spanish, the issuing State or organization should use one of the other two languages (shown in the table above) following the oblique character (/).

10.1.4 The year will normally be shown by the last two digits and be preceded by a blank space. However, an issuing State or organization may use the four-digit representation of the year in the VIZ.

10.1.5 As an example, a date of 12 July 1942 on an MRP data page issued in Italian with French translation of the month would normally appear as follows:

12*b*LUG*b*/JUILb42

where *b* = a single blank space, i.e. 12 LUG /JUIL 42

10.1.6 The month may, however, be written in numerical form in the visual inspection zone, at the discretion of the issuing State or organization. In this case, following a practice established to facilitate the visual inspection of travel documents, a date would be written DD*b*MM*b*YY, where *b* = a single blank space. For example, a date of 12 July 1942 would appear in the VIZ of the MRP data page as follows: 12 07 42.

10.1.7 *Unknown date of birth.* Where a date of birth is completely unknown, that data element shall appear as XX*b*XXX*b*XX where *b* = a single blank space. If only part of the date of birth is unknown, that part shall be represented by XX if it is the day or year, or by XXX if it is the month.

10.2 *Dates in the MRZ.* Such dates on the MRZ shall, in accordance with the principle set forth in ISO 8601 : 1988, be shown as a six-digit number consisting of the last two digits for the year (YY) immediately followed by two digits for the number of the month (MM) and by two digits for the day (DD). The structure is as follows: YYMMDD.

10.2.1 Following this format, the example given in 10.1.6 will be shown as: 420712.

10.2.2 If all or part of the date of birth is unknown, the relevant character positions shall be completed with filler characters (<).

Check digits in the MRZ

11. The data structure of the lower machine readable line in 6.6 provides for the inclusion of five check digits as follows:

Check digit	*Character positions (lower MRZ line) used to calculate check digit*	*Check digit position (lower MRZ line)*
Passport number	1-9	10
Date of birth	14-19	20
Date of expiry	22-27	28
Personal number	29-42	43
Composite check digits	1-10, 14-20, 22-43 *Note.— Positions 11-13 and 21 are excluded when calculating the composite check digit.*	44

12. Details on calculation of check digits in the MRZ are set out below.

12.1 The position of check digits and the data used in their calculation differ between MRTDs, and a table defining this information is set out in the section(s) specific to the preparation of the different types of MRTDs contained in the applicable part of Doc 9303.

12.2 A special check digit calculation has been adopted for use in MRTDs. The check digits shall be calculated on modulus 10 with a continuously repetitive weighting of 731 731 ..., as follows.

12.3 *Step 1*. Going from left to right, multiply each digit of the pertinent numerical data element by the weighting figure appearing in the corresponding sequential position.

12.4 *Step 2*. Add the products of each multiplication.

12.5 *Step 3*. Divide the sum by 10 (the modulus).

12.6 *Step 4*. The remainder shall be the check digit.

12.7 For data elements in which the number does not occupy all available character positions, the symbol < shall be used to complete vacant positions and shall be given the value of zero for the purpose of calculating the check digit.

Case No. 1:15-cv-02362-RBJ Document 64-20 filed 09/11/17 USDC Colorado pg 7 of 63

12.8 When the check digit calculation is applied to data elements containing alphabetic characters, the characters A to Z shall have the values 10 to 35 consecutively, as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

12.9 *Example 1 — Application of check digit to date field.* Using 27 July 1952 as an example, with the date in numeric form as specified in ISO 8601 : 1988, the calculation will be:

	Date:	5		2		0		7		2		7
	Weighting:	7		3		1		7		3		1
Step 1 (multiplication)	Products:	35		6		0		49		6		7
Step 2 (sum of products)		35	+	6	+	0	+	49	+	6	+	7 = 103
Step 3 (division by modulus)		$\frac{103}{10}$ = 10, remainder 3										

Step 4. Check digit is the remainder, 3. The date and its check digit shall consequently be written as 5207273.

12.10 *Example 2 — Application of check digit to document number field.* Using the number AB2134 as an example for coding a 9-character, fixed-length field (e.g. passport number), the calculation will be:

Sample data element:		A		B		2		1		3		4	<	<	<		
Assigned numeric values:		10		11		2		1		3		4	0	0	0		
Weighting:		7		3		1		7		3		1	7	3	1		
Step 1 (multiplication)	Products:	70		33		2		7		9		4	0	0	0		
Step 2 (sum of products)		70	+	33	+	2	+	7	+	9	+	4	+ 0	+ 0	+ 0	=	125
Step 3 (division by modulus)		$\frac{125}{10}$ = 12, remainder 5															

Step 4. Check digit is the remainder, 5. The number and its check digit shall consequently be written as AB2134<<<5.

12.11 *Example 3— Application of composite check digit to MRZ.* Using the lower line of MRZ data from an MRP data page that follows as an example for coding the composite check digit, the calculation will be:

Lower machine readable line (character positions 1-43):

HA672242<6UTO5802254M9601086<<<<<<<<<<<<<<08

Sample data element:		H	A	6	7	2	2	4	2	<	6
Assigned numeric values:		17	10	6	7	2	2	4	2	0	6
Weighting:		7	3	1	7	3	1	7	3	1	7
Step 1 (multiplication)	Products:	119	30	6	49	6	2	28	6	0	42

Zzyym v. Tillerson - AR 0483

Sample data element:		5	8	0	2	2	5	4	9	6	0
Assigned numeric values:		5	8	0	2	2	5	4	9	6	0
Weighting:		3	1	7	3	1	7	3	1	7	3
Step 1 (multiplication)	Products:	15	8	0	6	2	35	12	9	42	0

Sample data element:		1	0	8	6	<	<	<	<	<	<
Assigned numeric values:		1	0	8	6	0	0	0	0	0	0
Weighting:		1	7	3	1	7	3	1	7	3	1
Step 1 (multiplication)	Products:	1	0	24	6	0	0	0	0	0	0

Sample data element:		<	<	<	<	<	<	<	<	0	
Assigned numeric values:		0	0	0	0	0	0	0	0	0	
Weighting:		7	3	1	7	3	1	7	3	1	
Step 1 (multiplication)	Products:	0	0	0	0	0	0	0	0	0	
Step 2 (sum of products)		119	+ 30	+ 6	+ 49	+ 6	+ 2	+ 28	+ 6	+ 0	+ 42 +
Step 2 (sum of products)		15	+ 8	+ 0	+ 6	+ 2	+ 35	+ 12	+ 9	+ 4	+ 0 +
Step 2 (sum of products)		1	+ 0	+ 24	+ 6	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0 +
Step 2 (sum of products)		0	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0	+
Step 2 (sum of products)		= 448									
Step 3 (division by modulus)		$\frac{448}{10}$ = 44, remainder 8									

Step 4. Check digit is the remainder, 8. The lower line of MRZ data together with its composite check digit may consequently be written as follows:

HA672242<6UTO5802254M9601086<<<<<<<<<<<<<<08

Character sets and fonts

13. The character sets and fonts to be used on the MRP data page shall be as indicated hereunder.

13.1 *Captions*

13.1.1 Captions shall be printed in a clear, linear type font in a size of 1.0 mm to 1.8 mm (0.04 in to 0.07 in).

13.1.2 Captions shall be in the language of the issuing State or organization. When such language uses the Latin alphabet, regular font style should be used to print the captions.

13.1.3 Where the language of the issuing State or organization is not English, French or Spanish, the printed caption as defined in 13.1.2 shall be followed by an oblique character (/) and the equivalent of the caption in English, French or Spanish. An italic font style may be used for the second language.

Note.— Where the language of the issuing State or organization is English, French or Spanish, the issuing State or organization should use one of the other two languages to print the caption following the oblique character (/).

13.2 For additional details, see Section III, 5 through 8.

Portrait

14. *Portrait.* A portrait, representing only the holder of the MRP, shall occupy the rectangular area defined as Zone V as specified in the data element directory (5.3).

14.1 Where an overlaminate is used, the adhesion of the laminate to a glued-in photograph or certain types of digital images may be inadequate. In such cases, the margin between the portrait and the left-hand edge of the MRP data page should be increased by moving the portrait 4 mm (0.16 in) to the right (i.e. a total of 6 mm (0.24 in)) to ensure a secure and durable adherence of the laminate to the data page on the left-hand margin.

14.2 The portrait may have irregular edges. When a digitally printed reproduction is used, the portrait may have the background dropped out in order to provide protection against forgery or substitution.

Characteristics of the machine readable zone

15. Except as otherwise specified herein, the MRP data page shall conform with ISO 1831 : 1980 concerning the following matters:

Optical properties of the substrate to be used.
Optical and dimensional properties of the image patterns forming OCR characters.
Basic requirements related to the relative position of OCR characters on the substrate.

15.1 Machine readable data shall be arranged from left to right in fixed-length fields in two lines (upper and lower) in the order specified in the data structure tables shown in 6.5 and 6.6, respectively, and located on the document as shown in Appendix 3 to this section. Data shall be entered in each field, beginning with the left-hand character position.

15.2 Where the entered data do not occupy all the character positions specified for the relevant field, the symbol < shall be used to complete the redundant positions.

Quality specifications of the machine readable zone

16. In general, the print quality shall conform to ISO 1831 : 1980 Range X, except as otherwise provided herein. All quality specifications set forth hereunder shall apply to the MRP data page after final preparation, except where otherwise noted, and conform to the requirements in Section III, 2.

16.1 *Substrate quality.* Paragraphs 4.3 through 4.3.2 of ISO 1831 : 1980 shall be used for reference only.

16.2 *Substrate opacity.* The substrate used, measured before and after final preparation, shall be within the definition of high or medium opacity (ISO 1831 : 1980, 4.4.1 and 4.4.3).

16.3 *Substrate gloss.* The level of gloss is not specified.

16.4 *Fluorescence.* The reflectance of the substrate in the visible spectrum shall exhibit no visibly detectable fluorescence when irradiated by ultraviolet light, except where this is a predictable fluorescence for security reasons.

16.5 *Alternative substrates.* When a substrate other than paper is chosen, it is recommended that the above specifications be followed.

16.6 *Spectral band.* The OCR print shall be legible visually and shall be black (B425 through B680 as defined in ISO 1831 : 1980). The OCR print shall also absorb in the B900 band as defined in ISO 1831 : 1980 (i.e. near infra-red). Any protective layers must not adversely affect this property.

16.7 *Print contrast signal (PCS).* After final preparation, e.g. after the application of any protective layer, the minimum print contrast signal (PCS/min), when measured as specified in ISO 1831 : 1980, shall be as follows: PCS/min $\geq$ 0.6 at the B900 spectral band.

16.8 *Character stroke width.* The stroke width after final preparation shall be as specified for Range X in ISO 1831 : 1980 (5.3.1).

16.9 *Contrast variation ratio (CVR).* After final preparation, i.e. after the application of any protective layer, the CVR should be as shown for Range X in ISO 1831 : 1980, i.e. CVR < 1.50.

16.10 *Spots and extraneous marks.* ISO Standard 1831 : 1980 (5.4.4.6 and 5.4.5.12) shall apply at the reading surface (see also B. 6 of Annex B and C 5.10 of Annex C to ISO 1831 : 1980).

16.11 *Voids.* The value of "d" as defined in ISO 1831 : 1980 (5.4.5.9) shall be equal to 0.4 at the reading surface.

16.12 *Line separation.* See 6.4 and Appendix 3 to this section.

16.13 *Line spacing.* See 6.4 and Appendix 3 to this section.

16.14 *Position of print within the ERZ.* The two MRZ lines shall appear within the effective reading zone as defined in 15 and Appendix 4 to Section III.

16.15 *Skew.* The provisions relating to skew shall be as follows.

16.15.1 *Skew of MRZ characters.* The skew of individual MRZ characters on the MRP data page shall not exceed 3° measured from the reference edge.

16.15.2 *Skew of the MRZ lines.* The effect of the actual skew of the MRZ lines and the actual skew of the MRZ characters shall not exceed the limit specified in 16.15.1 nor should the skew of MRZ or character misalignment result in the MRZ lines or any part thereof appearing outside the printing zone as defined in Appendix 3 to this section.

16.16 *Differentiation between the letter "O" and the number zero.* The letter O and the number zero shall be as defined in ISO 1073-2 : 1976. Reader software should deduce whether a character is an "O" or a zero based on the field context (numeric, alphabetic or special).

Optional expansion of machine readable data capacity

17. Should a State or organization wish to expand the machine readable data capacity of the MRP beyond that defined for global interchange (see 7, Section III), and intend that data stored in such expanded capacity be readable in other than its own systems, the issuing State or organization shall use the following additional machine readable data technology, as appropriate (see informative Annex B), as specified below.

17.1 *Bar code.* See Annex A for details on the use of bar code(s) to expand the machine readable data capacity of an MRP.

Note.— The data structure and format for such technology are not yet defined. This subject will be addressed in a future amendment to these specifications.

18. Proper *co-existence* of the above optional machine readable data storage technology with the *mandatory OCR technology* is critical to ensure global interoperability of the MRP. Annex B provides informative details on the possible combinations available (scenarios) to assist the issuing State or organization, should it choose to use the above optional technology to expand the machine readable data capacity of the MRP in addition to the mandatory OCR technology.

Optional machine-assisted identity confirmation and document security feature verification using an MRP

19. Should a State or organization wish to provide for machine-assisted identity confirmation and/or machine-assisted document security feature verification with the MRP, the specifications and/or recommendations below should be applied to ensure global interoperability.

19.1 *Machine-assisted identity confirmation.* See Annex C for details.

19.2 *Machine-assisted document security feature verification.* See Annex D for details.

20. Proper *co-existence* of optional machine-assisted identity confirmation and document security feature verification technologies with the mandatory OCR technology and/or optional machine readable data expansion technologies is critical to ensure global interoperability of the MRP. Annex B provides informative details on the possible combinations available (scenarios), should the issuing State or organization choose to use machine-assisted identity confirmation or document security feature verification with the MRP.

Passport card

21. Should a State or organization wish to issue a machine readable passport card specifically for purposes such as facilitating travel to States accepting a passport card without visa for entry (*recognizing that issuing States or organizations must reach specific agreements with such receiving States on acceptance of the passport card*), facilitating identity confirmation of the rightful holder to enhance security or in case of loss/theft of the MRP, and/or *approved* use in automated passenger clearance schemes, the issuing State or organization shall issue an ID-1 size card in accordance with the specifications for a TD-1 in Part 3 of Doc 9303. This card, consistent with its status as a passport, shall be identified as a passport card and conform as follows.

21.1 *General layout.* The passport card shall comply with the specifications governing the general layout of the TD-1 (see Doc 9303, Part 3, Section IV).

21.2 *Detailed layout of VIZ.* The passport card shall comply with the specifications governing layout of the VIZ of the TD-1 (see Doc 9303, Part 3, Section IV) with the following exception.

21.2.1 *Name of document.* The name of the document (Field 01/Zone I) shall be 'PASSPORT CARD'.

21.3 *Detailed layout of the MRZ.* The passport card shall comply with the specifications governing layout of the MRZ for the TD-1 (see Doc 9303, Part 3, Section IV) with the following exception.

21.3.1 *Type of document.* The type of document (Line 1) shall be 'IP'.

ICAO

Doc 9303

Machine Readable Travel Documents

Seventh Edition, 2015

Part 1: Introduction



Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

ICAO

Doc 9303

Machine Readable Travel Documents

Seventh Edition, 2015

Part 1: Introduction

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/security/mrtd

Doc 9303, *Machine Readable Travel Documents*
Part 1 — *Introduction*
ISBN 978-92-9249-790-3

© ICAO 2015

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, without prior permission in writing from the International Civil Aviation Organization.

AMENDMENTS

Amendments are announced in the supplements to the *Products and Services Catalogue;* the Catalogue and its supplements are available on the ICAO website at www.icao.int. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of ICAO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

TABLE OF CONTENTS

		Page
1.	**FOREWORD**	**1**
2.	**SCOPE**	**1**
3.	**GENERAL CONSIDERATIONS**	**2**
3.1	ICAO's Leadership Role	2
3.2	Relative Costs and Benefits of Machine Readable Travel Documents	2
3.3	Operations	3
3.4	Note on the Supplement	3
3.5	Endorsement by ISO	3
4.	**DEFINITIONS AND REFERENCES**	**4**
4.1	Acronyms	4
4.2	Terms and Definitions	6
4.3	Key Words	21
4.4	Object Identifiers	22
4.5	The Use of Notes	24
5.	**GUIDANCE ON THE USE OF DOC 9303**	**24**
5.1	Doc 9303 Composition	24
5.2	Relationship between MRTD Form Factors and Relevant Doc 9303 Parts	26
6.	**REFERENCES (NORMATIVE)**	**26**

1. FOREWORD

ICAO's work on machine readable travel documents began in 1968 with the establishment, by the Air Transport Committee of the Council, of a Panel on Passport Cards. This Panel was charged with developing recommendations for a standardized passport book or card that would be machine readable, in the interest of accelerating the clearance of passengers through passport controls. The Panel produced a number of recommendations, including the adoption of optical character recognition (OCR) as the machine reading technology of choice due to its maturity, cost-effectiveness and reliability. In 1980, the specifications and guidance material developed by the Panel were published as the first edition of Doc 9303, titled *A Passport with Machine Readable Capability*, which became the basis for the initial issuance of machine readable passports by Australia, Canada and the United States.

In 1984, ICAO established what is now known as the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), comprised of government officials who specialize in the issuance and border inspection of passports and other travel documents, in order to update and enhance the specifications which had been prepared by the Panel. Subsequently, this group's terms of reference were expanded to include, first, the development of specifications for a machine readable visa and, later, specifications for machine readable cards that may be used as official travel documents.

In 1998, the New Technologies Working Group of the TAG/MRTD began work to establish the most effective biometric identification system and associated means of data storage for use in MRTD applications, particularly in relation to document issuance and immigration considerations. The bulk of the work had been completed by the time the events of 11 September 2001 caused States to attach greater importance to the security of a travel document and the identification of its holder. The work was quickly finalized and endorsed by the TAG/MRTD and the Air Transport Committee.

The resulting Technical Reports on the employment of biometrics and contactless chip technology, Logical Data Structure (LDS), and Public Key Infrastructure (PKI) were incorporated into Volume 2 of the Sixth Edition of Doc 9303, Part 1 (*Machine Readable Passports*) in 2006, and Volume 2 of the Third Edition of Doc 9303, Part 3 (*Machine Readable Official Travel Documents*) in 2008.

2. SCOPE

The Seventh Edition of Doc 9303 represents a restructuring of the ICAO specifications for Machine Readable Travel Documents. Without incorporating substantial modifications to the specifications, in this new edition Doc 9303 has been reformatted into a set of specifications for Size 1 Machine Readable Official Travel Documents (TD1), Size 2 Machine Readable Official Travel Documents (TD2), and Size 3 Machine Readable Travel Documents (TD3), as well as visas. This set of specifications consists of various separate documents in which general (applicable to all MRTDs) as well as MRTD form factor specific specifications are grouped. See Section 5.1 "Doc 9303 Composition" for an overview.

These specifications are not intended to be a standard for national identity documents. However, a State whose identity documents are recognized by other States as valid travel documents shall design its identity documents such that they conform to the specifications of Doc 9303-3 and Doc 9303-4, Doc 9303-5 or Doc 9303-6.

Although the specifications in Doc 9303-4 are intended for particular application to the passport, these specifications apply equally to other TD3 size identity documents, for example, the laissez-passer, the seafarer's identity document and refugee travel documents.

Zzyym v. Tillerson - AR 0494

The document at hand is Part 1. Part 1 introduces the Doc 9303 specifications. It describes the build-up of the twelve parts of Doc 9303, provides general information on ICAO, and guidance on the terminology and abbreviations used throughout the specifications.

3. GENERAL CONSIDERATIONS

3.1 ICAO's Leadership Role

ICAO's initiative to develop standard specifications for passports and other travel documents followed the tradition established by the League of Nations Passport Conferences of the 1920s and the work of the League's successor, the United Nations Organization. ICAO's mandate to continue in its leadership role stems from the Convention on International Civil Aviation (the "Chicago Convention") which covers the full range of requirements for efficient and orderly civil aviation operations, including provisions for clearance of persons through border controls, i.e.:

a) the requirement for persons travelling by air and aircraft crews to comply with immigration, customs and passport regulations (Article 13);

b) the requirement for States to facilitate border clearance formalities and prevent unnecessary delays (Article 22);

c) the requirement that States collaborate in these matters (Article 23); and

d) the requirement for States to develop and adopt internationally standard procedures for immigration and customs clearance (Article 37 j)).

Under this mandate, ICAO develops and maintains international Standards in Annex 9 — *Facilitation* to the Chicago Convention for implementation by Member States. In the development of such Standards, it is a fundamental precept that if public authorities are to facilitate inspection formalities for the vast majority of air travellers, those authorities must have a satisfactory level of confidence in the reliability of travel documents and in the effectiveness of inspection procedures. The production of standardized specifications for travel documents and the data contained therein is aimed at building that confidence.

In 2004, the Assembly of ICAO affirmed that cooperative work on specifications to strengthen the security and integrity of travel documents should be pursued by the Organization as a matter of high priority. In addition to the International Organization for Standardization (ISO), consultants to the TAG/MRTD include the International Air Transport Association (IATA), the Airports Council International (ACI), and the International Criminal Police Organization (INTERPOL).

In 2005, the then 188 Member States of ICAO approved a new Standard that all States must begin issuing machine readable passports in accordance with Doc 9303 no later than the year 2010. No later than the year 2015 all non-machine readable travel documents must have expired. This Standard is published in the 13th Edition (2011) of Annex 9 — *Facilitation*.

3.2 Relative Costs and Benefits of Machine Readable Travel Documents

Experience with the issuance of machine readable passports, in conformity with the specifications set forth in Doc 9303, indicates that the cost of producing MRTDs may be no greater than that of producing conventional documents, though the cost will be higher when biometric identification and electronic travel documents are implemented. As traffic volumes grow and more States focus on how they can rationalize their clearance processes with the employment of

computerized databases and electronic data interchange, the MRTD plays a pivotal part in modern, enhanced compliance systems. Equipment to read the documents and access the databases may entail a substantial investment, but this can be expected to be returned by the improvements in security, clearance speed and accuracy of verification which such systems provide. Use of MRTDs in automated clearance systems may also make it possible for States to eliminate both the requirement for paper documents, such as passenger manifests and embarkation/disembarkation cards, and the administrative costs associated with the related manual procedures.

3.3 Operations

The basic machine readable travel document, with its OCR readability, is designed for both visual and mechanical reading.

ICAO Member States have recognized that standardization is a necessity and that the benefits of adopting the Doc 9303 standard formats for passports and other travel documents extend beyond the obvious advantages for States that have the machine readers and databases for use in automated clearance systems. In fact, the physical characteristics and data security features of the documents themselves offer strong defence against alteration, forgery or counterfeit. Moreover, adoption of the standardized format for the visual zone of an MRTD facilitates inspection by airline and government officials, with the result that clearance of low-risk traffic is expedited, problem cases are more readily identified, and enforcement is improved. The optional introduction of biometric identification with data stored on a contactless integrated circuit will provide greater security and resistance to fraud and thus make it easier for the legitimate document holder to obtain visas for travel and to be processed through border inspection systems.

Note.— It is recognized that situations will arise where an eMRTD will not interface correctly with a reader at a border. There are several reasons why this might occur, of which a failure of the eMRTD is only one. ICAO emphasizes that an eMRTD which fails to read is nevertheless a valid document. However, a failure to read could be the result of fraudulent attack, and the receiving State should establish its own procedures for dealing with this possibility, which should involve more stringent inspection of the document and its holder but also allow that the failure involves no fraudulent intent.

3.4 Note on the Supplement

ICAO will issue from time to time a "Supplement to Doc 9303". The Supplement will contain information intended to clarify, amplify or elaborate on issues with respect to travel document specifications, as well as to correct errors encountered from implementation experiences. It is intended that the information contained in the Supplement will augment the existing guidance in Doc 9303 as well as in Technical Reports issued by ICAO. The Supplement will be issued on a continuing and consistent basis.

The specifications of Doc 9303 should always be read in conjunction with the additional information set out in the latest release of the Supplement which will be available on the ICAO web site at http://www.icao.int/security/mrtd.

3.5 Endorsement by ISO

The technical specifications sections of Doc 9303 have received the endorsement of the International Organization for Standardization as ISO Standard 7501. Such endorsement is made possible by means of a liaison mechanism through which manufacturers of travel documents, readers and other technologies provide technical and engineering advice to the TAG/MRTD under the auspices of ISO. Through this working relationship, the ICAO specifications have achieved, and are expected to continue to receive, the status of worldwide standards by means of a simplified procedure within ISO.

The liaison mechanism with ISO has been successfully applied not only to the endorsement of new specifications for travel documents as ISO standards but also to the approval of amendments to the specifications. Subsequent revisions to Doc 9303 will therefore be processed for ISO endorsement in the same manner as previously.

4. DEFINITIONS AND REFERENCES

4.1 Acronyms

Acronym	Full form
3DES	Triple DES
AA	Active Authentication
AFS	Anti-Fraud Specialist
AES	Advanced Encryption Standard
AID	Application Identifier
APDU	Application Protocol Data Unit
AO	Authorizing Officer
BAC	Basic Access Control
BER	Basic Encoding Rules
BLOB	Binary Large Object
CA	Certification Authority
CAN	Card Access Number
CBEFF	Common Biometric Exchange Format Framework
CID	Card IDentifier
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
DER	Distinguished Encoding Rule
DES	Data Encryption Standard
DH	Diffie Hellmann
DN	Distinguished Name
DO	Data Object
DOVID	Diffractive Optically Variable Image Device
DS	Document Signer
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECDH	Elliptic Curve Diffie Hellmann

Acronym	Full form
ECDSA	Elliptic Curve Digital Signature Algorithm
ECKA	Elliptic Curve Key Agreement
EEPROM	Electrically Erasable Programmable Read Only Memory
eMRP	Electronic Machine Readable Passport
eMRTD	Electronic Machine Readable Travel Document
eMROTD	Electronic Machine Readable Official Travel Document
ERZ	Effective Reading Zone
FAR	False Acceptance Rate
FIPS	Federal Information Processing Standard
FRR	False Rejection Rate
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
ICC	Integrated Circuit Card
IFD	InterFace Device
IR	InfraRed light
IS	Inspection System
LDS	Logical Data Structure
MAC	Message Authentication Code
MRP	Machine Readable Passport
MRTD	Machine Readable Travel Document
MROTD	Machine Readable Official Travel Document in the form of a card
MRV-A	Full size (Format A) Machine Readable Visa
MRV-B	Small size (Format B) Machine Readable Visa
MRZ	Machine Readable Zone
NAD	Node ADdress
NIST	National Institute of Standards and Technology
NTWG	New Technologies Working Group
OCR	Optical Character Recognition
OCR-B	Optical Character Recognition font defined in ISO 1073-2
OID	Object IDentifier
OVD	Optically Variable Device
OVF	Optically Variable Feature
PACE	Password Authenticated Connection Establishment

Acronym	Full form
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
PIX	Proprietary Identifier eXtension (PIX).
PKD	Public Key Directory
PKI	Public Key Infrastructure
RID	Registered IDentifier (RID)
ROM	Read Only Memory
RSA	Rivest, Shamir and Adleman
SHA	Secure Hash Algorithm
SM	Secure Messaging
SO_D	Document Security Object
SSC	Send Sequence Counter
TAG/MRTD	Technical Advisory Group on Machine Readable Travel Documents
TD1	Size 1 Machine Readable Official Travel Document
TD2	Size 2 Machine Readable Official Travel Document
TD3	Size 3 Machine Readable Travel Document
TLV	Tag Length Value
UID	Unique IDentifier
UV	UltraViolet light
VIZ	Visual Inspection Zone
WSQ	Wavelet Scalar Quantization

4.2 Terms and Definitions

Term	Definition
Algorithm	A specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result.
Anti-scan pattern	An image usually constructed of fine lines at varying angular displacement and embedded in the security background design. When viewed normally, the image cannot be distinguished from the remainder of the background security print but when the original is scanned or photocopied the embedded image becomes visible.
Application Identifier (AID)	Data element that identifies an application. eMRTD applications use a Standard AID that is one of four categories of AID. It consists of a registered application provider identifier (RID) and a proprietary application identifier extension (PIX).
Asymmetric	Different keys needed on each end of a communication link.

Term	Definition
Asymmetric algorithm	This type of cryptographic operation uses one key for encryption of plain text and another key for decryption of associated cipher text. These two keys are related to each other and are called a Key Pair.
Asymmetric keys	A separate but integrated user key pair comprised of one public key and one private key. Each key is one-way, meaning that a key used to encrypt information cannot be used to decrypt the same information.
Authentication	A process that validates the claimed identity of a participant in an electronic transaction.
Authenticity	The ability to confirm that the Logical Data Structure and its components were created by the issuing State or organization.
Authorization	A security process to decide whether a service can be given or not.
Authorized receiving organization	Organization authorized to process an official travel document (e.g. an aircraft operator) and, as such, potentially allowed in the future to record details in the optional capacity expansion technology.
Barcode	A means of storing data as a pattern of lines or dots.
Biographical data (biodata)	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the MRTD, or on the chip if present.
Biometric	A measurable, unique, physical characteristic or personal behavioural trait used to recognize the identity, or verify the claimed identity, of a enrollee.
Biometric Data	The information extracted from the biometric and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data).
Biometric Identification	A means of identifying or confirming the identity of the holder of an MRTD by the measurement of one or more properties of the holder's person.
Biometric matching	The process of using an algorithm that compares templates derived from the biometric reference and from the live biometric input, resulting in a determination of match or non-match.
Biometric reference template	A data set which defines a biometric measurement of a person which is used as a basis for comparison against a subsequently submitted biometric sample(s).
Biometric sample	Raw data captured as a discrete, unambiguous, unique and linguistically neutral value representing a biometric characteristic of an enrollee as captured by a biometric system (for example, biometric samples can include the image of a fingerprint as well as its derivative for authentication purposes).
Biometric system	An automated system capable of: 1. capturing a biometric sample from an end user for an MRP; 2. extracting biometric data from that biometric sample; 3. comparing that specific biometric data value(s) with that contained in one or more reference templates; 4. deciding how well the data match, i.e. executing a rule-based matching process specific to the requirements of the unambiguous identification and person authentication of the enrollee with respect to the transaction involved; and

Case No. 1:15-cv-02362-RBJ Document 64-20 filed 09/11/17 USDC Colorado pg 25 of 63

Term	Definition
	5. indicating whether or not an identification or verification of identity has been achieved.
Biometric template	Extracted and compressed data taken from a biometric sample.
Biometric verification	A means of identifying or confirming the identity of the holder of an MRTD by the measurement and validation of one or more unique properties of the holder's person.
Bit	A binary digit. The smallest possible unit of information in a digital code.
Black-line white-line design	A design made up of fine lines often in the form of a guilloche pattern and sometimes used as a border to a security document. The pattern migrates from a positive to a negative image as it progresses across the page.
Block	A string or group of bits that a block algorithm operates on.
Block algorithm	See: block cipher.
Block cipher	Algorithms that operate on plain text in blocks (strings or groups) of bits.
Bootstrapping	A method of testing the reliability of a data set.
Breeder Document	Documentation used as evidence of identity when applying for a travel document.
Brute-force attack	Trying every possible key and checking whether the resulting plain text is meaningful.
Byte	A sequence of eight bits usually operated on as a unit.
Caption	Printed word or phrase to identify a data field. In exceptional circumstances, when multiple different official languages do not fit in the data field, numbers can be used. These numbers must be accompanied by explanatory text at another location in the MRP.
Capture	The method of taking a biometric sample from the end user.
Card	Medium according to ISO/IEC 7810, ISO/IEC 7811, ISO 7812 used to carry information.
Certificate	A digital document which proves the authenticity of a public key.
Certificate Revocation List (CRL)	A list of revoked certificates within a given infrastructure.
Certification Authority (CA)	A trustworthy body that issues digital certificates for PKI.
Chemical sensitizers	Security reagents to guard against tampering by chemical erasure, such that irreversible colours develop when bleach and solvents come into contact with the document.
Cipher	Secret writing based on a key, or set of predetermined rules or symbols.
Collation marks	See: Index marks.
Colour shifting ink	Inks changing their visual characteristic depending on the viewing angle and/or the quality of a stimulating (light) source.
Comparison	The process of comparing a biometric sample with a previously stored reference template or templates. See also "One-to-many" and "One-to-one".

Zzyym v. Tillerson - AR 0501

Term	Definition
Contactless integrated circuit	A semi-conductor device which stores MRTD data and which communicates with a reader using radio frequency energy according to ISO/IEC 14443.
Common Biometric Exchange Format Framework (CBEFF)	A common file format that facilitates exchange and interoperability of biometric data.
Control Number	A number assigned to a document at the time of its manufacture for record-keeping and security purposes.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means.
Country code	A two- or three-letter code as defined in ISO 3166-1, used to designate a document issuing authority or nationality of the document holder.
Cryptography	Science of transforming information into an enciphered, unintelligible form using an algorithm and a key.
Data Group	A series of related Data Elements grouped together within the Logical Data Structure.
Data Encryption Standard (DES)	A method of data encryption specified in FIPS 46-3.
Data Feature	The incorporation of encoded information into the document data or image structure, usually into the personalization data, especially the portrait.
Data Page	The page of the passport book, preferably the second or penultimate page, which contains the biographical data of the document holder. See "Biographical data".
Decryption	The act of restoring an encrypted file to its original state through the use of a key.
Deviation List	Signed list issued by an issuing State specifying non-conformities in travel documents and/or keys and certificates.
Deviation List Signer	An entity that digitally signs a Deviation List. The Deviation List signer is authorized by its national CSCA to perform this function through the issuance of a Deviation List Signer certificate.
Diffractive Optically Variable Device	A security feature containing a holographic or equivalent image within its construction, the image changing its appearance with angle of viewing or illumination.
Diffractive Optically Variable Image Device (DOVID) Laminate or Overlay	A laminate or overlay containing a DOVID either covering a whole area or located so as to protect key data on the document.
Digital signature	The result of a cryptographic operation enabling the validation of information by electronic means. This is NOT the displayed signature of the MRTD holder in digital form.
Digital Signature Algorithm (DSA)	Asymmetric algorithm published by NIST in FIPS 186. This algorithm only provides digital signature function.
Digital Watermark	See: Steganography.

Term	Definition
Displayed signature	The original written signature or the digitally printed reproduction of the original.
Directory/Public Key Directory (PKD)	A repository for storing information. Typically, a directory for a particular PKI is a repository for the public key encryption certificates issued by that PKI's Certification Authority, along with other client information. The directory also keeps cross-certificates, Certification Revocation Lists, and Authority Revocation Lists.
Document blanks	A document blank is a travel document that does not contain personalized data. Typically, document blanks are the base stock from which personalized travel documents are created.
Document number	A number that uniquely identifies a document. It is recommended that the document number and the control number be identical.
Document signer	A body which issues a biometric document and certifies that the data stored on the document is genuine in a way that will enable detection of fraudulent alteration.
Duplex design	A design made up of an interlocking pattern of small irregular shapes, printed in two or more colours and requiring very close register printing in order to preserve the integrity of the image.
Eavesdropping	The unauthorized interception of data communication.
Effective reading zone (ERZ)	A fixed-dimensional area, common to all MRTDs, in which the machine readable data in the MRZ can be read by document readers.
Electrically Erasable Programmable Read Only Memory (EEPROM)	A non-volatile memory technology where data can be electrically erased and rewritten.
Electronic Machine Readable Passport (eMRP)	A TD3 size MRTD conforming to the specifications of Doc 9303-4, that additionally incorporates a contactless integrated circuit including the capability of biometric identification of the holder. Commonly referred to as "ePassport".
Electronic Machine Readable Travel Document (eMRTD)	An MRTD (passport, visa or card) that has a contactless integrated circuit embedded in it and the capability of being used for biometric identification of the MRTD holder in accordance with the standards specified in the relevant Part of Doc 9303 — *Machine Readable Travel Documents.*
Electronic MROTD	A TD1 or TD2 size MROTD conforming to the specifications of Doc 9303-5 or Doc 9303-6, respectively, that additionally incorporates a contactless integrated circuit including the capability of biometric identification of the holder.
Embedded image	An image or information encoded or concealed within a primary visual image. Also see steganography.
Encryption	The act of disguising information through the use of a key so that it cannot be understood by an unauthorized person.
End user	A person who interacts with a biometric system to enroll or have his[1] identity checked.

1. Throughout this document, the use of the male gender should be understood to include male and female persons.

Term	Definition
Enrollee	A human being, i.e. natural person, assigned an MRTD by an issuing State or organization.
Enrollment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.
ePassport	Commonly used name for an eMRP. See Electronic Machine Readable Passport (eMRP).
Extraction	The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.
Failure to acquire	The failure of a biometric system to obtain the necessary biometric to enroll a person.
Failure to enroll	The failure of a biometric system to enroll a person.
False Acceptance	When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity.
False Acceptance Rate (FAR)	The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The false acceptance rate may be estimated as FAR = NFA/NIIA or FAR = NFA/NIVA where FAR is the false acceptance rate, NFA is the number of false acceptances, NIIA is the number of impostor identification attempts, and NIVA is the number of impostor verification attempts.
False match rate	Alternative to "false acceptance rate"; used to avoid confusion in applications that reject the claimant if his biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of "false acceptance" and "false rejection".
False non-match rate	Alternative to "false rejection rate"; used to avoid confusion in applications that reject the claimant if his biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of "false acceptance" and "false rejection".
False rejection	When a biometric system fails to identify an enrollee or fails to verify the legitimate claimed identity of an enrollee.
False rejection rate (FRR)	The probability that a biometric system will fail to identify an enrollee or verify the legitimate claimed identity of an enrollee. The false rejection rate may be estimated as follows: FRR = NFR/NEIA or FRR = NFR/NEVA where FRR is the false rejection rate, NFR is the number of false rejections, NEIA is the number of enrollee identification attempts, and NEVA is the number of enrollee verification attempts. This estimate assumes that the enrollee identification/verification attempts are representative of those for the whole population of enrollees. The false rejection rate normally excludes "failure to acquire" errors.
Fibres	Small, thread-like particles embedded in a substrate during manufacture.
Field	Specified space for an individual data element within a zone.
Fingerprint(s)	One (or more) visual representation(s) of the surface structure of the holder's fingertip(s).

Term	Definition
Fluorescent ink	Ink containing material that glows when exposed to light at a specific wavelength, usually UV.
Forgery	Fraudulent alteration of any part of the genuine document.
Fraudulent Alteration	Involves the alteration of a genuine document in an attempt to enable it to be used for travel by an unauthorized person or to an unauthorized destination. The biographical details of the genuine holder, particularly the portrait, form the prime target for such alteration.
Front-to-back (see-through) register	A design printed on both sides of an inner page of the document which, when the page is viewed by transmitted light, forms an interlocking image.
Full frontal (facial) image	A portrait of the holder of the MRTD produced in accordance with the specifications established in Doc 9303.
Full size (Format-A) machine readable visa (MRV-A)	An MRV conforming with the dimensional specifications contained in Doc 9303-7, sized to completely fill a passport visa page.
Gallery	The database of biometric templates of persons previously enrolled, which may be searched to find a probe.
Ghost Image	See: Shadow Image.
Global interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to obtain and exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye readable and machine readable data in all eMRTDs.
Globally Interoperable Biometric	Refers to Face Image as set forth in Doc 9303-9.
Guilloche design	A pattern of continuous fine lines, usually computer generated, and forming a unique image that can only be accurately re-originated by access to the equipment, software and parameters used in creating the original design.
Hash	A mathematical formula that converts a message of any length into a unique fixed-length string of digits known as "message digest" that represents the original message. A hash is a one-way function, that is, it is infeasible to reverse the process to determine the original message. Also, a hash function will not produce the same message digest from two different inputs.
Heat-sealed laminate	A laminate designed to be bonded to the biographical data page of a passport book by the application of heat and pressure.
Holder	A person possessing an MRTD, submitting a biometric sample for verification or identification whilst claiming a legitimate or false identity. A person who interacts with a biometric system to enroll or have his identity checked.

Term	Definition
Identification/Identify	The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the eMRTD holder whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with "Verification".
Identification card (ID-card)	A card used as an identity document.
Identifier	A unique data string used as a key in the biometric system to name a person's identity and its associated attributes. An example of an identifier would be an MRTD number.
Identity	The collective set of distinct personal and physical features, data and qualities that enable a person to be definitively identified from others. In a biometric system, identity is typically established when the person is registered in the system through the use of so-called "breeder documents" such as birth certificate and citizenship certificate.
Identity Document	Document used to identify its holder and issuer, which may carry data required as input for the intended use of the document.
Image	A representation of a biometric as typically captured via a video, camera or scanning device. For biometric purposes this is stored in digital form.
Impostor	A person who applies for and obtains a document by assuming a false identity, or a person who alters his physical appearance to represent himself as another person for the purpose of using that person's document.
Index marks	These marks are printed on the outside edge of each page in consecutive order starting from the top on the first page to a lower position on the following page and so on. The register mark of the last page appears at the bottom. This printing method leads to the appearance of a continuous stripe on the edge of the passport. Any page that has been removed will register as a gap. When printed in UV colour, this stripe becomes visible only under UV light. Also called collation marks.
Infra-red drop-out ink	An ink which forms a visible image when illuminated with light in the visible part of the spectrum and which cannot be detected in the infrared region.
Infra-red ink	An ink which is visible in the infrared light spectrum.
Initialization (of a smart card)	The process of populating persistent memory (EEPROM, etc.) with data that are common to a large number of cards while also including a minimal amount of card unique items (e.g. ICC serial number and Personalization keys).
Inspection	The act of a State or organization examining an MRTD presented to it by a traveller (the MRTD holder) and verifying its authenticity.
Inspection system	A system used for inspecting MRTDs by any public or private entity having the need to validate the MRTD, and using this document for identity verification, e.g. border control authorities, airlines and other transport operators, financial institutions.
Intaglio	A printing process used in the production of security documents in which high printing pressure and special inks are used to create a relief image with tactile feel on the surface of the document.

Term	Definition
Integrated Circuit (IC)	Electronic component designed to perform processing and/or memory functions.
Integrated Circuit Card (IC card, ICC)	A card into which been inserted one or more ICs.
Integrity	The ability to confirm that the Logical Data Structure and its components have not been altered from that created by the issuing State or organization.
Interface	A standardized technical definition of the connection between two components.
Interface device	Any terminal, communication device or machine to which the ICC is connected during operation.
Interoperability	The ability of several independent systems or sub-system components to work together.
Iris (printing)	See: Rainbow Printing.
Issuer data block	A series of Data Groups that are written to the optional capacity expansion technology by the issuing State or organization.
Issuing authority	The entity accredited for the issuance of an MRTD to the rightful holder.
Issuing State	The country issuing the MRTD.
Issuing organization	Organization authorized to issue an official MRTD (e.g. the United Nations Organization, issuer of the laissez-passer).
JPEG and JPEG2000	Standards for the data compression of images, used particularly in the storage of facial images.
Key exchange	The process for getting session keys into the hands of the conversants.
Key management	The process by which cryptographic keys are provided for use between authorized communicating parties.
Key pair	A pair of digital keys — one public and one private — used for encrypting and signing digital information.
Label	A self-adhesive sticker which is used as the data page within the passport. This is not a generally recommended practice, particularly for longer-term validity documents.
Laissez-passer	A document, generally similar to a passport, issued under the auspices of a supranational entity (e.g. United Nations).
Laminate	A clear material, which may have security features designed to be securely bonded to protect the biographical data or other page of the document.
Laser engraving	A process whereby personalized data are “burned” into the substrate with a laser. The data may consist of text, portraits and other security features.
Laser perforation	A process whereby numbers, letters or images are created by perforating the substrate with a laser.
Latent image	A hidden image formed within a relief image which is composed of line structures which vary in direction and profile resulting in the hidden image appearing at predetermined viewing angles, achieved by intaglio printing.

Term	Definition
Lenticular Feature	Security feature in which a lens structure is integrated in the surface of the document or used as a verification device.
Level 1 inspection	Cursory examination for rapid inspection at the point of usage (easily identifiable visual or tactile features).
Level 2 inspection	Examination by trained inspectors with simple equipment.
Level 3 inspection	Inspection by forensic specialists.
Live capture	The process of capturing a biometric sample by an interaction between an MRTD holder and a biometric system.
Logical Data Structure (LDS)	The Logical Data Structure describes how data are stored and formatted in the contactless IC of an eMRTD.
Machine Assisted Document Verification	A process using a device to assist in the verification of the authenticity of the document in respect to data and/or security.
Machine Readable Official Travel Document (MROTD)	A document, usually in the form of a card of TD1 or TD2 size, that conforms to the specifications of Doc 9303-5 and Doc 9303-6 and may be used to cross international borders by agreement between the States involved.
Machine Readable Passport (MRP)	A passport conforming with the specifications contained in Doc 9303-4. Normally constructed as a TD3 size book containing pages with information on the holder and the issuing State or organization and pages for visas and other endorsements. Machine readable information is contained in two lines of OCR-B text, each with 44 characters.
Machine Readable Travel Document (MRTD)	Official document, conforming with the specifications contained in Doc 9303, issued by a State or organization which is used by the holder for international travel (e.g. MRP, MRV, MROTD) and which contains mandatory visual (eye readable) data and a separate mandatory data summary in a format which is capable of being read by machine.
Machine Readable Visa (MRV)	A visa conforming with the specifications contained in Doc 9303-7. The MRV is normally attached to a visa page in a passport.
Machine Readable Zone (MRZ)	Fixed dimensional area located on the MRTD, containing mandatory and optional data formatted for machine reading using OCR methods.
Machine-verifiable biometric feature	A unique physical personal identification feature (e.g. facial image, fingerprint or iris) stored electronically in the chip of an eMRTD.
Master key	Root of the derivation chain for keys.
Master List Signer	An entity that digitally signs a Master List of CSCA certificates. The Master List signer is authorized by its national CSCA to perform this function through the issuance of a Master List Signer certificate.
Match/Matching	The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. A decision to accept or reject is then based upon whether this score exceeds the given threshold.

Case No. 1:15-cv-02362-RBJ Document 64-20 filed 09/11/17 USDC Colorado pg 33 of 63

Term	Definition
Message	The smallest meaningful collection of information transmitted from sender to receiver. This information may consist of one or more card transactions or card transaction-related information.
Message Authentication Code (MAC)	A MAC is a message digest appended to the message itself. The MAC cannot be computed or verified unless a secret is known. It is appended by the sender and verified by the receiver which is able to detect a message falsification.
Metallic ink	Ink exhibiting a metallic-like appearance.
Metameric inks	A pair of inks formulated to appear to be the same colour when viewed under specified conditions, normally daylight illumination, but which are a mismatch at other wavelengths.
Microprint	Printed text or symbols smaller than 0.25 mm/0.7 pica points.
MRP data page	A fixed-dimensional page within the MRP containing a standardized presentation of visual and machine readable data.
Multiple biometric	The use of more than one biometric.
Non-volatile memory	A semiconductor memory that retains its content when power is removed (i.e. ROM, EEPROM).
One-to-a-few	A hybrid of one-to-many identification and one-to-one verification. Typically the one-to-a-few process involves comparing a submitted biometric sample against a small number of biometric reference templates on file. It is commonly referred to when matching against a "watch list" of persons who warrant detailed identity investigation or are known criminals, terrorists, etc.
One-to-many	Synonym for "Identification".
One-to-one	Synonym for "Verification".
Operating system	A programme which manages the various application programmes used by a computer.
Optically Variable Device (OVD)	Security Feature displaying different colours or image appearance depending on viewing angle or verification conditions.
Optically Variable Feature (OVF)	An image or feature whose appearance in colour and/or design changes dependent upon the angle of viewing or illumination. Examples are: features including diffraction structures with high resolution (diffractive optically variable image device/DOVID), holograms, colour-shifting inks (e.g. ink with optically variable properties) and other diffractive or reflective materials.
Out-of-band	Refers to communications which occur outside of a previously established communication method or channel.
Overlay	An ultra-thin film or protective coating that may be applied to the surface of a document in place of a laminate.
Padding	Appending extra bits to either side of a data string up to a predefined length.
Penetrating numbering ink	Ink containing a coloured component, which penetrates deep into a substrate.

Term	Definition
Personal Identification Number (PIN)	A numeric security code used as a mechanism for local one-to-one verification with the purpose to ascertain whether the card holder is in fact the natural person authorized to access or use a specific service such as the right to unlock certain information on the card.
Personalization	The process by which the portrait, signature and biographical data are applied to the document.
Phosphorescent ink	Ink containing a pigment that glows when exposed to light of a specific wavelength, the reactive glow remaining visible and then decaying after the light source is removed.
Photochromic ink	An ink that undergoes a reversible colour change when exposed to light of a specified wavelength.
Photo-substitution	A type of forgery in which the portrait in a document is substituted for a different one after the document has been issued.
Physical security	The range of security measures applied during production and personalization to prevent theft and unauthorized access to the process.
PKD participant	An ICAO Member State or other entity issuing or intending to issue eMRTDs that follows the arrangements for participation in the ICAO PKD.
Portrait	A visual representation of the facial image of the holder of the document.
Private Key	A cryptographic key known only to the user, employed in public key cryptography in decrypting or signing information.
Probe	The biometric sample of the enrollee whose identity is sought to be established.
Public Key	The public component of an integrated asymmetric key pair, used in encrypting or verifying information.
Public key certificate	The public key information of an entity signed by the certification authority and thereby rendered unforgettable.
Public key cryptography	A form of asymmetric encryption where all parties possess a pair of keys, one private and one public, for use in encryption and digital signing of data.
Public Key Directory (PKD)	The central database serving as the repository of Document Signer Certificates, CSCA Master Lists, Country Signing CA Link Certificates and Certificate Revocation Lists issued by Participants, together with a system for their distribution worldwide, maintained by ICAO on behalf of Participants in order to facilitate the validation of data in eMRTDs.
Public Key Infrastructure (PKI)	A set of policies, processes and technologies used to verify, enrol and certify users of a security application. A PKI uses public key cryptography and key certification practices to secure communications.
Public key system	A cryptographic method using pairs of keys, one of which is private and one is public. If encipherment is done using the public key, decipherment requires application of the corresponding private key and vice versa.
Rainbow printing (iris or split fountain printing)	A technique whereby two or more colours of ink are printed simultaneously on a press to create a continuous merging of the colours similar to the effect seen in a rainbow. Also called prismatic, or iris printing.

Term	Definition
Random access	A means of storing data whereby specific items of data can be retrieved without the need to sequence through all the stored data.
Random Access Memory (RAM)	A volatile memory randomly accessible used in the IC that requires power to maintain data.
Reactive inks	Inks that contain security reagents to guard against attempts at tampering by chemical erasure (deletion), such that a detectable reaction occurs when bleach and solvents come into contact with the document.
Read only memory (ROM)	Non-volatile memory that is written once, usually during IC production. It is used to store operating systems and algorithms employed by the semiconductor in an integrated circuit card during transactions.
Read range	The maximum practical distance between the contactless IC with its antenna and the reading device.
Receiver data block	A series of Data Groups that are written to the optional capacity expansion technology by a receiving State or authorized receiving organization.
Receiving State	The country inspecting the holder's MRTD.
Registration	The process of making a person's identity known to a biometric system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.
Registration Authority (RA)	A person or organization responsible for the identification and authentication of an applicant for a digital certificate. An RA does not issue or sign certificates.
Relief (3-D) design (Medallion)	A security background design incorporating an image generated in such a way as to create the illusion that it is embossed or debossed on the substrate surface.
Response	A message returned by the slave to the master after the processing of a command received by the slave.
Rivest, Shamir and Adleman (RSA)	Asymmetric algorithm invented by Ron Rivest, Adi Shamir and Len Adleman. It is used in public-key cryptography and is based on the fact that it is easy to multiply two large prime numbers together, but hard to factor them out of the product.
Score	A number on a scale from low to high, measuring the success that a biometric probe record (the person being searched for) matches a particular gallery record (a person previously enrolled).
Secure hash algorithm (SHA)	Hash function specified by NIST and published as a federal information processing standard FIPS-180.
Secured message	A message that is protected against illegal alteration or origination.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means.
Security thread	A thin strip of plastic or other material embedded or partially embedded in the substrate during the paper manufacturing process. The strip may be metallized or partially de-metallized.

Term	Definition
See-through register (front-to-back)	See: front-to-back register.
Sensitive Data	Finger and iris image data stored in the LDS Data Groups 3 and 4, respectively. These data are considered to be more privacy sensitive than data stored in the other Data Groups.
Shadow Image	Used as a synonym to Ghost Image: A second representation of the holder's portrait on the document, reduced in contrast and/or saturation and/or size.
Sheet	The individual piece of substrate in a passport which comprises more than one passport page.
Size 1 machine readable official travel document (TD1)	A card with nominal dimensions guided by those specified for the ID-1 type card (ISO/IEC 7810) (excluding thickness).
Size 2 machine readable official travel document (TD2)	A card or label conforming with the dimensions defined for the ID-2 type card (ISO/IEC 7810) (excluding thickness).
Skimming	Electronically reading the data stored in the contactless IC without authorizing this reading of the document.
Small size (Format-B) machine readable visa (MRV-B)	An MRV conforming with the dimensional specifications contained in Doc 9303-7, sized to maintain a clear area on the passport visa page.
Steganography	An image or information encoded or concealed within a primary visual image.
Structure feature	A structure feature involves the incorporation of a measurable structure into or onto the MRTD. The presence of the structure may be detected and measured by the detection machine.
Substance feature	A substance feature involves the incorporation into the MRTD of a material which would not normally be present and is not obviously present on visual inspection. The presence of the material may be detected by the presence and magnitude of a suitable property of the added substance.
Symmetric algorithm	A type of cryptographic operation using the same key or set of keys for encryption of plain text and decryption of associated cipher text.
Synthetic	A non-paper based material used for the biographical data page or cards. The term "synthetic" is used synonymously for "plastic", which encompasses materials like polycarbonate, PET and similar materials and combinations thereof.
System	A specific IT installation, with a particular purpose and operational environment.
System integration	The process by which cardholder-facing, internal and partner-facing systems and applications are integrated with each other.

Term	Definition
System security policy	The set of laws, rules and practices that regulate how sensitive information and other resources are managed, protected and distributed within a specific system.
Tactile feature	A surface feature giving a distinctive "feel" to the document.
Taggant	A not-naturally occurring substance that can be added to the physical components of an MRTD, and is typically a Level 3 feature, requiring special equipment for detection.
Tagged ink	Inks containing compounds that are not naturally occurring substances and which can be detected using special equipment.
Tamper resistance	The capability of components within a document to withstand alteration.
Template/Reference template	Data which represent the biometric measurement of an enrollee used by a biometric system for comparison against subsequently submitted biometric samples.
Template size	The amount of computer memory taken up by the biometric data.
Thermochromic ink	An ink which undergoes a reversible colour change when the printed image is exposed to a specific change in temperature.
Threshold	A "benchmark" score above which the match between the stored biometric and the person is considered acceptable or below which it is considered unacceptable.
Trust Anchor	In cryptographic systems with hierarchical structure this is an authoritative entity for which trust is assumed and not derived.
Token image	A portrait of the holder of the MRTD, typically a full frontal image, which has been adjusted in size to ensure a fixed distance between the eyes. It may also have been slightly rotated to ensure that an imaginary horizontal line drawn between the centres of the eyes is parallel to the top edge of the portrait rectangle if this has not been achieved when the original portrait was taken or captured.
Usual Mark	Symbol that replaces a holder's written signature in case the holder is not able to sign.
UV dull substrate	A substrate that exhibits no visibly detectable fluorescence when illuminated with UV light.
Validation	The process of demonstrating that the system under consideration meets in all respects the specification of that system.
Variable laser image	A feature generated by laser engraving or laser perforation displaying changing information or images dependent upon the viewing angle.
Verification/verify	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. Contrast with "Identification".
Visual inspection zone (VIZ)	Those portions of the MRTD (data page in the case of MRP) designed for visual inspection, i.e. front and back (where applicable), not defined as the MRZ.
Watermark	A custom design, typically containing tonal gradation, formed in the paper or other substrate during its manufacture, created by the displacement of materials therein, and traditionally viewable by transmitted light.

Term	Definition
Wavelet Scalar Quantization (WSQ)	A means of compressing data used particularly in relation to the storage of fingerprint images.
Windowed or Transparent feature	Security feature created by the construction of the substrate, whereby part of the substrate is removed or replaced by transparent material, which can incorporate additional security features such as lenses or tactile elements.
X.509 v3 certificate	The internationally recognized electronic document used to prove identity and public key ownership over a communication network. It contains the issuer's name, user's identifying information, and issuer's digital signature.
Zone	An area containing a logical grouping of data elements on the MRTD. Seven (7) zones are defined for MRTDs.

4.3 Key Words

Key words are used to signify requirements.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" used in capitalized form in Doc 9303 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).

Guidance in the use. Imperatives of the type defined here must be used with care and sparingly. In particular, they MUST be used only where it is actually required for interoperation or to limit behaviour which has potential for causing harm (e.g. limiting retransmissions). For example, they must not be used to try to impose a particular method on implementers where the method is not required for interoperability.

Security considerations. These terms are frequently used to specify behaviour with security implications. The effects on security of not implementing a MUST or SHOULD, or doing something the specification says MUST NOT or SHOULD NOT be done, may be very subtle. Document authors should take the time to elaborate the security implications of not following recommendations or requirements as most implementers will not have had the benefit of the experience and discussion that produced the specification.

In case OPTIONAL features are implemented, they MUST be implemented as described in Doc 9303.

4.4 Object Identifiers

In Parts 9303-10, 9303-11, and 9303-12 ICAO Object Identifiers are specified. This paragraph lists these actual ICAO Object Identifiers:

```
-- ICAO security framework
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}


-- LDS security object
id-icao-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 1}


-- CSCA master list
id-icao-cscaMasterList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 2}

id-icao-cscaMasterListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-security
3}


-- Active Authentication protocol
id-icao-aaProtocolObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 5}


-- CSCA name change
id-icao-extensions OBJECT IDENTIFIER ::= {id-icao-mrtd-security 6}

id-icao-nameChange OBJECT IDENTIFIER ::= {id-icao-mrtd-security-extensions 1}


-- document type list, see TR "LDS and PKI Maintenance"
id-icao-documentTypeList OBJECT IDENTIFIER ::= {id-icao-mrtd-security-
extensions 2}
```

```
-- Deviation List Base Object identifiers
id-icao-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 7}

id-icao-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-security 8}


-- Deviation Object Identifiers and Parameter Definitions
id-Deviation-CertOrKey OBJECT IDENTIFIER ::= {id-icao-DeviationList 1}

id-Deviation-CertOrKey-DSSignature OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 1}

id-Deviation-CertOrKey-DSEncoding OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 2}

id-Deviation-CertOrKey-CSCAEncoding OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 3}

id-Deviation-CertOrKey-AAKeyCompromised OBJECT IDENTIFIER ::= {id-
Deviation-CertOrKey 4}

id-Deviation-LDS OBJECT IDENTIFIER ::= {id-icao-DeviationList 2}

id-Deviation-LDS-DGMalformed OBJECT IDENTIFIER ::= {id-Deviation-LDS 1}

id-Deviation-LDS-SODSignatureWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS
3}

id-Deviation-LDS-COMInconsistent OBJECT IDENTIFIER ::= {id-Deviation-LDS 4}

id-Deviation-MRZ OBJECT IDENTIFIER ::= {id-icao-DeviationList 3}

id-Deviation-MRZ-WrongData OBJECT IDENTIFIER ::= {id-Deviation-MRZ 1}

id-Deviation-MRZ-WrongCheckDigit OBJECT IDENTIFIER ::= {id-Deviation-MRZ 2}

id-Deviation-Chip OBJECT IDENTIFIER ::= {id-icao-DeviationList 4}

id-Deviation-NationalUse OBJECT IDENTIFIER ::= {id-icao-DeviationList 5}


-- LDS2 Object Identifiers
id-icao-lds2 OBJECT IDENTIFIER ::= {id-icao-mrtd-security 9}

id-icao-tsSigner OBJECT IDENTIFIER ::= {id-icao-mrtd-security-lds2 1}

id-icao-vSigner OBJECT IDENTIFIER ::= {id-icao-mrtd-security-lds2 2}

id-icao-bSigner OBJECT IDENTIFIER ::= {id-icao-mrtd-security-lds2 3}
```

Case No. 1:15-cv-02362-RBJ Document 64-20 filed 09/11/17 USDC Colorado pg 41 of 63


```
-- SPOC Object Identifiers
id-icao-spoc OBJECT IDENTIFIER ::= {id-icao-mrtd-security 10}

id-icao-spocClient OBJECT IDENTIFIER ::= {id-icao-mrtd-security-spoc 1}

id-icao-spocServer OBJECT IDENTIFIER ::= {id-icao-mrtd-security-spoc 2}
```

4.5 The Use of Notes

While in ISO/IEC standards notes are informative, in Doc 9303 notes are part of the normative text and used to emphasize requirements or additional information.

5. GUIDANCE ON THE USE OF DOC 9303

5.1 Doc 9303 Composition

Doc 9303 is comprised of twelve parts. Each part describes a specific aspect of the MRTD. The parts of Doc 9303 are composed in such way that the issuer of MRTDs can compose a complete set of relevant specifications, relevant to a specific type of MRTD (form factor). The relationship between these form factors and the parts of Doc 9303 is described in Section 5.2 of this Part 1.

The following parts form the complete Doc 9303 specifications for Machine Readable Travel Documents:

Part 1 — Introduction
The document at hand is Part 1.

Part 2 — Specifications for the Security of the Design, Manufacture and Issuance of MRTDs
Part 2 provides mandatory and optional specifications for the precautions to be taken by travel document issuing authorities to ensure that their MRTDs, and their means of personalization and issuance to the rightful holders, are secure against fraudulent attack. Mandatory and optional specifications are also provided for the physical security to be provided at the premises where the MRTDs are produced, personalized and issued and for the vetting of personnel involved in these operations.

Part 3 — Specifications common to all MRTDs
Part 3 of Doc 9303 is based on the Sixth Edition of Doc 9303, Part 1, Volume 1, *Machine Readable Passports – Passports with Machine Readable Data Stored in Optical Character Recognition Format* (2006) and the Third Edition of Doc 9303, Part 3, Volume 1, *Machine Readable Official Travel Documents – MRtds with Machine Readable Data Stored in Optical Character Recognition Format* (2008).

Part 3 defines specifications that are common to TD1, TD2 and TD3 size Machine Readable Travel Documents (MRTDs) including those necessary for global interoperability using visual inspection and machine readable (optical character recognition) means. Detailed specifications applicable to each document type appear in Doc 9303, Parts 4 through 7.

Part 4 — Specifications for Machine Readable Passports (MRPs) and other TD3 size MRTDs
Part 4 defines specifications that are specific to TD3 size Machine Readable Passports (MRPs) and other TD3 size Machine Readable Travel Documents (MRTDs). For brevity, the term MRP has been used throughout Part 4 and, except where stated, all the specifications herein shall apply equally to all other TD3 size MRTDs.

Part 5 — Specifications for TD1 size Machine Readable Official Travel Documents (MROTDs)
Part 5 defines specifications that are specific to TD1 size Machine Readable Official Travel Documents (MROTDs).

Part 6 — Specifications for TD2 size Machine Readable Official Travel Documents (MROTDs)
Part 6 defines specifications that are specific to TD2 size Machine Readable Official Travel Documents (MROTDs).

Part 7 — Machine Readable Visas
Part 7 defines the specifications for Machine Readable Visas (MRVs) which allow compatibility and global interchange using both visual (eye readable) and machine readable means. The specifications for visas can, where issued by a State and accepted by a receiving State, be used for travel purposes. The MRV shall, as a minimum, contain the data specified in a form that is legible both visually and by optical character recognition methods, as presented in Part 7.

Part 7 contains specifications for both Format-A as well as Format-B types of visas, and is based on the Third Edition of Doc 9303, Part 2, *Machine Readable Visas* (2005).

Part 8 — Emergency Travel Documents
Reserved for future use.

Part 9 —Deployment of Biometric Identification and Electronic Storage of Data in MRTDs
Part 9 defines the specifications, additional to those for the basic MRTD set forth in Parts 3, 4, 5, 6, and 7 of Doc 9303, to be used by States wishing to issue an electronic Machine Readable Travel Document (eMRTD) capable of being used by any suitably equipped receiving State to read from the document a greatly increased amount of data relating to the eMRTD itself and its holder. This includes mandatory globally interoperable biometric data that can be used as an input to facial recognition systems, and, optionally, to fingerprint or iris recognition systems. The specifications require the globally interoperable biometric data to be stored in the form of high-resolution images.

Part 10 — Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)
Part 10 defines a Logical Data Structure (LDS) for eMRTDs required for global interoperability. The contactless integrated circuit capacity expansion technology contained in an eMRTD selected by an issuing State or organization SHALL allow data to be accessible by receiving States. Part 10 defines the specifications for the standardized organization of these data. This requires the identification of all mandatory and optional Data Elements and a prescriptive ordering and/or grouping of Data Elements that SHALL be followed to achieve global interoperability for reading of details (Data Elements) recorded in the capacity expansion technology optionally included on an MRTD (eMRTD).

Part 11 — Security Mechanisms for MRTDs
Part 11 provides specifications to enable States and suppliers to implement cryptographic security features for Machine Readable Travel Documents (eMRTDs) offering ICC read-only access.

Part 11 specifies cryptographic protocols to:

- prevent skimming of data from the contactless IC;
- prevent eavesdropping on the communication between the IC and reader;
- provide authentication of the data stored on the IC based on the PKI described in Part 12, and provide authentication of the IC itself.

Part 12 — Public Key Infrastructure for MRTDs
Part 12 defines the Public Key Infrastructure (PKI) for the eMRTD application. Requirements for issuing States or organizations are specified, including operation of a Certification Authority (CA) that issues certificates and CRLs. Requirements for receiving States and their Inspection Systems validating those certificates and CRLs are also specified.

5.2 Relationship between MRTD Form Factors and relevant Doc 9303 Parts

Table 1-1 describes which parts of Doc 9303 are relevant for specific types of MRTDs (form factors).

Table 1-1. Form factors cross-reference table

	Doc 9303 Part											
	1	2	3	4	5	6	7	8	9	10	11	12
TD3 size MRTD (MRP)	√	√	√	√								
TD3 size eMRTD (eMRP)	√	√	√	√					√	√	√	√
TD1 size MROTD	√	√	√		√							
TD1 size eMROTD	√	√	√		√				√	√	√	√
TD2 size MROTD	√	√	√			√						
TD2 size eMROTD	√	√	√			√			√	√	√	√
MRV	√	√	√				√					

6. REFERENCES (NORMATIVE)

Certain provisions of international Standards, referenced in this text, constitute provisions of Doc 9303. Where differences exist between the specifications contained in Doc 9303 and the referenced Standards, to accommodate specific construction requirements for machine readable travel documents, including machine readable visas, the specifications contained herein shall prevail.

Annex 9 Convention on International Civil Aviation ("Chicago Convention"), Annex 9 – *Facilitation.*

RFC 2119 RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC2119, March 1997.

— END —


ISBN 978-92-9249-790-3
9
789292
497903

ICAO

Doc 9303

Machine Readable Travel Documents

Seventh Edition, 2015

Part 4: Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs



Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

ICAO

Doc 9303

Machine Readable Travel Documents

Seventh Edition, 2015

Part 4: Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/security/mrtd

Doc 9303, *Machine Readable Travel Documents*
Part 4 — *Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs*
ISBN 978-92-9249-793-4

© ICAO 2015

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, without prior permission in writing from the International Civil Aviation Organization.

AMENDMENTS

Amendments are announced in the supplements to the *Products and Services Catalogue;* the Catalogue and its supplements are available on the ICAO website at www.icao.int. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of ICAO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

TABLE OF CONTENTS

		Page
1.	**SCOPE**	**1**
2.	**CONSTRUCTION AND DIMENSIONS OF THE MRP AND MRP DATA PAGE**	**1**
2.1	Construction	1
2.2	MRP Data Page Nominal Dimensions	1
2.3	MRP Data Page Edge Tolerances	2
2.4	MRP Data Page Margins	2
2.5	MRP Data Page Thickness	3
2.6	MRP Dimensions	4
3.	**GENERAL LAYOUT OF THE MRP DATA PAGE**	**4**
3.1	MRP Zones	5
3.2	Content and Use of Zones	5
3.3	Dimensional Flexibility of Zones I to V	8
4.	**CONTENTS OF THE MRP DATA PAGE**	**12**
4.1	Visual Inspection Zone (VIZ) (Zones I through VI)	12
4.2	Machine Readable Zone (MRZ) (Zone VII)	16
4.3	Representation of the Issuing State or Organization and Nationality of Holder in the MRZ and the VIZ	23
5.	**REFERENCES (NORMATIVE)**	**24**
APPENDIX A TO PART 4	**EXAMPLES OF A PERSONALIZED MRP DATA PAGE (INFORMATIVE)**	**APP A-1**
APPENDIX B TO PART 4	**CONSTRUCTION OF THE MACHINE READABLE ZONE OF THE PASSPORT DATA PAGE (INFORMATIVE)**	**APP B-1**

1. SCOPE

The Seventh Edition of Doc 9303 represents a restructuring of the ICAO specifications for Machine Readable Travel Documents. Without incorporating substantial modifications to the specifications, in this new edition Doc 9303 has been reformatted into a set of specifications for Size 1 Machine Readable Official Travel Documents (TD1), Size 2 Machine Readable Official Travel Documents (TD2), and Size 3 Machine Readable Travel Documents (TD3), as well as visas. This set of specifications consists of various separate documents in which general (applicable to all MRTDs) as well as MRTD form factor specific specifications are grouped.

This Part 4 of Doc 9303 is based on the Sixth Edition of Doc 9303, Part 1, *Machine Readable Passports*, Volume.1 (2006).

Doc 9303, Part 4 defines specifications that are specific to TD3 size Machine Readable Passports (MRPs) and other TD3 size Machine Readable Travel Documents (MRTDs). For brevity the term MRP has been used throughout this document and, except where stated, all the specifications herein shall apply equally to all other TD3 size MRTDs. This document should be read in conjunction with:

- Part 1 — *Introduction*;
- Part 2 — *Specifications for the Security of the Design, Manufacture and Issuance of MRTDs*;
- Part 3 — *Specifications Common to all MRTDs*.

Together these specifications provide for global data interchange of MRTDs both by visual (eye readable) and machine readable (optical character recognition) means.

Additional specifications providing for global data interchange of electronic data in eMRPs and eMROTDs can be found in Doc 9303, Parts 9 through 12.

2. CONSTRUCTION AND DIMENSIONS OF THE MRP AND MRP DATA PAGE

2.1 Construction

The MRP shall take the form of a book consisting of a cover and a minimum of eight pages and shall include a data page onto which the issuing State or organization enters the personal data relating to the holder of the document and data concerning the issuance and validity of the MRP.

2.2 MRP Data Page Nominal Dimensions

The nominal dimensions shall be as specified in ISO/IEC 7810 (except thickness) for the TD3 size MRTD, i.e.:

88.0 mm ± 0.75 mm × 125.0 mm ± 0.75 mm (3.46 in ± 0.03 in × 4.92 in ± 0.03 in).

Zzyym v. Tillerson - AR 0526

2.3 MRP Data Page Edge Tolerances

The edges of the data page following final preparation shall be within the area circumscribed by the concentric rectangles as illustrated in Figure 1.

Inner rectangle: 87.25 mm × 124.25 mm (3.44 in × 4.89 in)
Outer rectangle: 88.75 mm × 125.75 mm (3.49 in × 4.95 in)

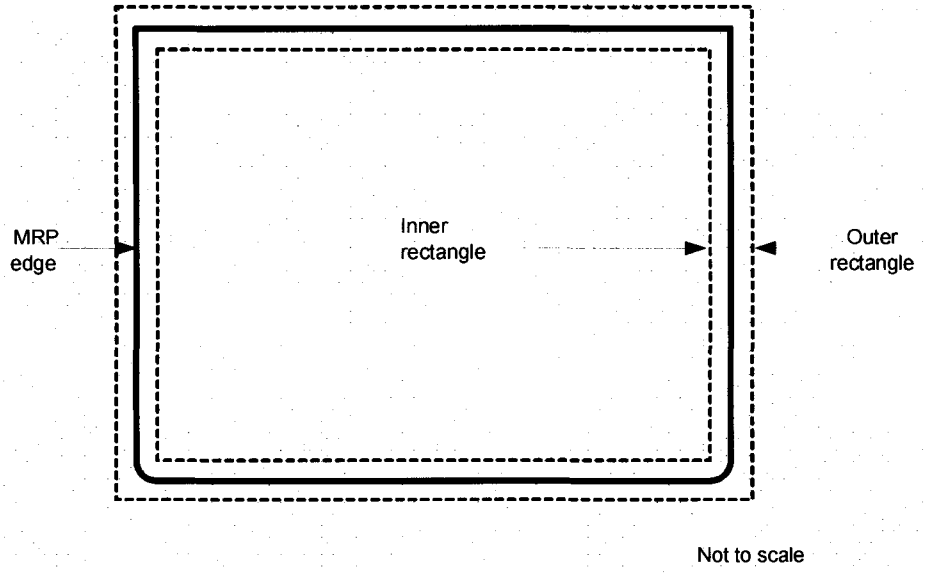


Figure 1. MRP data page dimensional illustration

2.4 MRP Data Page Margins

The dimensional specifications refer to the outer limits of the MRP data page. A margin of 2.0 mm (0.08 in) along the left and right hand edges and top edge must be left clear of data, as shown in Figure 2. The position of data in the machine readable zone is as shown in Figure 3.

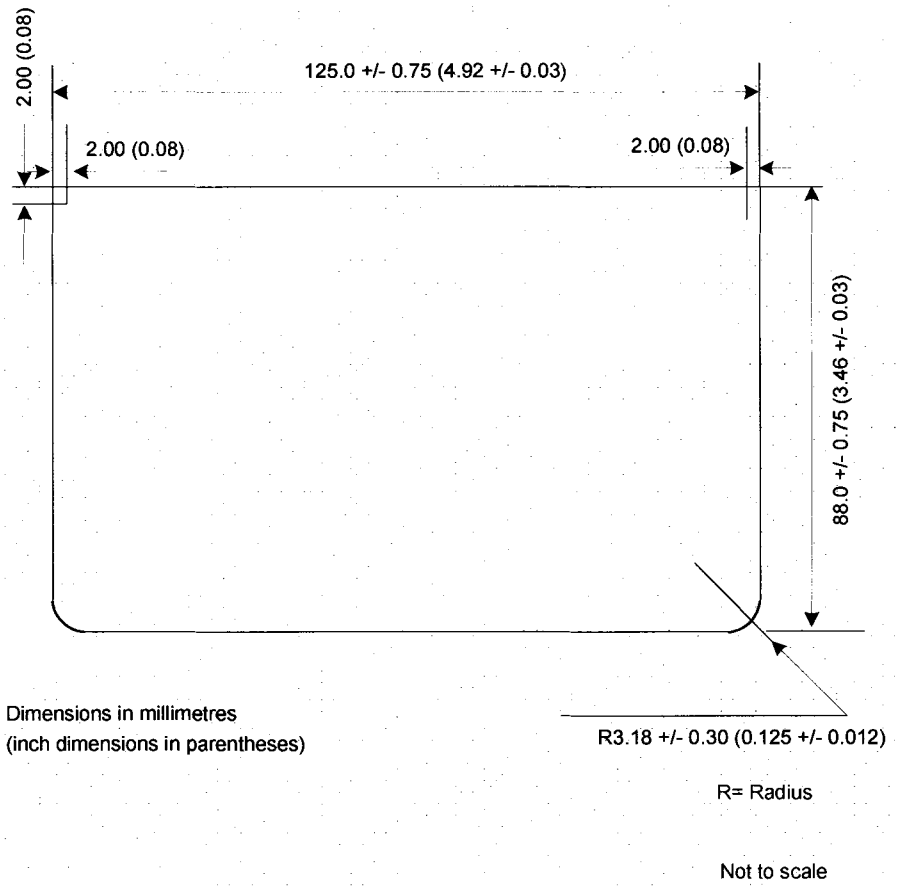


Figure 2. Edge margins of the MRP data page

2.5 MRP Data Page Thickness

The thickness, including any final preparation (e.g. laminate), shall be as follows:

- Minimum:

No minimum thickness is specified. However, States are advised that currently available materials are unlikely to provide an adequately robust data page if the thickness is below 0.15 mm (0.006 in);

- Maximum:

0.90 mm (0.035 in).

The thickness of the area within the machine readable zone shall not vary by more than 0.10 mm (0.004 in).

General note.— The decimal notation in these specifications conforms to ICAO practice. This differs from the ISO practice, which is to use a decimal point (.) in imperial measurements and a comma (,) in metric measurements.

2.6 MRP Dimensions

The dimensional specifications defined in Paragraphs 2.2 to 2.3 above also apply to the MRP book. If required for binding purposes, the 88.0 mm (3.46 in) dimension may be increased.

3. GENERAL LAYOUT OF THE MRP DATA PAGE

The MRP data page follows a standardized layout to facilitate reading of data globally by visual and machine readable means.

The MRP data page should either be an inner page in close proximity to an end leaf of the MRP or form part of the cover of the MRP. Where the MRP data page is part of the cover, precautions must be taken to ensure that the endleaf/cover assembly combined with the means of personalization are together resistant to fraudulent attack, particularly by delamination of the cover structure. Where the MRP data page is not constructed as part of the cover, the recommended practice is to locate the MRP data page on page 2 or on the penultimate page of the MRP. The location of the MRP data page in any other position in the MRP will give rise to problems for document examiners in the operation of swipe readers reading the MRZ. The MRZ shall be positioned adjacent to the outside long edge of the book, parallel to the spine of the book (see Figures 3 and 4).

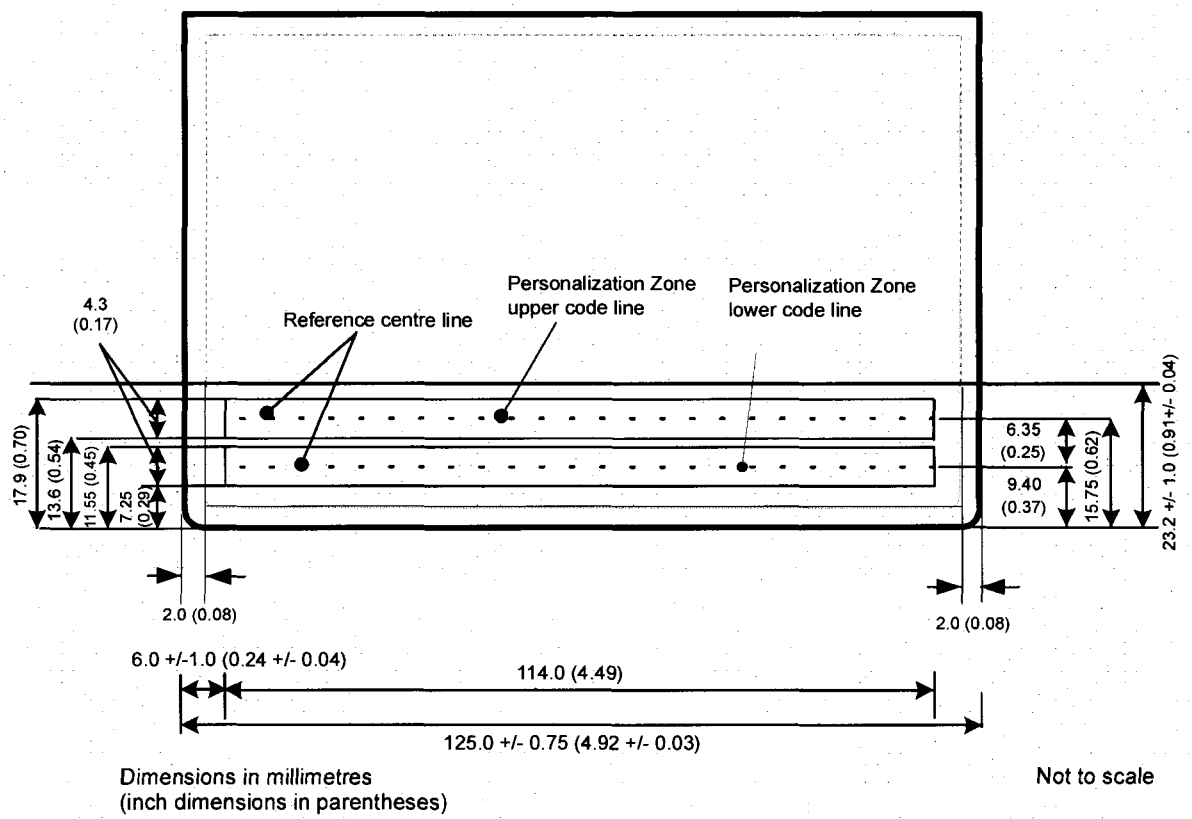


Figure 3. Schematic diagram of the Machine Readable Zone (MRZ)

3.1 MRP Zones

To accommodate the various requirements of States' laws and practices and to achieve the maximum standardization within those divergent requirements, the MRP data page is divided into seven zones as follows:

3.1.1 Front of MRP data page

Zone I	Mandatory header
Zone II	Mandatory and optional personal data elements
Zone III	Mandatory and optional document data elements
Zone IV	Mandatory holder's signature or usual mark (original or reproduction)
Zone V	Mandatory identification feature
Zone VII	Mandatory machine readable zone (MRZ)

3.1.2 Back of MRP data page, or an adjacent page

Zone VI	Optional data elements

3.2 Content and Use of Zones

Zones I to V, which, together with Zone VI, form the Visual Inspection Zone (VIZ), and Zone VII, which is the Machine Readable Zone (MRZ), contain mandatory elements in a standard sequence which represent the minimum requirements for the MRP data page. The optional elements in Zones II, III and VI accommodate the diverse requirements of issuing States or organizations, allowing for presentation of additional data at the discretion of the issuing State or organization, while achieving the desired level of standardization. The location of zones and standard sequence for data elements are set out in Figure 4. The technical specifications for the printing of data on the MRP data page are defined in Section 4. Figures 8, 9 and 10 outline the guidelines for positioning and adjusting the dimensional specifications of Zones I to V to accommodate the flexibility desired by issuing States or organizations. Some examples of personalized MRP data pages are shown in Appendix A.

3.2.1 Zone IV — Location of holder's signature or usual mark

Field 18, the holder's signature or usual mark (or a reproduction thereof), shall normally be placed in Zone IV of the MRP data page (see Figure 4). Where the issuing State or organization wishes to locate the holder's signature or usual mark on a page other than the MRP data page, it may, as specified in the Data Element Directory, relocate Field 18 to Zone VI on the back of the MRP data page or to the page adjacent to the MRP data page. In this case, the size of adjacent fields in the visual zone on the MRP data page may be increased.

3.2.2 Zone V — Position of holder's portrait

Within Zone V, the holder's portrait shall be at least 2.0 mm (0.08 in) from the left-hand edge of the MRP data page. The use of affixed or stick-on portrait photos is not permitted and these shall not be used. Instead, the portrait image shall be integrated with the biodata page using a secure personalization technology.

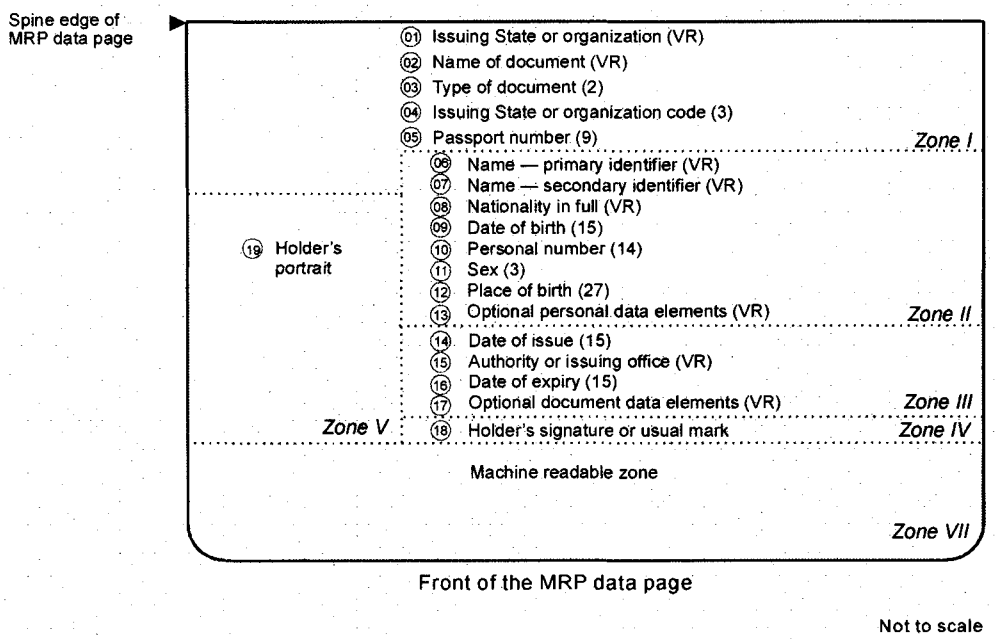


Figure 4. Sequence of data elements on front side of MRP data page

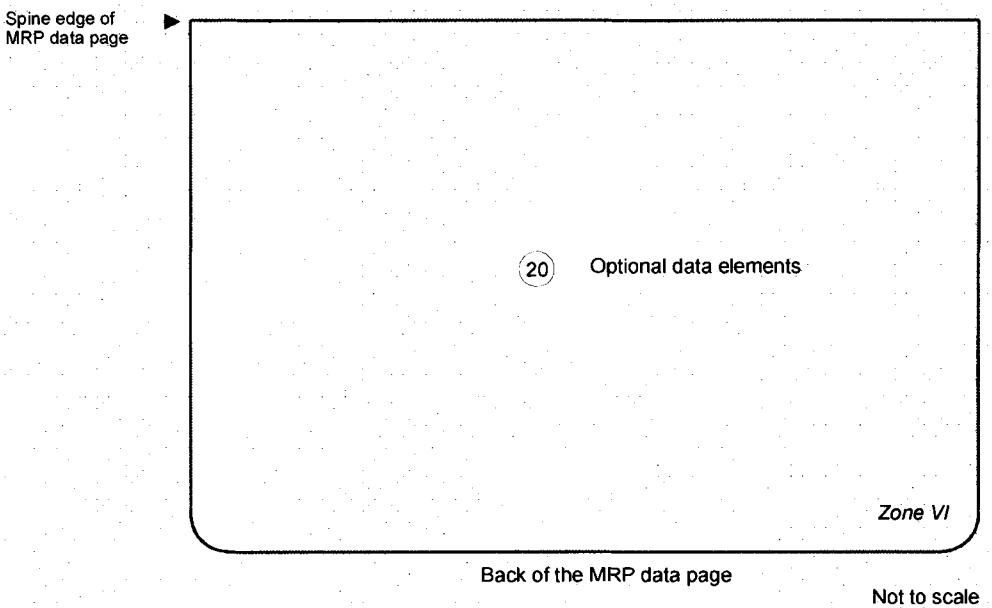


Figure 5. Data elements on reverse side

Notes to Figures 4 and 5:
Note 1.— (VR) = variable number of characters in field.
Note 2.— (n) = the maximum or fixed number of characters allowed in the field.
Note 3.— O = indicates the field number.

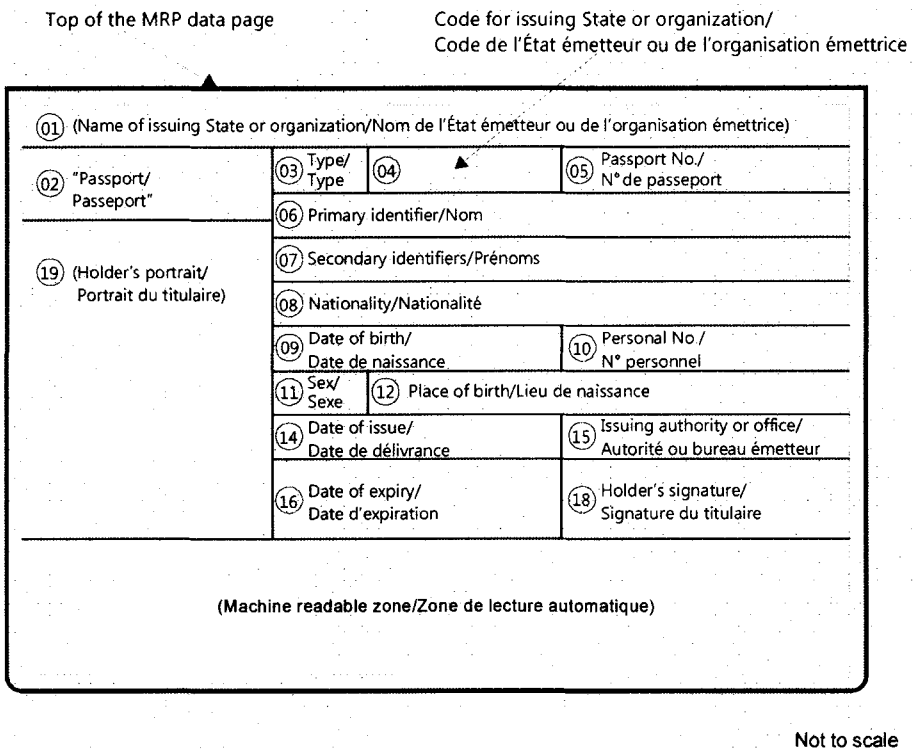
3.2.3 Data elements

The data elements to be included in the zones, the preparation of the zones and guidelines for the dimensional layout of zones shall be as described in Section 4 of this Part.

3.2.4 Mandatory zones

The MRP data page shall contain Zones I, II, III, V and VII. If the issuing State or organization's practice is to omit mandatory elements 01 and 02 (issuing State or organization, in full, and document, in full) from the header (Zone I), these data elements shall be placed on an adjacent or preceding page.

Zone IV shall be present either on the data page or on an adjacent page and contain the holder's signature or usual mark, i.e. original or reproduction. Alternatively, at the discretion of the issuing State or organization, the holder's signature may be located in Zone VI on the reverse side of the MRP data page. Zone V shall include the personal identification feature(s) which shall include a portrait solely of the rightful holder. At the discretion of the issuing State or organization, the name fields in Zone II and the holder's signature or usual mark in Zone IV may overlay Zone V provided this does not hinder recognition of the data in any of the three zones.



Note 1.— Optional data Fields 13 and 17 are excluded in the recommended practice.
Note 2.— Captions corresponding to the field names printed in the above illustration, except those within parentheses, shall be printed on the MRP data page.

Figure 6. Schematic of nominal layout of data elements

Data elements shall appear in a standard sequence as shown in Figures 4 and 5. Figure 6 is a schematic of the nominal layout of data elements on the front side of an MRP data page, and Figure 7 is a template for the position of the personalized data fields.

The dimensions and boundaries of Zone VII, the machine readable zone, are fixed. Zone VII conforms in height to the MRZ defined for all MRTDs so that the machine readable data lines fall within the effective reading zone (ERZ) specified in Doc 9303-3.

MRZ (Zone VII) data elements shall be as defined in Paragraph 4.2.2 and illustrated in Appendix B, Figure 15.

3.2.5 Optional data zone

Zone VI, which may be on the back of the data page or on an adjacent page, is a zone for optional data for use at the discretion of the issuing State or organization.

A template for the layout of personalized data elements on the front side of an MRP data page is shown in Figure 7.

3.3 Dimensional Flexibility of Zones I to V

Zones I to V may be adjusted in size and shape within the overall dimensional specifications of the MRP data page to accommodate the diverse requirements of issuing States or organizations. All zones, however, shall be bounded by straight lines, and all angles where straight lines join shall be right angles (i.e. 90 degrees). It is recommended that the zone boundaries not be printed on the MRP data page. The nominal position of the zones is shown in Figure 8.

When an issuing State or organization chooses to produce an MRP data page that contains a transparent or otherwise unprintable border, this will result in a reduction of the available area within the zones. The full MRP data page dimensions and zone boundaries shall be measured from the outside edge of this border, which is the external edge of the MRP data page.

Zone I shall be located along the top edge of the MRP data page and extend across the full 125.0 ± 0.75 mm (4.92 ± 0.03 in) dimension. (The top edge is the edge coincident with the spine of the MRP.) The issuing State or organization may vary the *vertical* dimension of Zone I, as required, but this dimension shall be sufficient to allow legible interpretation of the data elements in the zone and shall not be greater than 17.9 mm (0.70 in).

Zone V shall be located such that its left edge is coincident with the left edge of the MRP data page as shown in Figure 8. The dimensions of the portrait contained in Zone V are specified in Section 4.1.1.1, the Visual Data Element Directory, Field 19.

Zone V may move *vertically* along the left edge of the MRP data page and overlay a portion of Zone I as long as individual details contained in either zone are not obscured.

The upper boundary of Zone II shall be coincident with the lower boundary of Zone I.

When there is a specific requirement for the name fields to extend across the MRP data page, Zone II may extend up to the full 125.0 ± 0.75 mm (4.92 ± 0.03 in) dimension of the MRP data page. If the full dimension is used, Zone II shall overlay a portion of Zone V. In this case, issuing States or organizations shall ensure that data contained in either zone is not obscured.

The lower boundary of Zone II may be positioned at the discretion of the issuing State or organization. Enough space must be left for Zones III and IV below the boundary. This boundary does not need to be straight across the 125.0 ± 0.75 mm (4.92 ± 0.03 in) dimension of the MRP data page. This is illustrated in Figure 9.

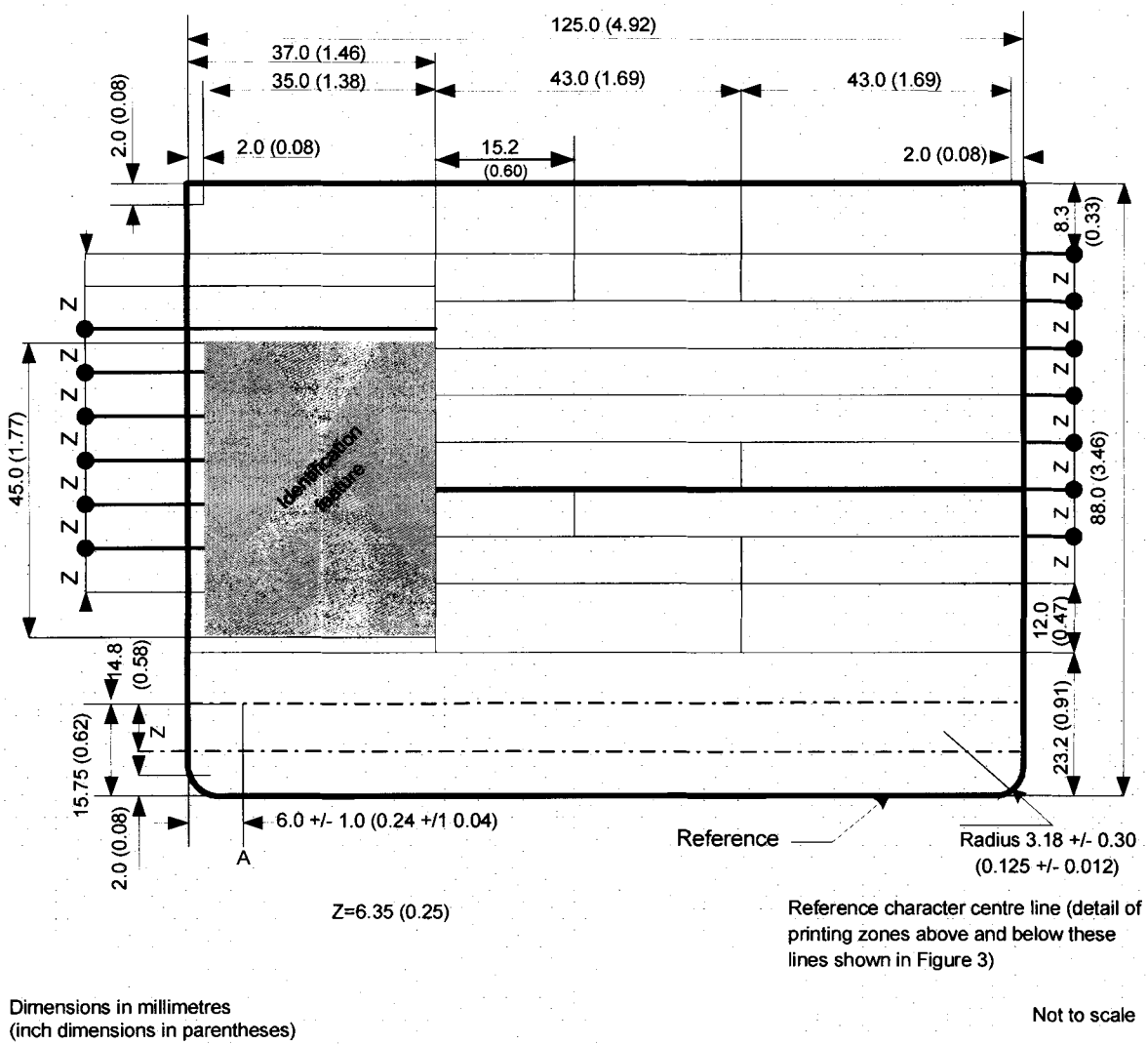


Figure 7. Template for the personalization data fields

Note 1.— To allow for variations during manufacture of the MRP, a tolerance of ± 1.0 mm (± 0.04 in) is allowed for the 23.2 mm (0.91 in) dimension of the MRZ and within that overall tolerance the boundary between the VIZ and the MRZ shall not be skewed more than 0.5 mm (0.02 in) over the 125.0 mm (4.92 in) dimension.

Note 2.— 'A' — There shall be no text to the left of this line in the MRZ.

Note 3.— Except for background security print there shall be no print in the 2.0 mm (0.08 in) margins.

Note 4.— The borderlines of the fields shall be omitted on the actual MRP data page.

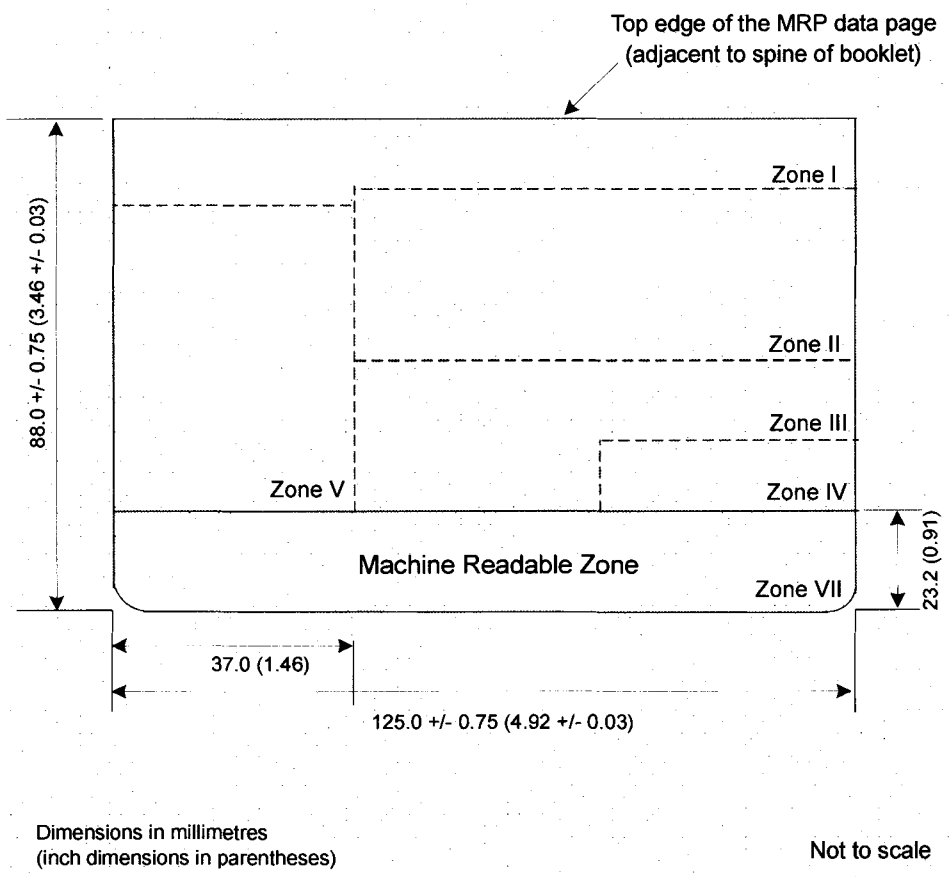


Figure 8. Nominal positions of Zones I-V

Note 1.— Dotted lines indicate zone boundaries whose positions are not fixed, enabling issuing States or organizations flexibility in the presentation of data. See paragraph 3.3.

Note 2.— Zone VI, where used, appears on the back of the data page or on an adjacent page.

Zone III should start at the right vertical boundary of Zone V and may extend, at the discretion of the issuing State or organization, to the right edge of the MRP data page. Figures 9 and 10 illustrate the flexibility permitted to issuing States or organizations.

If Zone IV is placed on the MRP data page, it shall be at the bottom of the VIZ on the front of the MRP data page, its lower boundary coincident with the top edge of the MRZ. Figures 8 and 9 show two alternative positions for Zone IV. Figure 10 shows an MRP data page where Zone IV has been placed on an adjacent page.

Zone IV may also overlay Zone V, though this practice is not recommended. In this case, issuing States or organizations shall ensure that individual details contained in either zone are not obscured. See Appendix A, Figure 13.

When an issuing State or organization wishes to have a displayed image of an MRP holder's fingerprint, the image may be displayed within the area designated for Zone II as illustrated in Appendix A, Figure 14.

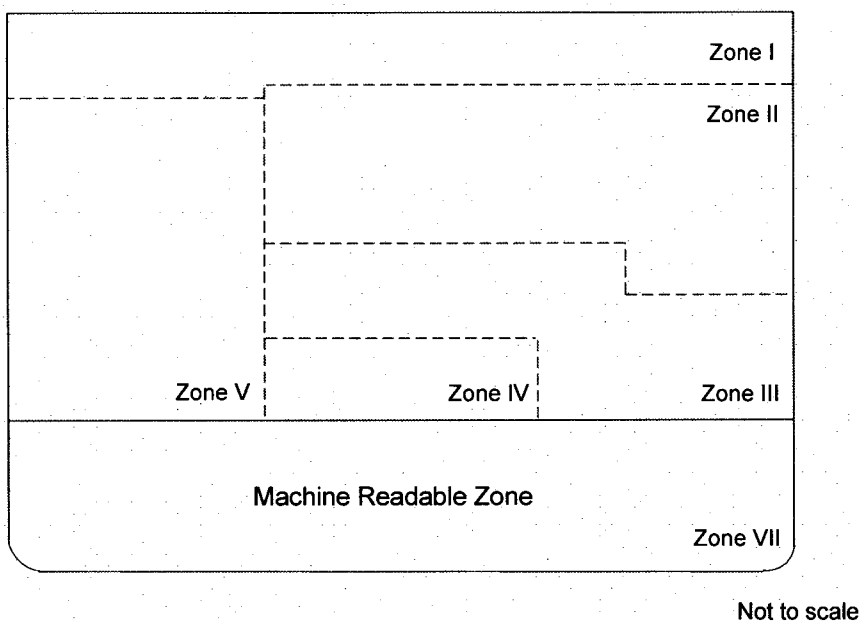


Figure 9. Example of flexible positioning of zones illustrating a staircase boundary between Zones II and III

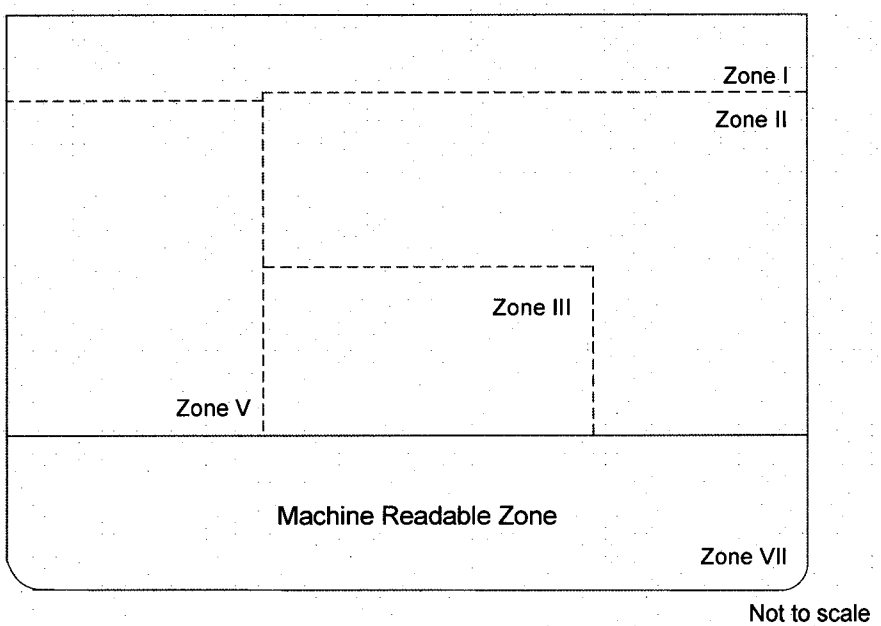


Figure 10. Example of flexible positioning of zones in which Zone IV (signature) is moved to an adjacent page and Zone III positioned such that it does not extend to the right-hand edge of the data page

4. CONTENTS OF THE MRP DATA PAGE

4.1 Visual Inspection Zone (VIZ) (Zones I through VI)

Guidance on the typeface, size and line spacing, the languages and character set, to be used in the VIZ may be found in Doc 9303-3.

If any optional field or data element is not used, the data may be spread more evenly in the visual zone of the MRP data page consistent with the requirement for sequencing zones and data elements.

4.1.1 Data element directory

The data elements in the VIZ are specified as follows:

4.1.1.1 Visual inspection zone — Data element directory

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
01/I (Mandatory)	Issuing State or organization (in full)	The name of the State or organization responsible for issuing the MRP shall be displayed in full. For additional details see Doc 9303-3.	Variable	Notes a, c, d, f, g. If omitted, shall appear on an adjacent or preceding page in the passport.
02/I (Mandatory)	Document	The word for "passport" in the language of the issuing State or organization, plus either PASSPORT (English), PASSEPORT (French) or PASAPORTE (Spanish) if the language of the issuing State or organization is not English, French or Spanish. For additional details see Doc 9303-3.	Variable	Notes a, c, d, g, m, n. If omitted, shall appear on an adjacent or preceding page in the passport.
03/I (Mandatory)	Document code	Capital letter P to designate an MRP. One additional capital letter may be used, in the character position after the letter P and at the discretion of the issuing State or organization, to designate other types of passports such as MRP issued to diplomatic staff,	2	Notes a, g, l, m.

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
		an MRP issued for travel on government business, or a passport issued for a special purpose.		
04/I (Mandatory)	Issuing State or organization (in code)	As abbreviated in the three-letter code specified in Doc 9303-3.	3 Fixed	Notes a, f, l.
05/I (Mandatory)	Passport Number	As given by the issuing State or organization to uniquely identify the document from all other MRTDs issued by the State or organization. For additional details see Doc 9303-3.	9	Notes a, b, c, g, l.
06/07/II (Mandatory)	Name	The full name of the holder, as identified by the issuing State or organization. For additional details see Doc 9303-3.	Variable	Notes a, c, g, k, l.
06/II (Mandatory)	Primary Identifier	Predominant component(s) of the name of the holder as described in Doc 9303-3. In cases where the predominant component(s) of the name of the holder (e.g. where this consists of composite names) cannot be shown in full or in the same order, owing to space limitations of Field(s) 06 and/or 07 or national practice, the most important component(s) (as determined by the State or organization) of the primary identifier shall be inserted.	Variable	Notes a, c, g, k, l.
07/II (Mandatory)	Secondary Identifier	Secondary component(s) of the name of the holder as described in Doc 9303-3. The most important component(s) (as determined by the State or organization) of the secondary identifier of the holder shall be inserted in full, up to the maximum dimensions of the field frame. Other components, where necessary, may be	Variable	Notes a, c, k, g, l.

Field/ zone no.	Data element	Specifications	Maximum no. of character positions	References and notes*
		represented by initials. Where the holder's name has only predominant component(s), this data field shall be left blank. A State may optionally utilize the whole zone comprising Fields 06 and 07 as a single field. In such a case, the primary identifier shall be placed first, followed by a comma and a space, followed by the secondary identifier.		
08/II (Mandatory)	Nationality	For details see Doc 9303-3.	Variable	Notes a, c, f, g, l, o.
09/II (Mandatory)	Date of birth	Holder's date of birth as recorded by the issuing State or organization. If the date of birth is unknown, see Doc 9303-3 for guidance.	Variable	Notes a, b, c, g, l.
10/II (Optional)	Personal number	Field optionally used for personal identification number given to holder by the issuing State or organization. For additional details see Doc 9303-3.	Variable	Notes a, b, c, e, g.
11/II (Mandatory)	Sex	Sex of the holder, to be specified by use of the single initial commonly used in the language of the State where the document is issued and, if translation into English, French or Spanish is necessary, followed by an oblique and the capital letter F for female, M for male, or X for unspecified.	3	Notes a, c, g, l.
12/II (Optional element in mandatory zone)	Place of birth	Field optionally used for city and State of the holder's birthplace. Refer to Doc 9303-3 for further details.	Variable	Notes a, c, e, f, g.