



ICAO | UNITING AVIATION

Tenth Symposium and Exhibition on Machine Readable Travel Documents
(MRTDs) and Border Security
October 7-9, 2014

Evolving ICAO MRTD Specifications
coming soon:
The New Seventh Edition of Doc 9303

Tom Kinneging
Manager R&D - Morpho Netherlands
Senior Expert Standardization - Safran Morpho
Convenor ISO/IEC JTC1 SC17 WG3



MRTD SPECIFICATIONS

Doc 9303

- Part 1 - Machine Readable Passports, Sixth edition - 2006
 - Volume 1 - Passports with Machine Readable data stored in OCR format
 - Volume 2 - Electronically enabled Passports with Biometric Identification Capability
- Part 2 - Machine Readable Visas, Third edition - 2005
- Part 3 - Machine Readable Official Travel Documents, Third edition - 2008
 - Volume 1 - MRtds with Machine Readable data stored in OCR format
 - Volume 2 - Electronically enabled MRtds with Biometric Identification Capability



MRTD SPECIFICATIONS

Supplement to Doc 9303

- Release 14 - May 2014
 - 176 pages
 - 253 issues



MRTD SPECIFICATIONS

8 Technical Reports

- TR - MRTDs: History, Interoperability and Implementation
- TR - CSCA Countersigning and Master List issuance
- TR - LDS and PKI Maintenance
- TR - Supplemental Access Control for MRTDs
- TR - Machine reading options for td1 size MRTDs
- TR - Machine Assisted Document Security Verification
- TR - Transliteration of Arabic Script in MRTDs
- TR - Travel Document Deviation List Issuance



MRTD SPECIFICATIONS

Doc 9303

- Part 1 - Machine Readable Passports, Sixth edition - 2006
 - Volume 1 - Passports with Machine Readable data stored in OCR format
 - Volume 2 - Electronically enabled Passports with Biometric Identification Capability
- Part 2 - Machine Readable Visas, Third edition - 2005
- Part 3 - Machine Readable Official Travel Documents, Third edition - 2008
 - Volume 1 - MRtds with Machine Readable data stored in OCR format
 - Volume 2 - Electronically enabled MRtds with Biometric Identification Capability
- Supplement to Doc 9303
- 8 Technical Reports



DOC 9303 REVISION

Three Activities

- Re-structuring
- Supplement incorporation
- Technical Reports integration



DOC 9303 7th EDITION

1. Introduction;
2. Specifications for the Security of Design, Manufacture and Issuance of MRTDs;
3. Specifications common to all Machine Readable Travel Documents;
4. Specifications specific to TD3 size MRTDs, Machine Readable Passports;
5. Specifications specific to TD1 size MRTDs, Machine Readable Official Travel Documents;
6. Specifications specific to TD2 size MRTDs, Machine Readable Official Travel Documents;
7. Machine Readable Visas;
8. Reserved for future use (Emergency Travel Documents);
9. The Deployment of Biometric Identification and Electronic Storage of Data in MRTDs;
10. Logical Data Structure;
11. Security Protocols;
12. Public Key Infrastructure for Machine Readable Travel Documents.



DOC 9303 7th EDITION PART 1

1	FOREWORD	1
2	SCOPE	2
3	GENERAL CONSIDERATIONS	3
3.1	ICAO's Leadership Role	3
3.2	Relative Costs and Benefits of Machine Readable Travel Documents	3
3.3	Operations	3
3.4	Note on the Supplement	4
3.5	Endorsement by ISO	4
4	DEFINITIONS AND REFERENCES	5
4.1	Acronyms	5
4.2	Terms and Definitions	7
4.3	Key Words	20
4.4	Object Identifiers	21
4.5	The use of Notes	22
5	GUIDANCE ON THE USE OF DOC 9303	23
5.1	Doc 9303 Composition	23
5.2	Relationship between MRTD Form Factors and relevant Doc 9303 Parts	24
6	REFERENCES (NORMATIVE)	25



DOC 9303 7th EDITION PART 2

1	SCOPE	1
2	SECURITY OF THE MRTD AND ITS ISSUANCE	2
3	MACHINE ASSISTED DOCUMENT VERIFICATION	3
3.1	Feature Types.....	3
3.2	Basic Principles	4
3.3	Machine Authentication and eMRTDS	5
4	SECURITY OF MRTD PRODUCTION AND ISSUANCE FACILITIES	6
5	PROVISION OF INFORMATION ON NEWLY ISSUED MRTDS	7
6	PROVISION OF INFORMATION ON LOST AND STOLEN MRTDS	8
	APPENDIX A SECURITY STANDARDS FOR MRTDS (INFORMATIVE)	9
A.1	Scope.....	9
A.2	Introduction	9
A.3	Basic Principles	9
A.4	Main threats to the security of travel documents.....	10
A.5	Security Features and Techniques.....	11
	APPENDIX B MACHINE ASSISTED DOCUMENT SECURITY VERIFICATION (INFORMATIVE)	21
B.1	Scope.....	21
B.2	Document Readers and Systems for Machine Authentication.....	21
B.3	Security features and their application for Machine Authentication.....	22
B.4	Selection criteria for machine verifiable security features	30
	APPENDIX C THE PREVENTION OF FRAUD ASSOCIATED WITH THE ISSUANCE PROCESS (INFORMATIVE)	31
C.1	Scope.....	31
C.2	Fraud and its prevention.....	31
C.3	Recommended measures against fraud.....	31
C.4	Procedures to combat fraudulent applications	32
C.5	Control of issuing facilities	33



DOC 9303 7th EDITION PART 3

5	CODES FOR NATIONALITY, PLACE OF BIRTH, LOCATION OF ISSUING STATE/AUTHORITY AND OTHER PURPOSES	3
2	PHYSICAL CHARACTERISTICS OF MRTDs	23
6	TRANSLITERATIONS RECOMMENDED FOR USE BY STATES	28
3	VISUAL INSPECTION ZONE (VIZ)	3
APPENDIX A	EXAMPLES OF CHECK DIGIT CALCULATION (INFORMATIVE)	35
3.1	Languages and Characters	5
APPENDIX B	ARABIC TRANSLITERATION -- DETAILS AND EXAMPLES (INFORMATIVE)	39
3.2	Interface	39
3.3	Captions/Fields	5
3.4	Example of Transliteration for Standard Arabic	39
3.4.1	Convention for Writing the Name of the Holder	39
3.4.2	Recommended Transliteration Scheme for Other Languages	40
3.4.3	Representation of Issuing State or Organization	40
3.4.4	Recommended Transliteration Scheme for Moroccan, Tunisian and Maghrib Arabic	41
3.4.5	Representation of Nationality	41
3.4.6	References (NORMATIVE)	42
3.7	Representation of Place of Birth	7
3.8	Representation of Dates	7
3.9	Displayed Identification Features of the Holder	9
4	MACHINE READABLE ZONE (MRZ)	17
4.1	Purpose of the MRZ	17
4.2	Properties of the MRZ	17
4.3	Constraints of the MRZ	17
4.4	Print Specifications	17
4.5	Machine Reading Requirements and the Effective Reading Zone	18
4.6	Convention for Writing the Name of the Holder	19
4.7	Representation of Issuing State or Organization and Nationality of Holder	20
4.8	Representation of Dates	20
4.9	Check Digits in the MRZ	21
4.10	Characteristics of the MRZ	21
4.11	Quality Specifications of the MRZ	21



DOC 9303 7th EDITION PART 4

1	SCOPE.....	1
2	CONSTRUCTION AND DIMENSIONS OF THE MRP AND MRP DATA PAGE.....	2
2.1	Construction.....	2
2.2	MRP data page nominal dimensions.....	2
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.....	3
3	GENERAL LAYOUT OF THE MRP DATA PAGE.....	4
3.1	MRP Zones.....	4
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.....	11
4.1	Visual Inspection Zone (VIZ) (Zones I through VI).....	11
4.2	Machine Readable Zone (MRZ) (Zone VII).....	15
4.3	Representation of the issuing State or organization and nationality of holder in the MRZ and the VIZ.....	21
	APPENDIX A - EXAMPLES OF A PERSONALIZED MRP DATA PAGE.....	22
	APPENDIX B – CONSTRUCTION OF THE MACHINE READABLE ZONE OF THE PASSPORT DATA PAGE.....	24
	REFERENCES.....	25



DOC 9303 7th EDITION PART 5

1	SCOPE	1
2	DIMENSIONS OF THE TD1-SIZE MROTD	1
2.1	Nominal dimensions	1
2.2	Edge tolerances	1
2.3	Margins	2
2.4	Thickness.....	2
3	GENERAL LAYOUT OF THE TD1 SIZE MROTD	2
3.1	TD1 Zones	3
3.2	Content and use of zones.....	4
3.3	Dimensional flexibility of Zones I to V	6
4	CONTENTS OF A TD1-SIZE MROTD	8
4.1	Visual Inspection Zone (VIZ) (Zones I through VI)	8
4.2	Machine Readable Zone (MRZ) (Zone VII)	10
APPENDIX A	EXAMPLES OF A PERSONALIZED TD1-SIZE MROTD	17
APPENDIX B	CONSTRUCTION OF THE MACHINE READABLE ZONE OF A TD1-SIZE MROTD	19
APPENDIX C	TECHNICAL SPECIFICATIONS FOR A MACHINE READABLE CREW MEMBER CERTIFICATE (CMC)	20
C.1	Scope	20
C.2	Content and use of zones	20
REFERENCES	22



DOC 9303 7th EDITION PART 6

1	SCOPE	1
2	DIMENSIONS OF THE TD2 SIZE MROTD	1
2.1	Nominal dimensions.....	1
2.2	Edge tolerances.....	1
2.3	Margins.....	2
2.4	Thickness.....	2
3	GENERAL LAYOUT OF THE TD2 SIZE MROTD TDTD	3
3.1	TD2 Zones	3
3.2	Content and use of zones.....	4
3.3	Dimensional flexibility of Zones I to V.....	6
4	CONTENTS OF A TD2-SIZE MROTD	8
4.1	Visual Inspection Zone (VIZ) (Zones I through VI)	8
4.2	Machine Readable Zone (MRZ) (Zone VII)	10
	APPENDIX A - EXAMPLES OF A PERSONALIZED TD2-SIZE MROTD	16
	APPENDIX B - CONSTRUCTION OF THE MACHINE READABLE ZONE OF A TD2-SIZE MROTD	18
	REFERENCES	19



DOC 9303 7th EDITION PART 7

1	SPECIFIC OPTIONAL BARCODES ON MACHINE READABLE VISAS	35
2	4. TECHNICAL SPECIFICATIONS FOR FORMAT-A MACHINE READABLE VISAS (MRV-A)	35
4.2	Definition	35
4.5	Dimensions and Placement of the MRV-A	35
4.2	Location of Bar Code(s)	35
4.4	General Layout of the MRV-A	36
4.4	Quality of Bar Code(s)	36
4.3	Content, Use and Dimensional Flexibility of Zones	36
4.3	Synoptologies and Logical Data Structure	36
4.4	Detailed Layout	36
4.6	Machine Reading of the Bar Code(s)	36
2.5	Machine Readable Zone (MRZ) (Mandatory Zone VII)	7
APPENDIX A	EXAMPLES OF PERSONALIZED MRV VISAS (INFORMATIVE)	37
2.6	Data Structure of Machine Readable Data for the MRV-A	37
A.1	Portrait Examples	37
A.2	MRV-A Diagrams	38
A.2	MRV-B Diagrams	38
3	TECHNICAL SPECIFICATIONS FOR FORMAT-B MACHINE READABLE VISAS (MRV-B)	38
APPENDIX B	CONSTRUCTION OF THE MRZ (INFORMATIVE)	39
B.1	Dimensions and Placement of the MRV-B	39
B.1	MRV-A MRZ Construction	39
B.2	General Layout of the MRV-B	40
B.2	MRV-B MRZ Construction	40
3.3	Content, Use and Dimensional Flexibility of Zones	19
APPENDIX C	POSITIONING IN PASSPORT (INFORMATIVE)	41
3.4	Detailed Layout	41
3.5	Machine Readable Zone (MRZ) (Mandatory Zone VII)	23
3.5	MRZ Positioning	23
3.6	Data Structure of Machine Readable Data for the MRV-B	42
3.6	MRV-B Positioning	42
3.7	Portrait	30
APPENDIX D	MATERIALS AND PRODUCTION METHODS (INFORMATIVE)	43
3.8	MRV-B Diagrams	31
	REFERENCES (NORMATIVE)	45



DOC 9303 7th EDITION PART 8

Part 8 - Specifications specific to
Emergency Travel Documents
(TBD)



DOC 9303 7th EDITION PART 9

1	SCOPE	1
2	EMRTD	2
2.1	Conformance to Doc 9303.....	2
2.2	Validity Period for an eMRTD.....	2
2.3	Chip Inside Symbol.....	2
2.4	Warning regarding Care in Handling an eMRP.....	3
3	BIOMETRIC IDENTIFICATION	4
3.1	ICAO Vision on Biometrics	4
3.2	Key Considerations.....	4
3.3	Key Processes with respect to Biometrics.....	5
3.4	Applications for a Biometric Solution	6
3.5	Constraints on Biometric Solutions.....	7
4	THE SELECTION OF BIOMETRICS APPLICABLE TO EMRTDS	8
4.1	Primary Biometric: Facial Image.....	8
4.2	Optional Additional Biometrics.....	10
5	STORAGE OF THE BIOMETRIC AND OTHER DATA IN A LOGICAL FORMAT IN A CONTACTLESS IC	12
5.1	Characteristics of the Contactless IC	12
5.2	Logical Data Structure	12
5.3	Security and Privacy of the Stored Data.....	12
6	TEST METHODOLOGIES FOR (E)MRTDS	14
	PLACEMENT OF THE CONTACTLESS IC IN AN EMRP (INFORMATIVE)	15
A.1	Location of the IC and its Associated Antenna.....	15
A.2	Precautions in eMRTD manufacture	15
A.3	Reading both the OCR and the data on the IC.....	15
A.4	Reader construction.....	16
	PROCESS FOR READING EMRTDS (INFORMATIVE)	17
	REFERENCE (NORMATIVE)	18



DOC 9303 7th EDITION PART 10

6	DATA ELEMENTS FORMING DATA GROUPS 1 THROUGH 16	20
2	REQUIREMENTS OF THE LOGICAL DATA STRUCTURE (REQUIRED)	21
6.1	DATA GROUP 1 - Encoded Identification Features – Face (REQUIRED)	21
6.2	DATA GROUP 2 - Encoded Identification Features – Face (REQUIRED)	23
6.3	DATA GROUP 3 - Additional Identification Feature - Finger(s) (OPTIONAL)	25
6.4	DATA GROUP 4 - Additional Identification Feature - Iris(es) (OPTIONAL)	28
6.5	DATA GROUP 5 - Displayed Portrait (OPTIONAL)	31
3	APPLICATION PROFILE FOR THE CONTACTLESS IC	32
6.7	DATA GROUP 7 - Displayed Signature or Usual Mark (OPTIONAL)	32
6.8	DATA GROUP 8 - Data Feature(s) (OPTIONAL)	33
6.9	DATA GROUP 9 - Structure Feature(s) (OPTIONAL)	33
6.10	DATA GROUP 10 - Substance Feature(s) (OPTIONAL)	34
6.11	DATA GROUP 11 - Additional Personal Detail(s) (OPTIONAL)	35
6.12	DATA GROUP 12 - Additional Document Detail(s) (OPTIONAL)	37
6.13	DATA GROUP 13 - Optional Detail(s) (OPTIONAL)	38
6.14	DATA GROUP 14 - Security Options (CONDITIONAL)	38
6.15	DATA GROUP 15 - Active Authentication Public Key Info (CONDITIONAL)	39
6.16	DATA GROUP 16 - Person(s) to Notify (OPTIONAL)	39
4	FILE STRUCTURE SPECIFICATIONS	8
4.1	Application Selection - DF	9
4.2	Data Groups	9
4.3	Data Elements Encoding Rules	9
4.4	Normative Tags Used in LDS Context	10
4.5	LDS Versioning	13
5	ELEMENTARY FILES	14
5.1	Header and Data Group Presence Information EF.COM (REQUIRED)	14
5.2	Document Security Object EF.SOD (REQUIRED)	14
5.3	EF.CardAccess (CONDITIONAL)	19



DOC 9303 7th EDITION PART 11

9	COMMON SPECIFICATIONS	30
2 9.1	ASSUMPTIONS AND NOTATIONS	30
9.2	Public Key Data Objects	33
9.3	Notations	34
9.3	Standardized Domain Parameters	34
3	SECURING ELECTRONIC DATA	35
9.5	Key Derivation Mechanism	35
4	ACCESS TO THE CONTACTLESS IC	36
9.6	Secure Messaging	36
4.1	Compliant Configurations	10
4.2	Chip Access Procedure	11
APPENDIX A	ENTROPY OF MRZ-DERIVED ACCESS KEYS (INFORMATIVE)	41
4.1	Basic Access Control	41
APPENDIX B	POINT CODING FOR THE ECDH-INTEGRATED MAPPING (INFORMATIVE)	42
4.4	Password Authenticated Connection Establishment	14
B.1	High-level Description of the Point Encoding Method	42
5	AUTHENTICATION OF DATA	22
B.2	Implementation for Affine Coordinates	22
B.3	Implementation for Jacobian Coordinates	43
5.1	Passive Authentication	22
APPENDIX C	WORKED EXAMPLE: BASIC ACCESS CONTROL (INFORMATIVE)	44
6	AUTHENTICATION OF THE CONTACTLESS IC	44
C.1	Compute Keys from Key Seed (K_{Seed})	44
C.1	Active Authentication	44
C.2	Derivation of Document Basic Access Keys (K_{Enc} and K_{MAC})	45
7	ADDITIONAL ACCESS CONTROL MECHANISMS	46
C.4	Secure Messaging	48
7.1	Extended Access Control for Additional Biometrics	27
APPENDIX D	WORKED EXAMPLE: PASSIVE AUTHENTICATION (INFORMATIVE)	51
APPENDIX E	WORKED EXAMPLE: ACTIVE AUTHENTICATION (INFORMATIVE)	52
APPENDIX F	WORKED EXAMPLE: PACE – GENERIC MAPPING (INFORMATIVE)	55
8.2	Password Authenticated Connection Establishment	28
8.3	Passive Authentication	28
8.4	Active Authentication	28
8.5	Extended Access Control to Additional Biometrics	28
8.6	Decryption of Additional Biometrics	29



DOC 9303 7th EDITION PART 12

7	CERTIFICATE AND CRL PROFILES	13
2	7.1 Overview of the Public Key Infrastructure.....	13
3	7.2 CRL Profile.....	24
3	ROLES AND RESPONSIBILITIES	24
8	CSCA MASTER LIST STRUCTURE	24
3.1	Country Signing Certification Authority.....	24
3.2	Signature Type.....	24
3.2	Inspector System Specification.....	24
3.4	Master List Signer.....	5
	APPENDIX A - LIFETIMES (INFORMATIVE)	26
4	KEY MANAGEMENT	6
A.1	Example 1.....	26
A.2	Example 2: Signer Keys and certificates.....	26
A.2	Example 3: Keys and Certificates.....	26
A.3	Certificate Revocation.....	8
4	APPENDIX B - CERTIFICATE & CRL PROFILE REFERENCE TEXT (INFORMATIVE)	27
4.4	Cryptographic Algorithms.....	27
5	APPENDIX C - EARLIER CERTIFICATE PROFILES (INFORMATIVE)	30
	DISTRIBUTION MECHANISMS	30
APPENDIX D - REC 5280 VALIDATION COMPATIBILITY (INFORMATIVE)		37
5.1	PKI Distribution Mechanism.....	37
5.1	PKI Distribution Mechanism.....	37
5.2	State Revocation Distribution Mechanism.....	37
5.2	Master List Distribution Mechanism.....	40
D.2	Modifications required to process CRLs.....	40
6	PKI TRUST AND VALIDATION	13
	References (normative).....	41
6.1	Trust Anchor Management.....	13
6.2	Certificate/CRL Validation and Revocation Checking.....	14



DOC 9303 7th EDITION

Usage

- ePassport Book

The collage displays 12 document covers from ICAO Doc 9303, 7th Edition, arranged in a grid. Each cover is blue with the ICAO logo and a numbered circle in the top right corner. The covers contain various technical specifications and protocols for Machine Readable Travel Documents (MRTDs).

- 1** Introduction
 - Amendments
 - Foreword
- 2** Specifications for the security of the design, manufacture & issuance of MRTDs
 - Security of the MRTD &
- 3** Specifications common to all MRTDs
 - Illustrative guidelines for portraits
 - Three letter codes
 - Transliterations
- 4** Specifications specific to ID3 size MRTDs - Machine Readable Passports
 - Construction & dimensions
 - MRP data page layout
 - use of zones
 - Section Zone
 - Readable Zone
 - data elements
 - diagrams
- 5** The deployment of biometric identification & electronic storage of data in MRTDs
- 6** Metrics solution solutions applicable to
- 7** A Logical Data Structure (LDS) for storage of biometrics & other data in the contactless IC
 - Process for reading eMRTDs
 - Requirements of the LDS
 - Mandatory & optional data elements
 - Ordering & grouping of data elements
 - Mapping principles for contactless IC
 - Data Group specifications
 - Worked examples
- 8** Protocols
 - Basic Access Control
 - PACE V2
 - Passive Authentication
 - Active Authentication
 - eMRTD production and personalization
 - eMRTD inspection
 - Worked examples
- 9** Public Key Infrastructure (PKI) for Machine Readable Travel Documents
 - Overview of the Public Key Infrastructure
 - Document Security Object (SOD)
 - Document Signer (DS)
 - Country Signing CA (CSCA)
 - Algorithms
 - Key management
 - CSCA Master List
 - Certificate Revocation Lists
 - Public Key Directory
 - Non conforming certificates
- 10**
- 11**
- 12**



DOC 9303 7th EDITION

Usage

- Non-chip TD1 size card





DOC 9303 7th EDITION

Maintenance

- Seventh edition - Revision 1
- Changes & Updates to individual parts → Revision 2
- No more Supplements
- Every 5 years new edition (as before)
- One ISO standard on editions ISO/IEC 7501



DOC 9303 REVISION

Timeline

- Project start - Mid 2011
- 3 Phases completed - Q3 2013
- Review cycles completed - Q1 2014
- Endorsed at TAG 22 - May 2014
- **ICAO Editorial and Translation**
- Publication - End 2014



DOC 9303 REVISION

Successful?

- Doc 9303 6th/3rd Edition
1049 pages
- Doc 9303 7th Edition
424 pages



Tom KINNEGING
Senior Expert Standardization
Manager R&D (CESE / CESP) Morpho BV

tom.kinneging@morpho.com
M +31 65 12 13 702
T +31 23 79 95 218

Morpho B.V.
P.O. Box 5300, 2000 GH Haarlem, The Netherlands
www.morpho.com

Thank you for your attention