



**TECHNICAL ADVISORY GROUP ON MACHINE READABLE
TRAVEL DOCUMENTS (TAG/MRTD)**

TWENTY-SECOND MEETING

Montréal, 21 to 23 May 2014

Agenda Item 2: Activities of the NTWG

REVISION OF DOC 9303 – Machine Readable Travel Documents

(Presented by the New Technologies Working Group)

1. INTRODUCTION

1.1 At its Twentieth meeting in September 2011 the TAG/MRTD endorsed Working Paper 8 on the revision of Doc 9303.

1.2 The TAG/MRTD agreed to the proposed boundaries of the project consisting of:

- a) Re-structuring Doc 9303 into 12 parts.
- b) Incorporation of issues from the Supplement into the re-structured Doc 9303.
- a) Incorporation of endorsed Technical Reports into the re-structured Doc 9303.

1.3 This Working Paper at hand provides the results of the revision project and suggestions for the way forward.

2. BACKGROUND

2.1 Doc 9303 presently consists of :

- a) Part 1 - sixth edition, published in 2006;
- c) Part 2 - third edition, published in 2005;

- d) Part 3 - third edition, published in 2008;
- e) Supplement to Doc 9303 - Release 13, published in 2013.

2.2 The TAG/MRTD recognized the fact that the three parts of Doc 9303 contain duplicate, mainly general, information. However the parts are issued as separate documents. As a result maintenance and keeping the specifications consistent is complex and time consuming. In the paper based editions of Doc 9303 this was the only way to issue the information in a comprehensive way, being necessary to comfort the audience, the users of the standards. Since 2009 ICAO issues Doc 9303 in electronic format. This new approach allows the user to download the complete standard, free of charge, or parts of it as he chooses. The electronic format opens up the possibility to improve maintainability as well as the readability through a more efficient structure.

2.3 The present release of the Supplement contains more than 200 issues. These issues have been analysed for integration into new editions of Doc 9303.

2.4 It is common practice that when new editions of Doc 9303 are issued, existing endorsed Technical Reports will be integrated into the standard. Six Technical reports have been candidates for this integration as part of the project.

3. CURRENT STATUS

3.1 The revision project has been conducted and resulted in the final draft of the seventh edition of Doc 9303.

3.2 Based on the requirements endorsed by the TAG/MRTD through TAG-MRTD/20-WP/08 the seventh edition consists of eleven parts (twelve parts specified):

Part 1 - Introduction;

Part 2 - Specifications for the Security of the Design, Manufacture and Issuance of Machine Readable Travel Documents;

Part 3 - Specifications common to all Machine Readable Travel Documents;

Part 4 - Specifications specific to Machine Readable Passports (MRPs) and other TD3 size Machine Readable Travel Documents (MRTDs);

Part 5 - Specifications specific to TD1 size MRTODs, Machine Readable Official Travel Documents;

Part 6 - Specifications specific to TD2 size MRTODs, Machine Readable Official Travel Documents;

Part 7 - Machine Readable Visas;

Part 8 - Reserved for future use (Emergency Travel Documents);

Part 9 - The Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs;

Part 10 - Logical Data Structure (LDS) for storage of biometrics and other data in the contactless IC;

Part 11 - Security Mechanisms for Machine Readable Travel Documents;

Part 12 - Public Key Infrastructure for Machine Readable Travel Documents.

3.3 Clarifications from Supplement releases up to Release 13 have been incorporated.

3.4 Technical Reports, previously endorsed by the TAG, have been incorporated. These are the following Technical Reports:

- a) TR “CSCA countersigning and Master List issuance”.
- b) TR “Supplemental Access Control for Machine Readable Travel documents”.
- c) TR “LDS and PKI Maintenance”.
- d) TR “Machine Reading Options for td1 size MRtds”.
- e) TR “Machine Assisted Document Security Verification”.
- f) TR “Transliteration of Arabic Script”.

3.5 The new structure allows for updating individual parts through new revisions, as such the necessity for issuing Supplement disappears.

3.6 ISO short form endorsement is expected to be on new editions of Doc 9303 as a whole and not on an individual revision of any part.

4. ACTION BY THE TAG/MRTD

4.1 The TAG/MRTD is invited to:

- a) recognize the work of the editorial team ISO/IEC JTC1 SC17 WG3/TF2 working on the seventh edition; and
- b) endorse the new format of the seventh edition of Doc 9303 and its contents; and
- c) decide on the future revision process as indicated in 3.5 and 3.6 of this Working Paper; and
- d) request the ICAO TRIP secretariat to undertake the necessary actions to start the ICAO editorial work in cooperation with TF2 and translation into the official ICAO languages; and
- e) endorse the publication of the seventh edition of Doc 9303 once the English version has been released by the ICAO editors, preferably before end 2014 followed by the other languages as soon as they are released.

Doc 9303



Machine Readable Travel Documents

**Part 1
Introduction**

Approved by the Secretary General
and published under his authority

Seventh Edition - Revision 1 - 2014

International Civil Aviation Organization

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

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

Doc 9303, Machine Readable Travel Documents
ISBN xxx-xx-xxxx-xxx-x

© ICAO 2014

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 TO DOC 9303-1, 7TH EDITION

Revision	Date	Description
01	xx-xx-2014	Initial release of the 7 th edition

DRAFT_4 FOR TAG_22

TABLE OF CONTENTS

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

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 of 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 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 these 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.

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 Contracting 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 Contracting 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].

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 for the failure to involve 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	Diffraction Optically Variable Image Device
DS	Document Signer
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECDH	Elliptic Curve Diffie Hellmann
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

Acronym	Full form
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
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
PIX	Proprietary Identifier eXtension (PIX).
PKD	Public Key Directory
PKI	Public Key Infrastructure
RID	Relative IDentifier (RID)

Acronym	Full form
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 and 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.
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.

Term	Definition
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: <ol style="list-style-type: none"> 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 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.

Term	Definition
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.
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".
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 Features	A data feature involves the incorporation of encoded information into the document data or image structure, usually into the personalization data, especially

Term	Definition
	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.
Diffraction 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.
Diffraction 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.
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 which 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	A MRTD conforming to the specifications of Doc 9303, that incorporates a

Term	Definition
Readable Travel Document (eMRTD)	contactless integrated circuit including the capability of biometric identification of the holder.
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.
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

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

Term	Definition
	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).
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

Term	Definition
Identification/Identify	with a biometric system to enroll or have his identity checked. 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 a 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.
Integrated Circuit (IC)	Electronic component designed to perform processing and/or memory functions.

Term	Definition
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.
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.

Term	Definition
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 approximating to ID-1 or ID-2 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 an 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.
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.

Term	Definition
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.
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 contracting State or other entity issuing or intending to issue eMRTDs

Term	Definition
	who follow 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 unforgeable.
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.
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.

Term	Definition
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.
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.

Term	Definition
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.
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 a 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.

Term	Definition
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.
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 the requirements in Parts 9, 10, 11, and 12.

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** only be used 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 implementors 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 implementors 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 the parts 10, 11, and 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}
```

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 emphasise 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 paragraph 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 Machine Readable Travel Documents

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 Machine Readable Travel Documents

Part 3 of Doc 9303 is based on Doc 9303 Part 1 Volume 1, Machine Readable Passports – Passports with Machine Readable Data Stored in Optical Character Recognition Format (Sixth Edition 2006) and Doc 9303 Part 3 Volume 1, Machine Readable Official Travel Documents – MRtds with Machine Readable Data Stored in Optical Character Recognition Format (Third Edition 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 Part 4 through Part 7.

Part 4 - Specifications Specific to Machine Readable Passports (MRPs) and other TD3 size Machine Readable Travel Documents (MRTDs)

Part 4 defines specifications that are specific to TD3 size Machine Readable Passports (MRP's) 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 specific to TD1 size MRTODs, Machine Readable Official Travel Documents

Part 5 defines specifications that are specific to TD1 size Machine Readable Official Travel Documents (MROTDS).

Part 6 - Specifications specific to TD2 size MRTODs, Machine Readable Official Travel Documents

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 (MRV) 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 Doc 9303 Part 2, Machine Readable Visas, Third edition - 2005.

Part 8 - Emergency Travel Documents

Reserved for future use.

Part 9 - The deployment of biometric identification and the 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 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 Machine Readable Travel Documents

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 to the communication between 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 Machine Readable Travel Documents

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

The following table describes which parts of Doc 9303 are relevant for specific types of MRTDs (form factors).

Table 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.

DRAFT_4 FOR TAG_22

Doc 9303



Machine Readable Travel Documents

Part 2

**Specifications for the Security of the Design, Manufacture and Issuance of
Machine Readable Travel Documents**

Approved by the Secretary General
and published under his authority

Seventh Edition – Revision 1 - 2014

International Civil Aviation Organization

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

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

Doc 9303, Machine Readable Travel Documents
Order Number: xxxx
ISBN xxx-xx-xxxx-xxx-x

© ICAO 2014

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 TO DOC 9303-2, 7TH EDITION

Revision	Date	Description
01	xx-xx-2014	Initial release of the 7 th edition

DRAFT_4 FOR TAG_22

TABLE OF CONTENTS

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

1 SCOPE

The seventh edition of Doc 9303 represents a restructuring of the ICAO specifications for Machine Readable Travel Documents. Without incorporating substantial modifications of 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 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.

The worldwide increase in the number of people travelling and the expected continuing growth, together with the growth in international crime, terrorism, and illegal immigration has led to increasing concerns over the security of travel documents and calls for recommendations on what may be done to help improve their resistance to attack or misuse. Historically, Doc 9303 has not made recommendations on the specific security features to be incorporated in travel documents. Each Issuing State has been free to incorporate such safeguards as it deemed appropriate to protect its nationally issued travel documents against counterfeiting, forgery and other forms of attack, as long as nothing was included which would adversely affect their OCR machine readability.

To meet the need of increased document security, ICAO's technical advisors decided it would be desirable to publish a set of "recommended minimum security standards" as a guideline for all States issuing machine readable travel documents.

- Appendix A to this Part describes security measures to be taken within the structure of the MRTD and of the premises in which it is produced.
- Appendix B describes optional means of achieving machine-assisted document verification.
- Appendix C describes the security measures to be taken to ensure the security of the personalization operations and of the documents in transit.

2 SECURITY OF THE MRTD AND ITS ISSUANCE

The MRTD, and its method of issuance, shall be designed to incorporate safeguards to protect the document against fraudulent attack during its validity period. Methods of fraudulent attack can be classified as follows:

- *Counterfeit* involves the creation of all or part of a document which resembles the genuine MRTD with the intention that it be used as if it were genuine. Counterfeits may be produced by attempting to duplicate or simulate the genuine method of manufacture and the materials used therein or by using copying techniques;
- *Fraudulent alteration, also known as forgery*, 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; and
- *Imposters*. “Imposter” is defined as someone representing himself¹ to be some other person. Security features should be incorporated to facilitate the visual and/or automated detection of the fraudulent use of the MRTD by an imposter

There are established methods of providing security against the above types of fraudulent attack. These involve the use of materials which are not readily available, combined with highly specialized design systems and manufacturing processes requiring special equipment and expertise. Appendix A to this Part lists some of the techniques currently known to be available to provide security to an MRTD enabling an inspecting officer to detect a counterfeit or fraudulently altered document either visually or with the aid of simple equipment such as a magnifying glass or ultraviolet lamp.

All MRTDs that conform to Doc 9303, shall use the specified Basic Security Features listed in Table 1 of Appendix A.

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

3 MACHINE ASSISTED DOCUMENT VERIFICATION

A travel document Issuing Authority may wish to incorporate into its MRTDs one or more security features which require the use of detection equipment to detect and verify their presence within the normal time for immigration clearance. This section provides advice on machine assisted authentication of security features incorporated in MRTDs made in accordance with the specifications set out in Doc 9303. Machine verifiable security features help confirm the authenticity of a genuine document made from genuine materials. Appendix B contains recommendations which cover machine authentication of the security features in the document itself (based on materials, on security printing and on copy protection techniques) as well as advice on reader technologies that apply to machine authentication of documents. Appendix A of this Part and the security standards recommended therein provide the basis for the considerations in this section, utilizing the security features recommended in the appendix and expanding the capabilities of advanced readers already installed at the borders to accommodate electronic Machine Readable Travel Documents (eMRTDs) and their verification.

The worldwide success of ICAO's electronic document initiative has led to the issuance of millions of eMRTDs as specified in Doc 9303. These advanced document concepts require the deployment of travel document readers equipped for reading contactless ICs at the points of document authentication, usually the points of entry at one country's borders. Such advanced readers feature not only the contactless IC reading capability, but also the means for high resolution image acquisition in the visual, infrared and ultraviolet spectral range.

The aim of the recommendations in this chapter is to improve the security of machine readable travel documents worldwide by using machine assisted document authentication procedures completely in line with:

- the layout of machine readable travel documents as specified in Doc 9303 maintaining backward compatibility;
- the security features recommended in Appendix A of this Part; and
- making use of the technical capabilities of advanced readers installed worldwide to accommodate eMRTDs.

However, it is necessary for each State to conduct a risk assessment of the machine assisted document authentication at its borders to identify their most beneficial aspects and minimize the risks. Doc 9303 does not specify any feature as a means of globally interoperable machine assisted document verification, as the use of a single feature worldwide would make the feature highly vulnerable to fraudulent attack. Therefore, to minimize risk States should apply a variety of security features.

3.1 Feature Types

There are three main categories of machine-verifiable security features. These are described below along with examples of security features that are capable of machine verification.

3.1.1 Structure Feature

A structure feature involves the incorporation of a measurable structure into or onto the MRTD data page. It is a security feature containing some form of verifiable information based on the physical construction of the feature. Examples include:

- the interference characteristic of a hologram or other optically variable device that can be uniquely identified by a suitable reader;
- retro-reflective images embedded within a security laminate; and
- controlled transmission of light through selective areas of the substrate.

3.1.2 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. It involves the identification of a defined characteristic of a substance used in the construction of the feature. Examples include:

- the use of pigments, usually in inks, which respond in specific and unusual ways to specific wavelengths of light (which may include infrared or ultraviolet light) or have magnetic or electromagnetic properties; and
- the incorporation into a component of the data page of materials, e.g. fibres whose individual size or size distribution conform to a predetermined specification.

3.1.3 Data Feature

The visible image of the MRTD data page may contain concealed information which may be detected by a suitable device built into the reader. The concealed information may be in the security printed data page but it is more usually incorporated into the personalization data especially the printed portrait.

Inserting the concealed information to the MRTD data page may involve the application of substance and or structure features in a way which achieves several levels of security. The term steganography, in this context, describes a special class of data features typically taking the form of digital information which is concealed within an image, usually either the personalization portrait or the background security printing. The information may be decoded by a suitable device built into a full page reader set to look for the feature in a specific location. The information might, for example, be the travel document number. The reader could then be programmed to compare the travel document number detected from the feature with the travel document number appearing in the MRZ. Such a comparison involves no access to any data stored in the contactless IC of an eMRTD. Examples of this type of feature are:

- encoded data stored on the document in magnetic media such as special security threads; and
- designs incorporating the concealed data which only becomes detectable when viewed using a specific wavelength of light, optical filters, or a specific image processing software.

In more complex forms the amount of stored data can be significant, and this can be verified by electronic comparison with data stored in the contactless IC of the eMRTD.

3.2 Basic Principles

All three feature types, namely structure, substance and data, may be incorporated in travel documents and verified with suitably designed readers. Readers are now becoming available that can detect such features and use the responses to confirm the authenticity of the document. Appendix B concentrates on features that can be verified by detection equipment built into the MRTD reader, and used during the normal reading process.

Machine assisted document security verification uses automated inspection technology to assist in verifying the authenticity of a travel document. It should not be used in isolation to determine proof of authenticity, but when used in combination with visible document security features the technology provides the examiner with a powerful new tool to assist in verifying travel documents.

Machine assisted document security verification features are optional security elements that may be included on the MRTD at the discretion of the Issuing Authority.

The machine verifiable security features may vary in size from less than 1 mm (0.04 in) square up to the whole area of the document. Figure 1 provides guidance on the positions these features should occupy on a MRTD data page to facilitate interoperability. To maintain backward compatibility, it is recommended to deploy machine authentication features within the positions and areas indicated.

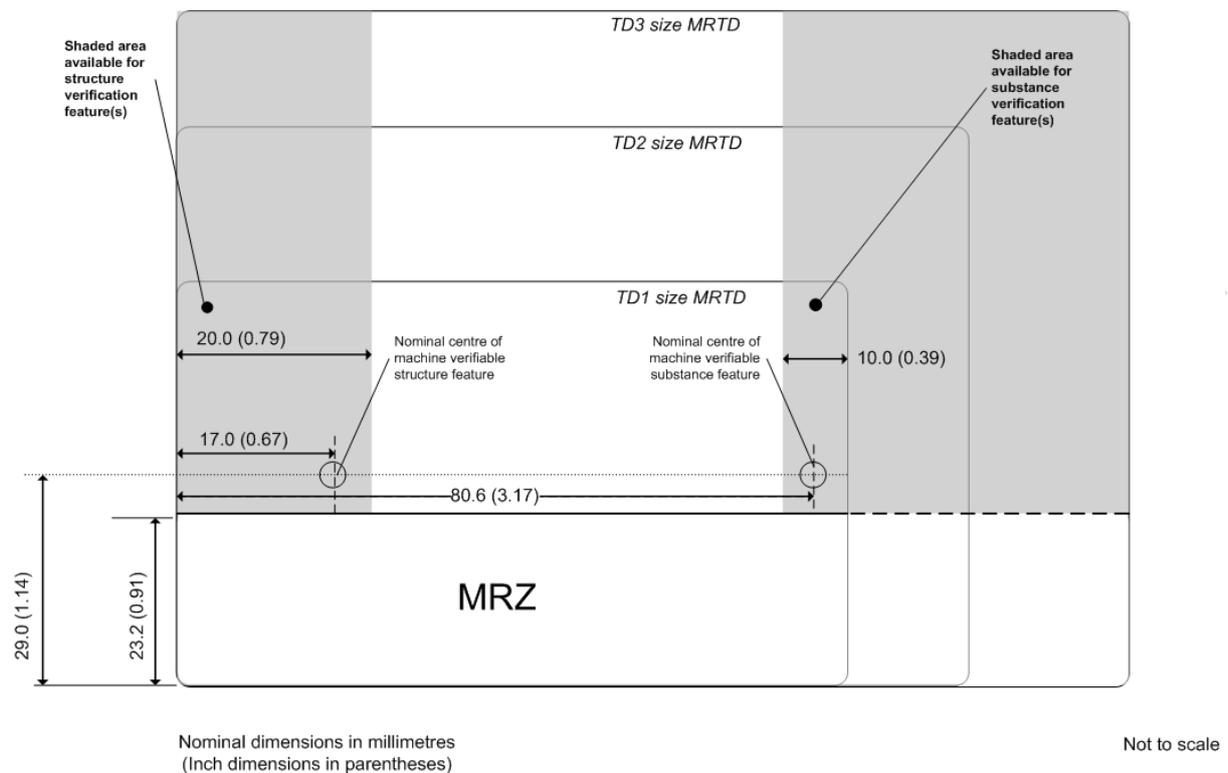


Figure 1: Three sizes of MRTD including the MRP (TD3 size) with recommended positions for machine assisted document verification features. The shaded area on the left is recommended for the incorporation of a structure feature and that on the right for the incorporation of a substance feature.

3.3 Machine Authentication and eMRTDS

The use of a fully compliant, contactless IC in an eMRTD offers excellent possibilities for machine authentication. However, machine authentication using the contactless IC fails if:

- the contactless IC is defective and fails to communicate; or
- there are no certificates available for checking the authenticity and integrity of the data on the contactless IC.

Therefore an alternative machine authentication is needed. This is especially relevant in Automated Border control (ABC) scenarios where the machine reader is used instead of a border official to read and validate the eMRTD. This alternative machine authentication establishes trust in the data used for decisions at the border.

A functioning contactless IC in an eMRTD can also aid machine authentication by storing the machine authentication features and its coordinates in the relevant Data Groups (DGs).

4 SECURITY OF MRTD PRODUCTION AND ISSUANCE FACILITIES

The State issuing the MRTD shall ensure that the premises in which the MRTD is printed, bound, personalized and issued are appropriately secure and that staff employed therein have an appropriate security clearance. Appropriate security shall also be provided for MRTDs in transit between facilities and from the facility to the MRTD's holder. Appendix C provides recommendations as to how these requirements can be met.

DRAFT_4 FOR TAG_22

5 PROVISION OF INFORMATION ON NEWLY ISSUED MRTDS

It is recommended that a State launching a new design of MRTD inform all other States of the details of the new MRTD including evident security features, preferably providing personalized specimens for use as a reference by the receiving State's department which is responsible for verifying the authenticity of such documents. The distribution of such specimens should be made to established contact points agreed by the receiving States.

DRAFT_4 FOR TAG_22

6 PROVISION OF INFORMATION ON LOST AND STOLEN MRTDS

States should provide specific information on lost or stolen MRTDs, such as the MRTD document number, to the central database operated by INTERPOL at the appropriate time and according to agreed procedures. This includes details of any unpersonalized MRTDs which may be stolen from a production or issuance facility or in transit.

DRAFT_4 FOR TAG_22

APPENDIX A SECURITY STANDARDS FOR MRTDS (INFORMATIVE)

A.1 Scope

This Appendix provides advice on strengthening the security of machine readable travel documents made in accordance with the specifications set out in Doc 9303. The recommendations cover the security of the materials used in the document's construction, the security printing and copy protection techniques to be employed, and the processes used in the production of document blanks. Also addressed are the security considerations that apply to the personalization and the protection of the biographical data in the document. All travel document Issuing Authorities shall consider this Appendix.

A.2 Introduction

This Appendix identifies the security threats to which travel documents are frequently exposed and the counter-measures that may be employed to protect these documents and their associated personalization systems. The lists of security features and/or techniques offering protection against these threats have been subdivided into: 1) basic security features and/or techniques considered essential and; 2) additional features and/or techniques from which States are encouraged to select items which are recommended for providing an enhanced level of security.

This approach recognizes that a feature or technique that may be necessary to protect one State's documents may be superfluous or of minor importance to another State using different production systems. A targeted approach that allows States flexibility to choose from different document systems (paper-based documents, plastic cards, etc.) and a combination of security features and/or techniques most appropriate to their particular needs is therefore preferred to a "one size fits all" philosophy. However, to help ensure that a balanced set of security features and/or techniques is chosen, it is necessary for each State to conduct a risk assessment of its national travel documents to identify their most vulnerable aspects and select the additional features and/or techniques that best address these specific problems.

The aim of the recommendations in this Appendix is to improve the security of machine readable travel documents worldwide by establishing a baseline for Issuing States. Nothing within these recommendations shall prevent or hinder States from implementing other, more advanced security features, at their discretion, to achieve a standard of security superior to the minimum recommended features and techniques set forth in this Appendix.

A summary table of typical security threats relating to travel documents and some of the security features and techniques that can help to protect against these threats is included.

A.3 Basic Principles

Production and storage of passport books and travel documents, including the personalization processes, should be undertaken in a secure, controlled environment with appropriate security measures in place to protect the premises against unauthorized access. If the personalization process is decentralized, or if personalization is carried out in a location geographically separated from where the travel document blanks are made, appropriate precautions should be taken when transporting the blank documents and any associated security materials to safeguard their security in transit and storage on arrival. When in transit blank books or other travel documents should contain the unique document number. In the case of passports the passport number should be on all pages other than the biographical data page where it can be printed during personalization.

There should be full accountability over all the security materials used in the production of good and spoiled travel documents and a full reconciliation at each stage of the production process with records maintained to account for all security material usage. The audit trail should be to a sufficient level of detail to account for every unit of security material used in the production and should be independently

audited by persons who are not directly involved in the production. Records certified at a level of supervision to ensure accountability should be kept of the destruction of all security waste material and spoiled documents.

Materials used in the production of travel documents should be of controlled varieties where applicable, and obtained only from reputable security materials suppliers. Materials whose use is restricted to high security applications should be used, and materials that are available to the public on the open market should be avoided.

Sole dependence upon the use of publicly available graphics design software packages for originating the security backgrounds should be avoided. These software packages may however be used in conjunction with specialist security design software.

Security features and/or techniques should be included in travel documents to protect against unauthorized reproduction, alteration and other forms of tampering, including the removal and substitution of pages in the passport book, especially the biographical data page. In addition to those features included to protect blank documents from counterfeiting and forgery, special attention must be given to protect the biographical data from removal or alteration. A travel document should include adequate security features and/or techniques to make evident any attempt to tamper with it.

The combination of security features, materials and techniques should be well chosen to ensure full compatibility and protection for the lifetime of the document.

Although this Appendix deals mainly with security features that help to protect travel documents from counterfeiting and fraudulent alteration, there is another class of security features (Level 3 features) comprised of covert (secret) features designed to be authenticated either by forensic examination or by specialist verification equipment. It is evident that knowledge of the precise substance and structure of such features should be restricted to very few people on a "need to know" basis. Among others, one purpose of these features is to enable authentication of documents where unequivocal proof of authenticity is a requirement (e.g., in a court of law). All travel documents should contain at least one covert security feature as a basic feature.

Important general standards and recommended practices for passport document validity period, one-person-one-passport principle, deadlines for issuance of Machine Readable Passports and withdrawal from circulation of non-MRPs and other guidance is found in ICAO Facilitation Annex 9.

There is no other acceptable means of data storage for global interoperability other than a contactless IC, specified by ICAO as the capacity expansion technology for use with MRTDs.

A.4 Main Threats to the Security of Travel Documents

The following threats to document security, listed in no particular order of importance, are identified ways in which the document, its issuance and use may be fraudulently attacked:

- counterfeiting a complete travel document;
- photo substitution;
- deletion/alteration of data in the visual or machine readable zone of the MRP data page;
- construction of a fraudulent document, or parts thereof, using materials from legitimate documents;
- removal and substitution of entire page(s) or visas;
- deletion of entries on visa pages and the observations page;
- theft of genuine document blanks;
- impostors (assumed identity; altered appearance); and
- tampering with the contactless IC (where present) either physically or electronically.

Detection of security features can be at any or all of the following three levels of inspection:

- Level 1 – cursory examination for rapid inspection at the point of usage (easily identifiable visual or tactile features);
- Level 2 – Examination by trained inspectors with simple equipment; and
- Level 3 – Inspection by forensic specialists.

To maintain document security and integrity, periodic reviews and any resulting revisions of document design should be conducted. This will enable new document security measures to be incorporated and to certify the document's ability to resist compromise and document fraud attempts regarding:

- photo substitution;
- delamination or other effects of deconstruction;
- Reverse engineering of the contactless IC as well as other components;
- modification of any data element;
- erasure or modification of other information;
- duplication, reproduction or facsimile creation;
- effectiveness of security features at all three levels: cursory examination, trained examiners with simple equipment and inspection by forensic specialists; and
- confidence and ease of second level authentication.

To provide protection against these threats and others, a travel document requires a range of security features and techniques combined in an optimum way within the document. Although some features can offer protection against more than one type of threat, no single feature can offer protection against them all. Likewise, no security feature is 100 per cent effective in eliminating any one category of threat. The best protection is obtained from a balanced set of features and techniques providing multiple integrated layers of security in the document that combine to deter or defeat fraudulent attack.

A.5 Security Features and Techniques

In the sections that follow, security features, techniques and other security measures are categorized according to the phases passed through during the production and personalization processes and the components of the travel document created thereby with regard to:

- 1) substrate materials;
- 2) security design and printing;
- 3) protection against copying, counterfeiting or fraudulent alteration; and
- 4) personalization techniques.

Issuing States are recommended to incorporate all of the basic features/measures and to select a number of additional features/measures from the list having first completed a full risk assessment of their travel documents. Unless otherwise indicated, the security features may be assumed to apply to all parts of a travel document including the cover and the binding of the booklet and to all the interior pages of a passport, comprising the biographical data page, end leaves and visa pages. Care must be taken to ensure that features do not interfere with the machine readability of the travel document.

A.5.1 Substrate Materials

A.5.1.1 Paper Forming the Pages of a Travel Document

Basic features:

- UV dull paper, or a substrate with a controlled response to UV, such that when illuminated by UV light it exhibits a fluorescence distinguishable in colour from the blue-white luminescence used in commonly available materials containing optical brighteners;
- watermark comprising two or more grey levels in the biographical data page and visa pages;
- appropriate chemical sensitizers in the paper, at least for the biographical data page (if compatible with the personalization technique); and
- paper with appropriate absorbency, roughness and weak surface tear.

Additional features:

- watermark in register with printed design;
- a different watermark on the data page to that used on the visa pages to prevent page substitution;
- a cylinder mould watermark;
- invisible fluorescent fibres;
- visible (fluorescent) fibres;
- security thread (embedded or window) containing additional security features such as micro print and fluorescence;
- a taggant designed for detection by special equipment, and
- a laser perforated security feature.

A.5.1.2 Paper or other Substrate in the Form of a Label Used as the Biographical Data Page of a Travel Document

Basic features:

- UV dull paper, or a substrate with a controlled response to UV, such that when illuminated by UV light it exhibits a fluorescence distinguishable in colour from the blue-white luminescence used in commonly available materials containing optical brighteners;
- appropriate chemical sensitizers in the paper (not normally possible in a plastic label substrate);
- invisible fluorescent fibres;
- visible (fluorescent) fibres; and
- a system of adhesives and/or other characteristics that prevents the label from being removed without causing clearly visible damage to the label and to any laminates or overlays used in conjunction with it.

Additional features:

- security thread (embedded or window) containing additional security features such as micro print and fluorescence;
- a watermark can be used in the paper of a data page in paper label form;
- a laser perforated security feature; and
- die cut security pattern within the label to create tamper evidence.

A.5.1.3 Security Aspects of Paper Forming the Inside Cover of a Passport Book

Paper used to form the inside cover of a passport book need not have a watermark. Although definitely not recommended, if an inside cover is used as a biographical data page (see A.5.5.1), alternative measures must be employed to achieve an equivalent level of security against all types of attack as provided by locating the data page on an inside page.

The paper forming the inside cover should contain appropriate chemical sensitizers when an inside cover is used as a biographical data page. The chemically sensitised paper should be compatible with the personalization technique, and the adhesive used to adhere the end paper to the cover material of the passport.

A.5.1.4 Synthetic Substrates

Where the substrate used for the biographical data page (or inserted label) of a passport book or MRTD card is formed entirely of plastic or a variation of plastic, it is not usually possible to incorporate many of the security components described in 5.1.1 through 5.1.3. In such cases additional security properties shall be included, including additional security printed features, enhanced personalization techniques and the use of optically variable features over and above the recommendations contained in 5.2 to 5.5.2. States should preferably ensure that the plastic substrate is manufactured under controlled conditions and contains distinctive properties, e.g. controlled fluorescence, to differentiate it from standard financial card substrates.

Basic Features:

- construction of the data page should be resistant to physical splitting into layers;
- UV dull substrate with a controlled response to UV, such that when illuminated by UV light it exhibits a fluorescence distinguishable in colour from the blue-white luminescence used in commonly available materials containing optical brighteners;
- appropriate measures should be used to incorporate the data page securely and durably into the machine readable travel document; and
- optically variable feature.

Additional features:

- windowed or transparent feature;
- tactile feature; and
- laser perforated feature.

A.5.2 Security Printing

A.5.2.1 Background and Text Printing

Basic features (see glossary of terms in Doc 9303-1):

- two-colour guilloche security background design pattern²;
- rainbow printing;
- microprinted text; and
- security background of the biographical data page printed in a design that is different from that of the visa pages or other pages of the document.

Additional features:

- single or multi-colour intaglio printing comprising a “black-line white-line” design on one or more of the end leaves or visa pages;
- latent (intaglio) image;
- anti-scan pattern;
- duplex security pattern;
- relief (3D) design feature;
- front-to-back (see-through) register feature.
- deliberate error (e.g. spelling);
- every visa page printed with a different security background design;
- tactile feature; and
- unique font(s).

A.5.2.2 Inks

Basic features:

- UV fluorescent ink (visible or invisible) on the biographical data page and all visa pages; and
- reactive ink, where the substrate of the document pages or of a label is paper, at least for the biographical data page (if compatible with the personalization technique).

2. Where the guilloche pattern has been computer-generated, the image reproduced on the document must be such that no evidence of a pixel structure shall be detectable. Guilloches may be displayed as positive images, where the image lines appear printed with white spaces between them, or as negative images, where the image lines appear in white, with the spaces between them printed. A two-colour guilloche is a design that incorporates guilloche patterns created by superimposing two elements of the guilloche, reproduced in contrasting colours.

Additional features:

- ink with optically variable properties;
- metallic ink;
- penetrating numbering ink; and
- metamerik ink;
- infrared drop-out ink;
- infrared absorbent ink;
- phosphorescent ink;
- tagged ink;
- invisible ink which fluoresces in different colours when exposed to different wave lengths.

A.5.2.3 Numbering

It is strongly recommended that the unique document number be used as the passport number.

Basic features:

- the passport number should appear on all sheets of the document and on the biographical data page of the document;
- the number in a document shall be either printed and/or perforated;
- the document number on a label shall be in a special style of figures or typeface and be printed with ink that fluoresces under ultraviolet light in addition to having a visible colour;
- the number on a data page of a passport made of synthetic substrate or on an MRTD card can be incorporated using the same technique as is used for applying the biographical data in the personalisation process; and
- for MRTD cards, the number should appear on both sides.

Additional features:

- if perforated, it is preferable that laser perforation is used. Perforate numbering of the data page is optional but, if used, care should be taken not to interfere with the clarity of the portrait or VIZ and not obstruct the MRZ in any way. It is desirable to perforate the cover of the passport; and
- if printed, it should ideally be in a special style of figures or typeface and be printed with an ink that fluoresces under ultraviolet light in addition to having a visible colour.

A.5.2.4 Special Security Measures for Use with Non-laminated Biographical Data Pages

The surface of the data page should be protected against soiling in normal use including regular machine reading of the MRZ, and against tampering.

If a page of a document is used for biographical data that is not protected by a laminate or an overlay as a protective coating (see 5.3.2, 5.4.3 and 5.4.4), additional protection shall be provided by the use of intaglio printing incorporating a latent image and microprinting and preferably utilizing a colour-shifting ink (e.g. ink with optically variable properties).

A.5.2.5 Special Security Measures for Use with Cards and Biographical Data Pages Made of Plastic

Where a travel document is constructed entirely of plastic, optically variable security features shall be employed which give a changing appearance with angle of viewing. Such devices may take the form of latent images, lenticular features, colour-shifting ink, or diffractive optically variable image features.

A.5.3 Protection Against Copying

A.5.3.1 Need for Anti-copy Protection

The current state of development of generally available digital reproduction techniques and the resulting potential for fraud means that high-grade security features in the form of optically variable features or other equivalent devices will be required as safeguards against copying and scanning. Emphasis should be placed on the security of the biographical data page of a passport book, travel

card or visa, based on an independent, complex optically variable feature technology or other equivalent devices complementing other security techniques. Particular emphasis should be given to easily identifiable, visual or tactile features which are examined at Level 1 inspection.

Appropriate integration of optically variable feature components or other equivalent devices into the layered structure of the biographical data page should also protect the data from fraudulent alteration. The optically variable components and all associated security materials used to create the layered structure must also be protected against counterfeiting.

A.5.3.2 Anti-copy Protection Methods

Subject to the minimum recommendations described in 5.4.3 and 5.4.4 on the need for lamination, optically variable features should be used on the biographical data page of a passport book, travel card or visa as a *basic feature*.

When a biographical data page of a passport book, travel card or visa is protected by a laminate film or overlay, an optically variable feature (preferably based on diffractive structure with tamper evident properties) should be integrated into the page. Such a feature should not affect the legibility of the entered data.

When the biographical data page is an encapsulated paper label, or a page in a passport, the biographical data must be suitably protected by a protective laminate or measures providing equivalent security in order to deter alteration and/or removal.

When the machine readable biographical data page of a passport book is made entirely of synthetic substrate, an optically variable feature should be incorporated. The inclusion of a diffractive optically variable feature is recommended to achieve an enhanced level of protection against reproduction.

Devices such as a windowed or transparent feature, a laser perforated feature, and others are considered to offer equivalent protection may be used in place of an optically variable feature.

When the travel document has no overlay or laminate protection, an optically variable feature (preferably based on diffractive structure) with intaglio overprinting or other printing technique shall be used.

A.5.4 Personalization Technique

A.5.4.1 Document Personalization

This is the process by which the portrait, signature and/or other biographical data relating to the holder of the document are applied to the travel document. These data record the personalized details of the holder and are at the greatest risk of counterfeit or fraudulent alteration. One of the most frequent types of document fraud involves the removal of the portrait image from a stolen or illegally obtained travel document and its replacement with the portrait of a different person. Documents with stick-in portrait photographs are particularly susceptible to photo substitution. Therefore, stick-in photographs are NOT permitted in MRTDs.

A.5.4.2 Protection Against Alteration

To ensure that data are properly secured against attempts at forgery or fraudulent alteration it is very strongly recommended to integrate the biographical data, including the portrait, signature (if it is included on the biographical data page) and main issue data, into the basic material of the document. A variety of technologies are available for personalizing the document in this way, including the following, but not precluding the development of new technologies, which are listed in no particular order of importance:

- laser toner printing;
- thermal transfer printing;
- ink-jet printing;
- photographic processes; and

- laser engraving.

The same personalizing technologies may also be used to apply data to the observations page of the passport. Laser toner should not be used to personalise visas or other security documents that are not protected by a secure laminate.

Authorities should carry out testing of their personalisation processes and techniques against malfeasance.

A.5.4.3 Choice of Document System

The choice of a particular technology is a matter for individual Issuing States and will depend upon a number of factors, such as the volume of travel documents to be produced, the construction of the document and whether it is to be personalized during the document or passport book making process or after the document or book has been assembled and whether a country issues passports centrally or from decentralised sites.

Whichever method is chosen, it is essential that precautions be taken to protect the personalized details against tampering. This is important because, even though eliminating the stick-in portrait reduces the risk of photo substitution, the unprotected biographical data remains vulnerable to alteration and needs to be protected by the application of a heat-sealed (or equivalent) laminate with frangible properties, or equivalent technology that provides evidence of tampering.

A.5.4.4 Protection Against Photo Substitution and Alteration of Data on the Biographical Data Page of a Passport Book

Basic features:

- personalizing the portrait and all biographical data by integration into the basic material;
- the security printed background (e.g., guilloche) shall merge within the portrait area;
- use of reactive ink and chemical sensitizers in the paper;
- there should be a visible security device overlapping the portrait without obstructing the visibility of the portrait; an optically variable feature is recommended; and
- use of a heat-sealed (or equivalent) secure laminate, or the combination of an personalizing technology and substrate material that provide an equivalent resistance to substitution and/or counterfeit of the portrait and other biographical data.

Additional features:

- displayed signature of the holder may be scanned and incorporated into the printing;
- steganographic image incorporated in the document;
- additional portrait image(s) of holder;
- machine-verifiable features as detailed in Doc 9303 9-12.

A.5.5 Additional Security Measures for Passport Books

A.5.5.1 Position of the Biographical Data Page

It is recommended that States place the data page on an inside page (the second or penultimate page). When the data page is situated on the inside cover of a MRP, the normal method of construction used in the manufacture of passport covers has facilitated fraudulent attacks on the data page, typically photo substitution or whole-page substitution. However, an Issuing State may place the data page on a cover provided that it ensures that the construction of the cover used in its passport offers a similar level of security against all types of fraudulent attack to that offered by locating the data page on an inside page. Placing the biographical data page on the cover is, nevertheless, strongly NOT recommended.

A.5.5.2 Whole-page Substitution

Issuing States' attention is drawn to the fact that with integrated biographical data pages replacing stick-in photographs in passports, some cases of whole-page substitution have been noted in which the entire biographical data page of the passport has been removed and substituted with a fraudulent one. Although whole-page substitution is generally more difficult to effect than photo substitution of a

stick-in photo, nevertheless, it is important that the following recommendations be adopted to help in combating this category of risk. As with all other categories of document fraud it is better to employ a combination of security features to protect against whole-page substitution rather than relying on a single feature which, if compromised, could undermine the security of the whole travel document.

Basic features:

- the sewing technology that binds the pages into the book must be such that it must be difficult to remove a page without leaving clear evidence that it has happened;
- security background of the biographical data page printed in a design that is different from that of the visa pages;
- page numbers integrated into the security design of the visa pages; and
- serial number on every sheet, preferably perforated.

Additional features:

- multi-colour and/or specifically UV fluorescent sewing thread;
- programmable thread-sewing pattern;
- UV cured glue applied to the stitching;
- index or collation marks printed on the edge of every visa page;
- laser perforated security features to the biographical data page; and
- biographical data printed on an inside page in addition to the data page.

Where self-adhesive labels are used, additional security requirements as described in A.5.1.2 and A.5.2.4 are advised including linking the label to the machine readable travel document by the travel document number.

A.5.6 Quality Control

Quality checks and controls at all stages of the production process and from one batch to the next are essential to maintain consistency in the finished travel document. This should include quality assurance (QA) checks on all materials used in the manufacture of the documents and the readability of the machine readable lines. The importance of consistency in the finished travel document is paramount because immigration inspectors and border control officers rely upon being able to recognize fake documents from variations in their appearance or characteristics. If there are variations in the quality, appearance or characteristics of a State's genuine travel documents, detection of counterfeit or forged documents is made more difficult.

A.5.7 Security Control of Production and Product

A major threat to the security of the MRP of an Issuing State can come from the unauthorized removal from the production facility of genuine finished, but unpersonalized, MRPs or the components from which MRPs can be made.

A.5.7.1 Protection Against Theft and Abuse of Genuine Document Blanks or Document Components

Blank documents should be stored in locked and appropriately supervised premises. The following measures should be adopted:

Basic measures:

- good physical security of the premises with controlled access to delivery/shipment and production areas, and document storage facilities;
- full audit trail, with counting and reconciliation of all materials (used, unused, defective or spoiled) and certified records of same;
- all document blanks and other security-sensitive components serially numbered with full audit trail for every document from manufacture to dispatch, as applicable;
- where applicable, tracking and control numbers of other principal document components (e.g. rolls or sheets of laminates, optically variable feature devices);
- secure transport vehicles for movement of blank documents and other principal document components (if applicable);
- details of all lost and stolen travel document blanks to be rapidly circulated between

governments and to border control authorities with details sent to the INTERPOL lost and stolen database;

- appropriate controls to be in place to protect the production procedures from internal fraud; and
- security vetting of staff.

Additional measures:

- CCTV coverage/recording of all production areas, where permitted, and
- Centralized storage and personalisation of blank documents in as few locations as possible.

Table 1: Summary of Security Recommendations

Elements	Basic features	Additional features
Substrate materials (A.5.1)		
Paper substrates (A.5.1.1)	<ul style="list-style-type: none"> – controlled UV response – two-tone watermark – chemical sensitizers – appropriate absorbency and surface characteristics 	<ul style="list-style-type: none"> – registered watermark – different watermark on the data page and visa page – cylinder mould watermark – invisible fluorescent fibres – visible (fluorescent) fibres – security thread – taggant – laser perforated security feature
Paper or other substrate in the form of a label (A.5.1.2)	<ul style="list-style-type: none"> – controlled UV response – chemical sensitizers – invisible florescent fibres – visible (florescent) fibres – system of adhesives 	<ul style="list-style-type: none"> – security thread – watermark – laser perforated security feature – die cut security pattern
Synthetic substrates (A.5.1.4)	<ul style="list-style-type: none"> – construction resistant to splitting – optically dull material – secure incorporation of data page – optically variable features – see 5.2 – 5.5 as appropriate 	<ul style="list-style-type: none"> – window or transparent feature – tactile feature – laser perforated feature
Security printing (A.5.2)		
Background and text printing (A.5.2.1)	<ul style="list-style-type: none"> – two-colour guilloche background – rainbow printing – microprinted text – unique data page design 	<ul style="list-style-type: none"> – intaglio printing – latent image – anti-scan pattern – duplex security pattern – relief design feature – front-to-back register feature – deliberate error – unique design on every page – tactile feature – unique font(s)

Elements	Basic features	Additional features
Inks (A.5.2.2)	<ul style="list-style-type: none"> – UV florescent ink – reactive ink 	<ul style="list-style-type: none"> – ink with optically variable properties – metallic ink – penetrating numbering ink – metameric ink – infrared drop-out ink – infrared absorbent ink – phosphorescent ink – tagged ink – invisible ink
Numbering (A.5.2.3)	<ul style="list-style-type: none"> – numbering on all sheets – printed and/or perforated number – special typeface numbering for labels – identical technique for applying numbering and biographical data on synthetic substrates and cards 	<ul style="list-style-type: none"> – laser perforated document number – special typeface
Personalization technique (A.5.4)		
Protection against photo substitution and alteration (A.5.4.4)	<ul style="list-style-type: none"> – integrated biographical data – security background merged within portrait area – reactive inks and chemical sensitizers in paper – visible security device overlapping portrait area – heat-sealed secure laminate or equivalent 	<ul style="list-style-type: none"> – displayed signature – steganographic image – additional portrait image(s) – biometric feature as per Volume 2
Additional security measures for passport books (A.5.5)		
Page substitution (A.5.5.2)	<ul style="list-style-type: none"> – secure sewing technology – UV fluorescent sewing thread – unique data page design – page numbers integrated into security design – serial number on every sheet 	<ul style="list-style-type: none"> – multi-colour sewing thread – programmable sewing pattern – UV cured glue to stitching – index marks on every page – laser perforated security feature – biographical data on inside page
Security control of production and product (A.5.7)		

Elements	Basic features	Additional features
Protection against theft and abuse (A.5.7.1)	<ul style="list-style-type: none"> – good physical security – full audit trail – serial numbers on blank documents as applicable – tracking and control numbers of components as applicable – secure transport of blank documents – international information exchange on lost and stolen documents – internal fraud protection procedures – security vetting of staff 	<ul style="list-style-type: none"> – CCTV in production areas – centralized storage and personalization

Note 1: The list of additional features is not exhaustive and Issuing States and organizations are encouraged to adopt other security features not explicitly mentioned in this Appendix.

Note 2: The descriptions in the table above are necessarily abbreviated from the main text. For ease of reference, the relevant sections of this Appendix are referenced by the paragraph numbers in parentheses in the “Elements” column of the above table.

Note 3: Certain of the features are repeated one or more times in the table. This indicates that the particular feature protects against more than one type of threat. It is only necessary to include these features once within any particular document.

Note 4: There are many other factors associated with passport security than are elaborated here. Appendices B and C provide additional guidance. Therefore, Appendices A, B, and C need to be considered collectively to ensure document issuance integrity.

Note 5: Any reference, direct or implied, to specific terms and/or technologies are solely intended to capture the terms and technologies in their generic form and do not have any association with specific vendors or technology providers.

APPENDIX B MACHINE ASSISTED DOCUMENT SECURITY VERIFICATION (INFORMATIVE)

B.1 Scope

This Appendix contains recommendations which cover machine authentication of the security features in the document itself (based on materials, on security printing and on copy protection techniques) as well as advice on reader technologies that apply to machine authentication of documents.

B.2 Document Readers and Systems for Machine Authentication

In order to verify traditional as well as innovative security features of MRTDs, it is important to have reading technology in place which accommodates the wide variety of travel documents in circulation. These readers have to be equipped with the appropriate sensors for the more common and advanced machine authentication features. This, of course, is a worldwide cost and infrastructure issue.

B.2.1 Standard Readers

Standard readers which are deployed at borders usually have the following hardware sensors:

- VIS, UV, IR illumination and high resolution image grabbing capabilities (minimum resolution 300 dpi) - this allows for reading the MRZ (preferably in the IR spectral range) and image processing of other features (in the VIS spectral range); and
- ISO 14443 compliant contactless IC readers (@ 13.56 MHz frequency).

Generally, standard readers are able to detect and verify the following security features:

- MRZ read & check digit verification;
- Contactless IC read & Passive Authentication (and, optionally, Active Authentication); and
- generic security checks (UV dull paper, IR readable MRZ, ...).

Further “intelligence” of these readers solely depends on software, not on extra hardware sensors, and would therefore easily be deployed at the discretion of the receiving state without investing extra money for dedicated equipment. Software capabilities of readers may include:

- pattern recognition using databases (based on VIS, UV and IR images);
- read & authenticate digital watermarks (steganographic features) to check for authentic issuance;
- detect and read out (alphanumeric) displays and their future security features; and
- detect and read out LED-in-plastic based security features.

B.2.2 Advanced Readers

Additionally, advanced readers may have the following hardware sensors, suited to authenticate special security features:

- Coaxial illumination for the verification of retro-reflective security overlays;
- laser diode or LED illumination for the verification of special structure features, e.g. for optically diffractive devices (DOVIDs);
- magnetic sensors for special substrate features, e.g. for the verification of magnetic fibres;
- spectral analysis or polarization detection devices; and
- transmission illumination of the MRP data page for the verification of registered watermarks, laser perforation, window-features and see-through registers – needs a special reader geometry to allow for the placement of the data page only (no cover behind) on the reader

Usually, advanced reading capabilities are all based on national/bilateral/multilateral/proprietary agreements and require dedicated hardware.

B.2.3 Background Systems, Public Key Infrastructure (PKI)

To authenticate certain types of machine verifiable features, a background system or a PKI may be necessary. This could be the existing MRTD PKI (the ICAO PKD being the most prominent part)

where States may exchange information on their security features within the logical data structure, secured by means of certificates.

B.3 Security Features and their Application for Machine Authentication

The following paragraphs describe major security features and techniques as identified in Appendix A on Security Standards and explain how machine authentication could be deployed for these security mechanisms. Issuing Authorities which selected security features from Appendix A may use the tables below to check what possibilities of machine authentication are in existence for such features.

B.3.1 Substrate Materials

B.3.1.1 Paper Forming the Pages of a Travel Document

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
Controlled UV response		X					UV intensity
Two-tone watermark					Transmission	F	pattern matching
Chemical sensitizers							N/A
Appropriate absorbency and surface characteristics							N/A
Additional features							
Registered watermark					Transmission	F	pattern matching
Different watermark on the data page and visa page					Transmission	F	pattern matching*
Cylinder mould watermark					Transmission	F	pattern matching
Invisible fluorescent fibers		X	X			F/V	pattern matching
Visible (fluorescent) fibers	X	X				F/V	pattern matching
Security thread	X	X			Transmission, Magnetic	F	pattern matching
Taggant					Special	F/V	Depends on taggant

Laser perforated security feature					Transmission	F/V	pattern matching
-----------------------------------	--	--	--	--	--------------	-----	------------------

* User interaction required and not suitable for Automated Border Control systems

B.3.1.2 Paper or other Substrate in the Form of a Label

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
Controlled UV response		X					UV intensity
Chemical sensitizers							N/A
Invisible fluorescent fibers		X	X			F/V	pattern matching
Visible (fluorescent) fibers	X	X				F/V	pattern matching
System of adhesives							N/A
Additional features							
Security thread	X				Transmission, Magnetic	F	pattern matching
Watermark					Transmission	F	N/A
Laser perforated security feature					Transmission	F/V	pattern matching
Die cut security pattern					Transmission	F	pattern matching

B.3.1.3 Synthetic Substrates

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
Construction resistant to							N/A

splitting							
Optically dull material		X					UV intensity
Secure incorporation of data page							N/A
Optically variable features							See 5.3
See 5.2 – 5.5 as appropriate							
Additional features							
Window or transparent feature					Transmission	F	pattern matching
Tactile feature					Retro-reflective	F/V	pattern matching
Laser perforated feature					Transmission	F/V	pattern matching
Surface characteristics	X		X		Retro-reflective	F	pattern matching

B.3.2 Security Printing

B.3.2.1 Background and Text Printing

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
Two-colour guilloche background	X	X	X			F	Pattern matching
Rainbow printing	X	X			High camera res	F	Pattern matching
Microprinted text	X	X	X		High camera res	F	Pattern matching
Unique data page design	X					F	Pattern matching
Additional features							
Intaglio printing	X	X	X			F	Pattern

							matching*
Latent image							N/A
Anti-scan pattern	X				High res camera	F	Pattern matching
Duplex security pattern					Transmission	F	Pattern matching*
Relief design feature					Retro-reflective	F	pattern matching
Front-to-back register feature					Transmission	F	Pattern matching
deliberate error	X	X	X			F	OCR, Pattern matching
Unique design on every page	X	X				F	Pattern matching#
Tactile feature					Retro-reflective	F	pattern matching
Unique font(s)	X	X	X				Pattern matching

* Impractical implementation for passport readers

User interaction required and not suitable for Automated Border Control systems

B.3.2.2 Inks

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
UV florescent ink		X				F/V	Pattern matching
Reactive inks					Special		Depending on ink
Additional features							
ink with optically variable properties	X				Variable illumination	F/V	Pattern matching

Metallic ink			X			F/V	Pattern matching
Penetrating numbering ink					Special	V	Pattern matching on both sides
Metameric inks	X	X	X			F	Optical filters and Pattern matching
Infrared dropout ink	X		X			F/V	Pattern matching
Infrared absorbent ink			X			F/V	Pattern matching
Phosphorescent ink		X	X			F/V	Pattern matching
Tagged ink					Special	F	Pattern matching
Invisible ink		X	X			F	Pattern matching
Magnetic ink					Magnetic	F/V	Pattern matching
Anti-Stokes-Ink			X			F/V	Optical filters and pattern matching

B.3.2.3 Numbering

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
Numbering on all sheets Printed and/or perforated number	X		X			F/V	OCR, Pattern matching
Special typeface numbering for labels	X		X			F/V	OCR, Pattern matching
Identical technique for applying numbering and biographical data on							N/A

Basic features							
Integrated biographical data							N/A
Security background merged within portrait area							N/A
Reactive inks and chemical sensitizers in paper							N/A
Visible security device overlapping portrait area	X				Variable illumination	F/V	Pattern matching
Heat-sealed secure laminate or equivalent	X					F/V	Pattern matching
Additional features							
Displayed signature							N/A
Steganographic feature	X	X	X			F/V	Decoding
Additional portrait image(s)	X	X	X	X		V	Pattern matching
Biometric feature as per Volume 2				X		V	RF reader

B 3.5 Additional Security Measures for Passport Books

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
Secure sewing technology							N/A
UV fluorescent sewing thread		X				F	Pattern matching
Unique data page design	X					F	Pattern matching
Page numbers integrated into security design	X	X			High camera res		Pattern matching

Serial number on every sheet							N/A
Additional features							
Multi-color sewing thread	X	X				F	Pattern matching
Programmable sewing pattern	X	X				F	Pattern matching
UV cured glue to stitching							N/A
Index marks on every page							N/A
Laser perforated security feature					Transmission	F/V	Pattern matching
Biographical data on inside page							N/A

B 3.6 Additional Security Measures Suited for Machine Authentication

The following security features are suited for machine authentication but are not listed in Appendix A.

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
MRZ read & check digit verification	X		X			F/V	Checksum calculation
Contactless IC read & Passive Authentication (+AA)				X			RF reader
detect and read out LED-in-plastic based security features	X	X	X	X		F/V	Use R/F to power LED in plastic
detect and read out (alphanumeric) displays and their future security features	X	X	X	X		F/V	Use R/F to power display in plastic
Detect & verify retro-reflective foil material	X				Coaxial lighting	F/V	Pattern matching

Barcodes	X	X	X			V	Decoding
----------	---	---	---	--	--	---	----------

B.4 Selection Criteria for Machine Verifiable Security Features

If an Issuing State considers incorporating security features for machine authentication in its MRTDs or a Receiving State plans to deploy readers systems which are able to machine authenticate MRTDs, various criteria for the selection of these features have to be considered.

Much like the selection process for the global interoperable biometric or the storage technology, these criteria comprise:

- security - most important criteria;
- availability, but exclusiveness for security documents (preferably more than one supplier available);
- dual-use, i.e. additional purpose of the feature beyond machine authentication, e.g. general anti-copy property or visual inspection;
- potential of the Machine Authentication feature to be personalized (i.e. individualized) with information from the passport to secure the personal data (e.g. the passport number, name etc.) in order to avoid re-use of parts of genuine passports;
- compatibility to issuing processes for MRTDs;
- compatibility (to existing and standardized properties of MRTDs);
- compatibility to control process at the border and elsewhere (e.g. no obstruction of basic security features, no extra time needed etc.);
- interoperability;
- sensor availability ;
- cost (for feature & sensor);
- Intellectual Property (IP) issues, e.g. patents;
- primary inspection vs. secondary;
- time required to actually utilize the feature;
- potential difficulties associated with the book manufacturing and/or the personalization processes; and
- durability, i.e. according to the relevant ISO and ICAO specifications for MRTDs

APPENDIX C THE PREVENTION OF FRAUD ASSOCIATED WITH THE ISSUANCE PROCESS (INFORMATIVE)

C.1 Scope

This Appendix describes the fraud risks associated with the process of MRTD application and issuance. These risks are a consequence of the benefits that can accrue from the possession of an MRTD that can be used to confirm the identity and citizenship of the holder. The Appendix recommends precautions that an Issuing State can take to prevent such fraud.

C.2 Fraud and its Prevention

Fraud perpetrated as part of the issuance process can be of several major types:

- theft of genuine blank MRTDs and completion to make them look valid;
- applying for the MRTD under a false identity using genuine evidence of nationality and/or identity stolen from another individual, or otherwise obtained improperly;
- applying for the MRTD under a false identity using manufactured false evidence of nationality and/or identity;
- using falsely declared or undeclared lost and/or stolen MRTDs that can be provided to people who might use them in look-alike fraud or with repetitive photo substitutions; and
- reliance on MRTD employees to manipulate the MRTD system to issue an MRTD outside the rules.

There are two additional categories in which the applicant applies under his own identity but with the intention to be complicit in the later fraudulent use of the MRTD by:

- altering a genuinely issued document to make it fit a bearer who is not the person to whom the MRTD was issued; and
- applying for an MRTD with the intention of giving or selling it to someone who resembles the true bearer.

C.3 Recommended Measures Against Fraud

To combat the above-mentioned threats, it is recommended that the MRTD-issuing authority of the State undertake the following measures, to the extent that adequate resources are available for their implementation.

A suitably qualified person should be appointed to be Head of Security directly responsible to the Chief Executive Officer of the Issuing Authority. The Head of Security should be responsible for ensuring that security procedures are laid down, observed and updated as necessary.

In each location where MRTDs are issued there should be a designated Security Manager. The Security Manager should be responsible for the implementation and updating of the security procedures and report directly to the Head of Security.

Vetting procedures should be established to ensure that all staff are recruited only after searches have verified their identity, ensured that they have no criminal record, and verified that their financial position is sound. Regular follow-up checks should also be made to detect staff whose changed circumstances mean they may succumb to temptations to engage in fraudulent activity.

All staff within the MRTD-issuing authority should be encouraged to adopt a positive attitude toward security matters. There should be a system of rewards for any staff member who reports incidents or identifies measures that prevent fraud.

Controls should be established that account for key components such as blank books and security laminates. Such items should each bear a unique serial number and should be kept locked in suitable secure storage. Only the required number should be issued at the start of each working day or shift. The counting of the items should be done and the figures agreed by two members of staff who should

also record the unique numbers of the items. The person to whom they are issued must account for all items at the end of the shift in the form of either personalized documents or defective product. All items should be returned to the secure store at the end of the working period, again having been counted by two people and the unique numbers logged. The records should be kept at least for the life of the issued MRTDs.

Defective product or materials should be destroyed under controlled conditions and the unique numbers recorded.

The issuance process should be divided into discrete operations that are carried out in separate locations within the facility. The purpose is to ensure that no one person can carry out the whole issuance process without venturing into one or more areas that the person has no authorization to enter.

C.4 Procedures to Combat Fraudulent Applications

The following procedures are recommended to prevent the issue of a genuine MRTD as a result of receipt of a fraudulent application.

The MRTD-issuing office should appoint an appropriate number of anti-fraud specialists (AFS) who have received a high level of training in the detection of all types of fraud used in MRTD application. There should be at least one AFS present in each location in which MRTD applications and applicants are processed. An AFS should at all times be available to support those whose task it is to process applications (Authorizing Officers [AO]) and thus to provide assistance in dealing with any suspicious application. AFS personnel should regularly provide training to AOs to increase their awareness of potential fraud risks.

The MRTD-issuing authority should establish close liaisons with the issuers of breeder documents such as birth and marriage certificates and driving licences. Access to a database of death certificates assists in the prevention of fraud where an application for an MRTD is made in the name of a deceased person. The State should ensure that the departments holding records of births, marriages and deaths are reconciled and the data stored in a database, secure access to which should be available to the MRTD-issuing office. The aim is to facilitate rapid verification that submitted breeder documents are genuine and that an application is not being made, for example, in the name of a deceased person.

An applicant for an MRTD who has not held one previously should be required to present himself at an MRTD-issuing office with supporting breeder documentation for an interview with an AO and, where necessary, an AFS.

An interview may also be used to process applications for an MRTD to replace an expiring one. Alternatively, provided the MRTD-issuing office has an adequate database of personal information, including portraits, a replacement application may be processed by submission of the documentation, including a new portrait, by mail. In such cases it is desirable that the application and new portrait be endorsed by a responsible person. The return of the expiring MRTD with the new application should be required.

The MRTD-issuing office should initiate procedures that would prevent the fraudulent issue of more than one MRTD to an individual who may have attempted to assume more than one identity. Computer database checks of stored portraits using facial recognition and, where available, fingerprints can assist in this process.

Procedures in the MRTD-issuing office should prevent an applicant from selecting the AO who will serve him. Conversely the work flow should be such as to prevent any employee from selecting which applications he is to process.

The issuance of an MRTD to a young child should require the attendance at the issuing office of, preferably, both parents and of the child. This is to lower the risk of child smuggling or abduction of a child by one parent.

The replacement of an MRTD claimed to be lost or stolen should be made only after exhaustive checks including a personal interview with the applicant.

It is recommended that details, particularly document numbers, of lost or stolen MRTDs be provided to the database operated by INTERPOL. This database is available to all participating countries and can be used in the development of watch lists.

C.5 Control of Issuing Facilities

A State should consider issuing all MRTDs from one or, at most, two centres. This reduces the number of places where blank documents and other secure components are stored. The control of such a central facility can be much tighter than is possible at each of many issuing centres. If central issuance is adopted, the provision of centres where applicants can attend interviews is required. Furthermore, since standard MRTDs cannot be issued instantly, a system should be established for the issue of emergency MRTDs.

DRAFT_4 FOR TAG_2

Doc 9303



Machine Readable Travel Documents

Part 3
Specifications Common to all Machine Readable Travel Documents

Approved by the Secretary General
and published under his authority

Seventh Edition - Revision 1 - 2014

International Civil Aviation Organization

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

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

Doc 9303, Machine Readable Travel Documents
Order Number: xxxx
ISBN xxx-xx-xxxx-xxx-x

© ICAO 2014

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 TO DOC 9303-3, 7TH EDITION

Revision	Date	Description
01	xx-xx-2014	Initial release of the 7 th edition

DRAFT_4 FOR TAG_22

TABLE OF CONTENTS

1	SCOPE	3
2	PHYSICAL CHARACTERISTICS OF MRTDS	4
3	VISUAL INSPECTION ZONE (VIZ)	5
3.1	Languages and Characters.....	5
3.2	Typeface and Type Size	5
3.3	Captions/Fields	5
3.4	Convention for Writing the Name of the Holder	6
3.5	Representation of Issuing State or Organization	6
3.6	Representation of Nationality	6
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
5	CODES FOR NATIONALITY, PLACE OF BIRTH, LOCATION OF ISSUING STATE/AUTHORITY AND OTHER PURPOSES	23
6	TRANSLITERATIONS RECOMMENDED FOR USE BY STATES	28
APPENDIX A	EXAMPLES OF CHECK DIGIT CALCULATION (INFORMATIVE)	35
APPENDIX B	ARABIC TRANSLITERATION – DETAILS AND EXAMPLES (INFORMATIVE)	39
B.1	Example of Transliteration for Standard Arabic	39
B.2	Recommended Transliteration Scheme for Other Languages	40
B.3	Recommended Transliteration Scheme for Moroccan, Tunisian and Maghrib Arabic	41
	REFERENCES (NORMATIVE)	42

1 SCOPE

The seventh edition of Doc 9303 represents a restructuring of the ICAO specifications for Machine Readable Travel Documents. Without incorporating substantial modifications of 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 3 of Doc 9303 is based on Doc 9303 Part 1 Volume 1, Machine Readable Passports – Passports with Machine Readable Data Stored in Optical Character Recognition Format (Sixth Edition 2006) and Doc 9303 Part 3 Volume 1, Machine Readable Official Travel Documents – MRtds with Machine Readable Data Stored in Optical Character Recognition Format (Third Edition 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 form factor appear in Doc 9303 Parts 4 through 7.

Part 3 should be read in conjunction with:

- Part 1 - Introduction;
- Part 2 - Specifications for the Security of the Design, Manufacture and Issuance of Machine Readable Travel Documents;

and the relevant form factor specific part:

- Part 4 - Specifications Specific to Machine Readable Passports (MRP's) and other TD3 Size Machine Readable Travel Documents (MRTD's);
- Part 5 - Specifications Specific to TD1 Size MROTD's, Machine Readable Official Travel Documents;
- Part 6 - Specifications Specific to TD2 Size MROTD's, Machine Readable Official Travel Documents; and
- Part 7- Machine Readable Visas.

These specifications also apply to machine readable travel documents that contain a contactless IC i.e. electronic machine readable travel documents (eMRTDs). Specifications specific to eMRTDs are contained in the following parts of Doc 9303:

- Part 9 - The Deployment of Biometric Identification and the Electronic Storage of Data in MRTDs;
- Part 10 - Logical Data Structure (LDS) for Storage of Biometrics and other Data in the Contactless IC;
- Part 11 - Security Mechanisms for Machine Readable Travel Documents; and
- Part 12 - Public Key Infrastructure for Machine Readable Travel Documents.

3 VISUAL INSPECTION ZONE (VIZ)

The Visual Inspection Zone of an MRTD comprises the mandatory and optional data elements designed for visual inspection. The optional data elements, together with the mandatory data elements, accommodate the diverse requirements of Issuing States and organizations while maintaining sufficient uniformity to ensure global interoperability for all MRTDs.

3.1 Languages and Characters

Latin-alphabet characters, i.e. A to Z, and Arabic numerals, i.e. 1234567890 shall be used to represent data in the VIZ. Diacritics are permitted. Latin-based national characters listed in Section 6 A – Transliteration of Multinational Characters, e.g. P and ß, may also be used in the VIZ without transliteration. When mandatory data elements are in a national language that does not use the Latin alphabet, a transliteration shall also be provided.

States that use other than Arabic numerals to represent numerical data in the VIZ shall provide a translation into Arabic numerals.

In the interests of facilitation optional data elements should be entered in both the national language and either English, French or Spanish. Optional data in Zone VI may be entered entirely in the national script and/or language.

3.2 Typeface and Type Size

The horizontal printing density, the typeface, the type size, the font and the vertical line spacing in the VIZ is at the discretion of the Issuing State or organization. For good legibility a type size with 10 characters per 25.4 mm (1.0 in) is recommended. A maximum of 15 characters per 25.4 mm (1.0 in) should not be exceeded. This type size has been chosen as the smallest in which information is clear and legible to a person with normal eyesight.

Use of upper-case characters is recommended. However, where a name includes a prefix, an appropriate mixture of upper and lower case characters may be used in the prefix (see 3.4 in this section).

Diacritical marks (accents) may be used with either lower- or upper-case characters at the option of the Issuing State or organization.

3.3 Captions/Fields

Captions shall be used to identify all fields for mandatory data elements in the VIZ except as specified in the data element directories for each form factor in Doc 9303 Parts 4-7.

Captions may be in the official language of the Issuing State or working language of the issuing organization. When such language uses the Latin alphabet, straight font style should be used to print the captions.

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

Where the official language of the Issuing State or working language of the issuing 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. An italic font style should be used for the second language.

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).

When an optional field is not used, the caption shall not appear on the travel document.

3.4 Convention for Writing the Name of the Holder

The name of the holder is generally represented in two parts; the primary identifier and the secondary identifier.

The Issuing State or organization shall establish which part of the name is the primary identifier. This may be the family name, the maiden name or the married name, the main name, the surname, and in some cases, the entire name where the holder's name cannot be divided into two parts. This shall be entered in the field for the primary identifier in the VIZ. It is recommended that upper-case characters be used, except in the case of a prefix, e.g. "von," "Mc" or "de la," in which case a mixture of upper and lower case is appropriate.

The remaining parts of the name are the secondary identifier. These may be the forenames, familiar names, given names, initials, or any other secondary names. These names shall be written in the field for the secondary identifier in the VIZ. It is recommended that upper-case characters be used throughout.

If a single field is used for the name, then the secondary identifier should be separated from the primary identifier by a single comma (,). A comma is not needed if multiple fields are used.

Prefixes and suffixes including titles, professional and academic qualifications, honours, awards, and hereditary status, should not be included in the VIZ. However, if an Issuing State or organization considers such a prefix or suffix to be legally part of the name, the prefix or suffix can appear in the VIZ. Numeric characters should not be written in the name fields of the VIZ; however, where the use of numeric characters is a legal naming convention in the Issuing States, these should be represented in Roman numerals. Any prefixes, suffixes or Roman numerals shall be entered in the secondary identifier field.

National characters may be used in the VIZ. If the national characters are not Latin-based, a transliteration into Latin characters shall be provided.

3.5 Representation of Issuing State or Organization

Where the name of the Issuing State or organization and/or the location of the issuing office or authority are in a national language that does not use Latin characters, the name of the State or other location 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) by 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.

Where the name of the Issuing State or organization or location of the issuing office or authority is in a language that uses the Latin alphabet, but 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.

3.6 Representation of Nationality

The nationality of the holder in the VIZ, in documents where this field is mandatory, shall be represented either by the three-letter code (see Section 5) or in full at the discretion of the Issuing State.

If the nationality is written in full and the national language of the Issuing State or working language of the issuing organization is a language that does not use Latin characters, the nationality 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) by which the nationality may be more commonly known to the international community.

The nationality in the different languages shall be separated by an oblique character (/) followed by at least one blank space.

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

3.7 Representation of Place of Birth

Inclusion of the place of birth is optional. If the place of birth is included it may be represented by the town, the city, the suburb, and/or the state.

If the town, city, or suburb are included and the national language of the Issuing State is a language that does not use Latin characters, the town, city, or suburb 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) by which they may be more commonly known to the international community.

The town, city, or suburb in the different languages shall be separated by an oblique character (/) followed by at least one blank space.

Where the national language of the Issuing State or working language of the issuing organization uses the Latin alphabet, but the town, city, or suburb is more familiar to the international community in its translation into another language or languages (particularly English, French or Spanish), the town, city, or suburb in the national language should be accompanied by one or more translations. The town, city, or suburb in the different languages shall be separated by an oblique character (/) followed by at least one blank space.

If the state is included it shall be represented by its ICAO three-letter code (see Section 5) except where no code for the state of birth exists, in which case the name shall be written in full and the requirements for translation and transliteration identified for town, city and suburb above apply.

Note: When choosing to include or omit the Place of Birth, the travel document Issuing State or organization should take into consideration any current political sensitivities linked to the state or territory and whether it is a state or territory recognized by visa-issuing authorities in other countries.

3.8 Representation of Dates

Dates in the VIZ of the MRTD shall be entered in accordance with the Gregorian calendar as follows:

Day

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 may be followed by a blank space.

Month

The month may be printed in full in the national language of the Issuing State or working language of the issuing organization or abbreviated, using up to four character positions.

Where the national language of the Issuing State or or working language of the issuing organization is not English, French or Spanish, the month shall be followed by an oblique character (/) and 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.

Where the national language of the Issuing State or working language of the issuing organization is English, French or Spanish, the Issuing State or organization may also use one of the other two languages (shown in the table below) following the oblique character (/).

Table 1: Abbreviations of Months in English, French and Spanish

<i>Month</i>	<i>English</i>	<i>French</i>	<i>Spanish</i>
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

The month may alternatively be printed in numerical form at the discretion of the Issuing State or organization, particularly where this might facilitate the use of the MRTD by states using other than the Gregorian calendar. In this case the date would be written DDbMMbYY or DDbMMbYYYY, where b = a single blank space.

Year

The year will normally be shown by the last two digits and may be preceded by a blank space.

When the month is represented numerically, the Issuing State or organization may use the four-digit representation of the year.

Examples:

12 July 1942 on an MRTD data page issued in Italian with French translation of the month could appear as :

12bLUGb/JUILb42

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

or

12 July 42 (Using English only)

or

12JUIL42 (Using French abbreviation)

or

12JUL 42 (Using English or Spanish abbreviation)

or

12 07 42 (Using numerical format).

or

12 07 1942 (using numerical format with 4 digit year).

Unknown date of birth. Where a date of birth is completely unknown, that data element shall appear in the date format used for dates of birth by the Issuing State or organization but with Xs representing unknown elements (numbers and/or letters) of the date.

Examples:

XXbXXbXX

XXbXXbXXXX

XXbXXbXX

where b = a single blank space.

If only part of the date of birth is unknown, only that part (day, month, year) of the date shall be represented by Xs as per the date format used by the Issuing State or organization.

3.9 Displayed Identification Features of the Holder

Doc 9303 identifies mandatory and optional identification feature(s) of the holder which must be displayed within the VIZ, i.e. facial image, signature or usual mark and/or single-digit fingerprint for each type of MRTD as well as the position, dimensions and scaling for the identification features.

3.9.1 Displayed Facial Image

To ensure compatibility with facial recognition systems the following guidelines and illustrations must be followed when taking photographs to be used as the facial image of the holder in an MRTD.

The displayed facial image shall depict a true likeness of the rightful holder of the MRTD and shall not be digitally altered or enhanced to change the subject's appearance in any way. It shall have been taken within the six months preceding the issue date of the MRTD.

3.9.1.1 Pose

The photograph shall show a close up of the head and shoulders with the subject facing square on and looking directly at the camera with both eyes visible and with a neutral expression with the mouth closed.

The pose should be such that an imaginary horizontal line drawn between the centres of the eyes is parallel to the top and bottom edges of the rectangular image.



The facial image shall be in focus from the crown (top of the head ignoring any hair) to the chin and from the nose to the ears.



If the additional detail of one ear is required (sometimes referred to as “half-on profile”), the face shall be at such an angle to the imaginary plane as to reveal the detail of the ear while maintaining full-face frontal details on that side of the face opposite to the exposed ear.

Both edges of the face must be clearly visible. The subject shall not be looking, portrait-style, over one shoulder.

The face shall be in sharp focus and clear with no blemishes such as ink marks or creases.

The eyes must be open and there must be no hair obscuring them.

If the subject wears glasses, the photograph must show the eyes clearly with no lights reflected in the glasses. The glasses shall not have tinted lenses. Avoid heavy frames if possible and ensure that the frames do not cover any part of the eyes. Glasses should appear only if permanently worn.



Head coverings shall not be accepted except in circumstances that the Issuing State specifically approves. Such circumstances may be religious, medical or cultural. The face must be visible from the hairline to the chin and forward of the ears.



Coverings, hair, headdress or facial ornamentation which obscure the face are not permitted.



The Issuing State shall use its discretion as to the extent to which facial ornaments (e.g. nose rings, studs), not obscuring the face, may appear in the portrait. A facial ornament should appear only if it is permanently worn.

A facial image of a baby should conform to the same specifications as for adults. Ideally, the baby should be in an upright position but it is acceptable to capture the facial image with the baby lying on a white or plain light-coloured blanket. Alternatively the baby may be placed in a baby seat but there shall be white or plain light-coloured background behind the head. The baby's eyes shall be open and no supporting hands visible.



There must be no other people or objects in the photograph.



3.9.1.2 Lighting, Exposure and Colour Balance

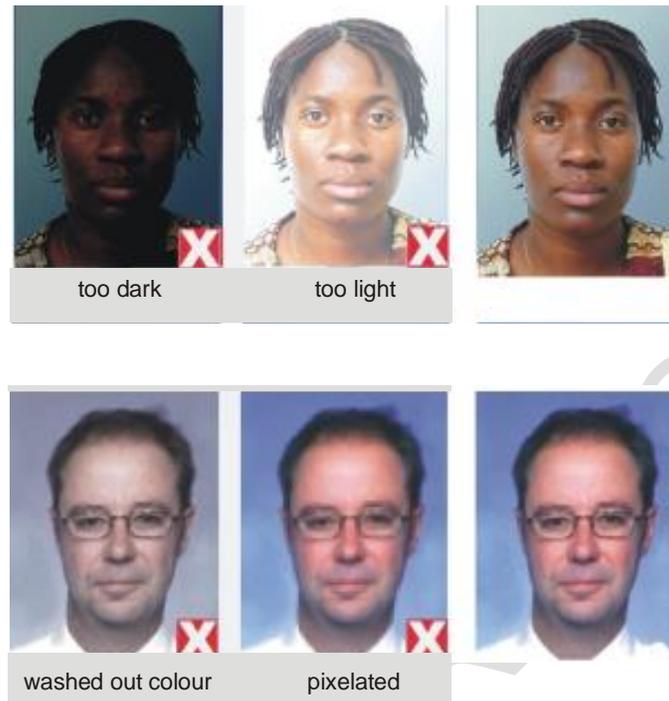
Adequate and uniform illumination shall be used to capture the facial image ensuring there are no shadows or reflections on the face or in the background.



The subject's eyes must not show red eye.



The photograph must have appropriate brightness and contrast.



The displayed portrait shall be monochrome greyscale [or black and white] or a true-colour representation of the holder. Where the picture is in colour, the lighting and photographic process must be colour balanced to render skin tones faithfully.

A uniform light-coloured background shall be used to provide a contrast to the face and hair. For colour portraits, light blue, beige, light brown, pale grey or white are recommended for the background.

3.9.1.3 Placement of the Portrait

The facial image shall be centred within Zone V with the the crown (top of the head ignoring any hair) nearest the top edge of the MRTD. The crown-to-chin portion of the facial image shall be 70 to 80 per cent of the longest dimension defined for Zone V, maintaining the aspect ratio between the crown-to-chin and ear-to-ear details of the face of the holder. The 70 to 80 per cent requirement may mean cropping the picture so that not all the hair is visible.

3.9.1.4 Digitally Printed Reproduction

The portrait, whether provided in paper or digital format, must be digitally printed in the MRTD. Necessary measures shall be taken by the Issuing State or organization to ensure that the displayed portrait is resistant to forgery and substitution.

Digital reproduction quality. The digital reproduction shall yield an accurate recognizable representation of the rightful holder of the document. The quality of the original captured portrait should at least be comparable to the minimum quality acceptable for photographs (resolution comparable to 6–8 line pairs per millimetre). To achieve this comparable image quality in a digital reproduction, careful attention must be given to the image capture, processing, digitization, compression and printing technology and the process used to produce the portrait, including the final preparation of the MRTD.

Border. A border or frame shall not be used to outline a digitally printed reproduction.

Coexistence with background security treatment(s). A digitally printed reproduction shall coexist with background security treatment(s) located within Zone V, i.e. background security printing shall not interfere with proper viewing of the displayed portrait, and vice versa.

Coexistence with final preparation treatment(s) of the MRTD. A displayed portrait shall coexist with final preparation treatment(s), i.e. final preparation treatment(s) shall not interfere with proper viewing of the displayed portrait, and vice versa.

3.9.1.5 Submission of Portrait to the Issuing Authority

Where the portrait is supplied to the issuing authority in the form of a print, the photograph, whether produced using conventional photographic techniques or digital techniques, should be on good or photo-quality paper and should be of the maximum specified dimensions.

Where the portrait is supplied to the issuing authority in digital form, the requirements specified by the issuing authority must be adhered to.

Submitted portraits should be 45.0 mm x 35.0 mm (1.77 in x 1.38 in) in dimension. This will provide adequate resolution for scaling to required size for use on the MRTD while having adequate resolution for facial recognition purposes.

3.9.1.6 Compliance with International Standards

The photograph shall comply with the appropriate definitions set out in [ISO/IEC 19794-5].

3.9.2 Displayed Signature or Usual Mark

A displayed signature or usual mark, the acceptability of which is at the Issuing State or organization's discretion, appears in Zone IV. A displayed signature or usual mark shall be an original created on the MRTD, a digitally printed reproduction of an original or, where permitted by specifications defined in Doc 9303 Parts 4-7 specific to the preparation of the different types of MRTDs, on a substrate that can be securely affixed to the MRTD. Necessary measures shall be taken by the Issuing State or organization to ensure that the displayed signature or usual mark is resistant to forgery and substitution. The displayed signature or usual mark shall meet the following requirements.

Orientation. The displayed signature or usual mark shall be displayed with its A-dimension parallel to the reference (longer) edge of the MRTD as defined in Figure 2.

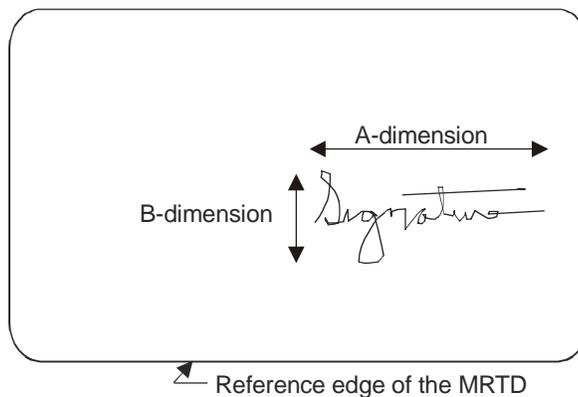


Figure 2: Orientation of the displayed signature or usual mark

Size. The displayed signature or usual mark shall be of such dimensions that it is discernible by the human eye (i.e. reduced in size by no more than 50 per cent), and the aspect ratio (A-dimension to B-dimension) of the original signature or usual mark is maintained.

Scaling for reproduction using digital printing. In the event the displayed signature or usual mark is scaled up or scaled down, the aspect ratio (A-dimension to B-dimension) of the original signature or usual mark shall be maintained.

Cropping for reproduction using digital printing. The Issuing State or organization should take steps to eliminate or minimize cropping.

Colour. The displayed signature or usual mark shall be displayed in a colour that affords a definite contrast to the background.

Borders. Borders or frames shall not be permitted or used to outline the displayed signature or usual mark.

3.9.3 Displayed Single-digit Fingerprint

A displayed single-digit fingerprint, if required by the Issuing State or organization, shall be either an original created on the MRTD substrate by the holder or, more probably, a digitally printed reproduction of an original. Necessary measures shall be taken by the Issuing State or organization to ensure that the single-digit fingerprint is resistant to forgery and substitution. The single-digit fingerprint shall meet the following requirements.

Orientation. The A-dimension (width) of the displayed single-digit fingerprint shall be parallel to the reference edge of the MRTD as defined in Figure 3. The top of the finger shall be that portion of the single-digit fingerprint furthest away from the reference edge of the MRTD. (See Doc 9303-6 Figure 10 and Figure 12.)

Size. The displayed single-digit fingerprint shall be a one-to-one replication (A-dimension versus B-dimension) of the original print.

Scaling for reproduction using digital printing. Scaling of a single-digit fingerprint shall not be permitted.

Cropping for reproduction using digital printing. The Issuing State or organization should take steps to eliminate or minimize cropping.

Colour. The displayed single-digit fingerprint shall be displayed in a colour that affords a definite contrast to the background.

Borders. Borders or frames shall not be permitted or used to outline the displayed single-digit fingerprint.

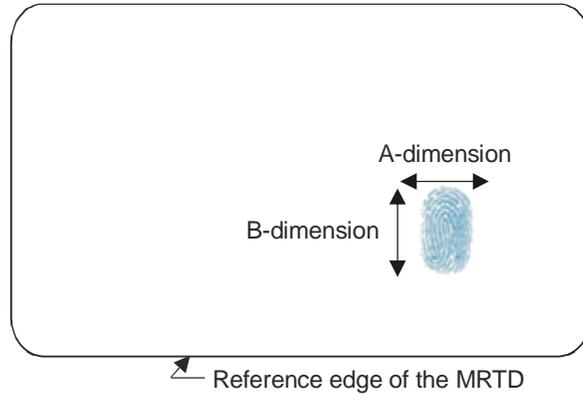


Figure 3: Orientation of the displayed single-digit fingerprint

DRAFT_4 FOR TAG_22

4 MACHINE READABLE ZONE (MRZ)

4.1 Purpose of the MRZ

MRTDs produced in accordance with Doc 9303 incorporate an MRZ to facilitate inspection of travel documents and reduce the time taken up in the travel process by administrative procedures. In addition, the MRZ provides verification of the information in the VIZ and may be used to provide search characters for a database inquiry. As well, it may be used to capture data for registration of arrival and departure or simply to point to an existing record in a database.

The MRZ provides a set of essential data elements in a format, standardized for each type of MRTD, that can be used by all receiving States regardless of their national script or customs.

The data in the MRZ are formatted in such a way as to be readable by machines with standard capability worldwide. It must be stressed that the MRZ is reserved for data intended for international use in conformance with international Standards for MRTDs. The MRZ is a different representation of the data than is found in the VIZ.

4.2 Properties of the MRZ

The data in the MRZ must be visually readable as well as machine readable. Data presentation must conform to a common standard such that all machine readers configured in conformance with Doc 9303 can recognize each character and communicate in a standard protocol (e.g. ASCII) that is compatible with the technology infrastructure and the processing requirements defined by the receiving State.

To meet these requirements, OCR-B typeface is the specified medium for storage of data in the MRZ. The MRZ as defined herein is recognized as the machine reading technology essential for global interchange and is therefore mandatory in all types of MRTDs.

4.3 Constraints of the MRZ

The only characters allowed in the MRZ are a common set of characters (Figure 4) which can be used by all States. National characters generally appear only in the computer-processing systems of the States in which they apply and are not available globally. They shall not, therefore, appear in the MRZ.

Diacritical marks are not permitted in the MRZ. Even though they may be useful to distinguish names, the use of diacritical marks in the MRZ would confuse machine-reading equipment, resulting in less accurate database searches and slower clearance of travellers.

The number of character positions available for data in the MRZ is limited and varies according to the type of MRTD. The length of the data elements inserted in the MRZ must conform to the size of the respective fields as specified in the MRZ data element directory in the applicable Part 4-7 of Doc 9303.

In some instances, names in the MRZ may not appear in the same form as in the VIZ. In the VIZ, non-Latin and national characters may be used to represent more accurately the data in the script of the Issuing State or organization. Such characters are not permitted in the MRZ.

4.4 Print Specifications

Machine readable data shall be printed in OCR-B type font, size 1, constant stroke width characters, at a fixed width spacing of 2.54 mm (0.1 in), i.e. horizontal printing density of 10 characters per 25.4 mm (1.0 in). Printed characters are restricted to those defined in Figure 4.



0123456789
ABCDEFGHI
JKLMNOPQR
STUVWXYZ <

Figure 4: Subset of OCR-B Characters from [ISO 1073-2] for use in machine readable travel documents

Note: for illustrative purposes only – the characters shown are larger than actual size.

4.5 Machine Reading Requirements and the Effective Reading Zone

Effective reading zone. A fixed-dimensional reading area (effective reading zone (ERZ) of 17.0 mm × 118.0 mm (0.67 in × 4.65 in)), sized to accommodate the largest MRTD, is defined to allow use of a single machine reader for all sizes of MRTDs. The location of the ERZ is as defined in Figure 5. The provision of the ERZ is not intended to allow additional tolerance for the printing positions defined in Parts 4,5,6 and 7 specific to the preparation of the different types of MRTDs. The ERZ is intended to allow for variances due to the manual placement of machine readable visas (MRVs) and the fanning effect of the pages that takes place when reading an interior page of an MRP. It also allows for the reading of MRTDs with either two or three lines of machine readable data.

To combat the threat to travel document security posed by, for example, photocopiers, security features are permitted in the MRZ, and any such security feature shall not interfere with accurate reading of the OCR characters at the B900 range, as defined in [ISO 1831]. While OCR characters must be visible, as specified in 4.2, to ensure that all MRTDs, including those with security features in the MRZ, can be successfully read, the OCR characters in the MRZ shall be machine readable at least in the near infrared portion of the spectrum (i.e. the B900 band defined in [ISO 1831]).

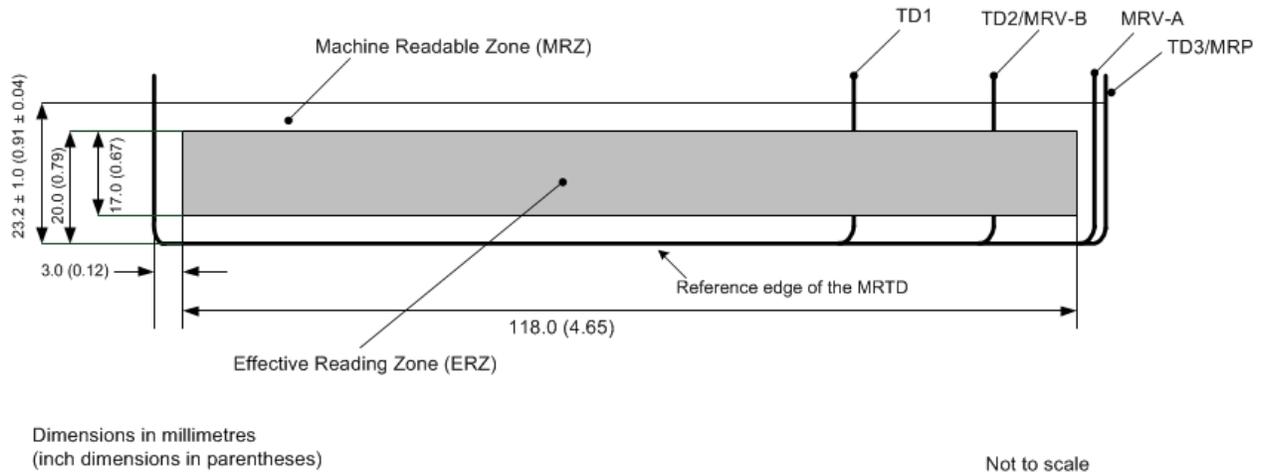


Figure 5: Schematic diagram of the MRTD effective reading zone

Note: The dimensions of the effective reading zone (ERZ) illustrated are based on a standardized ERZ for all machine readable travel documents to allow use of a single machine reader.

4.6 Convention for Writing the Name of the Holder

To achieve global interoperability, the primary and secondary identifiers in the MRZ shall be printed using upper-case OCR-B characters, illustrated in Figure 4, without diacritical marks, and conform to the number of character positions available. As such, names in the MRZ are represented differently from those in the VIZ. The Issuing State or organization shall transliterate national characters using only the allowed OCR-B characters and/or truncate, as specified in the form factor specific Parts 4-7 of Doc 9303. Transliteration tables for the most commonly used Latin, Cyrillic, and Arabic families of languages are provided in Section 6.

The primary identifier, using the Latin character transliteration (if applicable), shall be written in the MRZ as specified in the form factor specific Parts 4-7 of Doc 9303. The primary identifier shall be followed by two filler characters (<<). The secondary identifier, using the Latin character transliteration (if applicable), shall be written starting in the character position immediately following the two filler characters.

If the primary or secondary identifiers have more than one name component, each component shall be separated by a single filler character (<).

Filler characters (<) should be inserted immediately following the final secondary identifier (or following the primary identifier in the case of a name having only a primary identifier) through to the last character position in the machine readable line.

The number of character positions in the name field is limited and differs for the different types of MRTDs. If the primary and secondary identifiers, written in the relevant machine readable line using the above procedure, exceed the available character positions, then truncation shall be carried out using the procedure set out in the form factor specific Parts 4-7 of Doc 9303. In all other cases, the name shall not be truncated.

Examples of truncation of names are contained in the form factor specific Parts 4-7 of Doc 9303.

Prefixes and suffixes, including titles, professional and academic qualifications, honours, awards, and hereditary status (such as Dr., Sir, Jr., Sr., II and III) shall not be included in the MRZ except where the Issuing State considers these to be legally part of the name. In such cases, prefixes or suffixes shall be represented as components of the secondary identifier(s).

Numeric characters shall not be used in the name fields of the MRZ.

Punctuation characters are not allowed in the MRZ. Where these appear as part of a name, they should be treated as follows:

Apostrophe:

This shall be omitted; name components separated by the apostrophe shall be combined, and no filler character shall be inserted in its place in the MRZ.

Example VIZ: D'ARTAGNAN
 MRZ: DARTAGNAN

Hyphen:

Where a hyphen appears between two name components, it shall be represented in the MRZ by a single filler character (<). (i.e. hyphenated names shall be represented as separate components).

Example VIZ: MARIE-ELISE
 MRZ: MARIE<ELISE

Comma:

Where a comma is used in the VIZ to separate the primary and secondary identifiers, the comma shall be omitted in the MRZ, and the primary and secondary identifiers shall be separated in the MRZ by two filler characters (<<).

Example VIZ: ERIKSSON, ANNA MARIA
 MRZ: ERIKSSON<<ANNA<MARIA

Otherwise, where a comma is used in the VIZ to separate two name components, it shall be represented in the MRZ as a single filler character (<).

Example VIZ: ANNA, MARIA
 MRZ: ANNA<MARIA

Other punctuation characters:

All other punctuation characters shall be omitted from the MRZ (i.e. no filler character shall be inserted in their place in the MRZ).

4.7 Representation of Issuing State or Organization and Nationality of Holder

The three-letter codes listed in Section 5 shall be used to complete the fields for the Issuing State or organization and the nationality of the holder in the MRZ.

4.8 Representation of Dates

Dates in the MRZ of the MRTD shall be shown as a six-digit string 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.

Following this format, 12 July 1942 will be shown as: 420712.

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

4.9 Check Digits in the MRZ

A check digit consists of a single digit computed from the other digits in a series. Check digits in the MRZ are calculated on specified numerical data elements in the MRZ. The check digits permit readers to verify that data in the MRZ is correctly interpreted.

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.

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.

Step 2. Add the products of each multiplication.

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

Step 4. The remainder shall be the check digit.

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.

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

Data elements included in the check digit calculation and check digit location for each document type are contained in the form factor specific Parts 4-7 of Doc 9303. Examples of check digit calculation are found in Informative Appendix A to this Part.

4.10 Characteristics of the MRZ

Except as otherwise specified herein, the MRTD shall conform with [ISO 1831] concerning the following matters:

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

Machine readable data shall be arranged from left to right in fixed-length fields in two lines (upper and lower) except for TD1 size travel documents where there are three lines (upper, middle and lower). The data is presented in the order specified in the data structure tables in the form factor specific Parts 4-7 of Doc 9303 and located on the document as shown in those parts. Data shall be entered in each field, beginning with the left-hand character position.

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

4.11 Quality Specifications of the MRZ

In general, the print quality shall conform to [ISO 1831] Range X, except as otherwise provided herein. Except where otherwise noted, all quality specifications set forth hereunder shall conform to the

requirements of Section 2 of this Part and shall apply to the MRTD after final preparation and, in the case of visas, after placement in the passport or other travel document.

Substrate quality. [ISO 1831], 4.3 through 4.3.2, shall be used for reference only.

Substrate opacity. The substrate used, measured before and after final preparation (and for visas prior to placement in the passport or other travel document), shall be within the definition of at least medium opacity as specified in [ISO 1831], 4.4.1 and 4.4.3.

Substrate gloss. The level of gloss is not specified.

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.

Alternative substrates. The aforementioned quality specifications should be followed irrespective of the substrate material.

Spectral band. The OCR print shall be legible visually and shall be black (B425 through B680 as defined in [ISO 1831]). The OCR print shall also absorb in the B900 band as defined in [ISO 1831] (i.e. near infrared). This property must test successfully when the characters are machine-read through any protective material that may have been applied to the surface of the document.

Print contrast signal (PCS). After final preparation, the minimum print contrast signal (PCS/min), when measured as specified in [ISO 1831], shall be as follows: $PCS / \min \geq 0.6$ at the B900 spectral band.

Character stroke width. The stroke width after final preparation shall be as specified for Range X in [ISO 1831], 5.3.1.

Contrast variation ratio (CVR). After final preparation, the CVR should be as is shown for Range X in [ISO 1831], i.e. $CVR < 1.50$.

Spots and extraneous marks. [ISO 1831], 5.4.4.6 and 5.4.5.12 shall apply at the reading surface (see also B.6 of Appendix B and C.5.10 of Appendix C to [ISO 1831]).

Voids. The value of "d" as defined in [ISO 1831], 5.4.5.9 shall be equal to 0.4 at the reading surface.

Line separation. Refer to the form factor specific Parts 4-7 of Doc 9303.

Line spacing. Refer to the form factor specific Parts 4-7 of Doc 9303.

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 3 degrees measured from the reference edge nor shall the skew of MRZ or character misalignment result in the MRZ lines or any part thereof appearing outside the printing zone as defined in the form factor specific Parts 4-7 of Doc 9303.

5 CODES FOR NATIONALITY, PLACE OF BIRTH, LOCATION OF ISSUING STATE/AUTHORITY AND OTHER PURPOSES

Part A — Letter Codes

The following are the two- and three-letter codes for entities specified and regularly updated in [ISO 3166-1], with extensions for certain States and organizations being identified by an asterisk. The current version of the codes may be obtained from the [ISO 3166] maintenance agency - [ISO 3166/MA], ISO's focal point for country codes.

<i>Entity (short name)</i>	2-letter code	3-letter code	<i>Entity (short name)</i>	2-letter code	3-letter code
Afghanistan	AF	AFG	Bonaire, Saint Eustatius and Saba	BQ	BES
Åland Islands	AX	ALA	Bosnia and Herzegovina	BA	BIH
Albania	AL	ALB	Botswana	BW	BWA
Algeria	DZ	DZA	Bouvet Island	BV	BVT
American Samoa	AS	ASM	Brazil	BR	BRA
Andorra	AD	AND	British Indian Ocean Territory	IO	IOT
Angola	AO	AGO	Brunei Darussalam	BN	BRN
Anguilla	AI	AIA	Bulgaria	BG	BGR
Antarctica	AQ	ATA	Burkina Faso	BF	BFA
Antigua and Barbuda	AG	ATG	Burundi	BI	BDI
Argentina	AR	ARG	Cambodia	KH	KHM
Armenia	AM	ARM	Cameroon	CM	CMR
Aruba	AW	ABW	Canada	CA	CAN
Australia	AU	AUS	Cape Verde	CV	CPV
Austria	AT	AUT	Cayman Islands	KY	CYM
Azerbaijan	AZ	AZE	Central African Republic	CF	CAF
Bahamas	BS	BHS	Chad	TD	TCD
Bahrain	BH	BHR	Chile	CL	CHL
Bangladesh	BD	BGD	China	CN	CHN
Barbados	BB	BRB	Christmas Island	CX	CXR
Belarus	BY	BLR	Cocos (Keeling) Islands	CC	CCK
Belgium	BE	BEL	Colombia	CO	COL
Belize	BZ	BLZ	Comoros	KM	COM
Benin	BJ	BEN	Congo	CG	COG
Bermuda	BM	BMU	Cook Islands	CK	COK
Bhutan	BT	BTN	Costa Rica	CR	CRI
Bolivia	BO	BOL	Côte d'Ivoire	CI	CIV

Croatia	HR	HRV
Cuba	CU	CUB
Curaçao	CW	CUW
Cyprus	CY	CYP
Czech Republic	CZ	CZE
Democratic People's Republic of Korea	KP	PRK
Democratic Republic of the Congo	CD	COD
Denmark	DK	DNK
Djibouti	DJ	DJI
Dominica	DM	DMA
Dominican Republic	DO	DOM
Ecuador	EC	ECU
Egypt	EG	EGY
El Salvador	SV	SLV
Equatorial Guinea	GQ	GNQ
Eritrea	ER	ERI
Estonia	EE	EST
Ethiopia	ET	ETH
Falkland Islands (Malvinas)	FK	FLK ¹
Faroe Islands	FO	FRO
Fiji	FJ	FJI
Finland	FI	FIN
France	FR	FRA
French Guiana	GF	GUF
French Polynesia	PF	PYF
French Southern Territories	TF	ATF
Gabon	GA	GAB
Gambia	GM	GMB
Georgia	GE	GEO
Germany	DE	D
Ghana	GH	GHA
Gibraltar	GI	GIB

Greece	GR	GRC
Greenland	GL	GRL
Grenada	GD	GRD
Guadeloupe	GP	GLP
Guam	GU	GUM
Guatemala	GT	GTM
Guernsey	GC	GGY
Guinea	GN	GIN
Guinea-Bissau	GW	GNB
Guyana	GY	GUY
Haiti	HT	HTI
Heard and McDonald Islands	HM	HMD
Holy See (Vatican City State)	VA	VAT
Honduras	HN	HND
Hong Kong Special Administrative Region of China	HK	HKG
Hungary	HU	HUN
Iceland	IS	ISL
India	IN	IND
Indonesia	ID	IDN
Interpol		XPO
Iran (Islamic Republic of)	IR	IRN
Iraq	IQ	IRQ
Ireland	IE	IRL
Isle of Man	IM	IMN
Israel	IL	ISR
Italy	IT	ITA
Jamaica	JM	JAM
Japan	JP	JPN
Jersey	JE	JEY
Jordan	JO	JOR
Kazakhstan	KZ	KAZ
Kenya	KE	KEN

¹ A dispute exists between the Governments of Argentina and the United Kingdom of Great Britain and Northern Ireland concerning sovereignty over the Falkland Islands (Malvinas).

Kiribati	KI	KIR
Kuwait	KW	KWT
Kyrgyzstan	KG	KGZ
Lao People's Democratic Republic	LA	LAO
Latvia	LV	LVA
Lebanon	LB	LBN
Lesotho	LS	LSO
Liberia	LR	LBR
Libyan Arab Jamahiriya	LY	LBY
Liechtenstein	LI	LIE
Lithuania	LT	LTU
Luxembourg	LU	LUX
Macau Special Administrative Region of China	MO	MAC
Madagascar	MG	MDG
Malawi	MW	MWI
Malaysia	MY	MYS
Maldives	MV	MDV
Mali	ML	MLI
Malta	MT	MLT
Marshall Islands	MH	MHL
Martinique	MQ	MTQ
Mauritania	MR	MRT
Mauritius	MU	MUS
Mayotte	YT	MYT
Mexico	MX	MEX
Micronesia (Federated States of)	FM	FSM
Moldova	MD	MDA
Monaco	MC	MCO
Mongolia	MN	MNG
Montenegro	ME	MNE
Montserrat	MS	MSR
Morocco	MA	MAR
Mozambique	MZ	MOZ
Myanmar	MM	MMR
Namibia	NA	NAM

Nauru	NR	NRU
Nepal	NP	NPL
Netherlands	NL	NLD
Netherlands Antilles		ANT
Neutral Zone	NT	NTZ
New Caledonia	NC	NCL
New Zealand	NZ	NZL
Nicaragua	NI	NIC
Niger	NE	NER
Nigeria	NG	NGA
Niue	NU	NIU
Norfolk Island	NF	NFK
Northern Mariana Islands	MP	MNP
Norway	NO	NOR
Oman	OM	OMN
Pakistan	PK	PAK
Palau	PW	PLW
Palestinian Territory, Occupied	PS	PSE
Panama	PA	PAN
Papua New Guinea	PG	PNG
Paraguay	PY	PRY
Peru	PE	PER
Philippines	PH	PHL
Pitcairn	PN	PCN
Poland	PL	POL
Portugal	PT	PRT
Puerto Rico	PR	PRI
Qatar	QA	QAT
Republic of Korea	KR	KOR
Réunion	RE	REU
Romania	RO	ROU
Russian Federation	RU	RUS
Rwanda	RW	RWA
Saint Barthélemy	BL	BLM
St. Helena	SH	SHN
Saint Kitts and Nevis	KN	KNA

Saint Lucia	LC	LCA
Saint Martin (French part)	MF	MAF
Sint Maarten (Dutch part)	SX	SXM
St. Pierre and Miquelon	PM	SPM
Saint Vincent and the Grenadines	VC	VCT
Samoa	WS	WSM
San Marino	SM	SMR
Sao Tome and Principe	ST	STP
Saudi Arabia	SA	SAU
Senegal	SN	SEN
Serbia	RS	SRB
Seychelles	SC	SYC
Sierra Leone	SL	SLE
Singapore	SG	SGP
Slovakia	SK	SVK
Slovenia	SI	SVN
Solomon Islands	SB	SLB
Somalia	SO	SOM
South Africa	ZA	ZAF
South Georgia and the South Sandwich Islands	GS	SGS
South Sudan	SS	SSD
Spain	ES	ESP
Sri Lanka	LK	LKA
Sudan	SD	SDN
Suriname	SR	SUR
Svalbard and Jan Mayen Islands	SJ	SJM
Swaziland	SZ	SWZ
Sweden	SE	SWE
Switzerland	CH	CHE
Syrian Arab Republic	SY	SYR
Taiwan, Province of China	TW	TWN
Tajikistan	TJ	TJK
Thailand	TH	THA
The former Yugoslav Republic of Macedonia	MK	MKD
Timor-Leste	TL	TLS

Togo	TG	TGO
Tokelau	TK	TKL
Tonga	TO	TON
Trinidad and Tobago	TT	TTO
Tunisia	TN	TUN
Turkey	TR	TUR
Turkmenistan	TM	TKM
Turks and Caicos Islands	TC	TCA
Tuvalu	TV	TUV
Uganda	UG	UGA
Ukraine	UA	UKR
United Arab Emirates	AE	ARE
United Kingdom	GB	
British		
— Citizen		GBR
— British Overseas Territories Citizen		GBD*
— National (Overseas)		GBN*
— Overseas citizen		GBO*
— Protected person		GBP*
— Subject		GBS*
United Republic of Tanzania	TZ	TZA
United States	US	USA
United States Minor Outlying Islands	UM	UMI
United Nations eLP	ZZ	
Uruguay	UY	URY
Uzbekistan	UZ	UZB
Vanuatu	VU	VUT
Vatican City State (Holy See)	VA	VAT
Venezuela	VE	VEN
Viet Nam	VN	VNM
Virgin Islands (British)	VG	VGB
Virgin Islands (U.S.)	VI	VIR
Wallis and Futuna Islands	WF	WLF
Western Sahara	EH	ESH
Yemen	YE	YEM

Zambia	ZM	ZMB
--------	----	-----

Zimbabwe	ZW	ZWE
----------	----	-----

Part B — Codes for Use in United Nations Travel Documents

- *UNO — Designates the United Nations Organization or one of its officials.
- *UNA — Designates a specialized agency of the United Nations or one of its officials.
- *UNK — Designates a resident of Kosovo to whom a travel document has been issued by the United Nations Interim Administration Mission in Kosovo (UNMIK).

Part C — Codes for other Issuing Authorities

- *XOM — Designates the Sovereign Military Order of Malta or one of its emissaries.
- *XCC — Designates the Caribbean Community or one of its emissaries (CARICOM).
- *XPO — Designates the International Criminal Police Organization (INTERPOL).
- *XCO — Designates the Common Market for Eastern and Southern Africa (COMESA).

Part D — Codes for Persons Without a Defined Nationality

- *XXA — Stateless person, as defined in Article 1 of the 1954 Convention Relating to the Status of Stateless Persons.
- *XXB — Refugee, as defined in Article 1 of the 1951 Convention Relating to the Status of Refugees as amended by the 1967 Protocol.
- *XXC — Refugee, other than as defined under the code XXB above.
- *XXX — Person of unspecified nationality, for whom the Issuing State does not consider it necessary to specify any of the codes XXA, XXB or XXC above, whatever that person's status may be. This category may include a person who is neither stateless nor a refugee but who is of unknown nationality and legally residing in the State of issue.

6 TRANSLITERATIONS RECOMMENDED FOR USE BY STATES

The following tables contain the most commonly used national characters of the Latin, Cyrillic and Arabic families of languages.

A. Transliteration of Multinational Latin-Based Characters

<i>Unicode</i>	<i>National character</i>	<i>Description</i>	<i>Recommended transliteration</i>
00C1	Á	A acute	A
00C0	À	A grave	A
00C2	Â	A circumflex	A
00C4	Ä	A diaeresis	AE or A
00C3	Ã	A tilde	A
0102	Ă	A breve	A
00C5	Å	A ring	AA or A
0100	Ā	A macron	A
0104	Ą	A ogonek	A
0106	Ć	C acute	C
0108	Ĉ	C circumflex	C
010C	Č	C caron	C
010A	Ć	C dot accent	C
00C7	Ç	C cedilla	C
0110	Ð	Eth	D
010E	Ď	D caron	D
00C9	É	E acute	E
00C8	È	E grave	E
00CA	Ê	E circumflex	E
00CB	Ë	E diaeresis	E
011A	Ě	E caron	E
0116	Ė	E dot accent	E
0112	Ē	E macron	E
0118	Ę	E ogonek	E
0114	Ĕ	E breve	E
011C	Ĝ	G circumflex	G
011E	Ğ	G breve	G
0120	Ġ	G dot accent	G
0122	Ģ	G cedilla	G
0126	Ĥ	H bar	H
0124	ĥ	H circumflex	H
	İ	I without dot (Turkey)	I

<i>Unicode</i>	<i>National character</i>	<i>Description</i>	<i>Recommended transliteration</i>
00CD	í	I acute	I
00CC	ì	I grave	I
00CE	î	I circumflex	I
00CF	ï	I diaeresis	I
0128	ĩ	I tilde	I
0130	ï	I dot accent	I
012A	ī	I macron	I
012E	ł	I ogonek	I
012C	İ	I breve	I
0134	ĵ	J circumflex	J
0136	ķ	K cedilla	K
0141	ł	L slash	L
0139	ĺ	L acute	L
013D	ł	L caron	L
013B	ł	L cedilla	L
013F	ł	L dot	L
0143	ń	N acute	N
00D1	ñ	N tilde	N or NXX
0147	ň	N caron	N
0145	ņ	N cedilla	N
014B	η	Eng	N
00D8	ø	O slash	OE
00D3	ó	O acute	O
00D2	ò	O grave	O
00D4	ô	O circumflex	O
00D6	ö	O diaeresis	OE or O
00D5	õ	O tilde	O
0150	ő	O double acute	O
014C	ō	O macron	O
014E	ö	O breve	O
0154	ř	R acute	R
0158	ř	R caron	R
0156	ŗ	R cedilla	R
015A	ś	S acute	S
015C	ŝ	S circumflex	S
0160	š	S caron	S
015E	ş	S cedilla	S
0166	ƒ	T bar	T
0164	ť	T caron	T
0162	ţ	T cedilla	T

<i>Unicode</i>	<i>National character</i>	<i>Description</i>	<i>Recommended transliteration</i>
00DA	Ú	U acute	U
00D9	Ù	U grave	U
00DB	Û	U circumflex	U
00DC	Ü	U diaeresis	UE or UXX or U
0168	Û	U tilde	U
016C	Ǔ	U breve	U
0170	Ű	U double acute	U
016E	Û	U ring	U
016A	Ū	U macron	U
0172	Ų	U ogonek	U
0174	Ŵ	W circumflex	W
00DD	Ý	Y acute	Y
0176	Ŷ	Y circumflex	Y
0178	ÿ	Y diaeresis	Y
0179	Ź	Z acute	Z
017D	Ž	Z caron	Z
017B	Ž	Z dot	Z
00FE	Þ	Thorn (Iceland)	TH
00C6	Æ	ligature AE	AE
0132	←	ligature IJ	IJ
0152	Œ	ligature OE	OE
00DF	ß	double s (Germany)	SS

B. Transliteration of Cyrillic Characters

<i>Unicode</i>	<i>National character</i>	<i>Recommended transliteration</i>
0410	А	A
0411	Б	B
0412	В	V
0413	Г	G (except Belorussian and Serbian = H)
0414	Д	D
0415	Е	E
0401	Ё	E (except Belorussian = IO)
0416	Ж	ZH (except Serbian = Z)
0417	З	Z
0418	И	I (except Ukrainian = Y)
0406	І	I
0419	Й	I

<i>Unicode</i>	<i>National character</i>	<i>Recommended transliteration</i>
041A	К	K
041B	Л	L
041C	М	M
041D	Н	N
041E	О	O
041F	П	P
0420	Р	R
0421	С	S
0422	Т	T
0423	У	U
0424	Ф	F
0425	Х	KH (except Serbian and in the language spoken in the former Yugoslav Republic of Macedonia = H)
0426	Ц	TS (except Serbian and in the language spoken in the former Yugoslav Republic of Macedonia = C)
0427	Ч	CH (except Serbian = C)
0429	Ш	SH (except Serbian = S)
0429	Щ	SHCH (except Bulgarian = SHT)
042B	Ы	Y
042A	Ъ	IE
042D	Э	E
042E	Ю	IU
042F	Я	IA
0476	Ѹ	Y
0490	Ґ	G
045E	Ў	U
046A	Ж	U
	ƒ	G (except in the language spoken in the former Yugoslav Republic of Macedonia = GJ)
0452	Ђ	D
0405	Š	DZ
0408	Ј	J
041A	Ќ	K (except in the language spoken in the former Yugoslav Republic of Macedonia = KJ)
0459	Љ	LJ
045A	Њ	NJ
04BB	ћ	C

Unicode	National character	Recommended transliteration
040F	Ѓ	DZ (except in the language spoken in the former Yugoslav Republic of Macedonia = DJ)
0454	Є	IE
0407	Ї	I

C. Transliteration of Arabic Script

Unicode	Arabic letter	Name	MRZ
0621	ء	hamza	XE
0622	آ	alef with madda above	XAA
0623	أ	alef with hamza above	XAE
0624	ؤ	waw with hamza above	U
0625	إ	alef with hamza below	I
0626	ئ	yeh with hamza above	XI
0627	ا	alef	A
0628	ب	beh	B
0629	ة	teh marbuta	XTA
062A	ت	teh	T
062B	ث	theh	XTH
062C	ج	jeem	J
062D	ح	hah	XH
062E	خ	khah	XKH
062F	د	dal	D
0630	ذ	thal	XDH
0631	ر	reh	R
0632	ز	zain	Z
0633	س	seen	S
0634	ش	sheen	XSH
0635	ص	sad	XSS
0636	ض	dad	XDZ
0637	ط	tah	XTT
0638	ظ	zah	XZZ
0639	ع	ain	E

063A	غ	ghain	G
0640	.	tatwheel	(Not encoded)
0641	ف	feh	F
0642	ق	qaf	Q
0643	ك	kaf	K
0644	ل	lam	L
0645	م	meem	M
0646	ن	noon	N
0647	ه	heh	H
0648	و	waw	W
0649	ى	alef maksura	XAY
064A	ي	yeh	Y
064B	َ	fathatan	(Not encoded)
064C	ِ	dammatan	(Not encoded)
064D	ُ	kasratan	(Not encoded)
064E	َ	fatha	(Not encoded)
064F	ِ	damma	(Not encoded)
0650	ُ	kasra	(Not encoded)
0651	ّ	shadda	[DOUBLE] ²
0652	◌◌◌	sukun	(Not encoded)
0670	◌◌	superscript alef	(Not encoded)
0671	أ	alef wasla	XXA
0679	ط	Tteh	XXT
067E	پ	Peh	P
067C	ت	teh with ring	XRT
0681	هـ	hah with hamza above	XKE
0685	هـ	hah with 3 dots above	XXH
0686	چ	Tchah	XC
0688	ط	Ddal	XXD
0689	د	dal with ring	XDR
0691	ر	Rreh	XXR

² Shadda denotes doubling: Latin character or sequence is repeated eg عَبَّاس becomes EBBAS; فضّة becomes FXDZXDZXA.H.

0693	ر	reh with ring	XRR
0696	ړ	reh with dot below and dot above	XRX
0698	ژ	Jeh	XJ
069A	ږ	seen with dot below and dot above	XXS
069C	ښ	seen with 3 dots below and 3 dots above	(Not encoded)
06A2	ف	feh with dot moved below	(Not encoded)
06A7	ق	qaf with dot above	(Not encoded)
06A8	ق	qaf with 3 dots above	(Not encoded)
06A9	ک	keheh	XKK
06AB	ک	kaf with ring	XXK
06AD	گ	Ng	XNG
06AF	گ	gaf	XGG
06BA	ن	noon ghunna	XNN
06BC	ښ	noon with ring	XXN
06BE	ه	heh doachashmee	XDO
06C0	ه	heh with yeh above	XYH
06C1		heh goal	XXG
06C2		heh goal with hamza above	XGE
06C3		teh marbuta goal	XTG
06CC	ی	farsi yeh	XYA
06CD	ی	yeh with tail	XXY
06D0	ی	Yeh	Y
06D2	ی	Yeh barree	XYB
06D3	ی	yeh barree with hamza above	XBE

APPENDIX A EXAMPLES OF CHECK DIGIT CALCULATION (INFORMATIVE)

Example 1 — Application of check digit to date field.

Using 27 July 1952 as an example, with the date in numeric form, 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)		$\frac{103}{10} = 10, \text{ remainder } 3$						

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

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)		$\frac{125}{10} = 12, \text{ remainder } 5$							

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

Examples of the calculation of composite check digits.

The calculation method for composite check digits is the same for all MRTDs. However, the location and number of the digits to be included in the calculation is different between the different types of documents. For completeness, examples of each are included here.

Example 3— Composite check digit calculation for ID3 documents.

Example 5— Composite check digit calculation for TD2 documents.

Using the lower line of MRZ data that follows as an example for coding the composite check digit, the calculation will be:

Lower machine readable line (character positions 1–35):

HA672242<6UT05802254M9601086<<<<<<<<

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

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:	<
Assigned numeric values:	0
Weighting:	7
Step 1 (multiplication) Products:	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	+	42	+	0	+
Step 2 (sum of products)	1	+	0	+	24	+	6	+	0	+	0	+	0	+	0	+	0	+	0	+
Step 2 (sum of products)	0																			
Step 2 (sum of products)	=	448																		

$$\frac{448}{10} = 44, \text{ remainder } 8$$

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<6UT05802254M9601086<<<<<<<8.

APPENDIX B ARABIC transliteration – DETAILS AND EXAMPLES (INFORMATIVE)

B.1 Example of Transliteration for Standard Arabic

The following:

ابو بكر محمد بن زكريا الرازي

can be encoded in the MRZ as:

ابو	Alef (ا) - Beh (ب) - Waw (و) => ABW
بكر	Beh (ب) - Kaf (ك) - Reh (ر) => BKR
محمد	Meem (م) - Hah (ح) - Meem (م) - Dal (د) => MXHMD
بن	Beh (ب) - Noon (ن) => BN
زكريا	Zain (ز) - Kaf (ك) - Reh (ر) - Yeh (ي) - Alef (ا) => ZKRYA
الرازي	Alef (ا) - Lam (ل) - Reh (ر) - Alef (ا) - Zain (ز) - Yeh (ي) => ALRAZY

ie. ABW<BKR<MXHMD<BN<ZKRYA<ALRAZY

The advantages of this transliteration are:

1. The name in the Arabic script is always transliterated to the same Latin representation. This means that database matches are more likely to result;
2. The process is reversible - the name in the Arabic script can be recovered.

To recover the name in the Arabic script:

ABW	A=Alef (ا) - B=Beh (ب) - W=Waw (و) => ابو
BKR	B=Beh (ب) - K=Kaf (ك) - R=Reh (ر) => بكر
MXHMD	M=Meem (م) - XH=Hah (ح) - M=Meem (م) - D=Dal (د) => محمد
BN	B=Beh (ب) - N=Noon (ن) => بن
ZKRYA	Z=Zain (ز) - K=Kaf (ك) - R=Reh (ر) - Y=Yeh (ي) - A=Alef (ا) => زكريا
ALRAZY	A=Alef (ا) - L=Lam (ل) - R=Reh (ر) - A=Alef (ا) - Z=Zain (ز) - Y=Yeh (ي) => الرازي

The rationale for omitting the harakat and other diacritical marks is that they are optional and mostly not used. Therefore they should be treated the same way as the diacritical marks on European national characters (eg é, è, ç) which are used for pronunciation purposes.

As well, the optional inclusion of the harakat would be detrimental for accurate database matches.

B.2 Recommended Transliteration Scheme for Other Languages

Persian is spoken in Iran (Farsi), Afghanistan (Dari), Tajikistan and Uzbekistan.

Pashto is spoken in Afghanistan and western Pakistan.

Urdu is spoken in Pakistan and India.

Unicode	Arabic letter	Language	Name	MRZ
0679	ٹ	Urdu	Tteh	XXT
067E	پ	Persian, Urdu	Peh	P
067C	ټ	Pashto	teh with ring	XRT
0681	ه	Pashto	hah with hamza above	XKE
0685	ه	Pashto	hah with 3 dots above	XXH
0686	ت	Persian, Urdu	Tcheh	XC
0688	ڈ	Urdu	Ddal	XXD
0689	د	Pashto	dal with ring	XDR
0691	ڑ	Urdu	Rreh	XXR
0693	ر	Pashto	reh with ring	XRR
0696	ر	Pashto	reh with dot below and dot above	XRX
0698	ژ	Persian, Urdu	Jeh	XJ
069A	ښ	Pashto	seen with dot below and dot above	XXS
06A9	ک	Persian, Urdu	keheh	XKK
06AB	ک	Pashto	kaf with ring	XXK
06AD	گ		Ng	XNG
06AF	گ	Persian, Urdu	gaf	XGG
06BA	ن	Urdu	noon ghunna	XNN
06BC	ن	Pashto	noon with ring	XXN
06BE	ھ	Urdu	heh doachashmee	XDO
06C0	ہ	Urdu	heh with yeh above	XYH
06C1		Urdu	heh goal	XXG
06C2		Urdu	heh goal with hamza above	XGE
06C3		Urdu	teh marbuta goal	XTG

06CC	ى	Persian, Urdu	farsi yeh	XYA ³
06CD	ی	Pashto	yeh with tail	XXY
06D0	ې	Pashto	Yeh	Y ⁴
06D2	ے	Urdu	Yeh barree	XYB
06D3	ء	Urdu	yeh barree with hamza above	XBE

B.3 Recommended Transliteration Scheme for Moroccan, Tunisian and Maghrib Arabic

Moroccan, Tunisian and Maghrib Arabic add four letters to the standard Arabic script:

Unicode	Arabic letter	Name	MRZ
069C	ثیں	seen with 3 dots below and 3 dots above (Moroccan)	(note 1)
06A2	فہ	feh with dot moved below (Maghrib)	(note 1)
06A7	قہ	qaf with dot above (Maghrib)	(note 1)
06A8	قہ	qaf with 3 dots above (Tunisian)	(note 1)

Note 1: These characters are obsolete and not transliterated

³ The letter "farsi yeh" (ى) is functionally identical to the standard "yeh" (ي) but in the isolated and final forms is graphically identical to the standard "alef maksura" (ى), so could be transliterated as 'Y' or "XAY". Database matching algorithms should take this into account.

⁴ The character "Pashto yeh" (ې) is functionally identical to the standard "yeh" (ي).

REFERENCES (NORMATIVE)

- | | |
|-------------------|---|
| [ISO 1073-2] | ISO 1073-2:1976, Alphanumeric character sets for optical character recognition – Part 2: Character set OCR-B – Shapes and dimensions of the printed image |
| [ISO 1831] | ISO 1831:1980, Printing Specifications for optical character recognition |
| [ISO 3166-1] | ISO 3166-1:2006 Codes for the representation of names of countries and their subdivisions – Part 1:Country codes |
| [ISO/IEC 7810] | ISO/IEC 7810:2003, Identification Cards – Physical Characteristics |
| [ISO/IEC 19794-5] | ISO/IEC 19794-5:2011, Information technology — Biometric data interchange formats — Part 5: Face image data |

DRAFT_4 FOR TAG_22



Machine Readable Travel Documents

Part 4
Specifications Specific to Machine Readable Passports (MRPs) and other
TD3 Size Machine Readable Travel Documents (MRTDs)

Approved by the Secretary General
and published under his authority

Seventh Edition — Revision 1 – 2014

International Civil Aviation Organization

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

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

Doc 9303, Machine Readable Travel Documents
Order Number: xxxx
ISBN xxx-xx-xxxx-xxx-x

© ICAO 2014

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 TO DOC 9303-4, 7TH EDITION

Revision	Date	Description
01	xx-xx-2014	Initial release of the 7 th edition

DRAFT_4 FOR TAG_22

TABLE OF CONTENTS

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).....	14
4.3	Representation of the Issuing State or Organization and Nationality of Holder in the MRZ and the VIZ.....	19
	APPENDIX A - EXAMPLES OF A PERSONALIZED MRP DATA PAGE (INFORMATIVE)	20
	APPENDIX B – CONSTRUCTION OF THE MACHINE READABLE ZONE OF THE PASSPORT DATA PAGE (INFORMATIVE)	22
	REFERENCES (NORMATIVE)	23

1 SCOPE

The seventh edition of Doc 9303 represents a re-structuring of the ICAO specifications for Machine Readable Travel Documents. Without incorporating substantial modifications of 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 Doc 9303 Part 1, Machine Readable Passports Volume.1, 6th Edition 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 Machine Readable Travel Documents;
- Part 3 - Specifications Common to all Machine Readable Travel Documents.

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

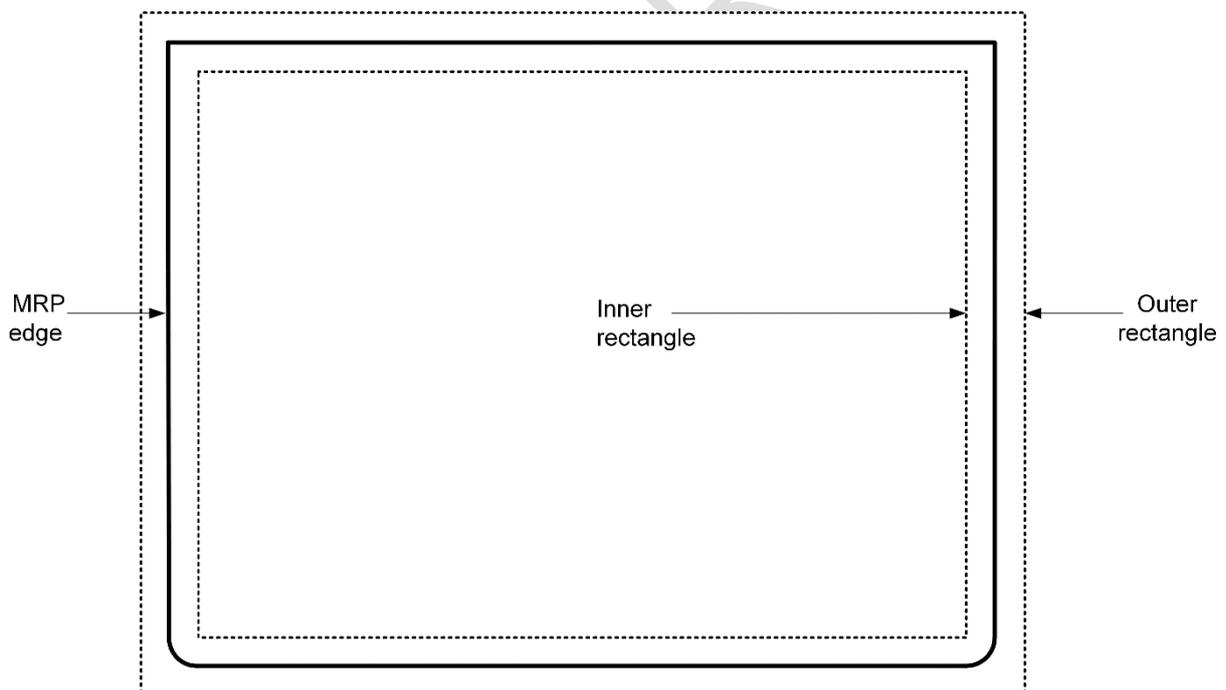
The nominal dimensions shall be as specified in ISO/IEC 7810 (except thickness) for the TD3 size MRTD, i.e.:

88.0 mm \pm 0.75 mm \times 125.0 mm \pm 0.75 mm (3.46 in \pm 0.039 in \times 4.92 in \pm 0.039 in).

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 \times 124.25 mm (3.44 in \times 4.89 in)
Outer rectangle: 88.75 mm \times 125.75 mm (3.49 in \times 4.95 in)



Not to scale

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.

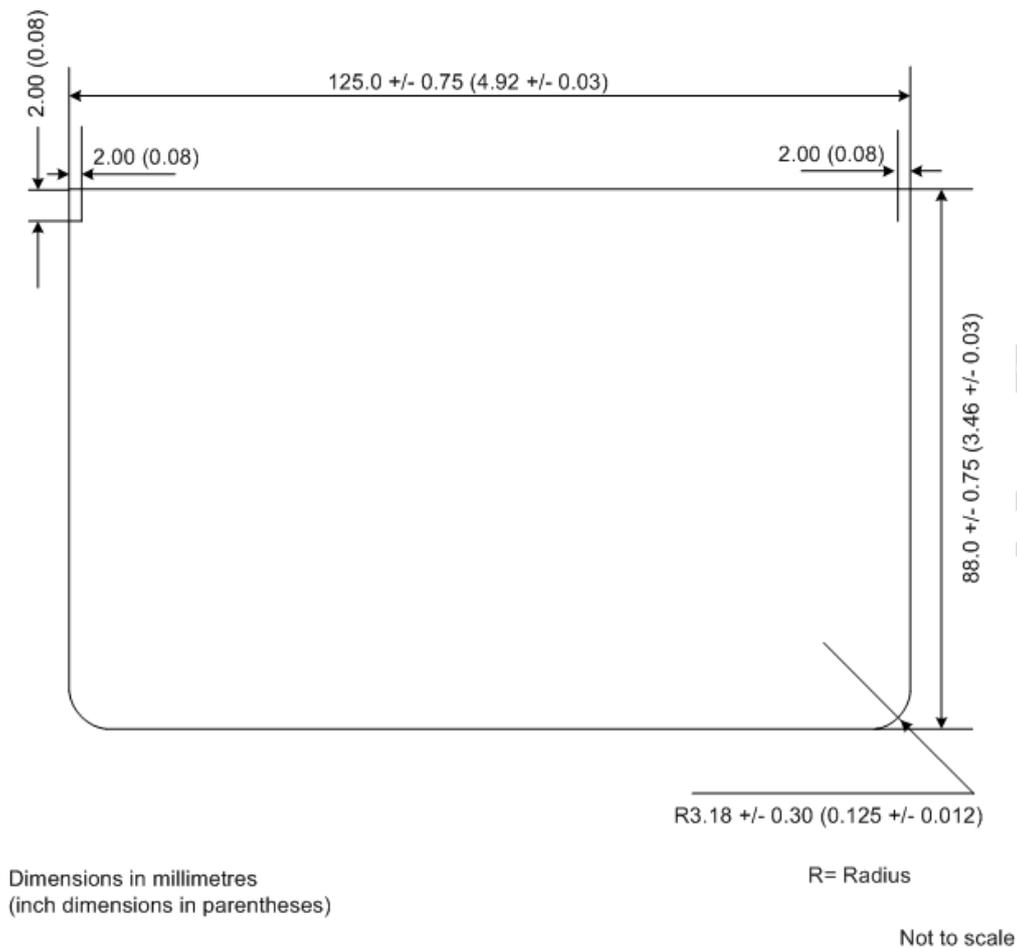


Figure 2: Edge margins of the MRP data page

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).

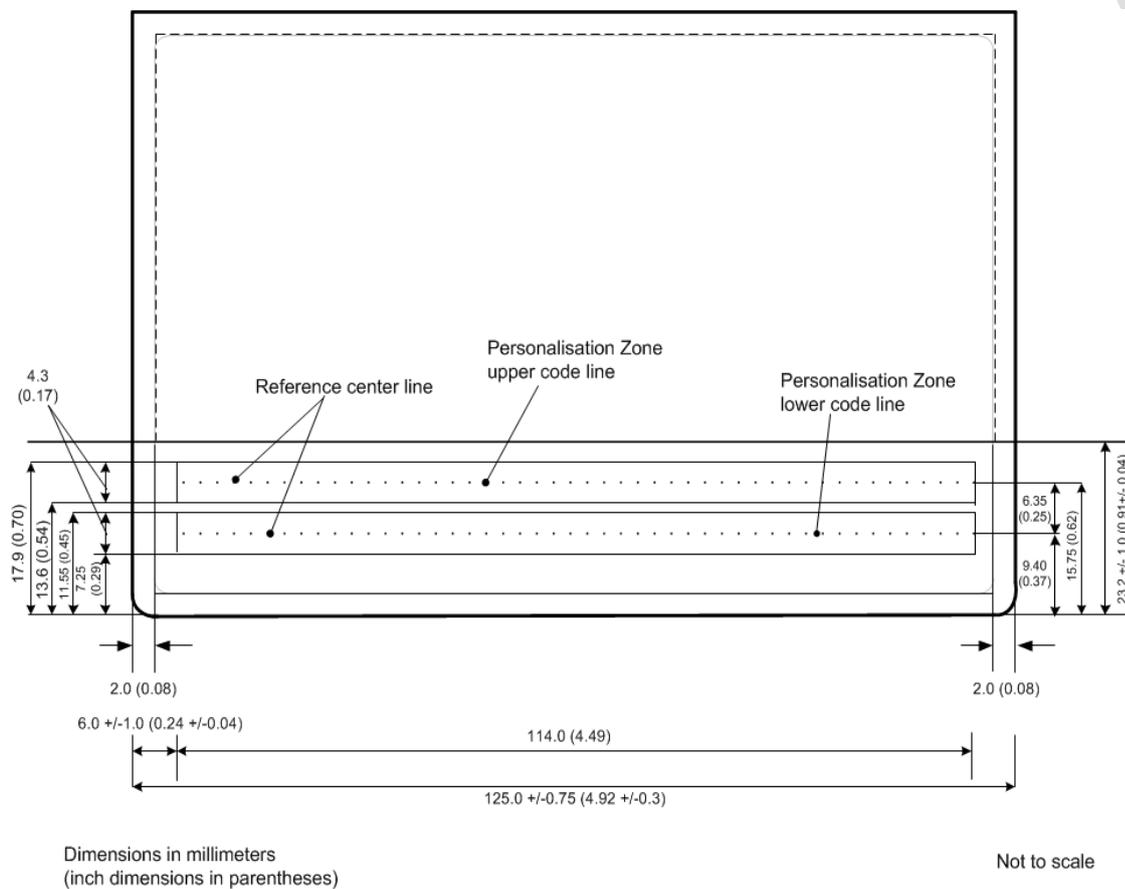


Figure 3: Schematic diagram of the Machine Readable Zone (MRZ)

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 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 Chapter 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 be located in Zone VI, Field 18 on the back of the MRP data page or on 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.

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 this Part (Part 4) of the specifications.

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.

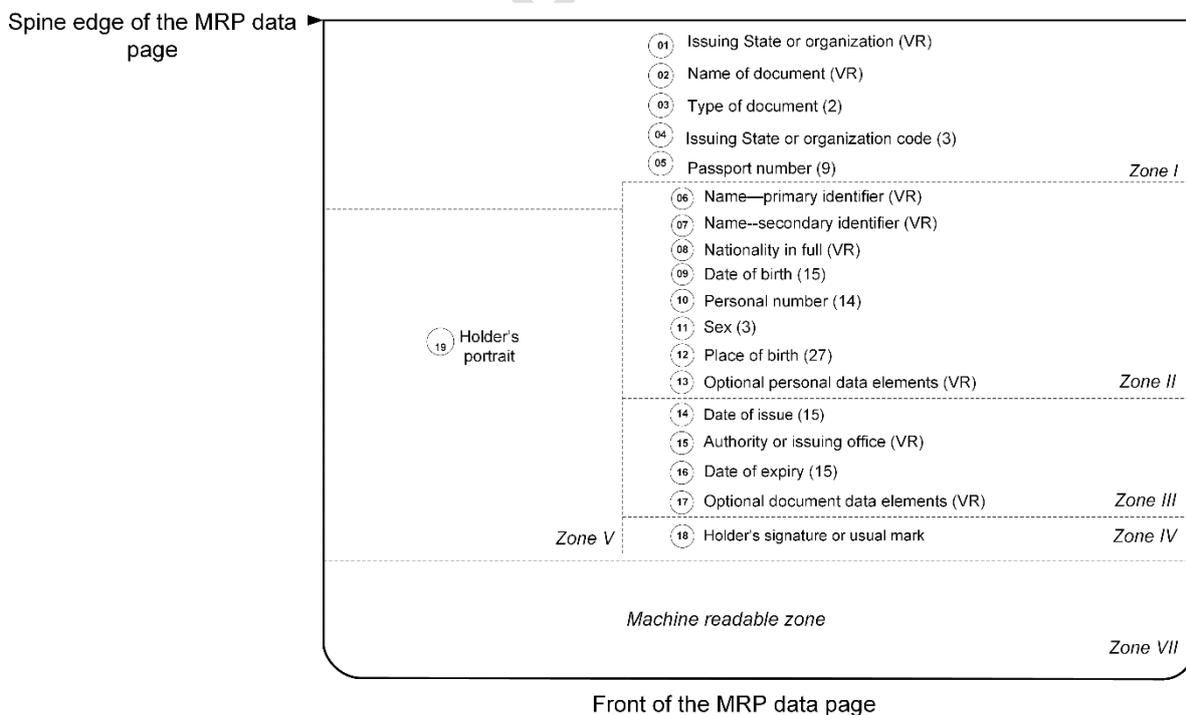
Data elements shall appear in a standard sequence as shown in Figures 4 and 5. Figure 6 is a schematic of the nominal layout of data elements on the front side of an MRP data page and Figure 7 is a template for the position of the personalized data fields.

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 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.



Not to scale

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

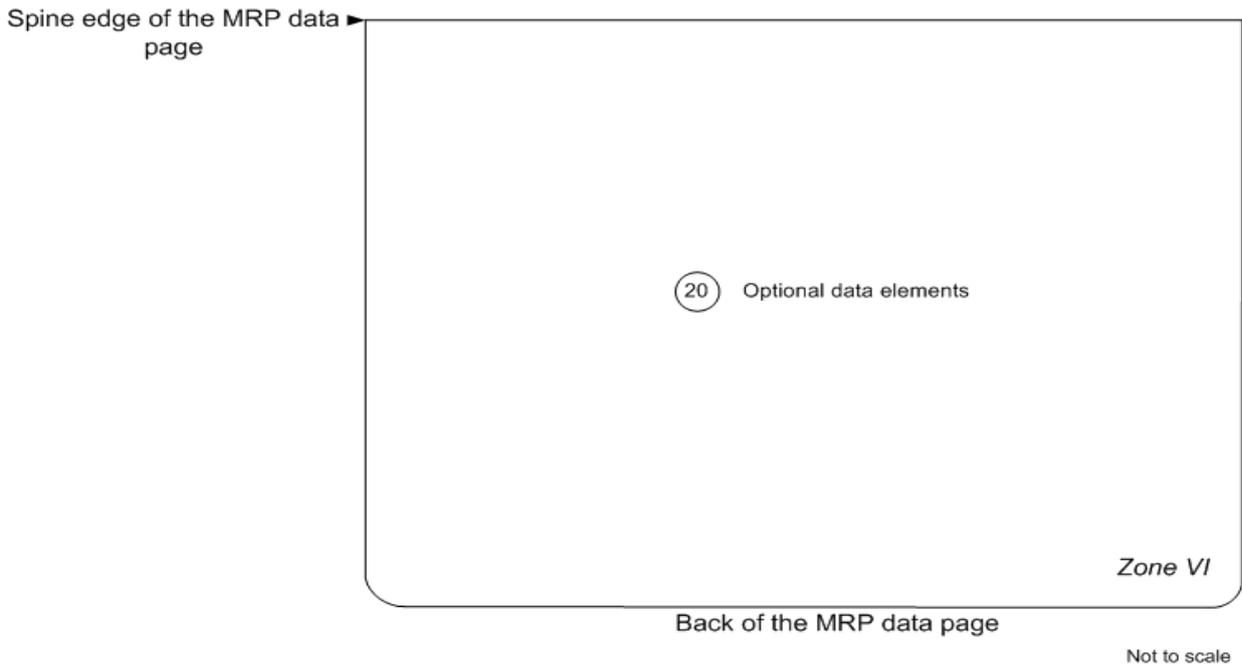


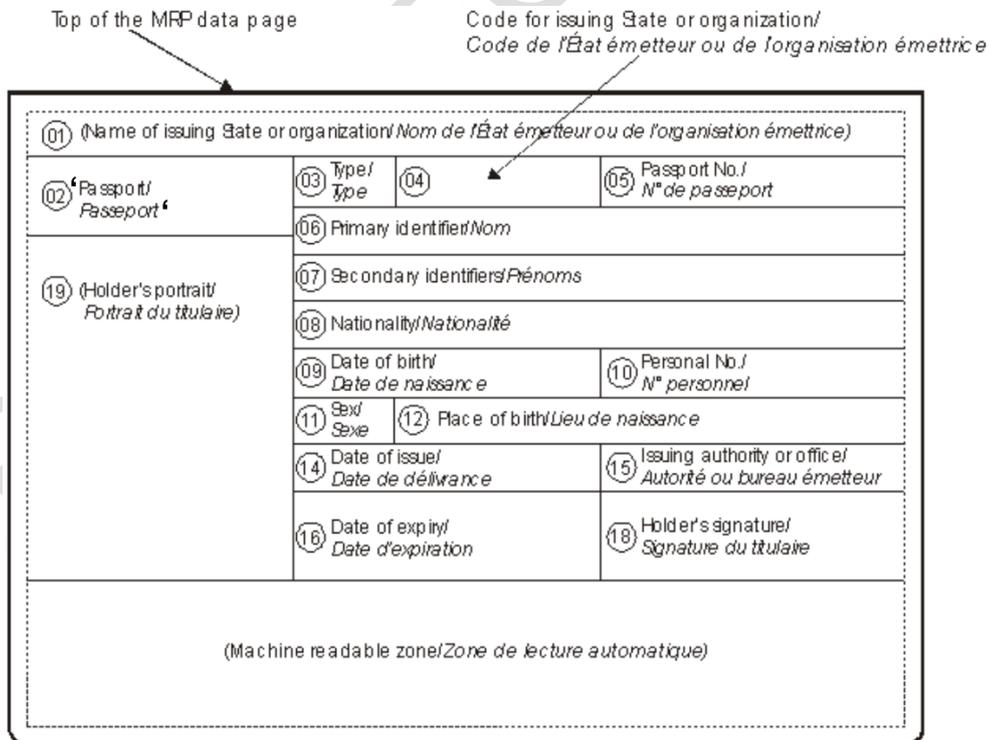
Figure 5: Data elements on reverse side

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



Not to scale

Figure 6: Schematic of nominal layout of data elements

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.

(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.

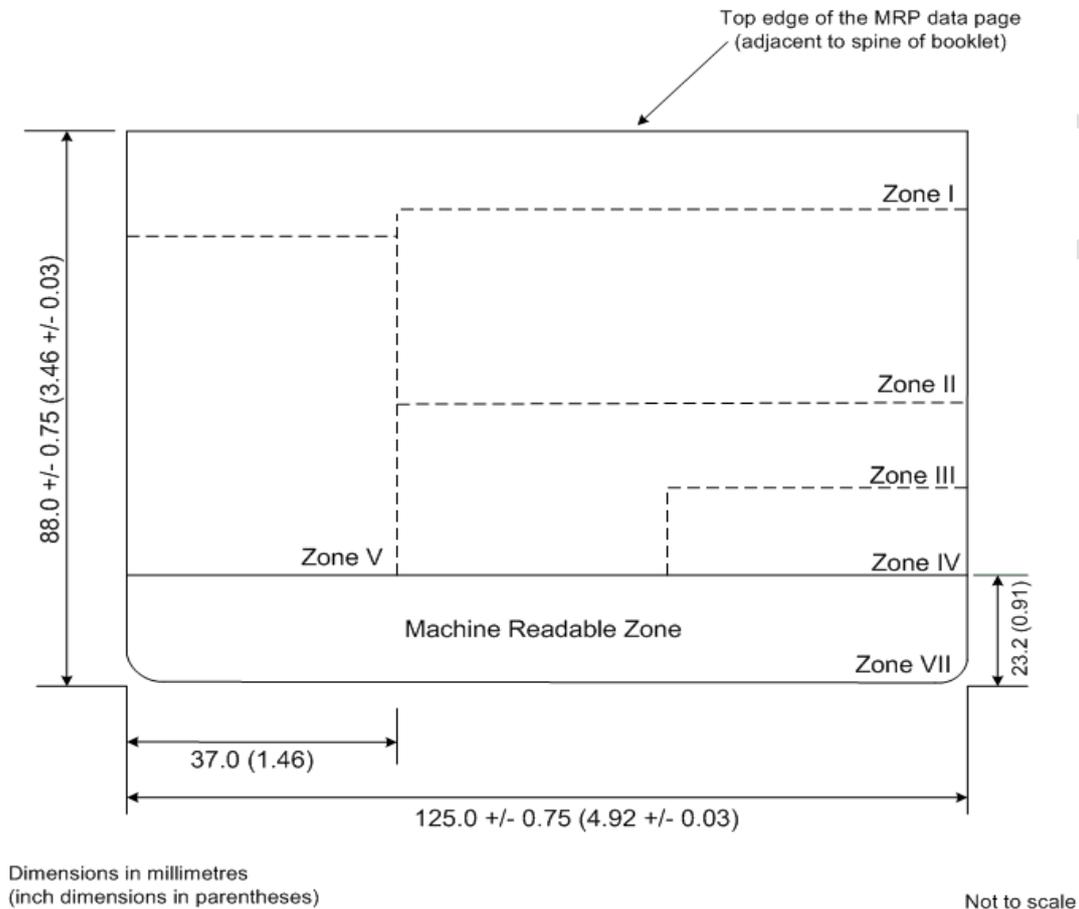


Figure 8: Nominal positions of zones I-V

Notes:

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

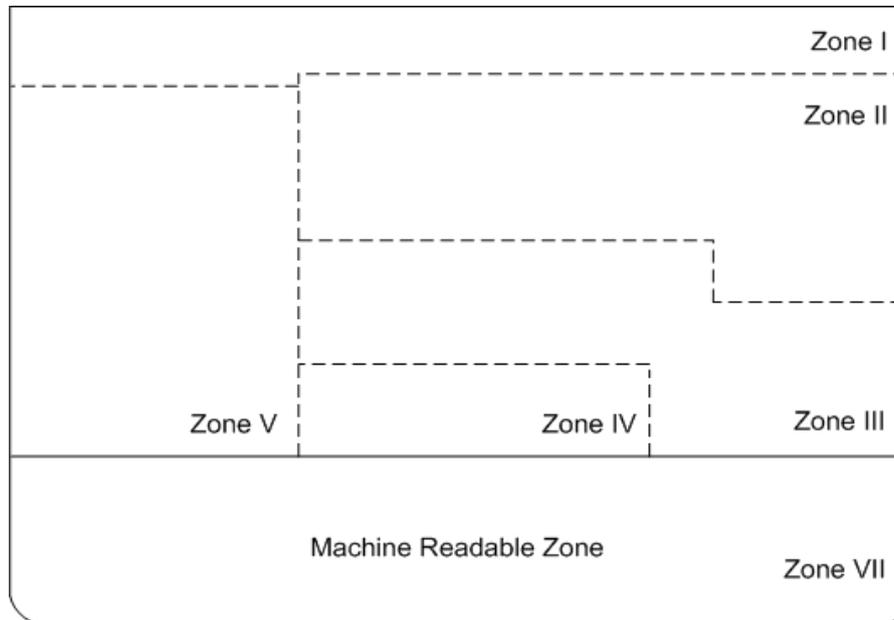
Zone V shall be located such that its left edge is coincident with the left edge of the MRP data page as shown in Figure 8. The dimensions of the portrait contained in Zone V are specified in Paragraph 4.1.1.1, the Visual data element directory, field 19.

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.



Not to scale

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

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.

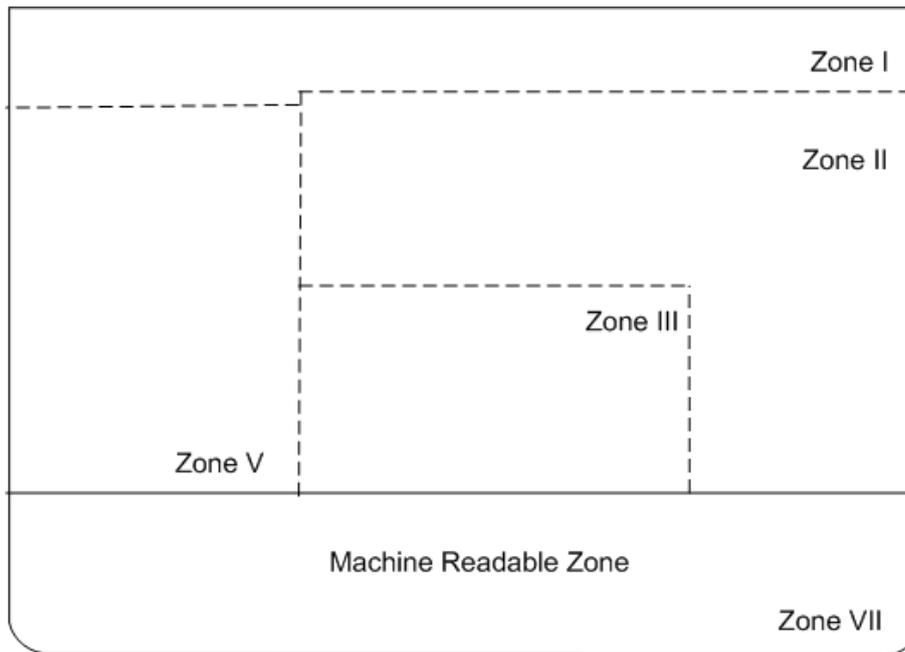


Figure 10: Example of flexible positioning of zones in which Zone IV (signature) is moved to an adjacent page and Zone III positioned such that it does not extend to the right-hand edge of the data page

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	Variable	Notes a, c, d, g, m, n. If omitted, shall appear on an adjacent or

Field/ zone no.	Data element	Specifications	Maximum no. of character positions	References and notes*
		language of the Issuing State or organization is not English, French or Spanish. For additional details see Doc 9303-3		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, an MRP issued for travel on government business, or a passport issued for a special purpose.	2	Notes a, g, l, m
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 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	Variable	Notes a, c, k, g, l

Field/ zone no.	Data element	Specifications	Maximum no. of character positions	References and notes*
		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 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 a dash 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
13/II (Optional element in mandatory zone)	Optional personal data elements	Optional personal data elements e.g. personal identification number or fingerprint, at the discretion of the Issuing State or organization. If a fingerprint is included in this field, it should be presented as a 1:1 representation of the original. If a date is included it shall follow the form of presentation described in Doc 9303-3.	Variable	Notes a, b, c, e, g, i
14/III (Mandatory)	Date of issue	For details see Doc 9303-3	Variable	Notes a, b, c, g, i, l
15/III (Mandatory)	Authority or Issuing Organization	Authority or Issuing Organization for the MRP. This field shall be used to indicate the Issuing Authority or Issuing Organization and, optionally, its location, which may be personalized within this field. For additional details see Doc 9303-3	Variable	Notes a, b, c, f, g, j, l
16/III (Mandatory)	Date of expiry	Date of expiry of the MRP. For additional details see Doc 9303-3	Variable	Notes a, b, c, g, l
17/III Optional element in mandatory	Optional document data elements	Optional data elements relating to the document. For additional details see Doc 9303-3	Variable	Notes a, b, c, e, g

Field/ zone no.	Data element	Specifications	Maximum no. of character positions	References and notes*
zone				
18/IV (Mandatory)	Holder's signature or usual mark	At the discretion of the Issuing State or organization, the signature or usual mark may be located in Zone VI. The size of the field to be allocated to the signature or usual mark on the adjoining page shall be at the discretion of the Issuing State or organization, subject to the overall dimensional limits of the MRP. For additional details see Doc 9303-3	Variable	Notes e, j
19/V (Mandatory)	Identification Feature	This field shall contain a portrait of the holder. The portrait shall not be larger than 45.0 mm x 35.0 mm (1.77 in x 1.38 in) nor smaller than 32.0 mm x 26.0 mm (1.26 in x 1.02 in). The position of the field concerned shall be aligned to the left of Zones II, III and IV See Doc 9303-3 for additional specifications for the portrait.		Note d
20/VI (Optional)	Optional data Elements	Additional optional data elements at the discretion of the Issuing State or organization. For additional details see Doc 9303-3		Notes a, b, c, e, g, i

Notes can be found following paragraph 4.2.2.2

4.2 Machine Readable Zone (MRZ) (Zone VII)

4.2.1 Data Position, Data Elements and Print Position in the MRZ

4.2.1.1 Data Position

The MRZ is located on the front of the MRP data page. Figure 3 defines the location of the MRZ and the nominal position of the data therein.

4.2.1.2 Data Elements

The data elements corresponding to Fields 03 to 09, 11 and 16 of the VIZ shall be personalized in machine readable form, in the MRZ, beginning with the left most character position in each field in the sequence indicated in the data structure specifications shown below. Figure 15 indicates the structure of the MRZ.

4.2.1.3 Print Position

The position of the left-hand edge of the first character shall be 6.0 ± 1.0 mm (0.24 ± 0.04 in) from the left-hand edge of the document. Reference centre lines for the OCR lines and the minimum starting position for the first character of each line are shown in Figure 3. The positioning of the characters is indicated by those reference lines and by the printing zones for the two code lines in Figure 7.

4.2.2 Data Structure of Machine Readable Data for the MRP Data Page

4.2.2.1 Data Structure of the Upper Machine Readable Line

MRZ character positions (line 1)	Field no. in VIZ	Data element	Specifications	Number of characters	References and notes*
1 to 2	03	Document code	The first character shall be P to designate an MRP. One additional letter may be used, at the discretion of the Issuing State or organization, to designate a particular MRP. If the second character position is not used for this purpose, it shall be filled by the filler character (<).	2	Notes a, d, m
3 to 5	04	Issuing State or organization	The three-letter code specified in Doc 9303-3 shall be used. Spaces shall be replaced by filler characters (<).	3	Notes a, d, f
6 to 44	06, 07	Name	For details see Doc 9303-3	39	Notes a, c, d
		Punctuation in the name	Representation of punctuation is not permitted in the MRZ. For details on apostrophes, hyphens and commas etc. see Doc 9303-3		
		Name prefixes and suffixes	For details see Doc 9303-3		
		Filler	When all components of the primary and secondary identifiers and required separators (filler characters) do not exceed 39 characters in total, all name components shall be included in the MRZ and all unused character positions shall be completed with filler characters (<) repeated up to position 44 as required.		
		Truncation of the name	When the primary and secondary identifiers and required separators (filler characters) exceed the number of character positions available for names (i.e. 39), they shall be truncated as follows: Characters shall be removed from one or more components of the primary identifier until three character positions are freed, and two filler characters (<<) and the first character of the first component of the secondary identifier can be inserted. The last character (position 44) shall be an alphabetic character (A through Z). This indicates that truncation may have occurred. Further truncation of the primary identifier may be carried out to allow characters of the secondary identifier to be included, provided that the name field shall end with an alphabetic character (position 44). This indicates that truncation may have occurred. When the name consists of only a primary identifier which exceeds the number of character positions available for the name, i.e. 39, characters shall be removed from one or more components of the name until the last character in the name field is an alphabetic character.		Notes a, d

* Notes can be found following paragraph 4.2.2.2

4.2.2.2 Data Structure of the Lower Machine Readable Line

MRZ character positions (line2)	Field no. in VIZ	Data element	Specifications	Number of Characters	References and notes*
1 to 9	05	Passport Number	As given by the Issuing State or organization to uniquely identify the document. Any special characters or spaces in the passport number as shown in the VIZ shall be replaced by the filler character (<). The number shall be followed by the filler character (<) repeated up to position 9 as required.	9	Notes a, b, d
10		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4	1	Notes b, d
11 to 13	08	Nationality	As a three-letter code representing the holder's nationality as listed in Doc 9303-3. Spaces are replaced by filler characters.	3	Notes a, d, f
14 to 19	9	Date of birth	See Doc 9303-3 for details	6	Notes b, d, i
20		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4	1	Notes b, d
21	11	Sex	F = female; M = male; < = unspecified.	1	Notes a, d
22 to 27	16	Date of expiry	See Doc 9303-3 for details.	6	Notes b, d, i
28		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Notes b, d
29 to 42	10	Personal number or other optional data elements	Any special characters, including spaces in the personal identification number given to the holder by the Issuing State or organization, shall be replaced by the filler character (<). The number shall be followed by the filler character (<) repeated up to position 42 as required. When the personal number field is not used, the character positions 29 to 42 in the second MRZ line should be completed with filler characters (<) (see also under "check digit", character position 43 below).	14	Notes a, b, d
43		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4. 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, d
44		Composite check Digit	Composite check digit for characters of machine readable data of the lower line in positions 1 to 10, 14 to 20 and 22 to 43, including values for letters that are a part of the number fields and their check digits. Shall be calculated as specified in Doc 9303-3	1	Notes b, d

* Notes to the Visual and Machine Readable data element directories:

- a) Alphabetic characters (A to Z) as defined in Doc 9303-3.
- b) Numeric characters (0 to 9) as defined in. Doc 9303-3

4.2.4 Check digits in the Machine Readable Zone

The data structure of the lower machine readable line specified in paragraph 4.2.2.2 provides for the inclusion of five check digits as follows:

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

4.3 Representation of the Issuing State or Organization and Nationality of Holder in the MRZ and the VIZ

Use of three-letter Country codes is mandatory in the MRZ and Field 04 in the VIZ and optional for the holder's nationality in the VIZ. Specific locations are defined in the following table:

	<i>Zone</i>	<i>Field no.</i>	<i>Character position no.</i>	<i>Number of character positions</i>
Issuing State or organization	VIZ	04	3-5	3
	MRZ (upper line)			3
Holder's nationality	VIZ	08	11-13	variable
	MRZ (lower line)			3

REFERENCES (NORMATIVE)

[ISO/IEC 7810] ISO/IEC 7810:2003, Identification Cards – Physical Characteristics

DRAFT_4 FOR TAG_22

Doc 9303



Machine Readable Travel Documents

Part 5
**Specifications specific to TD1 Size MROTDs, Machine Readable Official
Travel Documents**

Approved by the Secretary General
and published under his authority

Seventh Edition — Revision 1 - 2014

International Civil Aviation Organization

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

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

Doc 9303, Machine Readable Travel Documents
Order Number: xxxx
ISBN xxx-xx-xxxx-xxx-x

© ICAO 2014

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 TO DOC 9303-5, 7TH EDITION

Revision	Date	Description
01	xx-xx-2014	Initial release of the 7 th edition

DRAFT_4 FOR TAG_22

TABLE OF CONTENTS

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	3
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
4.3	Representation of the Issuing State or Organization and Nationality of the Holder in the MRZ and the VIZ.....	15
APPENDIX A	EXAMPLES OF A PERSONALIZED TD1 SIZE MROTD (INFORMATIVE)	16
APPENDIX B	CONSTRUCTION OF THE MACHINE READABLE ZONE OF A TD1 SIZE MROTD (INFORMATIVE) 18	
APPENDIX C	TECHNICAL SPECIFICATIONS FOR A MACHINE READABLE CREW MEMBER CERTIFICATE – CMC (INFORMATIVE)	19
C.1	Scope	19
C.2	Content and Use of Zones	19
REFERENCES (NORMATIVE)	21

1 SCOPE

The seventh edition of Doc 9303 represents a re-structuring of the ICAO specifications for Machine Readable Travel Documents. Without incorporating substantial modifications of 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 5 of Doc 9303 is based on Doc 9303 Part 3, Machine Readable Official Travel Documents Volume 1, 3rd Edition 2008.

Doc 9303-5, defines specifications that are specific to TD1 Size Machine Readable Official Travel documents (MROTDs) and should be read in conjunction with:

- Part 1 - Introduction;
- Part 2 - Specifications for the security of the design, manufacture and issuance of Machine Readable Travel Documents;
- Part 3 - Specifications common to all Machine Readable Travel Documents.

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 may be found in Doc 9303 Parts 9 through 12.

2 DIMENSIONS OF THE TD1 SIZE MROTD

2.1 Nominal Dimensions

The nominal dimensions shall be those specified in ISO/IEC 7810 for the ID-1 type card:

53.98 mm × 85.6 mm (2.13 in × 3.37 in).

2.2 Edge Tolerances

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

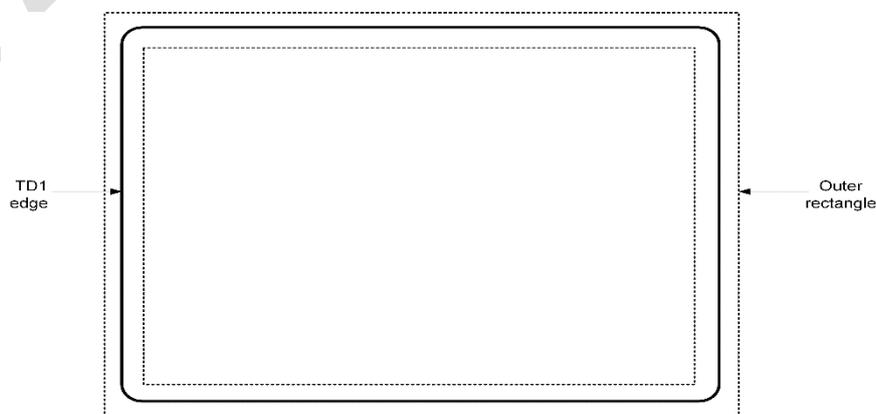


Figure 1: TD1 dimensional illustration

Inner rectangle: 53.25 mm × 84.85 mm (2.10 in × 3.34 in)
Outer rectangle: 54.75 mm × 86.35 mm (2.16 in × 3.40 in)

In no event shall the dimensions of the finished TD1 document exceed the dimensions of the outer rectangle, including any final preparation (e.g. laminate edges).

2.3 Margins

The dimensional specifications refer to the outer limits of the TD1. A margin of 2.0 mm (0.08 in) along each outer edge, with the exception of the header zone, must be left clear of data. See Figure 2

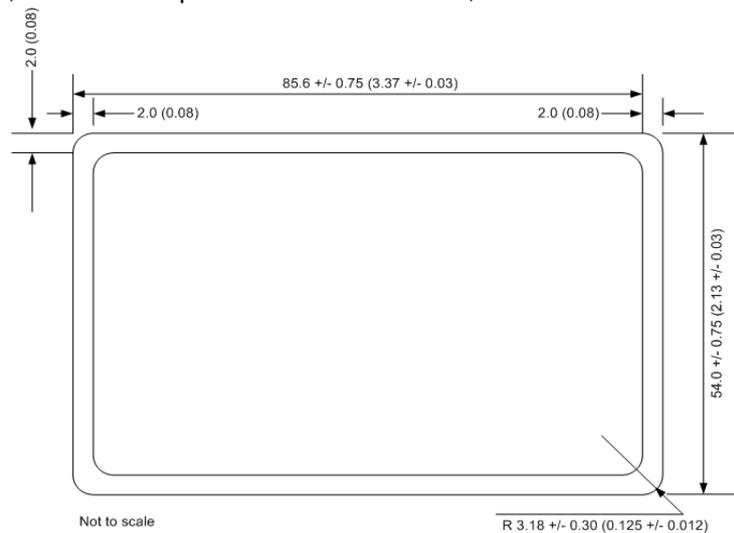


Figure 2: Edge margins and nominal dimensions of a TD1 Size MROTD

2.4 Thickness

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

- *Minimum:*
0.25 mm (0.01 in);
- *Maximum:*
1.25 mm (0.05 in).

The thickness of the area within the machine readable zone shall not vary by more than 0.1 mm (0.004 in).

Note.— The tolerances specified above differ from those specified in ISO/IEC 7810 for the ID-1 size card. This is for historical reasons; TD1 cards were originally produced using encapsulated pouch card methods which are incapable of achieving the permitted tolerances of ISO/IEC 7810. Some cards may still be produced using these techniques and others where the personalization process renders it impractical to achieve ISO/IEC 7810 tolerances. Wherever possible, however, dimensions and tolerances should conform to ISO/IEC 7810.

General note.— The decimal notation used 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.

3 GENERAL LAYOUT OF THE TD1 SIZE MROTD

The MROTD follows a standardized layout to facilitate reading of data globally by both visual and machine readable means (global interoperability).

3.1 TD1 Zones

To accommodate the various requirements of States' laws and practices and to achieve the maximum standardization within those divergent requirements, the MROTD is divided into seven zones as listed below in paragraphs 3.1.1 and 3.1.2. Zones I through VI constitute the visual inspection zone (VIZ). Zone VII is the machine readable zone (MRZ).

The location, contents and dimensional specifications of zones are described below in Paragraphs 3.2 to 3.3.

3.1.1 Front of the TD1

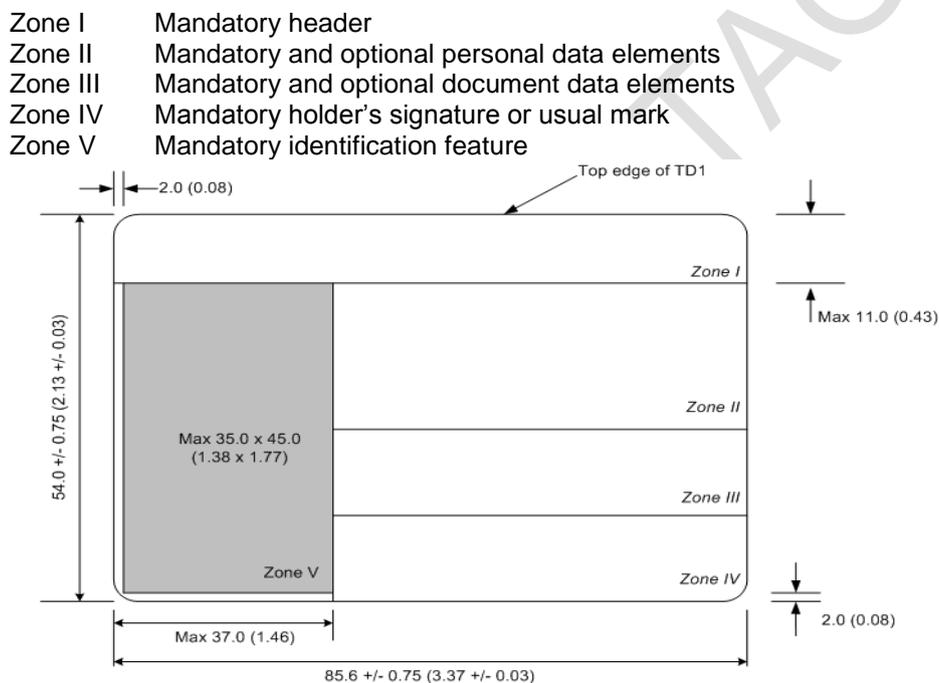


Figure 3: Nominal layout of the zones on the front side of a TD1 Size MROTD

3.1.2 Back of the TD1

Zone VI Optional data elements

Zone VII Mandatory Machine Readable Zone (MRZ)

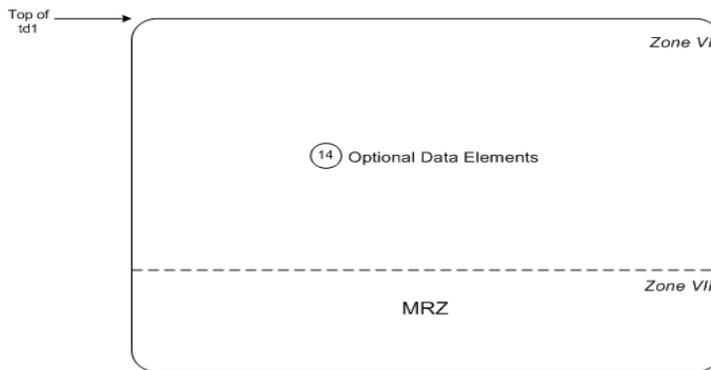


Figure 4: Layout of zones on the reverse side of a TD1

3.2 Content and Use of Zones

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 hereunder.

Zones I to V and Zone VII contain mandatory elements which represent the minimum requirements for the TD1. 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 shown in Figures 3 to 5. Figures 7 to 9 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. Examples of a personalized TD1 are shown in Appendix A, Figures 11 to 14.

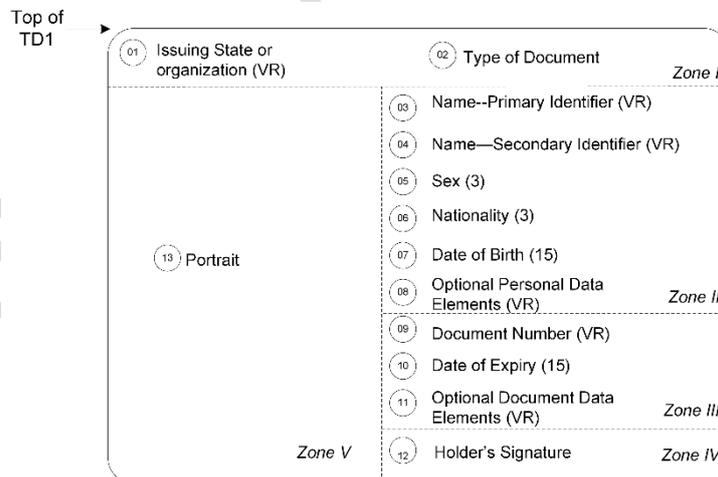


Figure 5: Sequence of data elements on the front side of a TD1

3.2.1 Mandatory Zones

Zone I on the front of the MROTD identifies the Issuing State or organization and the document.

Data elements shall appear in a standard sequence in Zones II and III. Zones II and III each contain a field in which optional data elements may be included. The optional field in Zone II shall be used for personal data elements and the optional field in Zone III for document-related data elements. Where an

Issuing State or organization does not use the optional fields in Zones II and III, there is no need to reserve the space for them on the TD1.

Zone IV contains the holder’s signature or usual mark. The Issuing State or organization shall decide the acceptability of a holder’s usual mark.

Zone V shall contain the personal identification feature(s) which shall include a portrait solely of the 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.

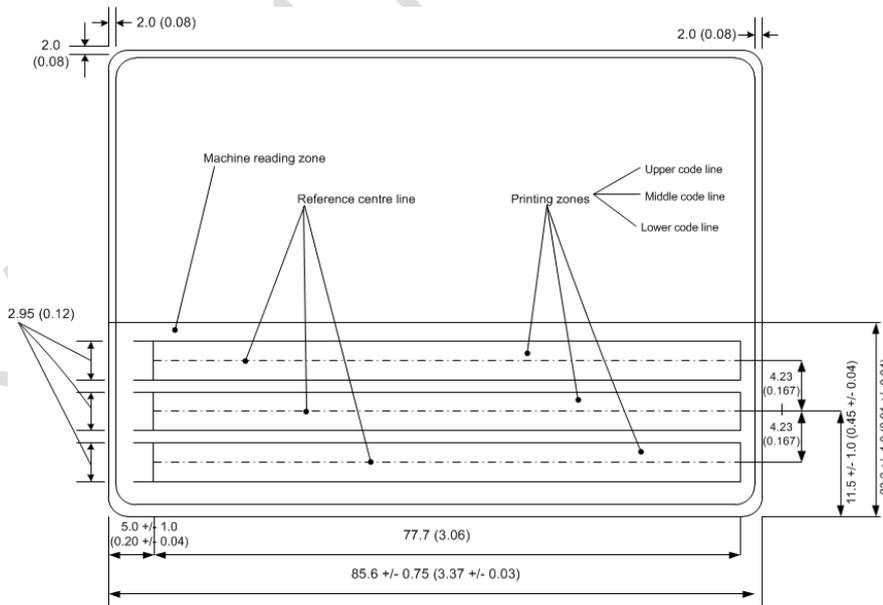
The standard position for the holder’s portrait is along the left edge of the front of the TD1, as described in paragraph 3.3 and illustrated in Figure 3.

When an Issuing State or organization chooses, for its own or for bilateral purposes, to expand the machine readable data capacity of a TD1 through use of an integrated circuit with contacts, the holder’s portrait (Zone V) shall be relocated such that its right edge is coincident with the right edge of the front of the TD1. Zones II, III and IV shall in turn be relocated to have their left edge coincident with the left edge of the front of the TD1. The specifications for Zones II through IV are similar to those defined in paragraph 3.3, but adjusted to accommodate the relocation of the portrait to the right and to avoid the area containing the contacts of the IC as defined by ISO/IEC 7816-2.

The size of the portrait is given in the data element directory for the Visual Zone Paragraph 4.1.1.1 field 13/V.

Zone VII shall contain the machine readable data. Because of the smaller size of the TD1, to accommodate the required data, three lines of machine readable data are included in the MRZ. Detailed specifications for the MRZ of the TD1 are given in Paragraph 4.2. 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 ICAO Doc 9303-3.

All MRZ data elements shall be shown in Zone VII. For a TD1 Size MROTD, these are defined in Paragraph 4.2.2 and positioned as shown below.



Not to scale

Figure 6: Position and dimensions of Zone VII the Machine Readable Zone

Optional Data Zone

Zone VI, which appears on the back of the MROTD, is a zone for optional data for use at the discretion of the Issuing State or organization. Zone VI will always appear irrespective of whether or not it is used.

3.2.2 Card Access Number

In the case of TD1 Size MROTDs containing a contactless IC, Issuing States or organizations may, at their discretion, wish to include a Card Access Number (CAN) on the front side of the card to facilitate machine reading and data capture from the card. Specifically, the purpose of the CAN is to enable the front side of the card to be read AND the chip to be accessed without flipping the card to read the MRZ on the rear. When the chip supports PACE V2, this can be accomplished by adding a CAN on the front side of a TD1 Size card. The CAN and its position on the front side of the MROTD are specified as follows:

The CAN is a 6-digit number, comprised solely of numerals, 0 to 9. There is no check digit, since the check is implicitly performed by the protocol. Font, field and background are conforming to the specifications for the MRZ set out in Doc 9303-3. Vertical position is conforming to the vertical position of any one of the three MRZ lines as specified in this document and shown in Figure 6, above. The horizontal position shall be at the discretion of the Issuing State or organization, but shall not overlap the portrait area (Zone V) or interfere with the legibility of other data in the VIZ.

Further information concerning the technical specifications, derivation and implementation of CAN's may be found in Doc 9303-11.

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 TD1 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 TD1. Examples of flexible location of the zones are shown in Figures 7 to 10.

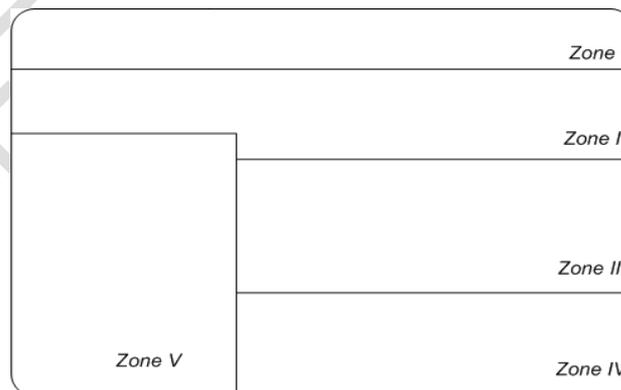


Figure 7: Flexible zone layout with Zone II extending above the portrait

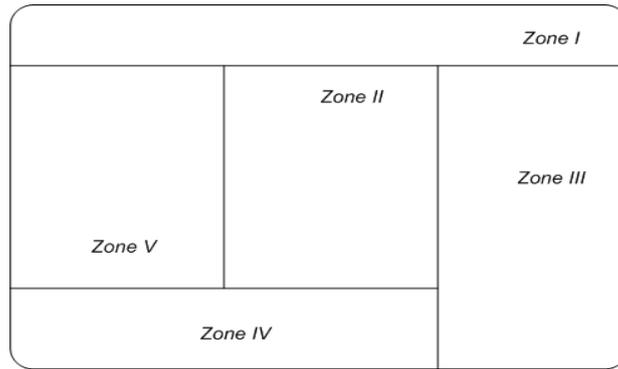


Figure 8: Flexible zone layout with Zone IV, Signature, beneath the portrait

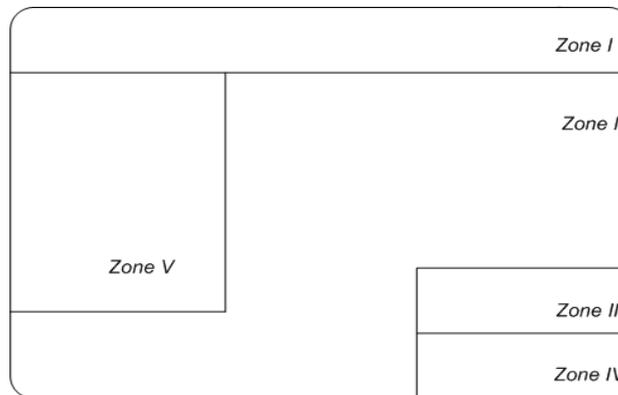


Figure 9: Flexible zone layout with Zone II extending beneath the portrait

When an Issuing State or organization chooses to produce a TD1 that contains a transparent or otherwise unprintable border around the card, this will result in a reduction of the available area within the zones. The full TD1 dimensions and zone boundaries shall be measured from the outside edge of this border, which is the external edge of the TD1.

Zone I shall be located along the top edge of the TD1 and extend across the full width of the document. 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 11.0 mm (0.43 in).

Zone V shall be located such that its left edge is coincident with the left edge of the TD1. Zone V may vary in size but shall not exceed the maximum dimensions specified in Figure 10.

Zone V may move *vertically* along the left edge of the TD1 and overlay a portion of Zone I as long as individual details contained in either zone are not obscured. The scope for such movement is illustrated in Figure 10.

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 field to extend across the TD1, Zone II may extend up to the full width of the TD1 as illustrated in Figure 13. In the event 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 are not obscured. Figures 8 and 10 illustrate a Zone II design less than the full dimensional width of the document.

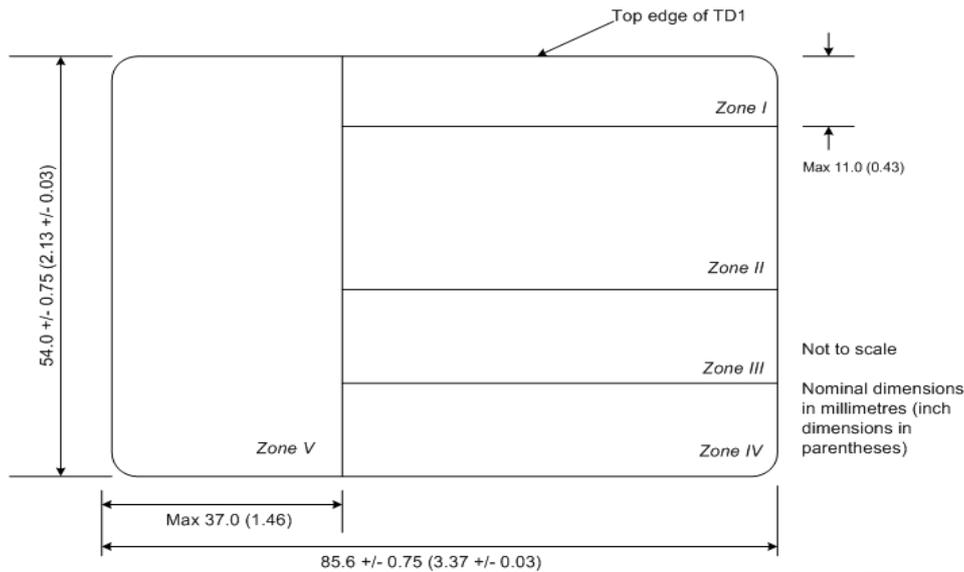


Figure 10: Alternate layout showing flexibility for Zone V to overlay a portion of Zone I

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 longer dimension of the TD1. Figure 9 illustrates a Zone II with the lower boundary on two levels. The flexible design for the Zone II illustrated conforms with the specifications defined above.

Zone III may 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 TD1. Figures 7 to 9 illustrate some options for a flexible layout of Zone III.

The position of Zone IV is illustrated in the above diagrams, Figures 7 to 10 and in the examples in Appendix A, figures 11 and 13. Zone IV may overlay Zone V, as illustrated in figure 13, although this is not recommended practice. In this case, Issuing States or organizations shall ensure that individual details contained in either zone are not obscured.

4 CONTENTS OF A TD1 SIZE MROTD

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

All data in the VIZ shall be clearly legible.

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 TD1 consistent with the requirement for sequencing zones and data elements.

4.1.1 Data Element Directory

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	The name of the State or organization responsible for issuing the travel document shall be displayed. See Doc 9303-3 for further details.	Variable	Notes a, c, e, h, i
02/I (Mandatory)	Document	The type or designation of the document. For additional details see Doc 9303-3	Variable	Notes a, b, c, e, i
03/04/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, i, l
03/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) 03 and/or 04 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, i, l
04/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 represented by initials. Where the holder's name has only predominant component(s), this data field shall be left blank. The State or organization may optionally utilize the whole zone comprising Fields 03 and 04 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.	Variable	Notes a, c, i, l
05/II (Mandatory)	Sex	Sex of the holder, to be specified by use of the single initial commonly used in the language of the State or organization 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, f, i, l
06/II (Mandatory)	Nationality	For details see Doc 9303-3	Variable	Notes a, h, l
07/II (Mandatory)	Date of birth	Holder's date of birth as recorded by the Issuing State or organization. For unknown dates see Doc 9303-3.	15	Notes a, b, c, i, l
08/II Optional element in mandatory	Optional personal data elements	Optional personal data elements, e.g. personal identification number or fingerprint, at the discretion of the Issuing State or organization. If a fingerprint is included in this field, it should	Variable	Notes a, b, c, d, g, i

Field/ zone no.	Data element	Specifications	Maximum no. of character positions	References and notes*
zone		be presented as a 1:1 representation of the original. If a date is included, it shall follow the form of presentation described in Doc 9303-3.		
09/III (Mandatory)	Document 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	Variable	Notes a, b, c, i, j, l
10/III (Mandatory)	Date of expiry	Date of expiry of the document. For additional details see Doc 9303-3	15	Notes a, b, c, i, l
11/III Optional element in mandatory zone	Optional document data elements	Optional data elements relating to the document. For additional details see Doc 9303-3	Variable	Notes a, b, c, d, g, i
12/IV (Mandatory)	Holder's signature or usual mark	Signature or usual mark of the holder. For additional details see Doc 9303-3		Note e
13/V (Mandatory)	Identification feature	This field shall contain a portrait of the holder. The portrait shall not be larger than 45.0 mm x 35.0 mm (1.77 in x 1.38 in) nor smaller than 32.0 mm x 26.0 mm (1.26 in x 1.02 in). The position of the field concerned shall be along the left edge of the front of the TD1 except where a State chooses to incorporate an integrated circuit with contacts (See Paragraph 3.2.1). See Doc 9303-3 for additional specifications for the portrait.		Note e
14/VI (Optional)	Optional data elements	Additional optional data elements at the discretion of the Issuing State or organization. For additional details see Doc 9303-3		Notes a, b, c, d, g, i

4.2 Machine Readable Zone (MRZ) (Zone VII)

4.2.1 Data Position, Data Elements and Print Position in the MRZ

4.2.1.1 Data Position

The MRZ is located on the back of the TD1. Figure 6 shows the nominal dimensions and position of the data in the MRZ

4.2.1.2 Data Elements

The data elements corresponding to specified fields of the VIZ shall be printed, in machine readable form, in the MRZ, beginning with the left most character position in each field in the sequence indicated in the data structure specifications. Figure 15 indicates the structure of the MRZ

4.2.1.3 Print Position

The position of the left-hand edge of the first character shall be 5.0 ± 1.0 mm (0.20 ± 0.04 in) from the left-hand edge of the document. Reference centre lines for the OCR lines and a nominal starting position for the first character of each line are shown in Figure 6. The positioning of the characters is indicated by those reference lines and by the printing zones of the three code lines in Figure 6.

4.2.2 Data Structure of Machine Readable Data for the TD1

4.2.2.1 Data Structure of the Upper Machine Readable Line

MRZ character positions (line 1)	Field no. in VIZ	Data element	Specifications	Number of characters	References and notes*
1 to 2	02	Document code	Two characters, the first of which shall be A, C or I, shall be used to designate the particular type of document. The second character shall be as specified in Note k.	2	Notes a, b, c, e, k
3 to 5	01	Issuing State or organization	The three-letter code specified in Doc 9303-3, shall be used. Spaces shall be replaced by filler characters (<).	3	Notes a, c, e
6 to 14	09	Document number	As given by the Issuing State or organization, to uniquely identify the document from all other MROTDs issued by the State or organization. Spaces shall be replaced by filler characters (<). For additional details see Doc 9303-3	9	Notes a, b, e, j
15		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Notes b, c, j
16 to 30	8, 11 or Zone VI	Optional data elements	For optional use. Unused character positions shall be completed with filler characters (<) repeated up to position 30 as required.	15	Notes a, b, c, e, j

4.2.2.2 Data Structure of the Middle Machine Readable Line

MRZ character positions (line 2)	Field no. in VIZ	Data element	Specifications	Number of characters	References and notes*
1 to 6	07	Date of birth	For details see Doc 9303-3	6	Notes b, c, e
7		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Note b
8	05	Sex	F = female; M = male; < = unspecified.	1	Notes a, c, e, f
9 to 14	10	Date of expiry	For details see Doc 9303-3	6	Notes b, e
15		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Note b
16 to 18	06	Nationality	For details see Doc 9303-3	3	Notes a, c, e, h

<i>MRZ character positions (line 2)</i>	<i>Field no. in VIZ</i>	<i>Data element</i>	<i>Specifications</i>	<i>Number of characters</i>	<i>References and notes*</i>
19 to 29	08, 11 or Zone VI	Optional data Elements	For use of the Issuing State or organization. Unused character positions shall be completed with filler characters (<) repeated up to position 29 as required. For additional details see Doc 9303-3	11	Notes a, b, c, e
30		Composite check Digit	Composite check digit to verify the data element of the upper and middle machine readable lines. Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Note b

4.2.2.3 Data Structure of the Lower Machine Readable Line

<i>MRZ character positions (line 3)</i>	<i>Field no. in VIZ</i>	<i>Data element</i>	<i>Specifications</i>	<i>Number of characters</i>	<i>References and notes*</i>
1 to 30	03, 04	Name	<p>The name consists of primary and secondary identifiers which shall be separated by two filler characters (<<). Components within the primary or secondary identifiers shall be separated by a single filler character (<).</p> <p>When the name of the document holder has only one part, it shall be placed first in the character positions for the primary identifier, filler characters (<) being used to complete the remaining character positions of the MRZ. For additional details see Doc 9303-3</p>	30 (Primary identifier(s), secondary identifier(s) and fillers)	Notes a, c, e
		Punctuation in the name	Representation of punctuation is not permitted in the MRZ For details on apostrophes, hyphens and commas etc see Doc 9303-3		
		Name prefixes and suffixes	For details see Doc 9303-3		
		Filler	When all components of the primary and secondary identifiers and required separators (filler characters) do not exceed 30 characters in total, all permitted name components shall be included in the MRZ, and all unused character positions shall be completed with filler characters (<) repeated up to position 30 as required.		
		Truncation of the name	When the primary and secondary identifiers and required separators (filler characters) exceed the number of character positions available for names		Notes a, c, e and 4.2.3

MRZ character positions (line 3)	Field no. in VIZ	Data element	Specifications	Number of characters	References and notes*
			(i.e. 30), they shall be truncated as follows: Characters shall be removed from one or more components of the primary identifier until three character positions are freed and two filler characters (<<) and the first character of the first component of the secondary identifier can be inserted. The last character (position 30) shall be an alphabetic character (A through Z). This indicates that truncation may have occurred. Further truncation of the primary identifier may be carried out to allow characters of the secondary identifier to be included, provided that the name field shall end with an alphabetic character (position 30). This indicates that truncation may have occurred. When the name consists of only a primary identifier which exceeds the number of character positions available for the name, i.e. 30, characters shall be removed from one or more components of the name until the last character in the name field is an alpha character.		

*Notes relating to paragraphs 4.1.2 and 4.2.2

- a) Alphabetic characters (A–Z). National characters may be included in the VIZ. In the MRZ only the characters defined in Doc 9303-3 shall be used.
- b) Numeric characters (0–9). National numerals may be additionally included in the VIZ. In the MRZ only the numerals 0–9 may be used as defined in Doc 9303-3.
- c) Punctuation may be included in the VIZ. In the MRZ only the filler character specified in Doc 9303-3 may be used.
- d) Optional data elements may appear in Zone VI.
- e) The field caption is not printed on the document.
- f) Where a person does not wish his/her sex to be identified or where an Issuing State or organization does not want to show this data, the filler character (<) shall be used in this field in the MRZ and an X in this field in the VIZ.
- g) The use of a caption to identify a field is at the option of the Issuing State or organization.
- h) In the case of a document issued by the United Nations Organization, or one of its specialized agencies, to a designated official, the appropriate organization code is used in lieu of nationality. See Doc 9303-3.
- i) Blank spaces between words shall count towards the maximum number of characters permitted in the field
- j) The number of characters in the VIZ may be variable; however, if the document number has more than 9 characters, the 9 principal characters shall be shown in the MRZ in character positions 6 to 14. They shall be followed by a filler character instead of a check digit to indicate a truncated number. The remaining characters of the document number shall be shown at the beginning of the field reserved for optional data elements (character positions 16 to 30 of the upper machine readable line) followed by a check digit and a filler character.
- k) The first character shall be A, C or I. Historically these three characters were chosen for their ease of recognition in the OCR-B character set. The second character shall be at the discretion of the Issuing State or organization except that V shall not be used, and C shall not be used after A except in the crew member certificate.
- l) The field caption shall be printed on the document.

4.2.3 Truncation of Names in the MRZ

The basic rules for writing the name of the holder in the VIZ and the MRZ appear in ICAO Doc 9303-3. for the VIZ and the MRZ. Where the name contains more characters than are available in the name field of the MRZ of the TD1, it is necessary to truncate the name. The following methods provide a number of options available for use at the discretion of the Issuing State or organization.

4.2.3.1 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 (lower line): NILAVADHANANANDA<<CHAYAPA<DE<K
- b) One or more name components truncated:
 Name: Nilavadhanananda Arnpol Petch Charonguang
 VIZ: NILAVADHANANANDA, ARNPOL PETCH CHARONGUANG
 MRZ (lower line): NILAVADHANANANDA<<ARNPOL<PE<CH

4.2.3.2 Truncated Names — Primary Identifier Truncated

- a) One or more components truncated to initials:
 Name: Dingo Potoroo Bennelong Woolloomooloo Warrandyte Warnambool
 VIZ: BENNELONG WOOLLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO
 POTOROO
 MRZ (lower line): BENNELONG<WOOLLOOMOOLOO<W<W<<DI
- b) One or more components truncated:
 Name: Dingo Potoroo Bennelong Woolloomooloo Warrandyte Warnambool
 VIZ: BENNELONG WOOLLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO
 POTOROO
 MRZ (lower line): BENNELONG<WOOLLOOM<WA<WARN<<D<P
- c) One or more components truncated to a fixed number of characters:
 Name: Dingo Potoroo Bennelong Woolloomooloo Warrandyte Warnambool
 VIZ: BENNELONG WOOLLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO
 POTOROO
 MRZ (lower line): BENNE<WOOLOO<WARRA<WARNA<<DIN<P

4.2.3.3 Names that Just Fit, Indicating Possible Truncation by Character in the Last Position of the Name Field, but which are not Truncated

Name: Jonathon Alec Papandropoulos
 VIZ: PAPANDROPOULOUS, JONATHON ALEC
 MRZ (lower line): PAPANDROPOULOUS<<JONATHON<ALEC

Note: Even though there is an alpha character in the 30th character position of this TD1 lower machine readable line, this name has not been truncated, but it must be assumed that it has been truncated.

4.2.4 Check digits in the MRZ

The method of calculating check digits is given in Doc 9303-3. For the TD1, the data structure of the machine readable lines in Paragraph 4.2.2 provides for the inclusion of four check digits as follows:

<i>Check digit</i>	<i>Character positions (upper MRZ line) used to calculate check digit</i>	<i>Check digit position (upper MRZ line)</i>
Document number check digit	6 – 14	15
<i>Check digit</i>	<i>Character positions (middle MRZ line) used to calculate check digit</i>	<i>Check digit position (middle MRZ line)</i>
Date of birth check digit	1 – 6	7
Date of expiry check digit	9 – 14	15
<i>Check digit</i>	<i>Character positions (upper/middle MRZ line) used to calculate check digit</i>	<i>Check digit position (middle MRZ line)</i>
Composite check digi	6 - 30 (upper line), 1 - 7, 9 - 15, 19 - 29 (middle line) <i>Note.— Positions 1 - 5 (upper line), positions 8, 16 - 18 (middle line) and positions 1 - 30 (lower line) are excluded in calculating the composite check digit.</i>	30

4.3 Representation of the Issuing State or Organization and Nationality of the Holder in the MRZ and the VIZ

Use of the three-letter codes listed in Doc 9303-3 is mandatory in the MRZ. In the VIZ, the name of the Issuing State or organization shall appear in full; the holder's nationality in the VIZ may appear either in full or in the form of the three-letter code. Specific locations are defined in the following table:

	<i>Zone</i>	<i>Field no.</i>	<i>Character position no.</i>	<i>Number of character positions</i>
Issuing State or organization	VIZ MRZ (upper line)	01	- 3 – 5	Variable 3
Holder's nationality	VIZ MRZ (middle line)	06	- 16 – 18	Variable 3

APPENDIX C TECHNICAL SPECIFICATIONS FOR A MACHINE READABLE CREW MEMBER CERTIFICATE – CMC (INFORMATIVE)

C.1 Scope

This Appendix defines the modifications to the TD1 specifications necessary to produce a Crew Member Certificate (CMC).

C.2 Content and Use of Zones

The layout of the seven zones and the data elements to be included in the zones shall be as specified in the Data Element Directories for a TD1 Size MROTD as described in this document, with the following modifications:

In Zone I, Field 1, the identification of the issuing authority or office may be entered below the name of the State.

In Zone I, Field 2, the type of document, i.e. crew member certificate, shall be entered in the national language of the State in which the document is issued, together with its translation into English, French or Spanish.

In Zone II, in addition to the personal data specified in the TD1, the name of the CMC holder’s employer and the holder’s employment classification, e.g. pilot or flight attendant, shall be entered.

In Zone VI, additional details of the holder’s travel status may be entered.

In Zone VII (MRZ), the first two (2) characters in the upper machine readable line, defining the type of document, shall be AC. Characters in positions 16, 17 and 18 in the upper line shall identify the holder’s employer using the two-character code specified in the IATA *Airline Coding Directory*, followed by a filler character. Alternatively, characters in positions 16, 17 and 18 shall be the three-letter code specified in ICAO Doc 8585, *Designators for Aircraft Operating Agencies, Aeronautical Authorities and Services*.

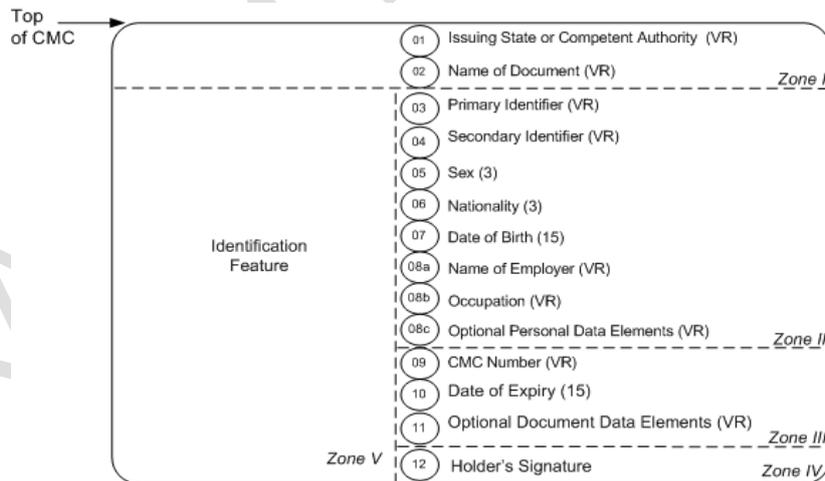


Figure 16: Layout of zones and data elements on the front side of a Crew Member Certificate

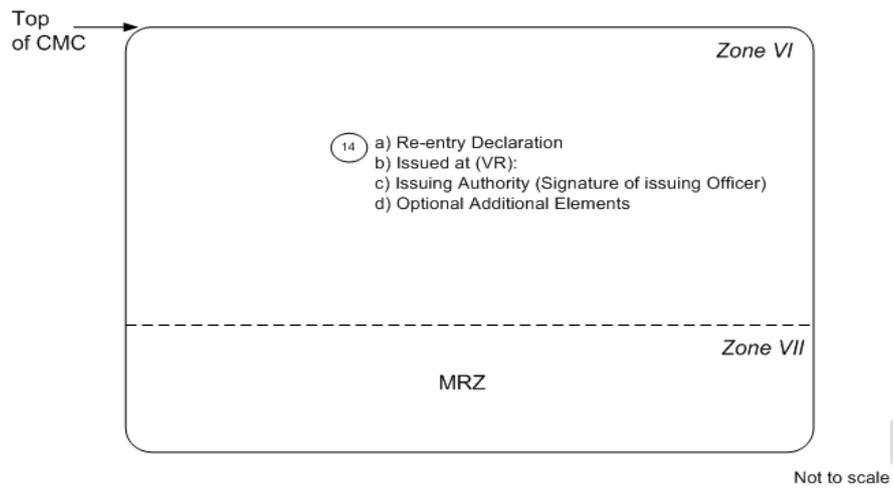


Figure 17: Layout of zones and data elements on the reverse side of a Crew Members Certificate

DRAFT_4 FOR TAG 22

REFERENCES (NORMATIVE)

ISO/IEC 7810 ISO/IEC 7810:2003, Identification Cards – Physical Characteristics

ISO/IEC7816-2 ISO/IEC7816-2:2007 Cards with contacts — Dimensions and location of the contacts

ISO 1073-2 ISO 1073-2:1976 -- Alphanumeric Character Sets for Optical Recognition CS Part 2: Character Set OCR-B -- shapes and dimensions of the printed image

IATA Airline Coding Directory (ACD) Published as an e-document by the International Air Transport Association

ICAO Doc 8585 and Designators for Aircraft Operating Agencies, Aeronautical Authorities Services

DRAFT_4 FOR TAG_22

Doc 9303



Machine Readable Travel Documents

**Part 6
Specifications Specific to TD2 Size MROTDs, Machine Readable Official
Travel Documents**

Approved by the Secretary General
and published under his authority

Seventh Edition — Revision 1 - 2014

International Civil Aviation Organization

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

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

Doc 9303, Machine Readable Travel Documents
Order Number: xxxx
ISBN xxx-xx-xxxx-xxx-x

© ICAO 2014

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 TO DOC 9303-6, 7TH EDITION

Revision	Date	Description
01	xx-xx-2014	Initial release of the 7 th edition

DRAFT_4 FOR TAG_22

TABLE OF CONTENTS

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	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
4.3	Representation of the Issuing State or Organization and Nationality of the Holder in the MRZ and the VIZ.....	14
	APPENDIX A - EXAMPLES OF A PERSONALIZED TD2 SIZE MROTD (INFORMATIVE)	15
	APPENDIX B - CONSTRUCTION OF THE MACHINE READABLE ZONE OF A TD2 SIZE MROTD (INFORMATIVE)	17
	REFERENCES (NORMATIVE)	18

DRAFT - 4 FOR MRG 22

1 SCOPE

The seventh edition of Doc 9303 represents a re-structuring of the ICAO specifications for Machine Readable Travel Documents. Without incorporating substantial modifications of 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 6 of Doc 9303 is based on Doc 9303 Part 3, Machine Readable Official Travel Documents Volume 1, 3rd Edition 2008.

Doc 9303-6, defines specifications that are specific to TD2 Size Machine Readable Official Travel Documents (MROTDs) and should be read in conjunction with:

- Part 1 - Introduction;
- Part 2 - Specifications for the Security of the Design, Manufacture and Issuance of Machine Readable Travel Documents;
- Part 3 - Specifications common to all Machine Readable Travel Documents.

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 may be found in Doc 9303 Parts 9 through 12.

2 DIMENSIONS OF THE TD2 SIZE MROTD

2.1 Nominal Dimensions

The nominal dimensions shall be guided by those in ISO/IEC 7810 (except thickness) for the ID-2 type card:

74.0 mm × 105.0 mm (2.91 in × 4.13 in).

2.2 Edge Tolerances

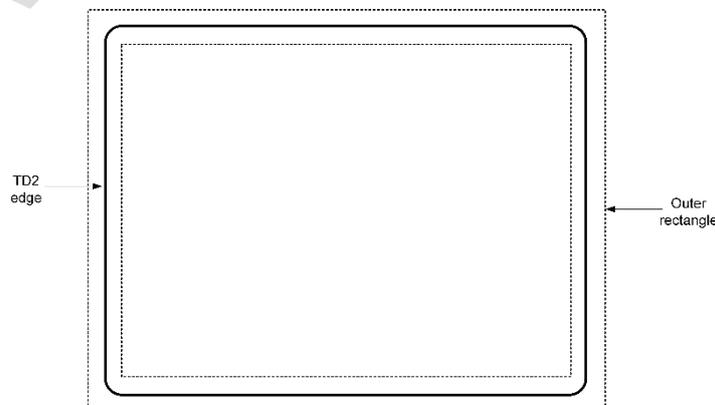
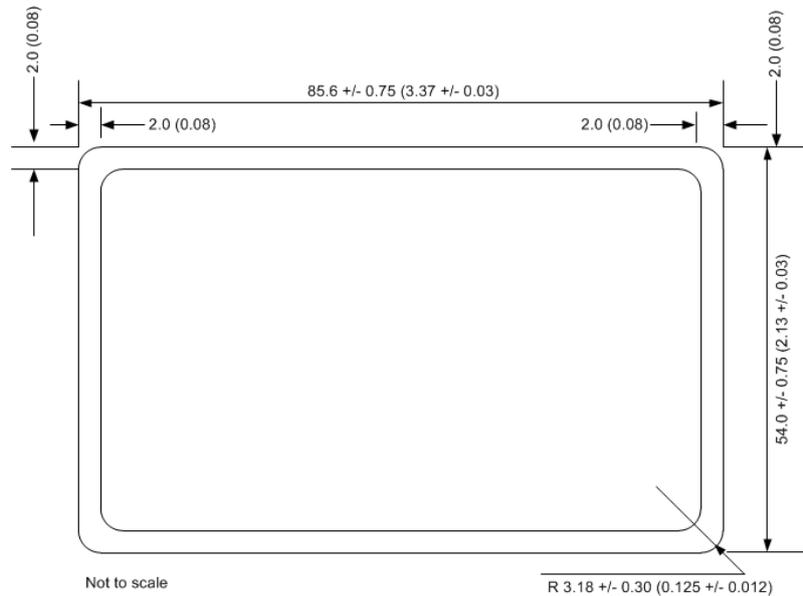


Figure 1: TD1 dimensional illustration

Inner rectangle: 73.25 mm × 104.25 mm (2.88 in × 4.10 in)
Outer rectangle: 74.75 mm × 105.75 mm (2.94 in × 4.16 in)

In no event shall the dimensions of the finished TD2 document exceed the dimensions of the outer rectangle, including any final preparation (e.g. laminate edges).

2.3 Margins



The dimensional specifications refer to the outer limits of the TD2. A margin of 2.0 mm (0.08 in) along each outer edge, with the exception of the header zone, must be left clear of data. See Figure 2.

2.4 Thickness

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

- *Minimum:* 0.25 mm (0.01 in);
- *Maximum:* 1.25 mm (0.05 in).

The thickness of the area within the machine readable zone shall not vary by more than 0.1 mm (0.004 in).

Note.— The dimensions and the tolerances specified above differ slightly from those specified in ISO/IEC 7810. This is for historical reasons; TD2 cards were originally produced using encapsulated pouch card methods which are incapable of achieving the permitted tolerances of ISO/IEC 7810. Some cards may still be produced using these techniques and others where the personalization process is incapable of achieving the tight tolerances ISO/IEC 7810 requires. Wherever possible, however, dimensions and tolerances should conform to ISO/IEC 7810.

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

3 GENERAL LAYOUT OF THE TD2 SIZE MROTD

The TD2 follows a standardized layout to facilitate reading of data globally by both visual and machine readable means (global interoperability).

3.1 TD2 Zones

To accommodate the various requirements of States' laws and practices and to achieve the maximum standardization within those divergent requirements, the TD2 is divided into seven zones as listed below in paragraphs 3.1.1 and 3.1.2. Zones I through VI constitute the visual inspection zone (VIZ). Zone VII is the machine readable zone (MRZ).

3.1.1 Front of the TD2

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
Zone V	Mandatory identification feature
Zone VII	Mandatory machine readable zone (MRZ)

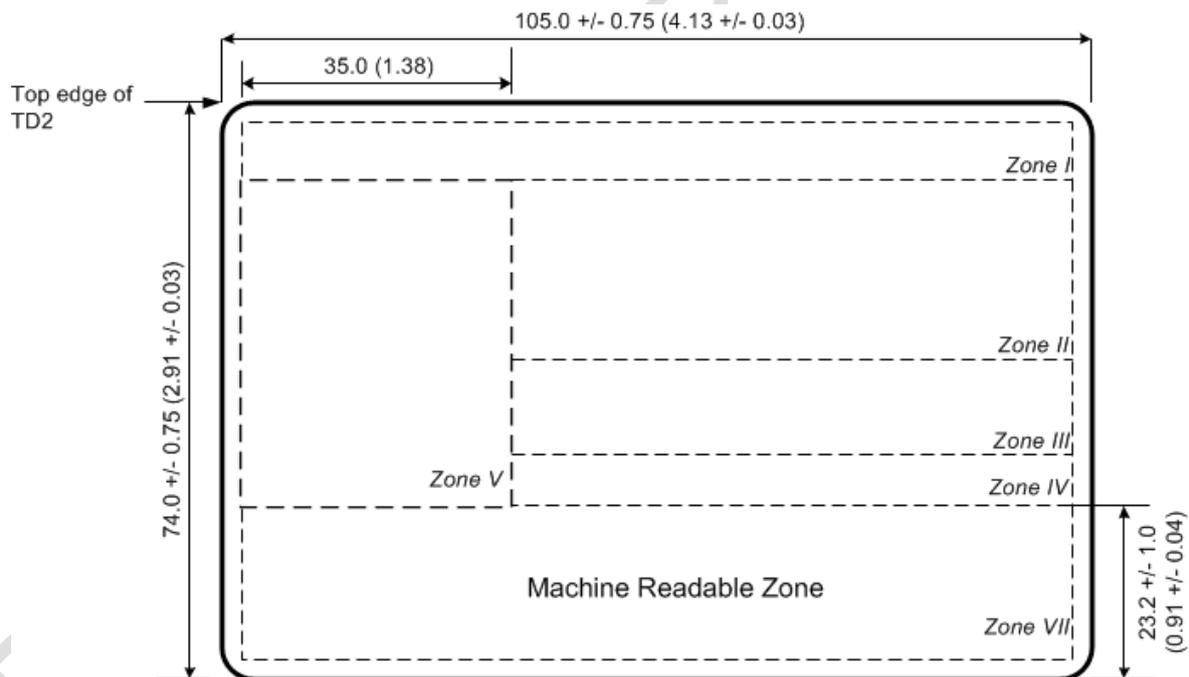


Figure 3: Nominal layout of the Zones on the front side of a TD2 Size MROTD

3.1.2 Back of the TD2

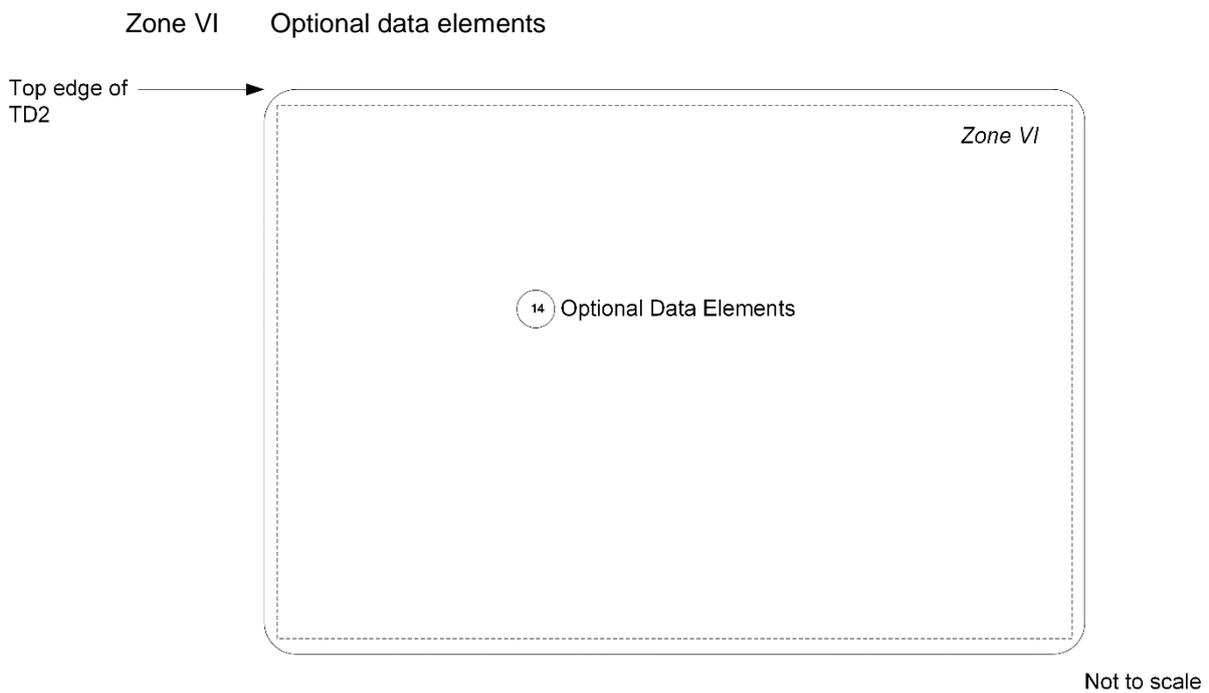


Figure 4: The reverse side of a TD2

3.2 Content and Use of Zones

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 hereunder and illustrated in Figures 4 and 5.

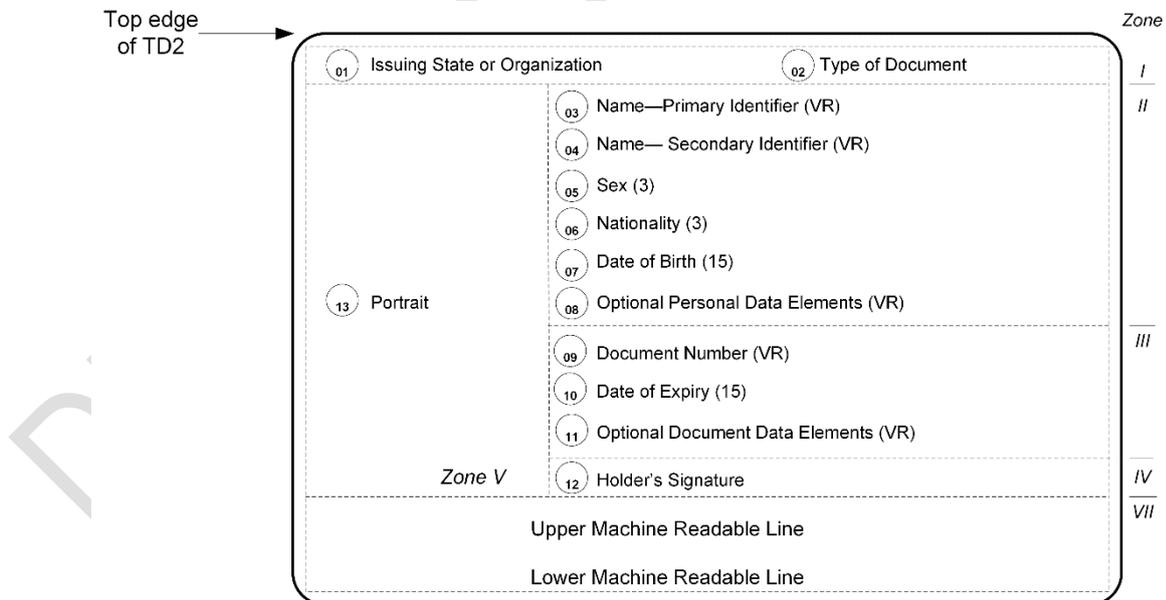


Figure 5: Sequence of data elements on the front side of a TD2

Zones I to V and Zone VII contain mandatory elements which represent the minimum requirements for the TD2. The optional elements in Zones II, III and VI accommodate the diverse requirements of Issuing States or organizations, allowing for presentation of additional data, while achieving the desired level of

standardization. The location of zones and data elements are set out in Figures 3 through 6. Figures 7 and 8 show some examples for positioning and adjusting the dimensional specifications of Zones I to V to accommodate the flexibility desired by Issuing States or organizations. Examples of a personalized TD2 are shown in Appendix A, Figures 9 - 12.

3.2.1 Mandatory Zones

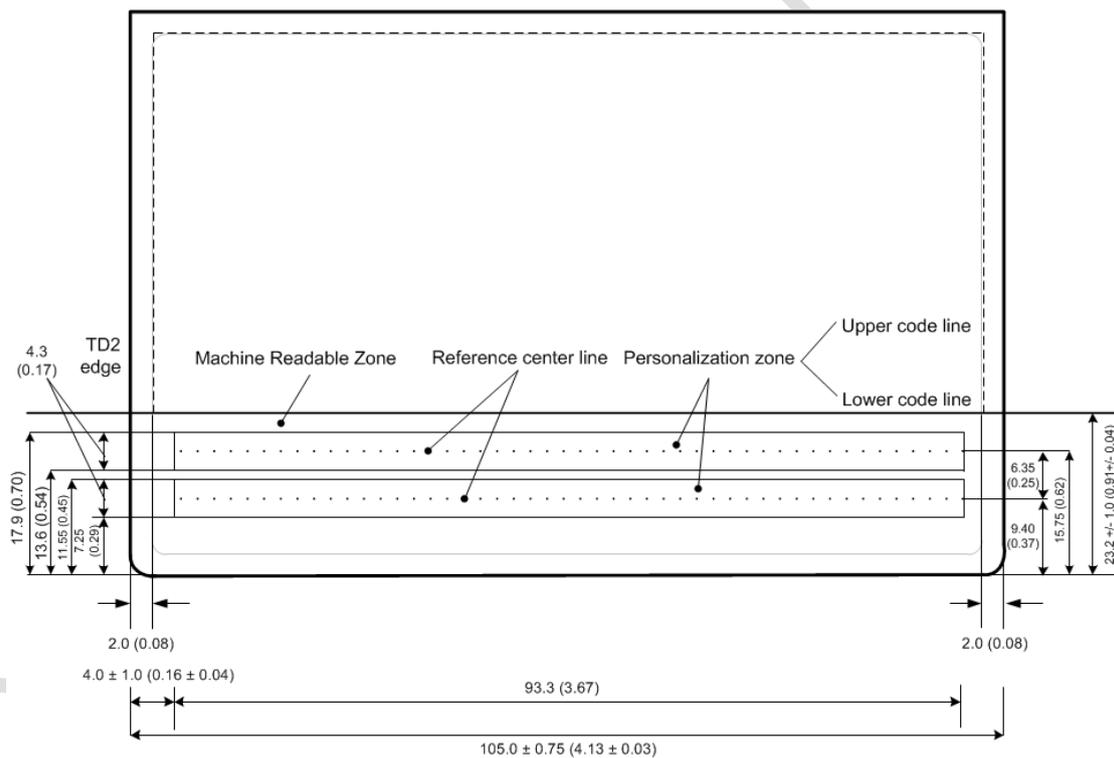
Zone I on the front of the TD2 identifies the Issuing State or organization and the document.

Data elements shall appear in a standard sequence in Zones II and III.

Zones II and III each contain a field in which optional data elements may be included. The optional field in Zone II shall be used for personal data elements and the optional field in Zone III for document-related details. Where an Issuing State or organization does not use the optional fields in Zones II and III, there is no need to reserve the space for them on the TD2.

Zone IV contains the holder's signature or usual mark. The Issuing State or organization shall decide the acceptability of a holder's usual mark.

Zone V shall contain the personal identification feature(s) which shall include a portrait solely of the holder. At the discretion of the Issuing State or organization, the name field 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.



Not to scale

Figure 6: Position and dimensions of Zone VII the Machine Readable Zone

The position for the holder's portrait is along the left edge of the front of the TD2, as described in Paragraph 3.3 and illustrated in Figure 3. The size of the portrait is specified in the Data Element Directory (Paragraph 4.1.1.1, item 13/V).

Zone VII, located on the front of the TD2, shall contain the machine readable data. 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 ICAO Doc 9303-3.

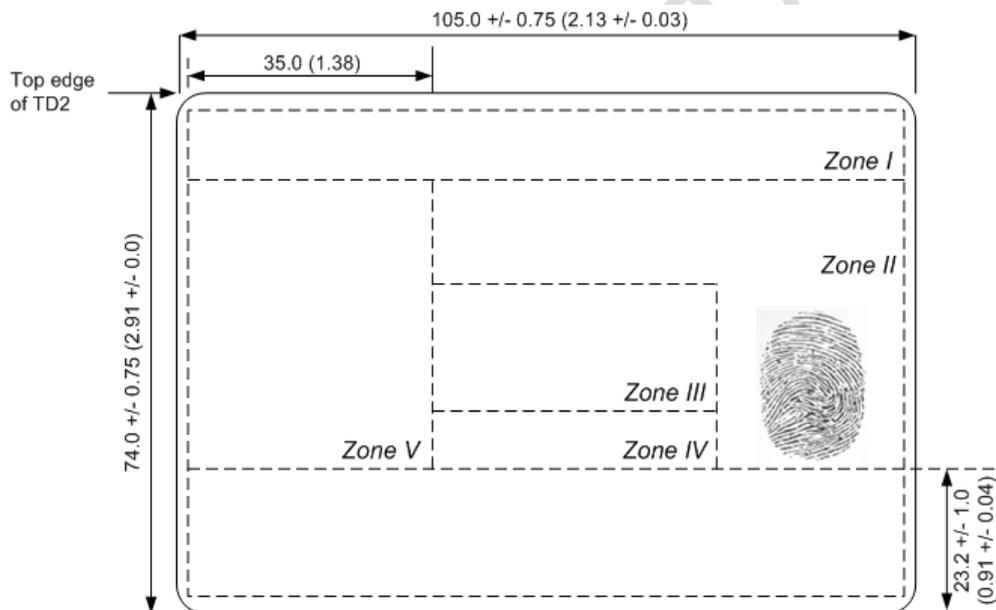
All MRZ data elements shall be as defined in the Data Element Directory, paragraph 4.2.2.

3.2.2 Optional Data Zone

Zone VI, on the back of the MROTD, is an optional zone for use at the discretion of the Issuing State or organization. Because the TD2 is a card, Zone VI will always appear, irrespective of whether or not it is used. See Figure 4.

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 TD2 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 TD2. Some examples of flexible positioning the zones is shown in Figures 7 and 8.



Not to scale

Figure 7: Zones III and IV have been reduced in size to permit the addition of an optional displayed identification feature eg a fingerprint, in Zone II

When an Issuing State or organization chooses to produce an TD2 that contains a transparent or otherwise unprintable border around the card, this will result in a reduction of the available area within the zones. The full TD2 dimensions and zone boundaries shall be measured from the outside edge of this border, which is the external edge of the TD2.

Zone I shall be located along the top edge of the TD2 and extend across the full width of the document. 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 11.0 mm (0.43 in).

Zone V shall be located such that its left edge is coincident with the left edge of the TD2. Zone V may vary in size but the portrait image shall not exceed 45mm x 35mm, the maximum dimensions specified in the Data Element Directory.

Zone V may move *vertically* along the left edge of the TD2 and overlay a portion of Zone I as long as individual details contained in either zone are not obscured. The scope for such movement is illustrated in Figure 8.

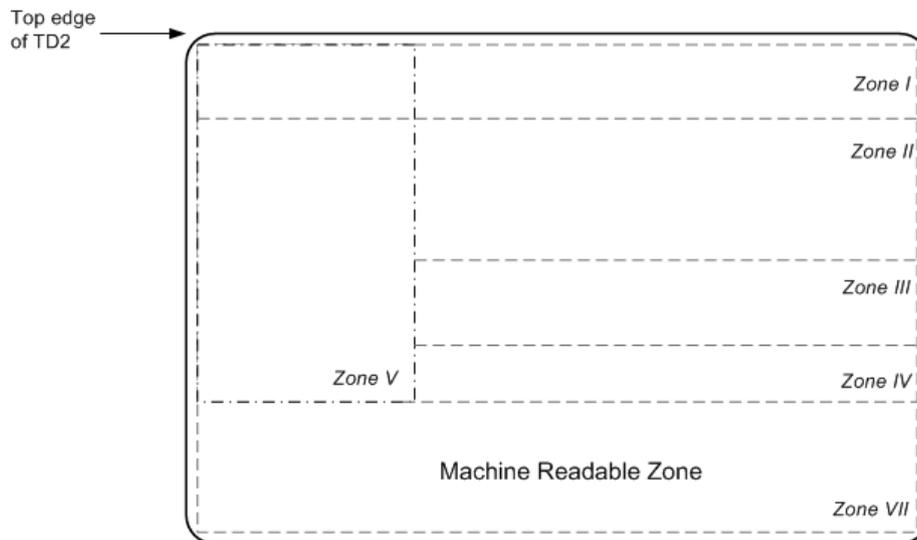


Figure 8: Illustrating the possibility for Zone V to overlay a portion of the Mandatory Header, Zone I

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 field to extend across the TD2, Zone II may extend up to the full width of the TD2. In the event the full dimension is used, Zone II shall overlay a portion of Zone V, as illustrated in Figure 12. In this case, Issuing States or organizations shall ensure that data contained in either zone are not obscured.

The lower boundary of Zone II may be positioned at the discretion of the Issuing State or organization, examples are shown in Figures 7 and 8. Enough space must be left for Zones III and IV. This boundary does not need to be straight across the longer dimension of the TD2. Figure 7 illustrates a Zone II with the lower boundary on two levels. The flexible design for the Zone II illustrated conforms with the specifications defined above.

Zone III may 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 TD2. Figures 7 and 8 also illustrate some options for a flexible layout of Zone III.

The position of Zone IV is illustrated in Figures 7 and 8 and in the examples shown in Appendix A.

Zone IV may also overlay Zone V, though this practice is not recommended, as illustrated in Figure 11. Zone IV may overlay Zone V, as illustrated in figure 11, although this is not recommended practice. In this case, Issuing States or organizations shall ensure that individual details contained in either zone are not obscured.

4 CONTENTS OF A TD2 SIZE MROTD

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

All data in the VIZ shall be clearly legible.

Guidance on the typeface, size and line spacing, the languages and character set, and the field captions 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 TD2 consistent with the requirement for sequencing zones and data elements.

4.1.1 Data Element Directory

4.1.1.1 Visual Inspection Zone — Data Element Directory

<i>Field/ zone no.</i>	<i>Data element</i>	<i>Specifications</i>	<i>Maximum no. of character positions</i>	<i>References and notes*</i>
01/I (Mandatory)	Issuing State or organization	The name of the State or organization responsible for issuing the travel document shall be displayed. See Doc 9303-3 for further details.	Variable	Notes a, c, e, h, i
02/I (Mandatory)	Document	The type or designation of the document. For additional details see Doc 9303-3	Variable	Notes a, b, c, e, i
03/04/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	Doc 9303-3 Notes a, c, i, l
03/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) 03 and/or 04 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, i, l
04/II (Mandatory)	Secondary identifier	Secondary component(s) of the name of the holder, as described in Doc 9303. 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 represented by initials. Where the holder's name has only predominant component(s), this data field shall be left blank. The State or organization may optionally utilize the whole zone comprising Fields 03 and 04 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.	Variable	Notes a, c, i, l
05/II (Mandatory)	Sex	Sex of the holder, to be specified by use of the single initial commonly used in the language of the State or organization where the document is	3	Notes a, c, f, i, l

<i>Field/ zone no.</i>	<i>Data element</i>	<i>Specifications</i>	<i>Maximum no. of character positions</i>	<i>References and notes*</i>
		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.		
06/II (Mandatory)	Nationality	. For details see Doc 9303-3	Variable	Notes a, h, I
07/II (Mandatory)	Date of birth	Holder's date of birth as recorded by the Issuing State or organization. For unknown dates see Doc 9303-3.	15	Notes a, b, c, i, I
08/II Optional element in mandatory zone	Optional personal data elements	Optional personal data elements, e.g. personal identification number or fingerprint, at the discretion of the Issuing State or organization. If a fingerprint is included in this field, it should be presented as a 1:1 representation of the original. If a date is included, it shall follow the form of presentation described in Doc 9303-3.	Variable	Notes a, b, c, d, g, i
09/III (Mandatory)	Document 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	Variable	Notes a, b, c, i, j, I
10/III (Mandatory)	Date of expiry	Date of expiry of the document. For additional details see Doc 9303-3	15	Notes a, b, c, i, I
11/III Optional element in mandatory zone	Optional document data elements	Optional data elements relating to the document.. For additional details see Doc 9303-3	Variable	Notes a, b, c, d, g, i, j
12/IV (Mandatory)	Holder's signature or usual mark	Signature or usual mark of the holder. For additional details see Doc 9303-3		Note g
13/V (Mandatory)	Identification Feature	This field shall contain a portrait of the holder. The portrait shall not be larger than 45.0 mm x 35.0 mm (1.77 in x 1.38 in) nor smaller than 32.0 mm x 26.0 mm (1.26 in x 1.02 in). The position of the field concerned shall be along the left edge of the front of the TD2. See Doc 9303-3 for additional specifications for the portrait.		Note e
14/VI (Optional)	Optional data elements	Additional optional data elements at the discretion of the Issuing State or organization.		Notes a, b, c, d, g, i

4.2 Machine Readable Zone (MRZ) (Zone VII)

4.2.1 Data Position, Data elements, and Print Position in the MRZ

4.2.1.1 Data Position

Figure 6 shows the nominal dimensions and position of the data in the MRZ.

4.2.1.2 Data Elements

The data elements corresponding to specified fields of the VIZ shall be printed, in machine readable form, in the MRZ, beginning with the left most character position in each field in the sequence indicated in the data structure specifications. Details on the data elements to be included in the MRZ are set out in Paragraph 4.2.2. Figure 13 indicates the structure of the MRZ.

4.2.1.3 Print Position

The position of the left-hand edge of the first character shall be 4.0 ± 1.0 mm (0.16 ± 0.04 in) from the left-hand edge of the document. Reference centre lines for the OCR lines and a nominal starting position for the first character of each line are shown in Figure 6. The positioning of the characters is indicated by those reference lines and by the printing zones for the two code lines.

4.2.2 Data Structure of Machine Readable Data for the TD2

4.2.2.1 Data Structure of the Upper Machine Readable Line

MRZ character positions (line 1)	Field no. in VIZ	Data element	Specifications	Number of characters	References and notes*
1 to 2	02	Document code	Two characters, the first of which shall be A, C or I, shall be used to designate the particular type of document. The second character shall be as specified in Note k.	2	Notes a, b, c, e, k
3 to 5		Issuing State or organization	The three-letter code specified in Doc 9303-3 shall be used. Spaces shall be replaced by filler characters (<).	3	Notes a, c, e
6 to 36	03, 04	Name	The name consists of primary and secondary identifiers which shall be separated by two filler characters (<<). Components within the primary or secondary identifiers shall be separated by a single filler character (<). When the name of the document holder has only one part, it shall be placed first in the character positions for the primary identifier, filler characters (<) being used to complete the remaining character positions of the MRZ. For additional details see Doc 9303-3	31 (Primary identifier(s), secondary identifier(s) and fillers)	Notes a, c, e
		Punctuation in the name	Representation of punctuation is not permitted in the MRZ. For details on apostrophes, hyphens and commas etc see Doc 9303-3		

<i>MRZ character positions (line 1)</i>	<i>Field no. in VIZ</i>	<i>Data element</i>	<i>Specifications</i>	<i>Number of characters</i>	<i>References and notes*</i>
		Name prefixes and suffixes	For details see Doc 9303-3		
		Filler	When all components of the primary and secondary identifiers and required separators (filler characters) do not exceed 31 characters in total, all permitted name components shall be included in the MRZ, and all unused character positions shall be completed with filler characters (<) repeated up to position 36 as required.		
		Truncation of the name	<p>When the primary and secondary identifiers and required separators (filler characters) exceed the number of character positions available for the name (i.e. 31), they shall be truncated as follows:</p> <p>Characters shall be removed from one or more components of the primary identifier until three character positions are freed and two filler characters (<<) and the first character of the first component of the secondary identifier can be inserted. The last character position (position 36 in the line, 31st character of the name) shall be an alphabetic character (A through Z). This indicates that truncation may have occurred.</p> <p>Further truncation of the primary identifier may be carried out to allow characters of the secondary identifier to be included, provided that the name field shall end with an alphabetic character (position 36 in the line, 31st character of the name). This indicates that truncation may have occurred.</p> <p>When the name consists of only a primary identifier which exceeds the number of character positions available for the name, i.e. 31, characters shall be removed from one or more components of the name until the last character in the name field shall be an alpha character.</p>		Notes: a, c, e and 4.2.3

4.2.2.2 Data Structure of the Lower Machine Readable Line

<i>MRZ character positions (line 1)</i>	<i>Field no. in VIZ</i>	<i>Data element</i>	<i>Specifications</i>	<i>Number of characters</i>	<i>References and notes*</i>
1 to 9	09	Document Number	As given by the Issuing State or organization, to uniquely identify the document from all other MROTDs issued by the State or organization. Spaces shall be replaced by filler characters (<). For additional details see Doc 9303-3	9	Notes a, b, e, j

MRZ character positions (line 1)	Field no. in VIZ	Data element	Specifications	Number of characters	References and notes*
10		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Notes b, c, j
11 to 13	06	Nationality	For details see Doc 9303-3	3	Notes a, c, e, h
14 to 19	07	Date of birth	For details see Doc 9303-3	6	Notes b, c, e
20		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Note b
21	05	Sex	F = female; M = male; < = non-specified.	1	Notes a, c, e, f
22 to 27	10	Date of expiry	For details see Doc 9303-3	6	Notes b, e
28		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Note b
29 to 35		Optional data elements	For use of the Issuing State or organization. Unused character positions shall be completed with filler characters (<) repeated up to position 35 as required. For additional details see Doc 9303-3	7	Notes a, b, c, d, e, j
36		Composite check digit	Composite check digit to verify the data elements of the lower machine readable line. Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Note b

* Notes for 4.1.1 and 4.2.2

- a) Alphabetic characters (A–Z). National characters may be included in the VIZ. In the MRZ only the characters defined in Doc 9303-3 shall be used.
- b) Numeric characters (0–9). National numerals may be additionally included in the VIZ. In the MRZ only the numerals 0–9 may be used as defined in Doc 9303-3.
- c) Punctuation may be included in the VIZ. In the MRZ only the filler character specified in Doc 9303-3 may be used.
- d) Optional data elements may appear in Zone VI.
- e) The field caption is not printed on the document.
- f) Where a person does not wish his/her sex to be identified or where an Issuing State or organization does not want to show this data, the filler character (<) shall be used in this field in the MRZ and an X in this field in the VIZ.
- g) The use of a caption to identify the field is at the option of the Issuing State or organization.
- h) In the case of a document issued by the United Nations Organization, or one of its specialized agencies, to a designated official, the appropriate organization code is used in lieu of nationality. See Doc 9303-3..

- i) A blank space (or spaces) is included. Blank spaces between words shall count towards the maximum number of characters permitted in the field.
- j) The number of characters in the VIZ may be variable; however, if the document number has more than 9 characters, the 9 principal characters shall be shown in the MRZ in character positions 1 to 9. They shall be followed by a filler character instead of a check digit to indicate a truncated number. The remaining characters of the document number shall be shown at the beginning of the field reserved for optional data elements (character positions 29 to 35 of the lower machine readable line) followed by a check digit and a filler character.
- k) The first character shall be A, C or I. Historically these three characters were chosen for their ease of recognition in the OCR-B character set. The second character shall be at the discretion of the Issuing State or organization except that V shall not be used, and C shall not be used after A.
- l) The field caption shall be printed on the document.

4.2.3 Truncation of Names in the MRZ

The basic rules for writing the name of the holder in the VIZ and the MRZ are contained in ICAO Doc 9303-3. Where the name contains more characters than are available in the name field of the MRZ of the TD2, it is necessary to truncate the name. The following methods provide a number of options available for use at the discretion of the Issuing State or organization.

4.2.3.1 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 (upper line): I<UTONILAVADHANANANDA<<CHAYAPA<DEJ<K
- b) One or more name components truncated:
 Name: Nilavadhanananda Arnpol Petch Charonguang
 VIZ: NILAVADHANANANDA, ARNPOL PETCH CHARONGUANG
 MRZ (upper line): I<UTONILAVADHANANANDA<<ARN<PET<CHARO

4.2.3.2 Truncated Names — Primary Identifier Truncated

- a) One or more components truncated to initials:
 Name: Dingo Potoroo Bennelong Woolloomooloo Warrandyte Warnambool
 VIZ: BENNELONG WOOLLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO
 POTOROO
 MRZ (upper line): I<UTOBENNELONG<W00L00M00L00<W<W<<D<P
- b) One or more components truncated:
 Name: Dingo Potoroo Bennelong Woolloomooloo Warrandyte Warnambool
 VIZ: BENNELONG WOOLLOOMOOLOO WARRANDYTE WARNAM
 BOOL, DINGO POTOROO
 MRZ (upper line): I<UTOBENNELONG<W00L00M<WAR<WARN<<<D<P
- c) One or more components truncated to a fixed number of characters:
 Name: Dingo Potoroo Bennelong Woolloomooloo Warrandyte Warnambool
 VIZ: BENNELONG WOOLLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO
 POTOROO
 MRZ (upper line): I<UTOBENNEL<W00L0<WARRA<WARNA<<<DIN<P

4.2.3.3 Names that Just Fit, Indicating Possible Truncation by Character in the Last Position of the Name Field, but which are not Truncated

Name: Jonathoon Alec Papandropoulos
 VIZ: PAPANDROPOULOUS, JONATHOON ALEC
 MRZ (upper line): I<UTOPAPANDROPOULOUS<<JONATHOON<ALEC

Note: Even though there is an alpha character in the 36th character position of this TD2 lower machine readable line, this name has not been truncated, but it must be assumed that it has been truncated.

4.2.4 Check Digits in the MRZ

The method of calculating check digits is given in Doc 9303-3. For the TD2, the data structure of the machine readable lines in Paragraph 4.2.2 provides for the inclusion of four check digits as follows:

<i>Check digit</i>	<i>Character positions (lower MRZ line) used to calculate check digit</i>	<i>Check digit position (lower MRZ line)</i>
Document number check digit	1 – 9	10
Date of birth check digit	14 – 19	20
Date of expiry check digit	22 – 27	28
Composite check digit	1 - 10, 14 - 20, 22 - 35 (lower line) <i>Note.— Positions 11 - 13 and position 21 (lower line) are excluded in calculating the composite check digit.</i>	36

4.3 Representation of the Issuing State or Organization and Nationality of the Holder in the MRZ and the VIZ

The use of the three-letter codes listed in Appendix 1 to Section IV is mandatory in the MRZ. In the VIZ, the name of the Issuing State or organization should appear in full; the holder's nationality in the VIZ may either appear in full or in the form of the three-letter code. Specific locations are defined in the following table.

	<i>Zone</i>	<i>Field no.</i>	<i>Character position no.</i>	<i>Number of character positions</i>
Issuing State or organization	VIZ	01	--	Variable
	MRZ (upper line)		3 – 5	3
Holder's nationality	VIZ	06	--	Variable
	MRZ (lower line)		11 – 13	3

REFERENCES (NORMATIVE)

- | | |
|---------------|---|
| ISO/IEC 7810 | ISO/IEC 7810:2003, Identification Cards – Physical Characteristics |
| ISO/IEC7816-2 | ISO/IEC7816-2:2007 Cards with contacts — Dimensions and location of the contacts |
| ISO 1073-2 | ISO 1073-2:1976 -- Alphanumeric Character Sets for Optical Recognition CS Part 2: Character Set OCR-B -- shapes and dimensions of the printed image |

DRAFT_4 FOR TAG_22

Doc 9303



Machine Readable Travel Documents

**Part 7
Machine Readable Visas**

Approved by the Secretary General
and published under his authority

Seventh Edition - Revision 1 - 2014

International Civil Aviation Organization

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

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

Doc 9303, Machine Readable Travel Documents
ISBN xxx-xx-xxxx-xxx-x

© ICAO 2014

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 TO DOC 9303-7, 7TH EDITION

Revision	Date	Description
01	xx-xx-2014	Initial release of the 7 th edition

DRAFT_4 FOR TAG_22

TABLE OF CONTENTS

1	SCOPE	1
2	TECHNICAL SPECIFICATIONS FOR FORMAT-A MACHINE READABLE VISAS (MRV-A)	2
2.1	Dimensions and Placement of the MRV-A.....	2
2.2	General Layout of the MRV-A.....	3
2.3	Content, Use and Dimensional Flexibility of Zones	3
2.4	Detailed Layout	5
2.5	Machine Readable Zone (MRZ) (Mandatory Zone VII)	7
2.6	Data Structure of Machine Readable Data for the MRV-A	8
2.7	Portrait.....	13
2.8	MRV-A Diagrams	14
3	TECHNICAL SPECIFICATIONS FOR FORMAT-B MACHINE READABLE VISAS (MRV-B)	18
3.1	Dimensions and Placement of the MRV-B.....	18
3.2	General Layout of the MRV-B.....	19
3.3	Content, Use and Dimensional Flexibility of Zones	19
3.4	Detailed Layout	21
3.5	Machine Readable Zone (MRZ) (Mandatory Zone VII)	23
3.6	Data Structure of Machine Readable Data for the MRV-B	25
3.7	Portrait.....	30
3.8	MRV-B Diagrams	31
4	USE OF OPTIONAL BARCODES ON MACHINE READABLE VISAS	35
4.1	Scope	35
4.2	Definition	35
4.3	Location of Bar Code(s)	35
4.4	Quality of Bar Code(s).....	36
4.5	Symbologies and Logical Data Structure.....	36
4.6	Machine Reading of the Bar Code(s).....	36
APPENDIX A	EXAMPLES OF PERSONALIZED MRV'S (INFORMATIVE)	37
A.1	MRV-A Examples.....	37
A.2	MRV-B Examples.....	38
APPENDIX B	CONSTRUCTION OF THE MRZ (INFORMATIVE)	39
B.1	MRV-A MRZ-Construction	39
B.2	MRV-B MRZ-Construction	40
APPENDIX C	POSITIONING IN PASSPORT (INFORMATIVE)	41
C.1	MRV-A Positioning	41
C.2	MRV-B Positioning	42
APPENDIX D	MATERIALS AND PRODUCTION METHODS (INFORMATIVE)	43
	REFERENCES (NORMATIVE)	45

1 SCOPE

The seventh edition of Doc 9303 represents a restructuring of the ICAO specifications for Machine Readable Travel Documents. Without incorporating substantial modifications of 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 7 of Doc 9303 is based on Doc 9303 Part 2, Machine Readable Visas, Third edition - 2005.

Part 7 defines the specifications for machine readable visas (MRV) which allow compatibility and global interchange using both visual (eye readable) and machine readable means. The specifications lay down standards for visas which 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 herein in a form that is legible both visually and by optical character recognition methods, as presented herein. Part 7 contains specifications for both Format-A as well as Format-B types of visas.

Part 7 should be read in conjunction with:

- Part 1 - Introduction;
- Part 2 - Specifications for the security of the design, manufacture and issuance of Machine Readable Travel Documents;
- Part 3 - Specifications common to all Machine Readable Travel Documents.

2 TECHNICAL SPECIFICATIONS FOR FORMAT-A MACHINE READABLE VISAS (MRV-A)

This section defines those specifications which are unique to Format-A machine readable visas (MRV-A) and are necessary for global interoperability. Specifications are included for the discretionary expansion of the machine readable data capacity of the MRV beyond that defined for global interoperability. The Format-A visa (MRV-A) is suitable for use by States who wish to have maximum space available to accommodate their data requirements and who do not need to maintain a clear area on the passport visa page adjacent to the visa.

2.1 Dimensions and Placement of the MRV-A

The dimensions and placement of the MRV-A shall be as follows:

MRV-A nominal dimensions. The nominal dimensions of the MRV-A shall be as follows:

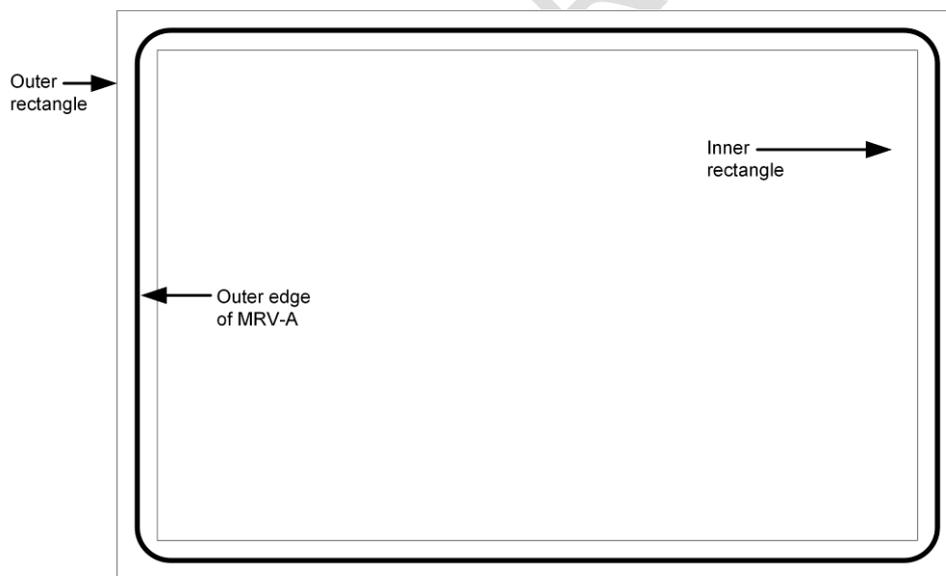
80.0 mm × 120.0 mm (3.15 in × 4.72 in)

MRV-A margins. The dimensional specifications refer to the outer limits of the MRV-A. A margin of 2.0 mm (0.08 in) along each outer edge, with the exception of the header zone, must be left clear of data.

MRV-A edge tolerances. The edges of the MRV-A shall be within the area circumscribed by the concentric rectangles as illustrated in **Error! Reference source not found.**

Inner rectangle: 79.0 mm × 119.0 mm (3.11 in × 4.69 in)

Outer rectangle: 81.0 mm × 121.0 mm (3.19 in × 4.76 in)



Not to scale

Figure 1 : MRV-A dimensional illustration

MRV-A thickness. If the visa is issued as a label, the increase in thickness once the label is attached to the passport visa page shall not exceed 0.19 mm (0.0075 in). The thickness of the area within the machine readable zone (MRZ) shall not vary by more than 0.05 mm (0.002 in). If a protective laminate is used, it is recommended that its thickness not exceed 0.15 mm (0.006 in).

General note: The decimal notation used in these specifications conforms to ICAO practice. This differs from ISO practice where a decimal point (.) in imperial measurements and a comma (,) in metric measurements are used.

Placement of the MRV-A. The MRV-A shall be positioned as follows:

The MRV-A shall be located on the passport visa page such that the MRZ is coincident with and parallel to the outside edge (reference edge) of the passport visa page, and the left edge of the MRV-A is coincident with and parallel to the left edge of the passport visa page as defined in APPENDIX C – C.1.

The MRZ shall be located such that the two OCR lines contained therein are within the Effective Reading Zone (ERZ) as defined in Doc 9303-3.

Only one MRV-A shall be located on a passport visa page (see APPENDIX C – C.1).

2.2 General Layout of the MRV-A

The MRV-A follows a standardized layout to facilitate reading of data globally, by visual and machine readable means, to accommodate the various requirements of States' laws and practices and to achieve the maximum standardization within those divergent requirements.

The standard layout incorporates space for a portrait and other identification feature(s). The inclusion of a portrait on a visa is strongly recommended in the interests of security, but States who are not yet able to apply portraits may fill this space with, for example, a national crest.

An MRV-A is divided into six zones as follows:

Zone I	Mandatory header
Zone II	Mandatory and optional personal data elements
Zone III	Mandatory and optional document data elements
Zone IV	Signature (original or reproduction) or authentication
Zone V	Mandatory zone for identification feature (feature optional)
Zone VII	Mandatory machine readable zone (MRZ)

Note 1: The signature in Zone IV of a visa is that of an issuing officer, not of the document holder. The signature may be replaced or accompanied by an official stamp.

Note 2: To facilitate inspection of visas at border control, the layout of the visa presents Zone III above Zone II.

Note 3: Zone VI is not available on an MRV issued in the form of a label.

Note 4: Zones I – V constitute the Visual Inspection Zone (VIZ).

Zones I and VII are mandatory. Certain data in Zones II and III are also mandatory. The mandatory components of these four Zones represent the minimum data requirements for an MRV-A. The optional data elements in Zones II, III and V and in optional Zone IV may be utilized to accommodate the diverse requirements of States, while achieving the desired level of standardization. The data elements which may be included in the various zones and their order are set out in 2.8. 2.8 also illustrates the dimensional specifications and tolerances for the layout of the MRV-A and the technical specifications for the printing of data elements within the zones, as well as the guidelines for positioning and adjusting the dimensional specifications of Zones I to V to accommodate the flexibility desired by issuing States. Examples of personalized MRV-As are shown in APPENDIX A – A.1. APPENDIX B – B.1 illustrates the format for the presentation of the machine readable data in Zone VII.

2.3 Content, Use and Dimensional Flexibility of Zones

The data elements to be included in the zones, the treatment of the zones and guidelines for the dimensional layout of zones shall be as described hereunder.

Zone I identifies the issuing State and the type of document. These elements are mandatory. The order of the data elements in this zone is left to the discretion of the issuing State.

To facilitate the checking of visas by airline personnel and control authorities, the essential details of the visa document shall be entered in a standard sequence in Zone III while essential personal details of the holder shall be entered in a standard sequence in Zone II. On a visa, Zone III appears above Zone II.

Zone IV provides space for an optional signature or authentication. This is normally the signature of the issuing officer or an official stamp. The application of an official stamp elsewhere on the document is not precluded except that it must not intrude into the MRZ or affect the legibility of entered data.

Zone VII conforms in height to the MRZ defined for all MRTDs so that the machine readable data lines fall within the ERZ specified in Doc 9303-3, thus allowing a single reader to be used for all types and sizes of MRTDs.

All MRZ data elements are mandatory and shall be shown as defined in 2.6 even though an issuing State may choose not to include a specific MRZ data element in the VIZ.

2.3.1 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 MRV-A to accommodate the diverse requirements of issuing States. 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 MRV-A. The nominal position of the zones is shown in 2.8 – Figure 4.

When an issuing State chooses to produce an MRV-A as a securely attached card containing a transparent or otherwise unprintable border around the card, the available area within the zones will be reduced. The full MRV-A dimensions and zone boundaries shall be measured from the outside edge of this border, which is the external edge of the MRV-A.

Zone I shall be adjacent and parallel to the top edge of the MRV-A and extend across the full $120.0 \text{ mm} \pm 1.0 \text{ mm}$ ($4.72 \text{ in} \pm 0.04 \text{ in}$) dimension. The issuing State may vary the *vertical* dimension of Zone I, as required, but this dimension shall be sufficient to allow legibility of the data elements in the zone, and the height shall not be greater than 12.0 mm (0.47 in) as defined in 2.8 – Figure 4.

Zone V shall be located such that its left edge is coincident with the left edge of the MRV-A, as defined in 2.8 – Figure 4. Zone V may vary in size but any variation from the nominal dimensions shall not exceed the tolerances specified in 2.8 – Figure 4.

Zone V may move *vertically* along the left edge of the MRV-A and overlay a portion of Zone I as long as individual details contained in either zone are not obscured. Zone V may, as a result, have its *lower external boundary* coincident with the top edge of the MRZ of the MRV-A and its *upper external boundary* coincident with the top edge of the MRV-A.

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

Zone III may extend to the full width of that portion of the MRV-A to the right of Zone V.

The lower boundary of Zone III (see 2.8 – Figure 4) may be positioned at the discretion of the issuing State. Enough space shall be left for Zone II and Zone IV (when used) below the boundary.

Normally, the upper boundary of Zone II should be coincident with the lower boundary of Zone III. The boundary does not have to be straight across the $120.0 \text{ mm} \pm 1.0 \text{ mm}$ ($4.72 \text{ in} \pm 0.04 \text{ in}$) dimension of the visa. Zone II may also overlay a portion of Zone V for the MRV-A if required. When this occurs, issuing States shall ensure that data contained in either zone are not obscured. See APPENDIX A – Figure 9.

Zone IV, when included on the MRV-A, shall be entered on the right hand side of the visa immediately above but not intruding into the MRZ. See 2.8 – Figure 5.

2.4 Detailed Layout

Visual Inspection Zone (VIZ) (Zones I-V). All data in the VIZ shall be clearly legible.

Print spacing. The design of the MRV-A in Zones II and III is based on a vertical line spacing of a maximum of 8 lines per 25.4 mm (1.0 in) and a horizontal printing density of a maximum of 15 characters per 25.4 mm (1.0 in). This spacing has been chosen as the smallest in which information is clear and legible. If any optional field or data element is not used, the entered data may be spread out in the VIZ of the MRV-A consistent with the requirement for sequencing zones and data elements. This horizontal printing density and the font and the vertical line spacing may be adjusted at the discretion of each State, provided that in the VIZ all data shall be printed in a size such that they can be easily read and assimilated by a person with normal eyesight. Typical configurations are shown in APPENDIX A. Zone VII, the mandatory MRZ, shall be printed with a line spacing as defined in 2.8 – Figure 3, and a horizontal printing density of 10 characters per 25.4 mm (1.0 in).

Data element directory. The data elements in the VIZ are specified as follows.

<i>Field/ zone no.</i>	<i>Data element</i>	<i>Specifications</i>	<i>Maximum no. of character positions</i>	<i>References and notes*</i>
01/I Mandatory	Issuing State	The State responsible for issuing the MRV-A. This shall be personalized, the type font being selected at the discretion of the issuing State. For transliteration rules, refer to Doc 9303-3.	Variable	Notes a, c, d, e, i
02/I Mandatory	Document	The word or words in the language of the issuing State for the document (visa or other appropriate document) which confers on the holder that State's authority to travel to a port of entry in its territory.	Variable	Notes a, c, d, e, i
03/III Mandatory	Place of issue	Post/location (usually a city) where the MRV-A is issued. A translation of the name into one or more languages, one of which should be English, French or Spanish, shall be given when the translated name is more familiar to the international community.	15	Notes a, b, c, ©, k
04/III Mandatory	Valid from (date)	In most cases this will be the date of issue of the MRV-A and indicates the first date from which the MRV-A can be used to seek entry. For some States the date of issue and the date the visa becomes valid may differ. In such cases the latter shall be indicated in this field and the date of issue may be shown in Field 09 (see below). For date format refer to Doc 9303-3.	8	Notes a, b, c, i, k
05/III Mandatory	Valid until (date)	In most cases this will be the date of expiry of the MRV-A and indicates the	8	Notes a, b, c, i, k

<i>Field/ zone no.</i>	<i>Data element</i>	<i>Specifications</i>	<i>Maximum no. of character positions</i>	<i>References and notes*</i>
		last day on which the MRV-A can be used to seek entry. For some States this will be the date by or on which the holder should have left the country concerned. For date format refer to Doc 9303-3.		
06/III Mandatorit	Number of entries	The number of entries for which the visa is valid.	8	Notes a, b, c, i, k
07/III Mandatory	Document number	The number given to the visa by the issuing State.	13	Notes a, b, c, i, j, k
08/III Mandatory	Type/class/category	This field shall include one or more of the following elements: <ul style="list-style-type: none"> the issuing State's indication of the type and/or class of visa granted in accordance with the law/practice of that State; the broad categorization of the type of visa granted, e.g. visitor/resident/temporary resident/student/diplomat, etc., in accordance with the law/practice of the issuing State; any limitations on the territorial validity of the visa. 	46	Notes a, b, c, i, k
09/III Optional	Additional information	This field may include necessary endorsements as to entitlements which attach to the visa. The issuing State may also use this field to include a) the maximum authorized duration of stay; b) conditions related to the granting of the visa; c) date of issue if different from "Valid from" date; and d) record of any fees paid.		Note g
10,11/II Mandatory	Name	See Doc 9303-3.	Variable	Notes a, c, i
10/II Mandatory	Primary identifier	See Doc 9303-3.	Variable	Notes a, c, i, k
11/II Optional	Secondary identifier	See Doc 9303-3.	Variable	Notes a, c, i
12/II Optional	Passport number	The number of the passport or other travel document in which the MRV-A is placed.	Variable	Notes a, b, c, g, i, j
13/II Optional	Sex	Sex of MRV-A holder, when included, is to be specified by use of the single initial commonly used in the language	3	Note a, f, g

<i>Field/ zone no.</i>	<i>Data element</i>	<i>Specifications</i>	<i>Maximum no. of character positions</i>	<i>References and notes*</i>
		of the State of issue. If translation into English, French or Spanish is necessary, followed by a dash and the capital letter F for female, M for male, or X for unspecified.		
14/II Optional	Date of birth	See Doc 9303-3.	9	Notes a, b, c, k
15/II Optional	Nationality	See Doc 9303-3.	Variable	Notes a, h, k
16/IV Optional	Signature or other authorization	An authorization which may be the signature of an issuing official and/or an official stamp.		
17/V Mandatory	Identification feature	<p>This field shall be entered on the document and should contain a portrait of the holder. If included, the portrait shall have a size of 36.0 ± 4.0 mm \times 29.0 ± 3.0 mm (1.42 ± 0.16 in \times 1.14 ± 0.12 in)</p> <p>If a State does not place an identification feature in this field, a national symbol or logo may be inserted instead.</p> <p>See Doc 9303-3-- 3.8.1 for additional specifications for the portrait.</p>		

* Notes can be found in 2.6.

2.5 Machine Readable Zone (MRZ) (Mandatory Zone VII)

2.5.1 MRZ Position

The MRZ is located at the bottom of the MRV-A. 2.8-- Figure 3 shows the nominal position of the data in the MRZ.

2.5.2 Data Elements

The data elements corresponding to Fields 01, 05, 10, 11, and 13 to 15 of the VIZ are mandatory in the MRZ and shall be printed in machine readable form, in the MRZ, beginning with the leftmost character position in each field in the sequence indicated in the data structure specifications shown below. APPENDIX B-- B.1 indicates the structure of the MRZ.

2.5.3 Print Specifications

Machine readable data shall be printed in OCR-B type font, size 1, constant stroke width, as specified in Doc 9303-3. The MRZ shall be printed with the line spacing as defined in 2.8— Figure 3 and a horizontal printing density of 10 characters per 25.4 mm (1.0 in).

2.5.4 Print Position

The position of the left-hand edge of the first character shall be $4.0 \text{ mm} \pm 1.0 \text{ mm}$ ($0.16 \text{ in} \pm 0.04 \text{ in}$) from the left-hand edge of the document. Reference centre lines for the two OCR lines and a nominal starting position for the first character of each line are shown in 2.8— Figure 3. The positioning of the characters is indicated by those reference lines and by the printing zones of the two code lines in 2.8— Figure 3.

2.6 Data Structure of Machine Readable Data for the MRV-A

Data structure of the upper machine readable line

MRZ field character positions (line 1)	Field no. in VIZ	Data element	Specifications	Number of characters	References and notes*
1 to 2		Type of document	Capital letter V to designate a machine readable visa. One additional character may be used, at the discretion of the issuing State, to designate a particular type of visa. If the second character position is not used for this purpose, it shall be filled by the filler character (<).	2	Notes a, b, c, e
3 to 5	1	Issuing State	See Doc 9303-3.	3	Notes a, c, e
6 to 44	10, 11	Name	See Doc 9303-3.	39	Notes a, c, e
		Punctuation in the name	Representation of punctuation is not permitted in the MRZ.		Doc 9303-3
		Apostrophes in the name	Components of the primary or secondary identifiers separated by apostrophes shall be combined, and no filler character (<) shall be inserted. Example: VI Z: D'ARTAGNAN MR Z: DARTAGNAN		Doc 9303-3
		Hyphens in the name	Hyphens (-) in the name shall be converted to the filler character (<) (i.e. hyphenated names shall be represented as separate components). Example: VI Z: MARIE-ELISE		Doc 9303-3

MRZ field
characterpositions Field no.
(line 1) in VIZData element Specifications Number of
characters References
and notes*

MR Z: MARIE<ELISE

Commas Doc 9303-3

When a comma is used in the VIZ to separate the primary and secondary identifiers, the comma shall be omitted in the MRZ and the primary and secondary identifiers shall be separated by two filler characters (<<).

When a comma is used in the VIZ to separate two name components, it shall be represented in the MRZ by a single filler character (<).

Name suffixes Doc 9303-3

Name suffixes (e.g. Jr., Sr., II or III) shall not be included in the MRZ except as permitted by Doc 9303— Part 3 as components of the secondary identifier.

Filler When all components of the primary and secondary identifiers and required separators (filler characters) do not exceed 39 characters in total, all name components shall be included in the MRZ and all unused character positions shall be completed with filler characters (<) repeated up to position 44 as required.

Truncation of the name Doc 9303-3
Note a

When the primary and secondary identifiers and required separators (filler characters) exceed the number of character positions available for names (i.e. 39), they shall be truncated as follows:

Characters shall be removed from one or more components of the primary identifier until three character positions are freed, and two filler characters (<<) and the first character of the first component of the secondary identifier can be inserted. The last character (position 44) shall be an alphabetic character (A through Z). This indicates that truncation may have occurred.

 MRZ field
 character

positions (line 1)	Field no. in VIZ	Data element	Specifications	Number of characters	References and notes*
-----------------------	---------------------	--------------	----------------	-------------------------	--------------------------

Further truncation of the primary identifier may be carried out to allow characters of the secondary identifier to be included, provided that the name field shall end with an alphabetic character (position 44). This indicates that truncation may have occurred.

When the name consists of only a primary identifier which exceeds the number of character positions available for the name, i.e. 39, characters shall be removed from one or more components of the name until the last character in the name field is an alphabetic character.

 Data structure of the lower machine readable line

 MRZ
 character

positions (line 2)	Field no. in VIZ	Data element	Specifications	Number of characters	References and notes*
-----------------------	---------------------	--------------	----------------	-------------------------	--------------------------

1 to 9	07 or 13	Passport or document number	At the discretion of the issuing State, either the passport number or the visa number shall be used in this field; however, the latter option can only be exercised where the visa number has 9 characters or fewer. Any special characters or spaces in the number shall be replaced by the filler character (<). The number shall be followed by the filler character (<) repeated up to position 9 as required.	9	Notes a, b, c, e, j
10		Check digit	See Doc 9303-3.	1	Notes b, e
11 to 13	16	Nationality	See Doc 9303-3.	3	Notes a, c, e, h

MRZ**character****positions****(line 2)**

Field no. in VIZ	Data element	Specifications	Number of characters	References and notes*	
14 to 19	15	Date of birth	See Doc 9303-3.	6	Notes b, c, e
20		Check digit	See Doc 9303-3.	1	Note b
21	14	Sex	F = Female; M = Male; < = non-specified.	1	Notes a, c, f, g
22 to 27	5	Valid until (date)	In most cases this will be the date of expiry of the MRV-A and indicates the last day on which the MRV-A can be used to seek entry. For some States this will be the date by or on which the holder should have left.	6	Doc 9303-3; Notes b, e
28		Check digit	See Doc 9303-3.	1	Note b
29 to 44		Optional data elements	For optional use of the issuing State. Unused character positions shall be completed with the filler character (<) repeated up to position 44 as required.	16	Notes a, b, c, e

*** Notes:**

- a) *Alphabetic characters (A–Z). National characters may be used in the VIZ. In the MRZ, only those characters specified in Doc 9303-3 shall be used.*
- b) *Numeric characters (0–9). National numerals may be additionally included in the VIZ. In the MRZ, only the numerals 0–9 may be used as defined in Doc 9303-3.*
- c) *Punctuation may be included in the VIZ. In the MRZ, only the filler character specified in Doc 9303-3 shall be used.*
- d) *The lengths of fields 01 and 02 are undefined, depending on type font and limits set by MRV-A size and position of other fields.*
- e) *The field caption is not printed on the document.*
- f) *Where a person does not wish his/her sex to be identified or where a State does not want to show this data, the filler character (<) shall be used in this field in the MRZ and an X in this field in the VIZ.*
- g) *The use of a caption to identify a field is at the option of the issuing State.*

- (c) *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 (upper line): V<UTONILAVADHANANANDA<<CHAYAPA<DEJTHAMRONG<K

- (b) One or more name components truncated:

Name: Nilavadhanananda Arnpol Petch Charonguang
 VIZ: NILAVADHANANANDA, ARNPOL PETCH CHARONGUANG
 MRZ (upper line): V<UTONILAVADHANANANDA<<ARNPOL<PETCH<CHARONGU

- (c) *Truncated names — Primary identifier truncated*(a) One or more components truncated to initials:

Name: Dingo Potoroo Bennelong Woolloomooloo Warrandyte Warnambool
 VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
 MRZ (upper line): V<UTOBENNELONG<WOOLOOMOOLOO<WARRANDYTE<W<<DI

- (b) One or more components truncated:

Name: Dingo Potoroo Bennelong Woolloomooloo Warrandyte Warnambool
 VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
 MRZ (upper line): V<UTOBENNELONG<WOOLOOM<WARRAND<WARNAM<<DINGO

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

Name: Dingo Potoroo Bennelong Woolloomooloo Warrandyte Warnambool
 VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
 MRZ (upper line): V<UTOBENNEL<WOOLOO<WARRAN<WARNAM<<DINGO<POTO

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 Papandropoulos
 VIZ: PAPANDROPOULOUS, JONATHON WARREN TREVOR
 MRZ (upper line): V<UTOPAPANDROPOULOS<<JONATHON<WARREN<TREVOR

Note: Even though there is an alphabetic character in the 44th character position of this MRV-A upper machine readable line, this name has not been truncated but it shall be assumed that it has been truncated.

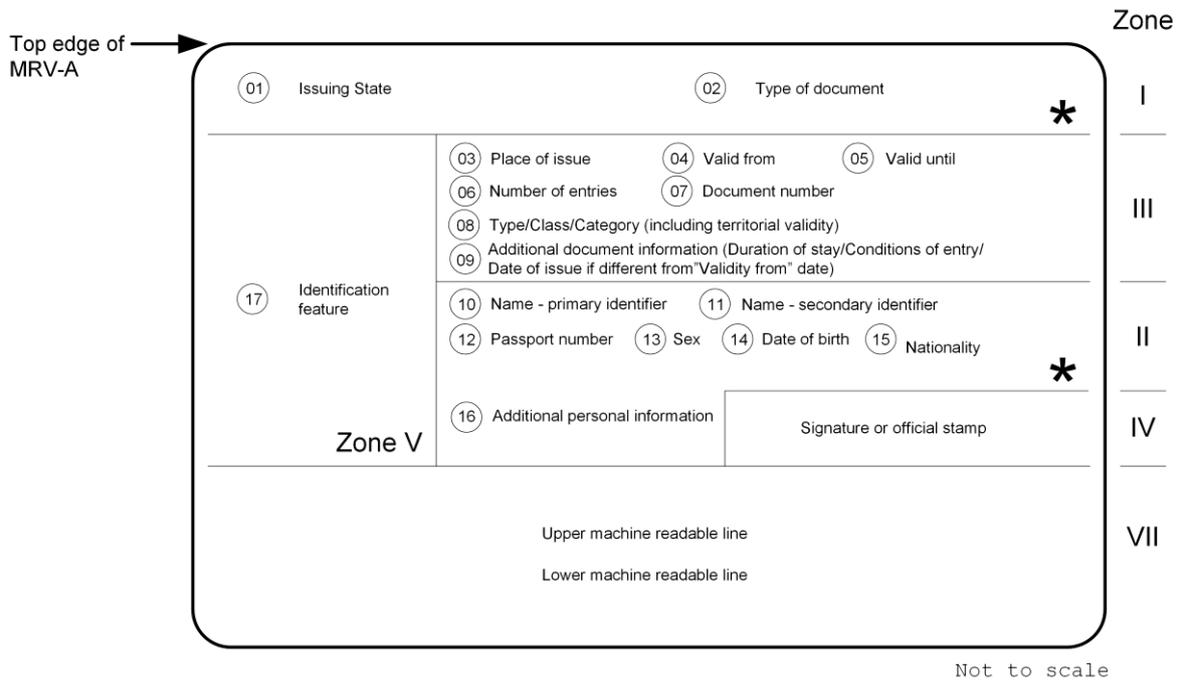
2.7 Portrait

Portrait. For the MRV-A, a portrait should be inserted in the rectangular area defined as Zone V. Such portrait, if included, shall represent only the holder of the MRV-A.

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

Zone V without an identification feature. A standard default image, such as a national symbol, crest or wording, should be selected and used in Zone V when an identification feature is not included.

2.8 MRV-A Diagrams



* Optional control number – to be preprinted at the option of the issuing State either horizontally where shown in Zone I or in Zone II or vertically anywhere along the right-hand edge of Zone V (where present).

Figure 2 : Location of data elements on a MRV-A

Note 1: VIZ based on maximum printing density of 8 lines per 25.4 mm (1.0 in) and horizontal printing density of 15 characters per 25.4 mm (1.0 in);

Note 2: MRZ based on horizontal printing of 10 characters per 25.4 mm (1.0 in);

Note 3: ○ = field numbers;

Note 4: The borderlines of the zones are not printed on the actual visa.

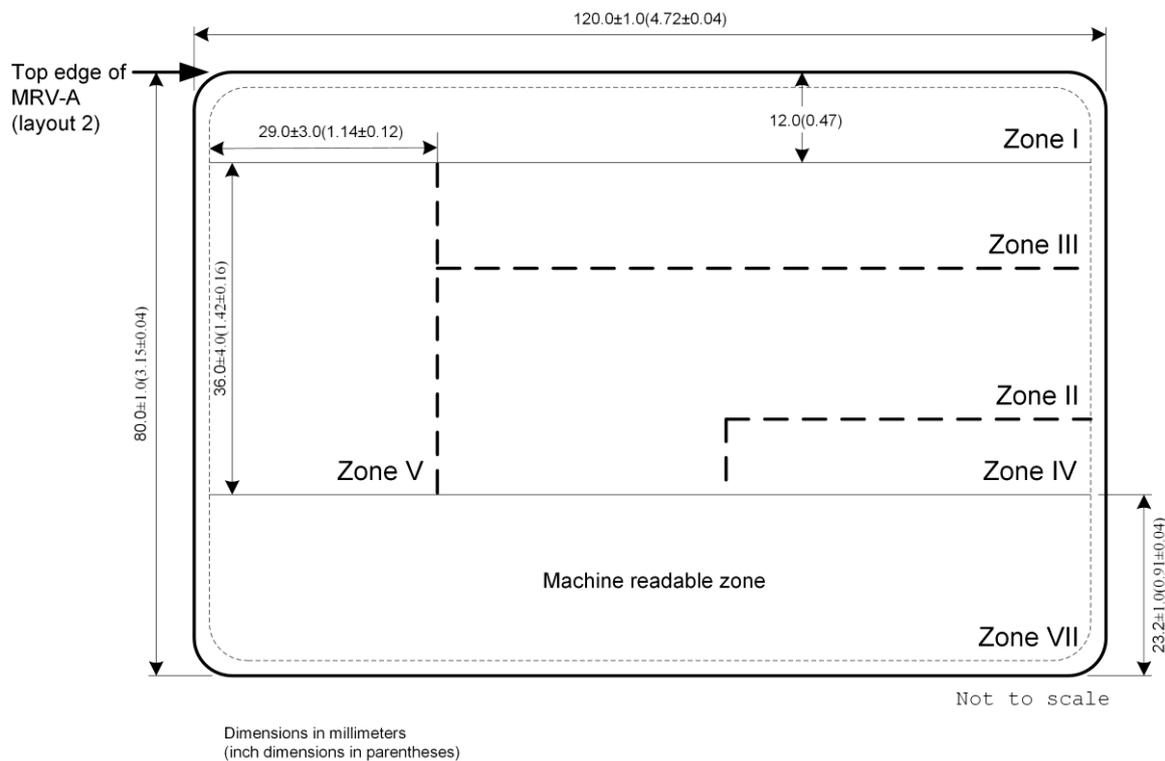


Figure 4 : Nominal positioning of zones on a MRV-A.

This diagram should be considered in conjunction with 2.3. It assumes that all the available space for data in the VIZ is used. The line spacing in the VIZ is the closest permitted at 8 lines per 25.4 mm (1.0 in). If an issuing State requires less information, the line spacing can be increased to print fewer lines in the VIZ.

Dotted lines indicate zone boundaries whose positions are not fixed, enabling issuing States flexibility in the presentation of data.

The dimensions of the identification feature (normally a portrait) shall be between a minimum of 32.0 mm × 26.0 mm (1.26 in × 1.02 in) and a maximum of 40.0 mm × 32.0 mm (1.57 in × 1.26 in). An issuing State may elect to issue an MRV in this format without an identification feature, replacing it with a crest or symbol.

Though the portrait position is defined as a rectangular area, it may have irregular edges or, if the portrait is digitally printed, have the background dropped out. Such techniques may be used to provide protection against fraudulent alteration.

Affixed photographs (even if protected by a laminate) shall not be applied. Identification features shall be personalized.

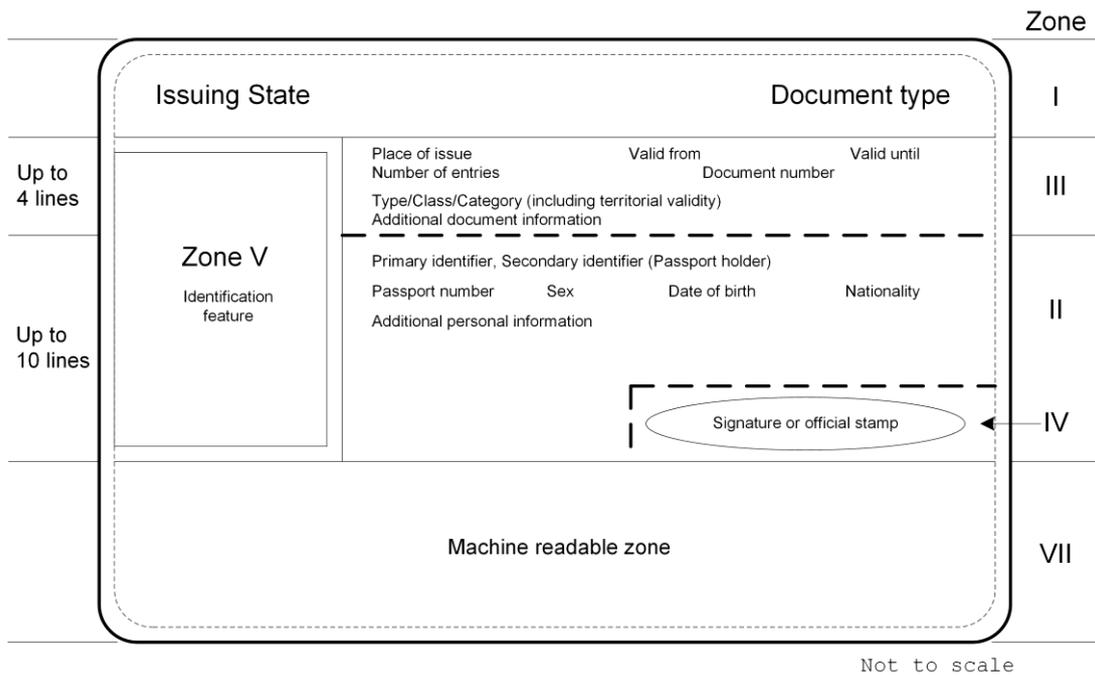


Figure 5 : Data elements on a format A Machine Readable Visa (MRV-A).

Note 1: Broken lines indicate zone borders whose position may be adjusted by the issuing State to optimize the presentation of the data. Solid lines indicate fixed zone borders. Zone border lines are not printed on the documents.

Note 2: Provided it is contained within the rectangular area, the identification feature may have irregular edges.

Note 3: An issuing State may elect to issue a visa with the identification feature replaced by a crest or symbol.

3 TECHNICAL SPECIFICATIONS FOR FORMAT-B MACHINE READABLE VISAS (MRV-B)

This section defines the specifications which are unique to Format-B machine readable visas (MRV-B) and are necessary for global interoperability. Specifications are included for the discretionary expansion of the machine readable data capacity of the MRV beyond that defined for global interchange. The Format-B visa (MRV-B) is suitable for use by States who wish to maintain a clear area on the passport visa page adjacent to the visa, so as to allow a seal to be placed on the visa and the passport page on which it is affixed.

3.1 Dimensions and Placement of the MRV-B

The dimensions and placement of the MRV-B shall be as follows:

MRV-B nominal dimensions. The nominal dimensions of the MRV-B are based on ISO/IEC 7810, ID-2 Type Card as follows:

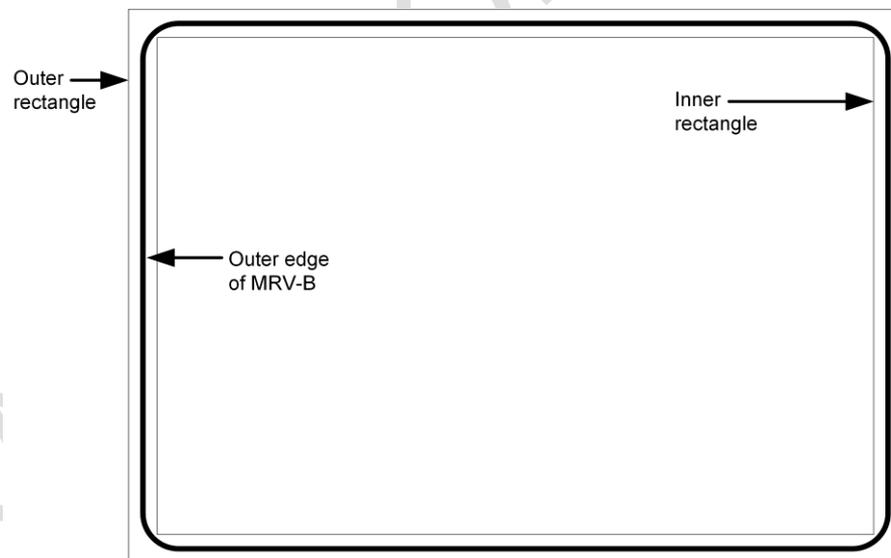
74.0 mm x 105.0 mm (2.91 in x 4.13 in)

MRV-B margins. The dimensional specifications refer to the outer limits of the MRV-B. A margin of 2.0 mm (0.08 in) along each outer edge, with the exception of the header zone, must be left clear of data.

MRV-B edge tolerances. The edges of the MRV-B shall be within the area circumscribed by the concentric rectangles as illustrated in **Error! Reference source not found.**

Inner rectangle: 73.0 mm x 104.0 mm (2.87 in x 4.09 in)

Outer rectangle: 75.0 mm x 106.0 mm (2.95 in x 4.17 in)



Not to scale

Figure 1 : MRV-B dimensional illustration

MRV-B thickness. If the visa is issued as a label, the increase in thickness once the label is attached to the passport visa page shall not exceed 0.19 mm (0.0075 in). The thickness of the area within the machine readable zone (MRZ) shall not vary by more than 0.05 mm (0.002 in). If a protective laminate is used, it is recommended that its thickness not exceed 0.15 mm (0.006 in).

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

Placement of the MRV-B. The MRV-B shall be positioned as follows:

The MRV-B shall be located on the passport visa page such that the MRZ is coincident with and parallel to the outside edge (*reference edge*) of the passport visa page, and the left edge of the MRV-B is coincident with and parallel to the left edge of the passport visa page as defined in APPENDIX C – C.2.

The MRZ shall be located such that the two OCR lines contained therein are within the Effective Reading Zone (ERZ) as defined in Doc 9303-3.

Only one MRV-B shall be located on a passport visa page (see APPENDIX C – C.2).

3.2 General Layout of the MRV-B

The MRV-B follows a standardized layout to facilitate reading of data globally, by visual and machine readable means, to accommodate the various requirements of States' laws and practices and to achieve the maximum standardization within those divergent requirements.

The standard layout incorporates space for a portrait and other identification feature(s). The inclusion of a portrait on a visa is strongly recommended in the interests of security, but States who are not yet able to apply portraits may fill this space with, for example, a national crest.

An MRV-B is divided into six zones as follows:

Zone I	Mandatory header
Zone II	Mandatory and optional personal data elements
Zone III	Mandatory and optional document data elements
Zone IV	Signature (original or reproduction) or authentication
Zone V	Mandatory zone for identification feature (feature optional)
Zone VII	Mandatory machine readable zone (MRZ)

Note 1: The signature in Zone IV of a visa is that of an issuing officer, not of the document holder. The signature may be replaced or accompanied by an official stamp.

Note 2: To facilitate inspection of visas at border control, the layout of the visa presents Zone III above Zone II.

Note 3: Zone VI is not available on an MRV issued in the form of a label.

Note 4: Zones I – V constitute the Visual Inspection Zone (VIZ).

Zones I and VII are mandatory. Certain data in Zones II and III are also mandatory. The mandatory components of these four Zones represent the minimum data requirements for an MRV-B. The optional data elements in Zones II, III and V and in optional Zone IV may be utilized to accommodate the diverse requirements of States, while achieving the desired level of standardization. The data elements which may be included in the various zones and their order are set out in 3.8. 3.8 also illustrates the dimensional specifications and tolerances for the two layouts of the MRV-B and the technical specifications for the printing of data elements within the zones, as well as the guidelines for positioning and adjusting the dimensional specifications of Zones I to V to accommodate the flexibility desired by issuing States. Examples of personalized MRV-Bs are shown in APPENDIX A – A.2. APPENDIX B – B.2 illustrates the format for the presentation of the machine readable data in Zone VII.

3.3 Content, Use and Dimensional Flexibility of Zones

The data elements to be included in the zones, the treatment of the zones and guidelines for the dimensional layout of zones shall be as described hereunder.

Zone I identifies the issuing State and the type of document. These elements are mandatory. The order of the data elements in this zone is left to the discretion of the issuing State.

To facilitate the checking of visas by airline personnel and control authorities, the essential details of the visa document shall be entered in a standard sequence in Zone III while essential personal details of the holder shall be entered in a standard sequence in Zone II. On a visa, Zone III appears above Zone II.

Zone IV provides space for an optional signature or authentication. This is normally the signature of the issuing officer or an official stamp. The application of an official stamp elsewhere on the document is not precluded except that it must not intrude into the MRZ or affect the legibility of entered data.

Zone VII conforms in height to the MRZ defined for all MRTDs so that the machine readable data lines fall within the ERZ specified in Doc 9303-3, thus allowing a single reader to be used for all types and sizes of MRTDs.

All MRZ data elements are mandatory and shall be shown as defined in 3.6 even though an issuing State may choose not to include a specific MRZ data element in the VIZ.

3.3.1 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 MRV-B to accommodate the diverse requirements of issuing States. 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 MRV-B. The nominal position of the zones is shown in 3.8 – Figure 4.

When an issuing State chooses to produce an MRV-B as a securely attached card containing a transparent or otherwise unprintable border around the card, the available area within the zones will be reduced. The full MRV-B dimensions and zone boundaries shall be measured from the outside edge of this border, which is the external edge of the MRV-B.

Zone I shall be adjacent and parallel to the top edge of the MRV-B and extend across the full $105.0 \text{ mm} \pm 1.0 \text{ mm}$ ($4.13 \text{ in} \pm 0.04 \text{ in}$) dimension. The issuing State may vary the *vertical* dimension of Zone I, as required, but the dimension shall be sufficient to allow legibility of the data elements, and the height shall not be greater than 12.0 mm (0.47 in) as defined in 3.8 – Figure 4.

Zone V shall be located such that its left edge is coincident with the left edge of the MRV-B, as defined in 3.8 – Figure 4. Zone V may vary in size but any variation from the nominal dimensions shall not exceed the tolerances specified in 3.8 – Figure 4.

Zone V may move *vertically* along the left edge of the MRV-B and overlay a portion of Zone I as long as individual details contained in either zone are not obscured. Zone V may, as a result, have its *lower external boundary* coincident with the top edge of the MRZ of the MRV-B and its *upper external boundary* coincident with the top edge of the MRV-B.

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

Zone III may extend to the full width of that portion of the MRV-B to the right of Zone V.

The lower boundary of Zone III (see 3.8 – Figure 4) may be positioned at the discretion of the issuing State. Enough space shall be left for Zone II and Zone IV (when used) below the boundary. The boundary does not need to be straight across the $105.0 \text{ mm} \pm 1.0 \text{ mm}$ ($4.13 \text{ in} \pm 0.04 \text{ in}$) dimension of the MRV-B.

Normally, the upper boundary of Zone II should be coincident with the lower boundary of Zone III. The boundary does not have to be straight across the $105.0 \text{ mm} \pm 1.0 \text{ mm}$ ($4.13 \text{ in} \pm 0.04 \text{ in}$) dimension of the visa. Zone II may also overlay a portion of Zone V for the MRV-B if required. When this occurs, issuing States shall ensure that data contained in either zone are not obscured. See APPENDIX A – A.1.

Zone IV, when included on the MRV-B, shall be entered on the right hand side of the visa immediately above but not intruding into the MRZ. See 3.8 – Figure 5.

3.4 Detailed Layout

Visual inspection zone (VIZ) (Zones I-V). All data in the VIZ shall be clearly legible.

Print spacing. The design of the MRV-B in Zones II and III is based on a vertical line spacing of a maximum of 8 lines per 25.4 mm (1.0 in) and a horizontal printing density of a maximum of 15 characters per 25.4 mm (1.0 in). This spacing has been chosen as the smallest in which information is clear and legible. If any optional field or data element is not used, the entered data may be spread out in the VIZ of the MRV-B consistent with the requirement for sequencing zones and data elements. This horizontal printing density and the font and the vertical line spacing may be adjusted at the discretion of each State, provided that in the VIZ all data shall be printed in a size such that they can be easily read and assimilated by a person with normal eyesight. Typical configurations are shown in APPENDIX A – A.2. Zone VII, the mandatory MRZ, shall be printed with a line spacing as defined in 3.8 – Figure 3, and a horizontal printing density of 10 characters per 25.4 mm (1.0 in).

Data element directory. The data elements in the VIZ are specified as follows.

<i>Field/ zone no.</i>	<i>Data element</i>	<i>Specifications</i>	<i>Maximum no. of character positions</i>	<i>References and notes*</i>
01/I Mandatory	Issuing State	The State responsible for issuing the MRV-B. This shall be personalized, the type font being selected at the discretion of the issuing State. For transliteration rules, refer to Doc 9303-3.	Variable	Notes a, c, d, e, i
02/I Mandatory	Document	The word or words in the language of the issuing State for the document (visa or other appropriate document) which confers on the holder that State's authority to travel to a port of entry in its territory.	Variable	Notes a, c, d, e, i
03/III Mandatory	Place of issue	Post/location (usually a city) where the MRV-B is issued. A translation of the name into one or more languages, one of which should be English, French or Spanish, shall be given when the translated name is more familiar to the international community.	15	Notes a, b, c, ©, k
04/III Mandatory	Valid from (date)	In most cases this will be the date of issue of the MRV-B and indicates the first date from which the MRV-B can be used to seek entry. For some States the date of issue and the date the visa becomes valid may differ. In such cases the latter shall be indicated in this field and the date of issue may be shown in Field 09 (see below). Date formats are specified in	8	Notes a, b, c, i, k

<i>Field/ zone no.</i>	<i>Data element</i>	<i>Specifications</i>	<i>Maximum no. of character positions</i>	<i>References and notes*</i>
		9303-3.		
05/III Mandatort	Valid until (date)	In most cases this will be the date of expiry of the MRV-B and indicates the last day on which the visa can be used to seek entry. For some States this will be the date by or on which the holder should have left the country concerned. Date formats are specified in 9303-3.	8	Notes a, b, c, i, k
06/III Mandatory	Number of entries	The number of entries for which the visa is valid.	8	Notes a, b, c, i, k
07/III Mandatory	Document number	The number given to the visa by the issuing State.	13	Notes a, b, c, i, j, k
08/III Mandatory	Type/class/category	This field shall include one or more of the following elements: <ul style="list-style-type: none"> the issuing State's indication of the type and/or class of visa granted in accordance with the law/practice of that State; the broad categorization of the type of visa granted, e.g. visitor/resident/temporary resident/student/diplomat, etc., in accordance with the law/practice of the issuing State; any limitations on the territorial validity of the visa. 	46	Notes a, b, c, i, k
09/III Optional	Additional information	This field may include necessary endorsements as to entitlements which attach to the visa. The issuing State may also use this field to include a) the maximum authorized duration of stay; b) conditions related to the granting of the visa; c) date of issue if different from "Valid from" date; and d) record of any fees paid.		Note g
10,11/II Mandatory	Name	See Doc 9303-3.	Variable	Notes a, c, i, k
10/II Mandatory	Primary identifier	See Doc 9303-3.	Variable	Notes a, c, i, k
11/II Optional	Secondary identifier	See Doc 9303-3.	Variable	Notes a, c, i
12/II Optional	Passport number	The number of the passport or other travel document in which the MRV-B	Variable	Notes a, b, c, g, i, j

<i>Field/ zone no.</i>	<i>Data element</i>	<i>Specifications</i>	<i>Maximum no. of character positions</i>	<i>References and notes*</i>
		is placed.		
13/II Optional	Sex	Sex of MRV-B holder, when included, is to be specified by use of the single initial commonly used in the language of the State of issue. If translation into English, French or Spanish is necessary, followed by a dash and the capital letter F for female, M for male, or X for unspecified.	3 Fixed	Notes a, f, g
14/II Optional	Date of birth	See Doc 9303-3.	9	Notes a, b, c, k
15/II Optional	Nationality	See Doc 9303-3.	Variable	Notes a, h, k
16/IV Optional	Signature or other authorization	An authorization which may be the signature of an issuing official or an official stamp.		
17/V Mandatory	Identification feature	This field shall appear on the document and should contain a portrait of the holder. If included, the portrait shall have a nominal size of 35.5 ± 3.5 mm (1.40 ± 0.14 in) \times 28.5 ± 2.5 mm (1.12 ± 0.1 in). If a State does not place an identification feature in this field, a national symbol or logo may be inserted instead. See Doc 9303-3-- 3.8.1 for additional specifications for the portrait.		Note e

* Notes can be found in 3.6.

3.5 Machine Readable Zone (MRZ) (Mandatory Zone VII)

3.5.1 MRZ Position

The MRZ is located at the bottom of the MRV-B. 3.8-- Figure 3 shows the nominal position of the data in the MRZ.

3.5.2 Data Elements

The data elements corresponding to Fields 01, 05, 10, 11, and 13 to 15 of the VIZ are mandatory in the MRZ and shall be printed in machine readable form, in the MRZ, beginning with the leftmost character position in each field in the sequence indicated in the data structure specifications shown below. APPENDIX B-- B.2 indicates the structure of the MRZ.

3.5.3 Print Specifications

Machine readable data shall be printed in OCR-B type font, size 1, constant stroke width, as specified in Doc 9303-3. The MRZ shall be printed with the line spacing as defined in 3.8, Figure 3, and a horizontal printing density of 10 characters per 25.4 mm (1.0 in).

3.5.4 Print Position

The position of the left-hand edge of the first character shall be $4.0 \text{ mm} \pm 1.0 \text{ mm}$ ($0.16 \text{ in} \pm 0.04 \text{ in}$) from the left-hand edge of the document. Reference centre lines for the two OCR lines and a nominal starting position for the first character of each line are shown in 3.8— Figure 3. The positioning of the characters is indicated by those reference lines and by the printing zones of the two code lines in 3.8— Figure 3.

DRAFT_4 FOR TAG_22

3.6 Data Structure of Machine Readable Data for the MRV-B

Data structure of the upper machine readable line

MRZ field character positions (line 1)	Field no. in VIZ	Data element	Specifications	Number of characters	References and notes*
1 to 2		Type of document	Capital letter V to designate an MRV. One additional character may be used, at the discretion of the issuing State, to designate a particular type of visa. If the second character position is not used for this purpose, it shall be filled by the filler character (<).	2	Notes a, b, c, e
3 to 5	1	Issuing State	See Doc 9303-3.	3	Notes a, c, e
6 to 36	10, 11	Name	See Doc 9303-3.	31	Notes a, c, e
		Punctuation in the name	Representation of punctuation is not permitted in the MRZ.		Doc 9303-3
		Apostrophes in the name	Components of the name in the VIZ, separated by apostrophes shall be combined, and no filler character (<) shall be inserted. <i>Example:</i> VI Z: D'ARTAGNAN MR Z: DARTAGNAN		Doc 9303-3
		Hyphens in the name	Hyphens (-) in the name shall be converted to the filler character (<) (i.e. hyphenated names shall be represented as separate components). <i>Example:</i> VI Z: MARIE-ELISE MR Z: MARIE<ELISE		Doc 9303-3
		Commas	When a comma is used in the VIZ to separate the primary and secondary identifiers, the comma shall be omitted in the MRZ and the primary and secondary identifiers shall be separated by two filler characters (<<). When a comma is used in the VIZ to separate two name components, it shall be represented in the MRZ by a single filler character (<).		Doc 9303-3

MRZ field
characterpositions Field no.
(line 1) in VIZData element Specifications Number of
characters References
and notes*

Name suffixes Name suffixes (e.g. Jr., Sr., II or III) shall not be included in the MRZ except as permitted by Doc 9303-3 as components of the secondary identifier. Doc 9303-3

Filler When all components of the primary and secondary identifiers and required separators (filler characters) do not exceed 31 characters in total, all name components shall be included in the MRZ and all unused character positions shall be completed with filler characters (<) repeated up to position 36 as required.

Truncation of the name When the primary and secondary identifiers and required separators (filler characters) exceed the number of character positions available for names (i.e. 31), they shall be truncated as follows: Doc 9303-3
Notes a, c, e

Characters shall be removed from one or more components of the primary identifier until three character positions are freed, and two filler characters (<<) and the first character of the first component of the secondary identifier can be inserted. The last character (position 36) shall be an alphabetic character (A through Z). This indicates that truncation may have occurred.

Further truncation of the primary identifier may be carried out to allow characters of the secondary identifier to be included, provided that the name field shall end with an alphabetic character (position 36). This indicates that truncation may have occurred.

When the name consists of only a primary identifier which exceeds the number of character positions available for the name, i.e. 31, characters shall be removed from one or more components of the name until the last character in the

MRZ field
characterpositions (line 1) Field no.
in VIZ

Data element

Specifications

Number of
charactersReferences
and notes*

name field is an alphabetic character.

Data structure of the lower machine readable line

MRZ field
characterpositions (line 2) Field no.
in VIZ

Data element

Specifications

Number of
charactersReferences
and notes*

1 to 9	07 or 12	Passport or document number	At the discretion of the issuing State, either the passport number or the visa number shall be used in this field; however, the latter option can only be exercised where the visa number has 9 characters or fewer. Any special characters or spaces in the number shall be replaced by the filler character (<). The number shall be followed by the filler character (<) repeated up to position 9 as required.	9	Notes a, b, c, e, j
10		Check digit	See Doc 9303-3.	1	Notes b, e
11 to 13	15	Nationality	See Doc 9303-3.	3	Notes a, c, e, h
14 to 19	14	Date of birth	See Doc 9303-3.	6	10.2; Notes b, c, e
20		Check digit	See Doc 9303-3.	1	Note b
21	13	Sex	F = Female; M = Male; < = non-specified.	1	Notes a, c, f, g
22 to 27	5	Valid until (date)	In most cases this will be the date of expiry of the MRV-B and indicates the last day on which the visa can be used to seek entry. For some States this will be the date by or on which the holder should have left. Date formats are specified in 9303-3.	6	Notes b, e
28		Check digit	See Doc 9303-3.	1	Note b
29 to		Optional data	For optional use of the issuing	8	Notes a, b, c,

MRZ field character positions (line 2)	Field no. in VIZ	Data element	Specifications	Number of characters	References and notes*
36		elements	State. Unused character positions shall be completed with the filler character (<) repeated up to position 36 as required.		e

* Notes:

- a) *Alphabetic characters (A–Z). National characters may be used in the VIZ. In the MRZ, only those characters specified in Doc 9303-3 shall be used.*
- b) *Numeric characters (0–9). National numerals may be used in the VIZ. In the MRZ, only those characters specified in Doc 9303-3 shall be used.*
- c) *Punctuation or other special characters may be used in the VIZ. In the MRZ, only the filler character specified in Doc 9303-3 shall be used.*
- d) *The lengths of fields 01 and 02 are undefined, depending on type font and limits set by MRV-B size and position of other fields.*
- e) *The field caption is not printed on the document.*
- f) *Where a person does not wish his/her sex to be identified or where a State does not want to show this data, the filler character (<) shall be used in this field in the MRZ and an X in this field in the VIZ.*
- g) *The use of a caption to identify a field is at the option of the issuing State.*
- h) *United Nations Laissez-passer are issued to officials of the United Nations Organization under the terms of the Convention on the Privileges and Immunities of the United Nations of 13 February 1946 and to officials of the Specialized Agencies of the United Nations under the terms of the Convention on the Privileges and Immunities of the Specialized Agencies of the United Nations of 21 November 1947. In the case of visas entered in the United Nations Laissez-passer, in keeping with the international character of United Nations officials, nationality shall not be shown. Instead the appropriate code shall be entered in accordance Doc 9303-3.*
- i) *The number of characters (in the field length) includes any blank spaces.*
- j) *The number of characters in the VIZ may be variable; however, if the document number has more than 9 characters, the 9 principal characters shall be shown in the MRZ in character positions 1 to 9.*
- k) *The field caption shall be printed on the document.*

3.6.1 Examples of names of the holder in the MRZ

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

Usual representation:

MRZ (upper line): V<UTOBENN<WOOL<WARR<WARN<<DINGO<POTO

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

Name: Stephen Trevor Papandropoulos
VIZ: PAPANDROPOULOUS, STEPHEN TREVOR
MRZ (upper line): V<UTOPAPANDROPOULOS<<STEPHEN<TREVOR

Note: Even though there is an alphabetic character in the 36th character position of this MRV-B upper machine readable line, this name has not been truncated but it shall be assumed that it has been truncated.

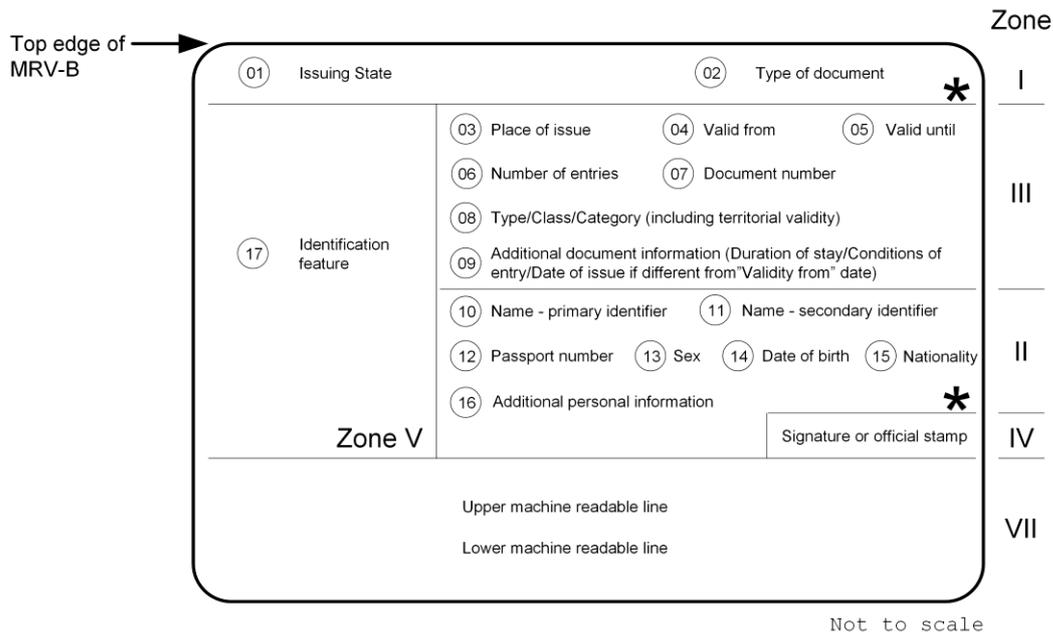
3.7 Portrait

Portrait. For the MRV Format-B the rectangular area defined in the data element directory as Zone V should contain a portrait. Such portrait, if included, shall represent only the holder of the MRV-B.

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

Zone V without an identification feature. A standard default image, such as a national symbol, crest or wording, should be selected and used in Zone V when an identification feature is not included.

3.8 MRV-B Diagrams



* Optional control number – to be preprinted at the option of the issuing State either horizontally where shown in Zone I or in Zone II or vertically anywhere along the right-hand edge of Zone V (where present).

Figure 2 : Location of data elements on a MRV-B.

Note: VIZ based on maximum printing density of 8 lines per 25.4 mm (1.0 in) and horizontal printing density of

- 15 characters per 25.4 mm (1.0 in)
- MRZ based on horizontal printing of 10 characters per 25.4 mm (1.0 in)
- F = field numbers
- The borderlines of the zones are omitted on the actual visa.

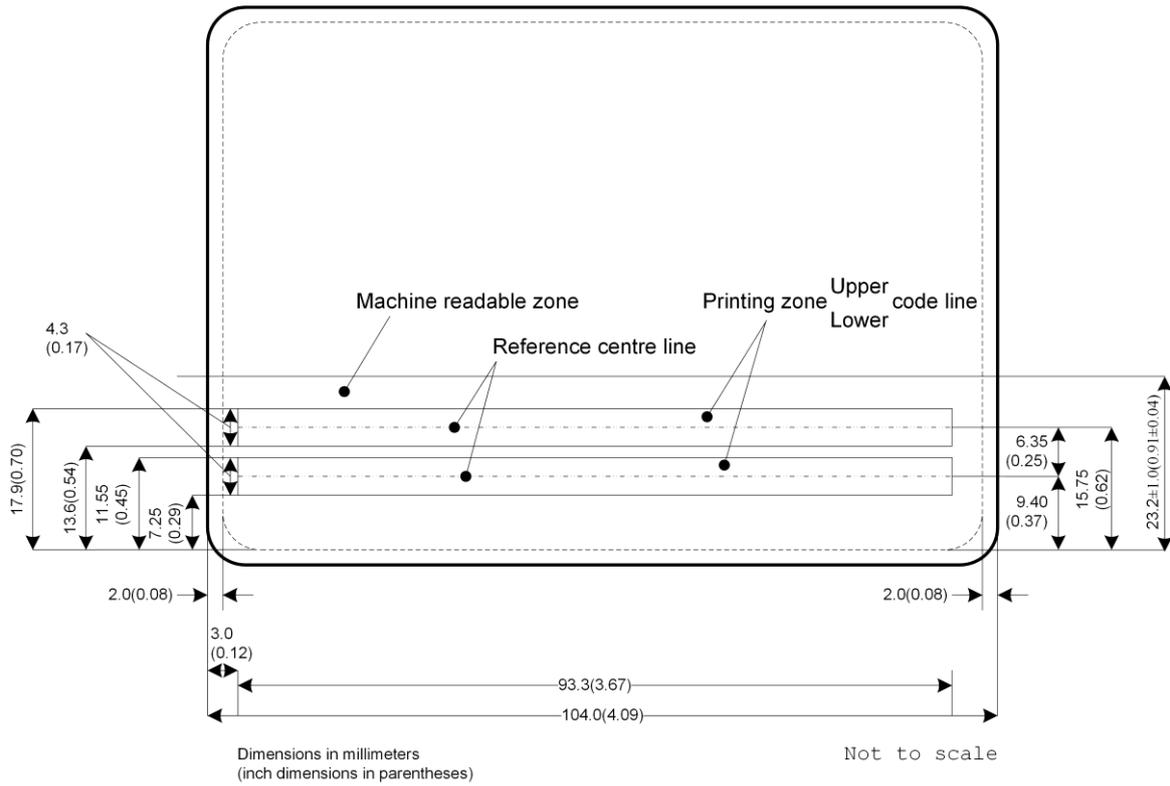


Figure 3 : Schematic diagram of the Machine Readable Zone of a MRV-B.

Note: For illustration purposes, the smallest option for the 105.0 mm (4.13 in) dimension of the MRV-B and the smallest option for the left-hand margin in the MRZ have been selected.

DRAFT

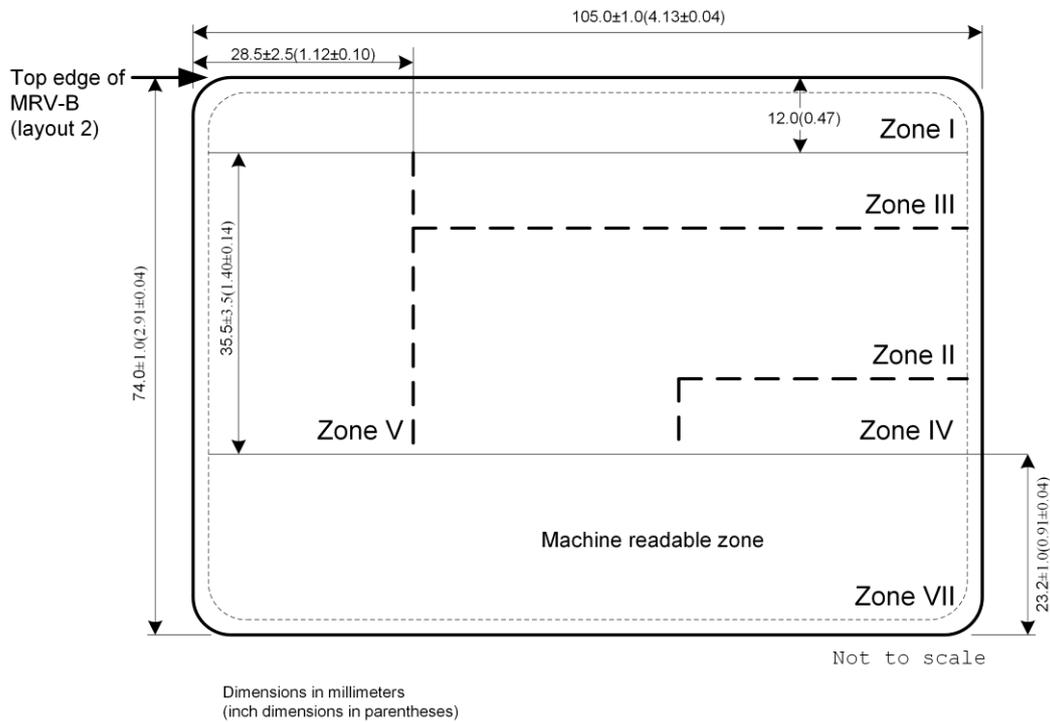


Figure 4 : Nominal positioning of zones on a MRV-B).

This diagram should be considered in conjunction with 3.3. It assumes that all the available space for data in the Visual Inspection Zone is used. The line spacing in the VIZ is the closest permitted at 8 lines per 25.4 mm (1.0 in). If an issuing State requires less information the line spacing can be increased to print fewer lines in the VIZ.

Dotted lines indicate zone boundaries whose positions are not fixed, enabling issuing States flexibility in the presentation of data.

The dimensions of the identification feature (normally a portrait) shall be between a minimum of 32.0 mm × 26.0 mm (1.26 in × 1.02 in) and a maximum of 39.0 mm × 31.0 mm (1.54 in × 1.22 in). An issuing State may elect to issue an MRV in this format without an identification feature, replacing it with a crest or symbol.

Though the portrait position is defined as a rectangular area, it may have irregular edges or, if the portrait is digitally printed, have the background dropped out. Such technique may be used to provide protection against fraudulent alteration.

Affixed photographs (even if protected by a laminate) shall not be applied. Identification features shall be personalized.

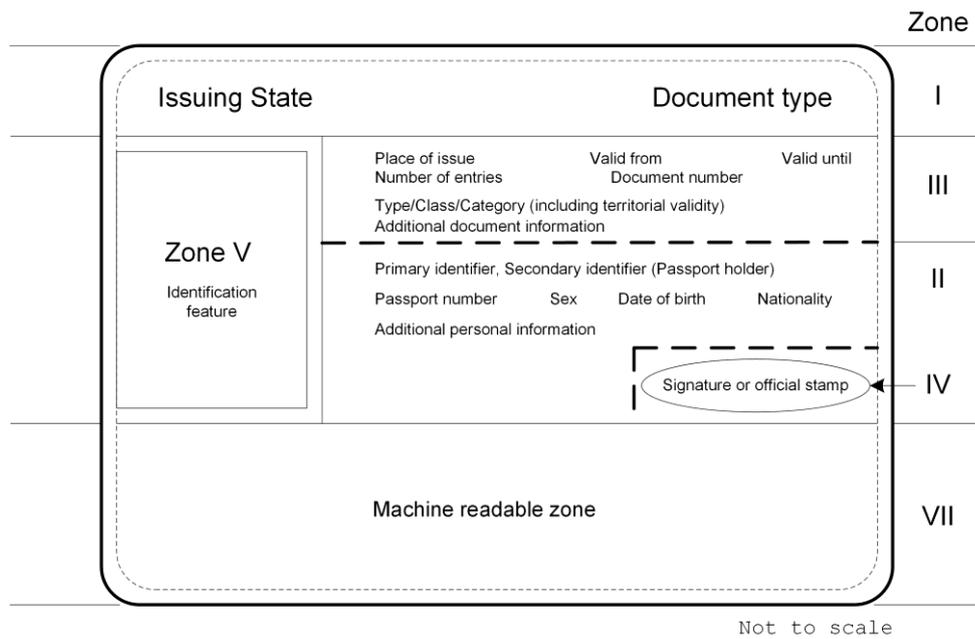


Figure 5 : Data elements on a format B Machine Readable Visa (MRV-B).

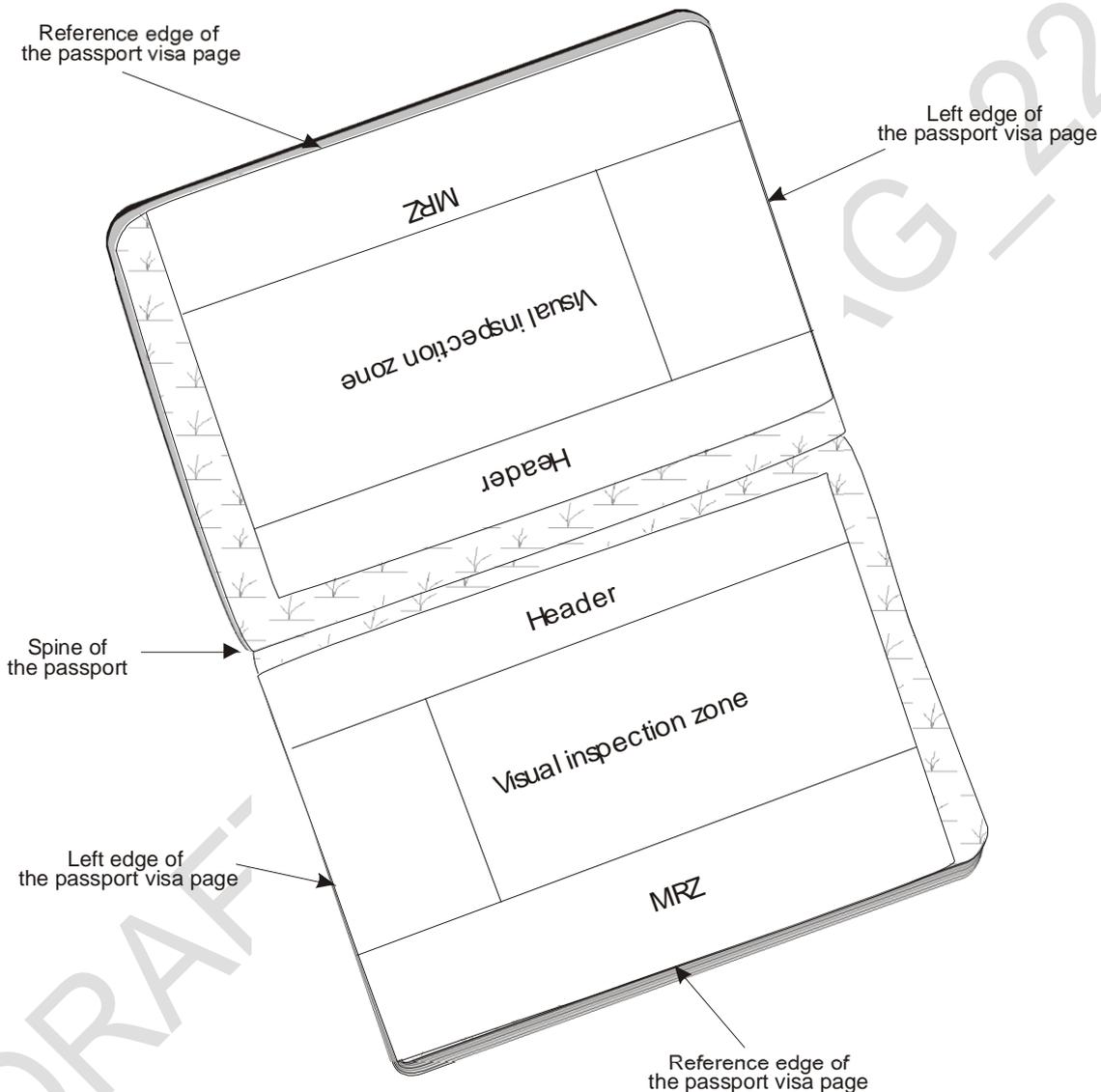
Note 1: Broken lines indicate zone borders whose position may be adjusted by the issuing State to optimize the presentation of the data. Solid lines indicate fixed zone borders. Zone border lines are not printed on the document.

Note 2: Provided it is contained within the rectangular area, the identification feature may have irregular edges.

Note 3: An issuing State may elect to issue a visa with the identification feature replaced by a crest or symbol.

APPENDIX C POSITIONING IN PASSPORT (INFORMATIVE)

C.1 MRV-A Positioning

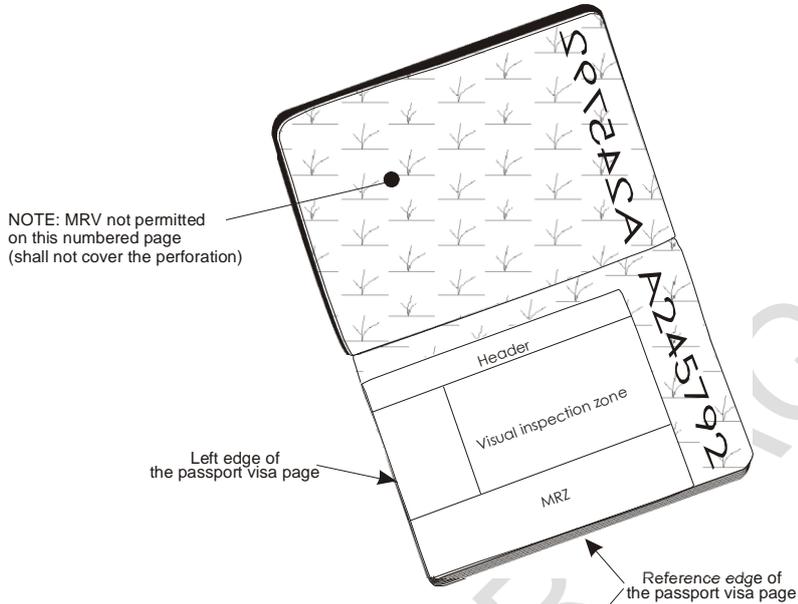


Each MRV shall be placed so that:

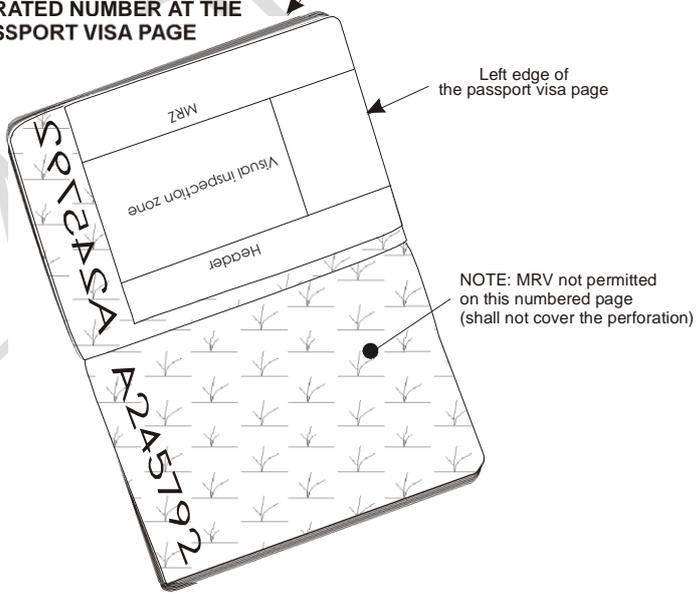
- the two OCR lines of the MRZ are parallel to the appropriate reference edge of the passport visa page;
- the leading characters of each OCR line are positioned with respect to the left edge of the passport visa page;
- the MRZ is immediately adjacent to the appropriate reference edge of the passport visa page;
- and no MRV may be placed on top of another, nor on the reverse of a page that already has an MRV affixed, nor on the reverse of an MRP data page.

C.2 MRV-B Positioning

EXAMPLE 1: PRINTED OR PERFORATED NUMBER AT THE TOP OF THE PASSPORT VISA PAGE



EXAMPLE 2: PRINTED OR PERFORATED NUMBER AT THE BOTTOM OF THE PASSPORT VISA PAGE



APPENDIX D MATERIALS AND PRODUCTION METHODS (INFORMATIVE)

Note 1: The following information reflects some past as well as current practices of MRV producers and is included here for guidance only. It is not an endorsement of any product or method.

Note 2: It is the responsibility of the issuing State to ensure that the MRV selected for issue is constructed in such a way that the document will perform satisfactorily for its required life.

Traditionally, visas have taken the form either of a label affixed to a page of the holder's passport or the application of an imprint onto the passport page usually with manual infilling for the personalization. Manual infilling is obviously impractical for machine readable visas where very precise characters for optical recognition are required. There is no fundamental reason why a visa should not be imprinted onto a passport page using a printer capable of printing OCR-B. However, an issuing State that elects to do this will find that many passports, which, of course, are issued by other States, have printed or perforated numbers or other printing on their pages which can absorb the infra red light used by the document reader and result in a failure to read at border control. In general, therefore, it is better to use a machine readable visa in the form of a label affixed to the passport page.

An MRV can have a life limited to a single entry into a country or it can allow multiple entries over the life of the passport or beyond. The issuing State should ensure that the MRV is appropriately durable for the required life. States should also ensure that their visas are resistant to fraud. States can achieve considerable protection against these threats where border control has access to a central database containing the details of the issuance of genuine visas. However this is not always practicable. The threats are:

- total counterfeiting of the document;
- removal of a visa from one passport and its placement in another;
- alteration of the personal information or validity data.

Substrate. Visas have been produced using either paper or a synthetic polymer as the substrate. The substrate should have adequate opacity to prevent any printing or perforations on the passport page affecting the machine reading. The substrate should exhibit no visible fluorescence when irradiated by ultra violet light. Common choices of security features for paper have included: chemical reactants, iridescent plaquettes, fibers (silk and/or synthetics, visible and/or invisible, fluorescent and/or non-fluorescent), and security threads. Synthetic polymer substrates may also incorporate some of these security features. Care must be taken to ensure that any chemical reactants used are unaffected by the adhesive used to affix the visa. It is desirable that the substrate be damaged by attempts to alter the data on the visa or to remove it from the passport. The damage may take the form of tearing or distortion.

Inks. Inks that are chemically fugitive, fluorescent, heat sensitive, and optically variable are means of enhancing security in the MRV.

Printing. Fine line printing, rainbow (split fountain) printing using guilloche patterns, intaglio printing, and incorporation of concealed images into the design are methods of enhancing both the security and aesthetics of the MRV.

Adhesive. Water-moistenable or pressure-sensitive adhesives have been used to affix visas into passports. The selected adhesive should achieve and maintain a strong bond even when heated. The adhesive/substrate combination should be such that the substrate tears or distorts before the adhesive bond fails.

Die cutting. Though the final size and shape of the visa is defined in these specifications, the size is too small for most types of visa infilling printers. It is therefore normal for an issuing State to procure visas in a sheet form suitable for the infilling printer with one or more visas contained within the sheet area, the visas being die cut to shape. It is important to ensure compatibility between the sheets of

visas and the printer to ensure that the visas do not become separated from the carrier sheet in the printer. It is also important to ensure that the edges of the sheet or of the die-cut shape are not contaminated with adhesive which can build up in the printer and result in misfeeding. Consistency of position of the die-cut shape relative to the edges of the sheet is important to ensure that the machine readable information is placed within the ERZ.

Personalization. Most forms of variable image printing, including laser (covered by a laminate), ink jet, dye sublimation and dot matrix printing have been used in the personalization of visas, with the first three used where a portrait is required. To minimize the risk of fraudulent removal of the personalization, the selected combination of substrate and infilling method should achieve a high penetration of the image into the substrate or a strong bond between the material forming the image and the substrate.

Protecting the personalization. Protective laminate or lacquer layers may be used to secure the data on the visa. Any laminate material should be firmly bonded to the substrate so that disruption of the substrate or destruction of the laminate material occurs when attempts are made to remove the laminate.

DRAFT - 4 FOR TAG - 2

REFERENCES (NORMATIVE)

Certain provisions of the following international Standards, referenced in this text, constitute provisions of Part 7 of Doc 9303. Where differences exist between the specifications contained in Part 7 and the referenced Standards, to accommodate specific construction requirements for machine readable travel documents, including machine readable visas, the specifications contained herein shall prevail.

[ISO/IEC WD 15438]	ISO/IEC JTC 1/SC 31 WD 15438, Automatic identification and data capture — 2D-bar code symbology specifications — PDF417
[ISO/IEC WD 15417]	ISO/IEC JTC 1/SC 31 WD 15417, Bar coding — Symbology specification — Code 128
[ISO/IEC 7810]	ISO/IEC 7810 : 2003, Identification cards — Physical characteristics
[ISO/IEC 10373-1]	ISO/IEC 10373-1 : 1998, Identification cards — Test methods — Part 1: General characteristics tests
[ISO 1073-2]	ISO 1073-2:1976, Alphanumeric character sets for optical recognition — Part 2: Character set OCR-B — Shapes and dimensions of the printed image
[ISO 3166-1]	ISO 3166-1:1997, Codes for the representation of names of countries and their subdivisions — Part 1: Country codes
[ISO 8601]	ISO 8601:2000, Data elements and interchange formats — Information interchange — Representation of dates and times
[EN 797]	EN 797:1995, Bar coding — Symbology specifications — “EAN/UPC”
[EN 799]	EN 799:1995, Bar coding — Symbology specifications — “Code 128”
[EN 800]	EN 800:1995, Bar coding — Symbology specifications — “Code 39”
[EN 1571]	EN 1571:1996, Bar coding — Data identifiers
[EN 1635]	EN 1635:1997, Bar coding — Test specifications — Bar code symbols
[ENV 12403]	ENV 12403:1998, Bar coding — Structured data files
[ENV 12925]	ENV 12925:1998, Bar coding — Symbology specifications — “PDF417”



Machine Readable Travel Documents

Part 8
Emergency Travel Documents

DRAFT 4 FOR TAG_22
[Par 8 under development]

Approved by the Secretary General
and published under his authority

Seventh Edition – Revision 1 - 2014

International Civil Aviation Organization

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

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

Doc 9303, Machine Readable Travel Documents
Order Number: xxxx
ISBN xxx-xx-xxxx-xxx-x

© ICAO 2014

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.

Doc 9303



Machine Readable Travel Documents

**Part 9
The Deployment of Biometric Identification and the Electronic Storage of
Data in eMRTDs**

Approved by the Secretary General
and published under his authority

Seventh Edition – Revision 1 - 2014

International Civil Aviation Organization

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

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

Doc 9303, Machine Readable Travel Documents
ISBN xxx-xx-xxxx-xxx-x

© ICAO 2014

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 TO DOC 9303-9, 7TH EDITION

Revision	Date	Description
01	xx-xx-2014	Initial release of the 7 th edition

DRAFT_4 FOR TAG_22

TABLE OF CONTENTS

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
APPENDIX A	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	16
A.4	Reader construction	16
APPENDIX B	PROCESS FOR READING EMRTDS (INFORMATIVE)	17
REFERENCES (NORMATIVE)	18

1 SCOPE

The seventh edition of Doc 9303 represents a restructuring of the ICAO specifications for Machine Readable Travel Documents. Without incorporating substantial modifications of 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 9 of Doc 9303 is based on Doc 9303 Part 1, sixth edition, Volume 2, Section II (2006), as well as Doc 9303 Part 3, third edition, Volume 2 (2008).

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 and to authenticate data relating to the eMRTD itself and verification of 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 on a high-capacity contactless integrated circuit (IC), the IC also being encoded with a duplicate of the MRZ data. The specifications also permit the storage of a range of optional data at the discretion of the issuing State. Since the use of the contactless integrated circuit is independent of the size of the document, all specifications apply to all eMRTD sizes in their electronically enabled form. Differences between eMRTD formats relate to the MRZ, with consequences for the storage of the MRZ in the contactless IC. These differences are indicated in the specifications of the Logical Data Structure in Doc 9303-10.

2 EMRTD

Note: The terms MRTD and eMRTD are used in this document as a generic reference to all types of Machine Readable Travel Documents in, respectively, optical character reading and electronically enabled forms. The terms TD1, TD2 and TD3 refer to the different form factors of MRTDs. All eMRTDs referred to in this volume are electronically enabled.

2.1 Conformance to Doc 9303.

An electronic MRTD (eMRTD) SHALL conform in all respects to the specifications provided in Doc 9303.

2.2 Validity Period for an eMRTD.

The validity period of an eMRTD is at the discretion of the issuing State; however, in consideration of the limited durability of documents and the changing appearance of the document holder over time, a validity period of not more than ten years is RECOMMENDED. States MAY wish to consider a shorter period to enable the progressive upgrading of the eMRTD as the technology evolves.

2.3 Chip Inside Symbol

Doc 9303-9 focuses on biometrics in relation to Machine Readable Travel Documents, using the term "eMRTD" to denote such biometrically-enabled and globally-interoperable MRTD. Any MRTD that does not comply with the specifications given in Doc 9303 may not be called an eMRTD and shall not display the Chip Inside symbol.

All eMRTDs shall carry the following symbol:



Figure 1 : Chip inside symbol

An electronic file of the symbol is available from the ICAO web site. The symbol SHALL only appear on an eMRTD that contains a contactless integrated circuit, with a data storage capacity of at least 32 kB, that is encoded in accordance with the Logical Data Structure (Doc 9303-10) with, as a minimum, the MRZ data in Data Group 1 and a facial image as specified in this part in Data Group 2, with all entered data secured with a digital signature as specified in Doc 9303-11. Unless an eMRTD conforms to these minimum requirements, it SHALL NOT be described as an eMRTD nor display the Chip inside symbol. The symbol shall appear on the front cover of the eMRTD if it is a TD3 size book (eMRP) either near the top or the bottom of the cover, or on the front side of the eMRTD if it is in the format of a card (eMROTD).

On a eMRP the symbol shall be included in the foil blocking or other image on the front cover. It is recommended that the symbol also be printed on the data page in a suitable colour and in a location which does not interfere with the reading of other data. The issuing State may also print the symbol on the inside page or cover of the passport book that contains the contactless IC and, at the State's discretion, elsewhere in the passport.

On an eMROTD the symbol SHALL appear on the front of the eMROTD preferably in Zone 1.

The image, as shown above, is a positive, i.e. the black part of the image shall be printed or otherwise imaged. It is RECOMMENDED that the symbol appears eye-visible and be easily recognizable.

Figure 2 shows the RECOMMENDED dimensions of the symbol as it is to appear on an eMRP cover or data page, or on an electronic TD2. The following are the corresponding dimensions in inches: 9.0 mm (0.35 in), 5.25 mm (0.21 in), 3.75 mm (0.15 in), 2.25 mm (0.09 in), 0.75 mm (0.03 in).

A smaller size of 4.2 × 7.2 mm (0.17 × 0.28 in), scaled in proportion, is RECOMMENDED for use on an electronic TD1.

The symbol MAY be scaled in proportion for use in, for example, background designs.

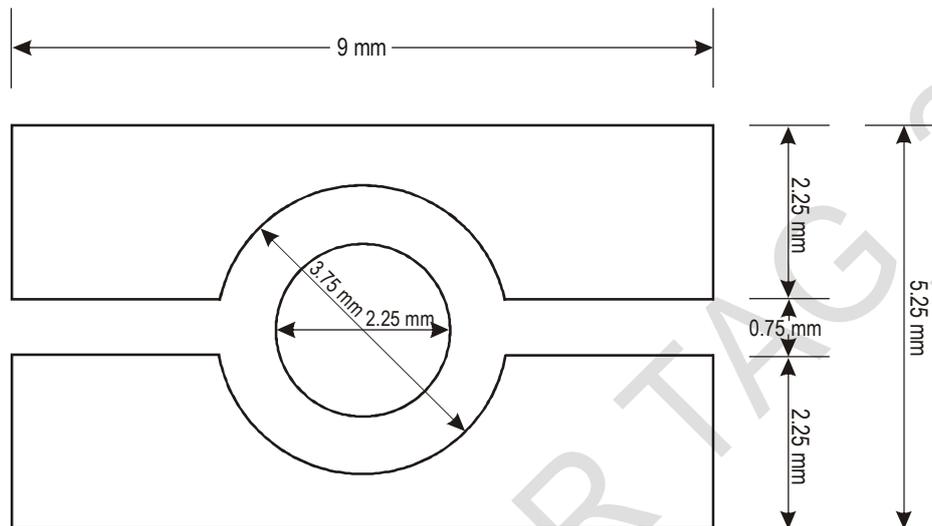


Figure 2 : Dimensions of the symbol

2.4 Warning regarding Care in Handling an eMRP.

It is suggested that a warning urging the holder of an eMRP to take care of the document be placed in an obvious location on the book. A suggested wording is:

“This passport contains sensitive electronics. For best performance please do not bend, perforate or expose to extreme temperatures or excess moisture”.

In addition, the issuing State may mark the part of the page containing the IC and the corresponding parts of some adjacent pages with the caveat:

“Do not stamp here”.

3 BIOMETRIC IDENTIFICATION

“Biometric identification” is a generic term used to describe automated means of recognizing a living person through the measurement of distinguishing physiological or behavioural traits.

A “biometric template” is a machine-encoded representation of the trait created by a computer software algorithm and enables comparisons (matches) to be performed to score the degree of confidence that separately recorded traits identify (or do not identify) the same person. Typically, a biometric template is of relatively small data size; however, each manufacturer of a biometric system uses a unique template format, and templates are not interchangeable between systems. To enable a State to select a biometric system that suits its requirements, the data have to be stored in a form from which the State’s system can derive a template. This requires that the biometric data be stored in the form of one or more images.

3.1 ICAO Vision on Biometrics

The ICAO vision for the application of biometrics technology encompasses:

- Specification of a primary interoperable form of biometrics technology for use at border control (verification, watch lists) as well as by carriers and document issuers, and specification of agreed supplementary biometric technologies;
- Specification of the biometrics technologies for use by document issuers (identification, verification and watch lists);
- Capability of data retrieval for 10 years, the maximum recommended validity for a travel document;;
- Having no proprietary element thus ensuring that any States investing in biometrics are protected against changing infrastructure or changing suppliers.

Doc 9303 considers only three types of biometric identification systems. With respect to the storage of these three biometric features in the contactless IC of an eMRTD the issuing State or organization SHALL conform to the relevant international standard.

The types of biometrics are:

- facial recognition – MANDATORY. MUST comply to [ISO/IEC 19794-5];
- fingerprint recognition – OPTIONAL. If used MUST comply to [ISO/IEC 19794-4];
- iris recognition – OPTIONAL. If used MUST comply to [ISO/IEC 19794-6].

Biometrics terms.

The following terms are used in biometric identification:

- “verify” means to perform a one-to-one match between proffered biometric data obtained from the eMRTD holder now and a biometric template created when the holder enrolled in the system;
- “identify” means to perform a one-to-many search between proffered biometric data and a collection of templates representing all of the subjects who have enrolled in the system.

Biometrics can be used in the identification function to improve the quality of the background checking performed as part of the passport, visa or other travel document application process, and they can be used to establish a positive match between the travel document and the person who presents it.

3.2 Key Considerations

In specifying biometric applications for eMRTDs, key considerations are:

- *Global Interoperability* — the crucial need to specify a system for deployment to be used in a universally interoperable manner;
- *Uniformity* — the need to minimize via specific standard setting, to the extent practical, the different solution variations that may potentially be deployed by member States;
- *Technical Reliability* — the need to provide guidelines and parameters to ensure member States deploy technologies that have been proven to provide a high level of confidence from an identity confirmation viewpoint; and that States reading data encoded by other States can be sure that the data supplied to them are of sufficient quality and integrity to enable accurate verification in their own system;
- *Practicality* — the need to ensure that recommended standards can be made operational and implemented by States without their having to introduce a plethora of disparate systems and equipment to ensure they meet all possible variations and interpretations of the standards;
- *Durability* — the requirement that the systems introduced will last the recommended maximum 10 year life of a travel document, and that future updates will be backward compatible.

3.3 Key Processes with respect to Biometrics

The major components of a biometric system are:

- *Establish identity* — ensuring that the identity of the enrollee is known without doubt
- *Capture* — acquisition of a raw biometric sample
- *Extract* — conversion of the raw biometric sample data to an intermediate form
- *Create template* — conversion of the intermediate data into a template
- *Compare* — comparison with the information in a stored reference template.

These processes involve:

- The *enrollment* process is the *capture* of a raw biometric sample. It is used for each new person (potential eMRTD holder) taking biometric image samples for storage. This capture process is the automatic acquisition of the biometric via a capture device such as a fingerprint scanner, photograph scanner, live-capture digital image camera, or live-capture iris zooming camera. Each capture device will need certain criteria and procedures defined for the capture process — for example, standard pose facing the camera straight-on for a facial recognition capture; whether fingerprints are captured flat or rolled; eyes fully open for iris capture. The resulting image is compressed and then stored for future confirmation of identity.
- The *template creation* process preserves the distinct and repeatable biometric features from the captured biometric image and generally uses a proprietary software algorithm to extract a template from the stored image. This defines that image in a way that it can subsequently be compared with another sample image captured at the time identity confirmation is required and a comparative score determined. Inherent in this algorithm is quality control, wherein through some mechanism, the sample is rated for quality. Quality standards need to be as high as possible since all future checks are dependent on the quality of the originally captured image. If the quality is not acceptable, the *capture* process should be repeated.
- The *identification* process takes the template derived from the new sample and compares it to templates of enrolled end users to determine whether the end user has enrolled in the system before, and if so, whether in the same identity.
- The *verification* process takes the new sample of an eMRTD holder and compares it to a template derived from the stored image of that holder to determine whether the holder is

presenting in the same identity.

3.4 Applications for a Biometric Solution

The key application of a biometrics solution is the identity verification of relating an eMRTD holder to the eMRTD he is carrying.

There are several typical applications for biometrics during the enrolment process of applying for an eMRTD.

The end user's biometric data generated by the enrolment process can be used in a search of one or more biometric databases (identification) to determine whether the end user is known to any of the corresponding systems (for example, holding an eMRTD under a different identity, having a criminal record, holding an eMRTD from another State).

When the end user collects the eMRTD (or presents himself for any step in the issuance process after the initial application is made and the biometric data are captured) his biometric data can be taken again and verified against the initially captured biometric data.

The identities of the staff undertaking the enrolment can be verified to confirm they have the authority to perform their assigned tasks. This may include biometric authentication to initiate digital signature of audit logs of various steps in the issuance process, allowing biometrics to link the staff members to those actions for which they are responsible.

There are also several typical applications for biometrics at the border.

Each time a traveller (i.e. eMRTD holder) enters or exits a State, his identity can be verified against the image created at the time his travel document was issued. This will ensure that the holder of a document is the legitimate person to whom it was issued and will enhance the effectiveness of any Advance Passenger Information (API) system. A State may find it desirable to store the biometric template or templates on the travel document along with the image, so that a traveller's identity can be verified in domestic locations where the biometric system is under the issuer's control.

Two-way check — The traveller's current captured biometric image data, and the biometric data from his travel document (or from a central database), can be matched (if applicable by constructing biometric templates of each) to confirm that the travel document has not been altered.

Three-way check — The traveller's current captured biometric image data, the biometric data from his travel document, and the biometric data stored in a central database can be matched (if applicable by constructing biometric templates of each) to confirm that the travel document has not been altered. This technique matches the person and his eMRTD with the database recording the data that were put in that eMRTD at the time it was issued.

Four-way check — A fourth confirmatory check, albeit not an electronic one, is visually matching the results of the three-way check with the digitized photograph on the data page of the traveller's eMRTD.

Besides the enrolment and border security applications of biometrics as manifested in one-to-one and one-to-many matching, States should also have regard to, and set their own criteria in regard to:

- Accuracy of the biometric matching functions of the system. Issuing States must encode the facia image, and optionally one or more fingerprint or iris biometrics on the eMRTD as per LDS specifications. (The biometric may also be stored on a database accessible to the receiving State.) Given an ICAO-standardized biometric image, receiving States must select their own biometric verification software and determine their own biometric scoring thresholds for identity verification acceptance rates and referral of impostors.

-
- Throughput (e.g. travellers per minute) of either the biometric system or the border-crossing system as a whole.
 - Suitability of a particular biometric technology (face or finger or eye) to the border-crossing application.

3.5 Constraints on Biometric Solutions

It is recognized that implementation of most biometrics technologies are subject to further development. Given the rapidity of technological change, any specifications (including those herein) must allow for, and recognize there will be, changes resulting from technology improvements.

The biometrics information stored on travel documents shall comply with any national data protection laws or privacy laws of the issuing State.

DRAFT_4 FOR TAG_22

4 THE SELECTION OF BIOMETRICS APPLICABLE TO EMRTDS

It has long been recognized that name and reputation are not sufficient traits to guarantee that the holder assigned a travel document (eMRTD) by the issuing State is the person at a receiving State purporting to be that same holder.

The only method of relating the person irrevocably to his travel document is to have a physiological characteristic, i.e. a biometric, of that person associated with his travel document in a tamper-proof manner.

4.1 Primary Biometric: Facial Image

After a five-year investigation into the operational needs for a biometric identifier which combines suitability for use in the eMRTD issuance procedure and in the various processes in cross-border travel consistent with the privacy laws of various States, ICAO specified that facial recognition become the globally interoperable biometric technology. A State may also optionally elect to use fingerprint and/or iris recognition in support of facial recognition.

In reaching this conclusion, ICAO observed that for the majority of States the following advantages applied to facial images:

- Facial photographs do not disclose information that the person does not routinely disclose to the general public.
- The photograph (facial image) is already socially and culturally accepted internationally.
- The facial image is already collected and verified routinely as part of the eMRTD application form process in order to produce an eMRTD to Doc 9303 specifications.
- The public is already aware of the capture of a facial image and its use for identity verification purposes.
- The capture of a facial image is non-intrusive. The end user does not have to touch or interact with a physical device for a substantial timeframe to be enrolled.
- Facial image capture does not require new and costly enrollment procedures to be introduced.
- Capture of a facial image can be deployed relatively immediately, and the opportunity to capture facial images retrospectively is also available.
- Many States have a legacy database of facial images, captured as part of the digitized production of travel document photographs, which can be verified against new images for identity comparison purposes.
- In appropriate circumstances, as decided by the issuing State, a facial image can be captured from an endorsed photograph, not requiring the person to be physically present.
- For watch lists, a photograph of the face is generally the only biometric available for comparison.
- Human verification of the biometric against the photograph/person is relatively simple and a familiar process for border control authorities.

Storage of the facial biometric. Facial recognition vendors all use proprietary algorithms to generate their biometric templates. These algorithms are kept secret by the vendors as their intellectual property and cannot be reverse-engineered to create a recognizable facial image. Therefore facial recognition templates are not interoperable between vendors — the only way to achieve interoperability with facial images is for the “original” captured photograph to be passed to the

receiving State. The receiving State then uses its own vendor algorithm (which may or may not be the same vendor/version as the issuing State used) to compare a facial image captured in real time of the eMRTD holder with the facial image read from the data storage technology in their eMRTD.

Image storage, compression and cropping

In the LDS structure, the variable size data item that has the most impact on LDS size is the displayed image. It is then necessary to define a level by which the image can be compressed by the issuing State without degrading the results of biometric comparison by the receiving State.

Biometric systems reduce the raw acquired image (face/fingerprint/iris) to a feature space that is used for matching. It follows that as long as compression does not compromise this feature space, it can be undertaken to reduce the storage requirements of the images retained.

Facial image data size.

An ICAO-standardized size portrait colour-scanned at 300 dpi results in a facial image with approximately 90 pixels between the eyes and a size of approximately 640 kB at 24 bits per pixel. Such an image can be compressed significantly using JPEG or JPEG 2000 techniques without significant loss of perceived image quality.

Studies undertaken using standard photograph images but with different vendor algorithms and JPEG and/or JPEG2000 compression showed the *minimum* practical image size for an ICAO-standardized eMRTD photo image to be approximately 12 kB of data. The studies showed higher compression beyond this size results in significantly less reliable facial recognition results. Twelve kilobytes cannot always be achieved as some images compress more than others at the same compression ratio — depending on factors such as clothes, colouring and hair style. In practice, facial image average compressed sizes in the 15 kB – 20 kB range should be the optimum for use in eMRTDs.

Cropping.

Whilst images can be cropped to save storage and show just the eye/nose/mouth features, the ability for a human to easily verify that image as being of the same person who is in front of them, or appearing in the photograph on the eMRTD, is diminished significantly. For example, in Figure 3 the image to the left provides a greater challenge in recognition than that on the right.



Figure 3 : Cropping

It is therefore RECOMMENDED that images stored in the LDS are to be either:

- not cropped, i.e. identical to the portrait printed on the eMRTD;
- cropped from chin to crown and edge-to-edge as a minimum, as shown in Figure 4.



Figure 4 : Cropping

To assist in the facial recognition process, the facial image SHALL be stored either as a full frontal image or as a token image in accordance with the specifications established in ISO/IEC 19794-5, Information technology — Biometric data interchange formats — Part 5: Facial image data. A token image is a facial image in which the image is rotated if necessary to ensure that an imaginary horizontal line drawn between the centres of the eyes is parallel to the top edge of the picture and the size adjusted. It is RECOMMENDED that the centres of the eyes be approximately 90 pixels apart as in Figure 5.

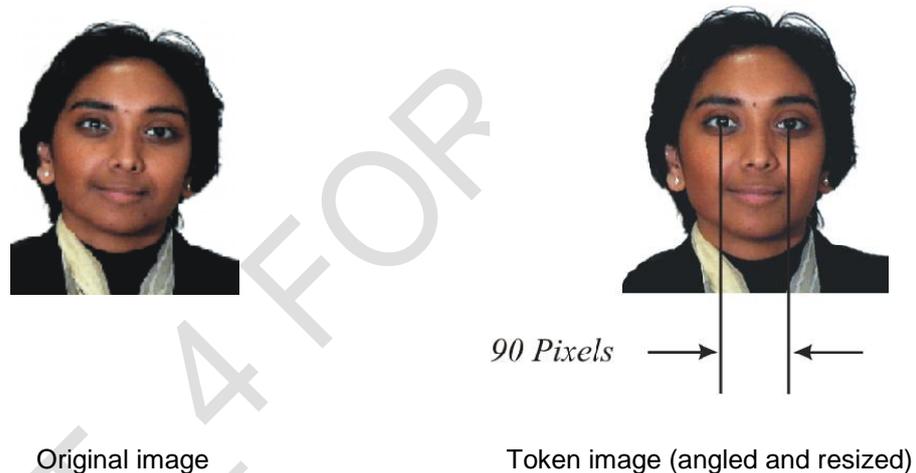


Figure 5 : Eye distance

The Logical Data Structure (see Doc 9303-10) can accommodate the storage of the eye coordinates.

Facial ornaments. The issuing State shall decide to what extent it permits facial ornaments to appear in stored (and displayed) portraits. In general, if such ornaments are permanently worn, they should appear in the stored image.

Optional fingerprint image size. When a State elects to store fingerprint image(s) on the contactless IC, the optimal image size SHOULD be approximately 10 kB of data per finger (e.g. when compressed with the typical WSQ compression technique).

Optional iris image size. When a State elects to store iris image(s) on the contactless IC, the optimal image size SHOULD be approximately 30 kB of data per eye.

4.2 Optional Additional Biometrics

States optionally can provide additional data input to their (and other States') identity verification processes by including multiple biometrics in their travel documents, i.e. a combination of face and/or fingerprint and/or iris. This is especially relevant where States may have existing fingerprint or iris

databases in place against which they can verify the biometrics proffered to them, for example, as part of an ID card system.

Storage of an optional fingerprint biometric.

There are three classes of fingerprint biometric technology: finger image-based systems, finger minutiae-based systems, and finger pattern-based systems. Whilst standards have been developed within these classes to make most systems interoperable amongst their class, they are not interoperable between classes. Three standards for fingerprint interoperability are therefore emerging: storage of the image data, storage of the minutiae data and storage of the pattern data. Where an issuing State elects to provide fingerprint data in its eMRTD, the storage of the fingerprint image is mandatory to permit global interoperability between the classes. The storage of an associated template is optional at the discretion of the issuing State.

Storage of an optional iris biometric.

Where an issuing State elects to provide iris data in its eMRTD, the storage of the iris image is mandatory to permit global interoperability. The storage of an associated template is optional at the discretion of the issuing State.

DRAFT - 4 FOR TAG - 22

5 STORAGE OF THE BIOMETRIC AND OTHER DATA IN A LOGICAL FORMAT IN A CONTACTLESS IC

It is REQUIRED that digital images be used and that these be electronically stored in the travel document.

5.1 Characteristics of the Contactless IC

A high-capacity contactless IC SHALL be the electronic storage medium specified by ICAO as the capacity expansion technology for use with eMRTDs in the deployment of biometrics.

Contactless IC and encoding. The contactless ICs used in eMRTDs SHALL conform to ISO/IEC14443 Type A or Type B and [ISO/IEC 7816-4]. The LDS SHALL be encoded according to the Random Access method. The read range (achieved by a combination of the eMRTD and the reader) should be up to 10 cm as noted in [ISO/IEC 14443].

Data storage capacity of the contactless IC.

The data storage capacity of the contactless IC is at the discretion of the issuing State but SHALL be a minimum of 32 kB. This minimum capacity is necessary to store the mandatory stored facial image (typically 15 — 20 kB), the duplicate MRZ data and the necessary elements for securing the data. The storage of additional facial, fingerprint and/or iris images may require a significant increase in data storage capacity. There is no maximum contactless IC data capacity specified.

Storage of other data.

A State MAY use the storage capacity of the contactless IC in an eMRTD to expand the machine readable data capacity of the eMRTD beyond that defined for global interchange. This can be for such purposes as providing machine readable access to breeder document information (e.g. birth certificate details), stored personal identity confirmation (biometrics) and/or document authenticity verification details.

5.2 Logical Data Structure

To ensure global interoperability for machine reading of stored details, a Logical Data Structure (LDS) defining the format for the recording of details in the contactless IC MUST be adhered to.

Structure of the stored data.

The Logical Data Structure is specified in Doc 9303-10. Doc 9303-10 describes in detail the mandatory and optional information to be included within specific biometric data blocks within the LDS.

Minimum data items to be stored in the LDS.

The minimum mandatory items of data to be stored in the LDS on the contactless IC SHALL be a duplication of the Machine Readable Zone data in Data Group 1 and the holder's facial image in Data Group 2. In addition, the IC in a compliant eMRTD SHALL contain the Security Object (EF.SOD) that is needed to validate the integrity of data created by the issuer — this is stored in Dedicated File No 1 as specified in the LDS (See Doc 9303-10). The Security Object (EF.SOD) consists of the hashes of the Data Groups in use.

5.3 Security and Privacy of the Stored Data

Both the issuing and any receiving States need to be satisfied that the data stored on the contactless IC have not been altered since they were recorded at the time of issue of the document. In addition, the privacy laws or practice of the issuing State may require that the data cannot be accessed except by an authorized person or organization. Accordingly ICAO has developed specifications in Doc 9303-11 and Doc 9303-12 regarding the application and usage of modern encryption techniques, particularly Public Key Infrastructure (PKI) schemes, which MUST be used by States in their Machine Readable Travel Documents made in accordance with Doc 9303. The intent is primarily to augment security through automated means of authentication of eMRTDs and their legitimate holders internationally. In addition, methods are recommended to implement international eMRTD authentication and to provide a path to the use of eMRTDs to facilitate biometric or e-commerce

applications. The specifications in Doc 9303-11 permit the issuing State to protect the stored data from unauthorized access by the use of Access Control.

This edition of Doc 9303 is based on the assumption that eMRTDs will not be written to after personalization. Therefore the personalization process SHOULD lock the contactless IC as a final step. Once the contactless IC has been locked (after personalization and before issuance) no further data can be written, modified, or deleted to/at/from the contactless IC. After issuance a locked contactless IC cannot be unlocked.

PKI.

The aim of the PKI scheme, as described, is mainly to enable eMRTD inspecting authorities (receiving States) to verify the authenticity and integrity of the data stored in the eMRTD. The specifications do not try to prescribe a full implementation of a complicated PKI structure, but rather are intended to provide a way of implementation in which States are able to make choices in several areas (such as active authentication, anti-skimming and access control, automated border crossing, etc.), thus having the possibility to phase in implementation of additional features without being non-compliant to the total framework.

Certificates are used for security purposes, along with a methodology for public key (certificate) circulation to member States, and the PKI is customized for ICAO purposes.

The PKI specifications are described in detail in Doc 9303-12.

6 TEST METHODOLOGIES FOR (E)MRTDS

ICAO, in corporation with ISO, has developed test methodologies for qualifying MRTDs with respect to their conformance to the specifications set out in Doc 9303. These test methodologies are specified in ICAO Technical Reports, which after endorsement by the Technical Advisory Group for Machine Readable Travel Documents (TAG-MRTD) are converted into international ISO/IEC standards, and as such being maintained in the ISO community under the coordination of ISO/IEC JTC1 SC17 WG3.

Issuing States and Organization are RECOMMENDED to qualify their MRTDs according to the test specifications listed hereunder:

- [ISO/IEC 18745-1] Physical tests for MRPs
- [ISO/IEC 10373-6] General tests for the contactless interface
- [ISO/IEC 10373-6 AMD 7]
(to be converted into [ISO/IEC 18745-2]) Specific tests on the contactless interface for eMRTDs
- [ICAO TR RF & PROTOCOL P3]
(to be converted into ISO/IEC 18745-3) LDS and Protocol testing
- [ICAO TR RF & PROTOCOL P4]
(to be converted into ISO/IEC 18745-4) Tests for inspection systems

APPENDIX A PLACEMENT OF THE CONTACTLESS IC IN AN EMRP (INFORMATIVE)

A.1 Location of the IC and its Associated Antenna

The location of the contactless IC with its associated antenna in the MRP is at the discretion of the issuing State. States should be aware of the importance of the need for the contactless IC to be protected against physical tampering and casual damage including flexing and bending.

Optional locations for the contactless IC and its antenna. The following locations have been identified:

Data page — placing the IC and antenna within the structure of a data page forming an internal page of the book.

Centre of booklet — placing the IC and its antenna between the centre pages of the book.

Cover — placement within the structure or construction of the cover.

Separate sewn-in page — incorporating the IC and its antenna into a separate page, which may be in the form of an ID3 size plastic card, sewn into the book during its manufacture.

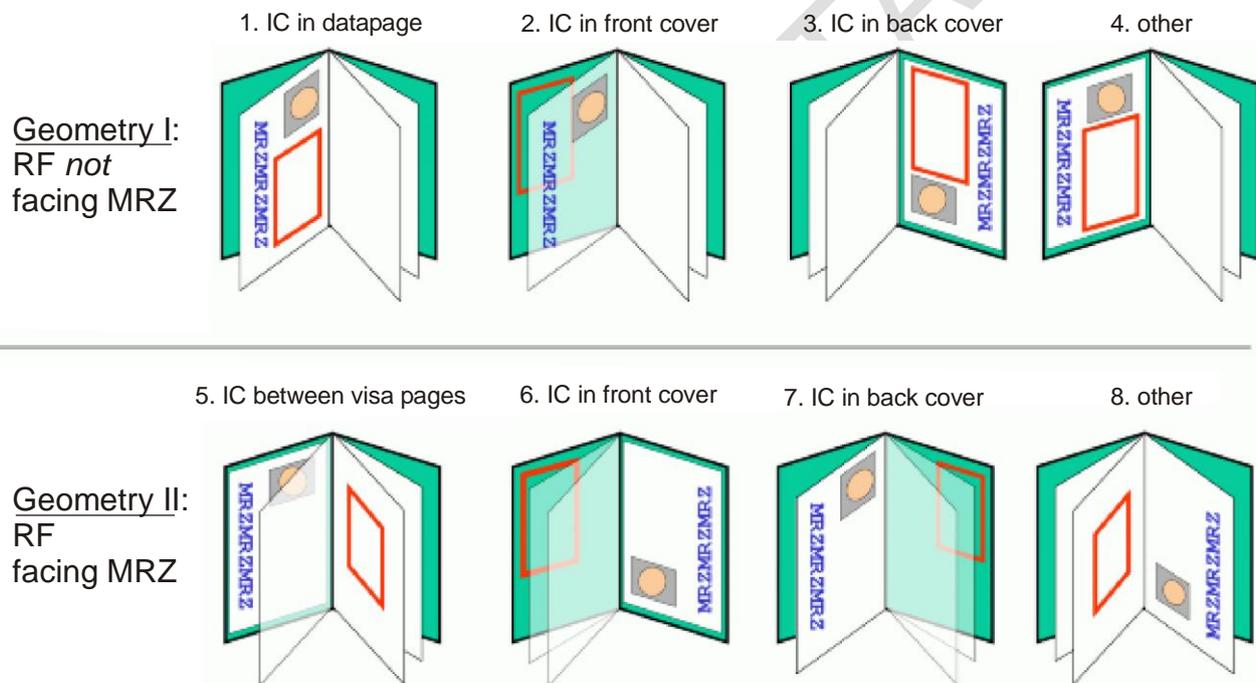


Figure 6 : Options for locations of the IC

Note: In these illustrations the IC and its antenna are shown as an outlined rectangle. The data page is shown with MRZMRZMRZ representing the MRZ and with a circle inside a rectangle indicating the portrait.

A.2 Precautions in eMRTD manufacture

States need to ensure the manufacturing process and the personalization process do not introduce unexpected damage to the IC or to its antenna. For example, excessive heat in lamination or image perforation in the area of the IC or its antenna may damage the IC assembly. Similarly, when the IC is in the front cover, foil blocking on the outside of the cover, after it is assembled, can also damage the IC or the connections to its antenna.

A.3 Reading both the OCR and the data on the IC

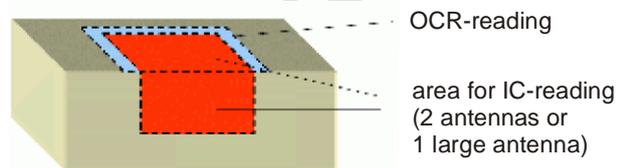
It is strongly recommended that a receiving State read both the OCR data and the data stored on the IC. Where a State has locked the IC against eavesdropping, the reading of the OCR is required in order to access the IC data. It is desirable that only one reader be used for both operations, the reader being equipped to read both. If the MRP is opened at the data page and placed on a whole page reader, some MRPs will have the IC situated behind the face of the data page, while others will have the IC in the part of the book that is not in the whole page reader.

A.4 Reader construction

States shall therefore install reading equipment capable of handling MRPs of both geometries, preferably capable of reading both OCR and the IC. Figure 7 shows possible reader configurations, each capable of reading the OCR and the IC. The book is half opened and two antennae ensure that the IC is read irrespective of whether it faces the MRZ or not. Also shown is a less satisfactory configuration in which the eMRTD is placed on an OCR reader or swiped through an OCR reader to read the MRZ and then on a reader for the IC data. This arrangement will be less convenient for immigration staff.

Concurrent reading process

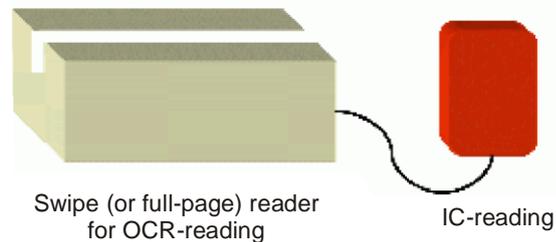
Full-page reader with 2 antennas perpendicularly orientated, or one large antenna covering the area of an opened book



or

2-step reading process

OCR-swipe or full-page reader, connected to separate RF-reader



1. Step: Swipe MRTD through/put on OCR-reader
2. Step: If chip exists, put MRTD on IC-Reader

Figure 7 : Reading process

Reading geometries. Reader manufacturers therefore need to consider how to design machine reading solutions that account for the various orientation possibilities and (ideally) are capable of reading the MRZ and the contactless IC simultaneously.

REFERENCES (NORMATIVE)

- [ICAO TR RF & PROTOCOL P3] RF protocol and application test standard for eMRTD - part 3: Tests for Application protocol and Logical Data Structure¹
- [ICAO TR RF & PROTOCOL P4] RF protocol and application test standard for eMRTD - part 4: Conformity tests for inspection systems²
- [ISO/IEC 7816-4] ISO/IEC 7816-4:2013, Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange
- [ISO/IEC 10373-6] **Error! Reference source not found.**
- [ISO/IEC 10373-6 AMD 7] **Error! Reference source not found.** – Amendment 7: Test methods for ePassport³
- [ISO/IEC 14443-1] ISO/IEC 14443-1:2008, Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 1: Physical Characteristics
- [ISO/IEC 14443-2] ISO/IEC 14443-2:2010, Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 2: Radio Frequency Power and Signal Interface
- [ISO/IEC 14443-3] ISO/IEC 14443-3:2011, Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and Anticollision
- [ISO/IEC 14443-4] ISO/IEC 14443-4:2008, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol
- [ISO/IEC 18745-1] ISO/IEC 18745-1:2014, **Error! Reference source not found.**
- [ISO/IEC 19794-4] ISO/IEC 19794-4:2005, Information technology - Biometric data interchange formats - Part 4: Finger image data
- [ISO/IEC 19794-5] ISO/IEC 19794-5:2005, Information technology - Biometric data interchange formats - Part 5: Face image data
- [ISO/IEC 19794-6] ISO/IEC 19794-6:2005, Information technology - Biometric data interchange formats - Part 5: Iris image data

1 to be converted into [ISO/IEC 18745-3]

2 to be converted into [ISO/IEC 18745-4]

3 to be converted into [ISO/IEC 18745-2]

Doc 9303



Machine Readable Travel Documents

Part 10

Logical Data Structure (LDS) for storage of biometrics and other data in the contactless IC

Approved by the Secretary General
and published under his authority

Seventh Edition - Revision 1 - 2014

International Civil Aviation Organization

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

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

Doc 9303, Machine Readable Travel Documents
Order Number: xxxx
ISBN xxx-xx-xxxx-xxx-x

© ICAO 2014

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 TO DOC 9303-10, 7TH EDITION

Revision	Date	Description
01	xx-xx-2014	Initial release of the 7 th edition

DRAFT_4 FOR TAG_22

TABLE OF CONTENTS

1	SCOPE	2
2	REQUIREMENTS OF THE LOGICAL DATA STRUCTURE	3
2.1	Security	3
2.2	Authenticity and Integrity of Data	3
2.3	Ordering of LDS	3
3	APPLICATION PROFILE FOR THE CONTACTLESS IC	5
3.1	Minimum Requirements for Interoperability.	5
3.2	Electrical Characteristics.....	5
3.3	Physical Characteristics.....	5
3.4	Data Storage Capacity of the Contactless IC	5
3.5	Storage of Other Data	5
3.6	Minimum Data Items To Be Stored In The LDS	5
3.7	Initialization, Anticollision, and Transmission Protocol According to ISO/IEC 14443	6
3.8	Command Set	6
3.9	Command Formats and Parameter Options	6
4	FILE STRUCTURE SPECIFICATIONS	9
4.1	Application Selection - DF	10
4.2	Data Groups	10
4.3	Data Elements Encoding Rules	10
4.4	Normative Tags Used in LDS Context	11
4.5	LDS Versioning	14
5	ELEMENTARY FILES	15
5.1	Header and Data Group Presence Information EF.COM (REQUIRED).....	15
5.2	Document Security Object EF.SO _D (REQUIRED)	15
5.3	EF.CardAccess (CONDITIONAL)	20
6	DATA ELEMENTS FORMING DATA GROUPS 1 THROUGH 16	21
6.1	DATA GROUP 1 - Machine Readable Zone Information (REQUIRED)	22
6.2	DATA GROUP 2 - Encoded Identification Features – Face (REQUIRED).....	24
6.3	DATA GROUP 3 - Additional Identification Feature - Finger(s) (OPTIONAL)	26
6.4	DATA GROUP 4 - Additional Identification Feature –Iris(es) (OPTIONAL).....	30
6.5	DATA GROUP 5 - Displayed Portrait (OPTIONAL)	32
6.6	DATA GROUP 6 - Reserved for Future Use	33
6.7	DATA GROUP 7 - Displayed Signature or Usual Mark (OPTIONAL)	33
6.8	DATA GROUP 8 - Data Feature(s) (OPTIONAL)	34
6.9	DATA GROUP 9 - Structure Feature(s) (OPTIONAL)	35
6.10	DATA GROUP 10 - Substance Feature(s) (OPTIONAL)	36
6.11	DATA GROUP 11 - Additional Personal Detail(s) (OPTIONAL)	36
6.12	DATA GROUP 12 - Additional Document Detail(s) (OPTIONAL).....	39
6.13	DATA GROUP 13 - Optional Details(s) (OPTIONAL)	40
6.14	DATA GROUP 14 - Security Options (CONDITIONAL)	40
6.15	DATA GROUP 15 - Active Authentication Public Key Info (CONDITIONAL)	41
6.16	DATA GROUP 16 - Person(s) to Notify (OPTIONAL).....	41
APPENDIX A	LOGICAL DATA STRUCTURE MAPPING EXAMPLES (INFORMATIVE)	43
A.1	EF.COM Common Data Elements.....	43
A.2	EF.DG1 Machine Readable Zone Information.....	43
A.3	EF.DG2 to EF.DG2 Biometric Templates	44
A.4	EF.DG5 to EF.DG7 Displayed Image Templates	44
A.5	EF.DG11 Additional Personal Details	44
A.6	EF.DG12 Additional Document Details.....	44
A.7	EF.DG16 Person(s) To Notify	45
REFERENCES (NORMATIVE)	46

1 SCOPE

The seventh edition of Doc 9303 represents a restructuring of the ICAO specifications for Machine Readable Travel Documents. Without incorporating substantial modifications of the specifications, in this new edition Doc 9303 has been reformatted into a set of specifications for Size 1 Machine Readable Official Travel Document (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 10 of Doc 9303 defines the Logical Data Structure (LDS) for eMRTDs required for global interoperability, and defines the specifications for the organization of data on the contactless IC. This requires the identification of all mandatory and optional Data Elements and a prescriptive ordering and/or grouping of Data Elements that MUST be followed to achieve global interoperability for electronic reading of the eMRTD.

Doc 9303-10 provides specifications to enable States and integrators to implement a contactless IC into an eMRTD travel document. This part defines all mandatory and optional data elements, file structures, and application profiles for the contactless IC.

Part 10 should be read in conjunction with:

- Part 1 – Introduction;
- Part 3 - Specifications Common to all Machine Readable Travel Documents;
- Part 4 - Specifications Specific to TD3 Size Machine Readable Passports (MRP);
- Part 5 - Specifications Specific to TD1 Size MRTDs, Machine Readable Official Travel Documents;
- Part 6 - Specifications Specific to TD2 Size MRTDs, Machine Readable Official Travel Documents.

and the relevant contactless IC parts:

- Part 11 – Security Mechanisms for Machine Readable Travel Documents;
- Part 12 – Public Key Infrastructure for Machine Readable Travel Documents.

2 REQUIREMENTS OF THE LOGICAL DATA STRUCTURE

The contactless IC capacity expansion technology contained in an eMRTD selected by an Issuing State or organization must allow data to be accessible by receiving States.

ICAO has determined that the predefined, standardized Logical Data Structure (LDS) shall meet a number of mandatory requirements:

- ensure efficient and optimum facilitation of the rightful holder;
- ensure protection of details recorded in the optional capacity expansion technology;
- allow global interoperability of capacity expanded data based on the use of a single LDS common to all eMRTDs;
- address the diverse optional capacity expansion needs of Issuing States and organizations;
- provide expansion capacity as user needs and available technology evolve;
- support a variety of data protection options;
- utilize existing international specifications to the maximum extent possible in particular the emerging international specifications for globally interoperable biometrics.

2.1 Security

Data integrity and authenticity are needed for trusted global interoperability.

Data Groups 1 to 16 inclusive SHALL be write protected. A hash for each Data Group in use SHALL be stored in the Document Security Object (EF.SOD).

Only the Issuing State or Organization shall have write access to these Data Groups. Therefore, there are no interchange requirements and the methods to achieve write protection are not part of this specification.

2.2 Authenticity and Integrity of Data

To allow confirmation of the authenticity and integrity of recorded details, an authenticity/integrity object is included. Each Data Group MUST be represented in this authenticity/integrity object, which is recorded within a separate elementary file (EF.SOD). Using the CBEFF structure utilized for Encoded Identification Feature Data Groups 2-4 and optional "additional biometric security" features defined in Doc 9303-12, identity confirmation details (e.g. biometric templates) MAY also be individually protected at the discretion of the Issuing State or organization.

2.3 Ordering of LDS

Only the Random Ordering Scheme SHALL be used for international interoperability.

2.3.1 Random Ordering Scheme

The Random Ordering Scheme allows Data Groups and Data Elements to be recorded following a random ordering which is consistent with the ability of the optional capacity expansion technology to allow direct retrieval of specific Data Elements even if they are recorded out of order. Variable length Data Elements are encoded as TLV data object specified in ASN.1

2.3.2 Random Access File Representation

The random access file representation has been defined with the following considerations and assumptions.

- Support a wide variety of implementations. The LDS includes a wide variety of optional Data Elements. These Data Elements are included to facilitate eMRTD authentication, rightful holder authentication, and to expedite processing at document/person points.
- The data structure must support:
 - A limited or extensive set of Data Elements;
 - Multiple occurrences of specific Data Elements;
 - Continuing evolution of specific implementations.
- Support at least one application data set;
- Allow for other national specific applications;
- Support optional Active Authentication of the document using a stored asymmetrical key pair;

- Support rapid access of selected Data Elements to facilitate rapid document processing:
 - Immediate access to necessary Data Elements;
 - Direct access to data templates, and biometric data.

2.3.3 Grouping of Data Elements

Groupings of Data Elements added by Issuing States or approved receiving organizations may or may not be present in an LDS. More than one recording of grouped Data Elements added by receiving States or approved receiving organizations can be present in the LDS.

The ability for a receiving State or approved receiving organization to add data to the LDS is not supported in this edition of Doc 9303.

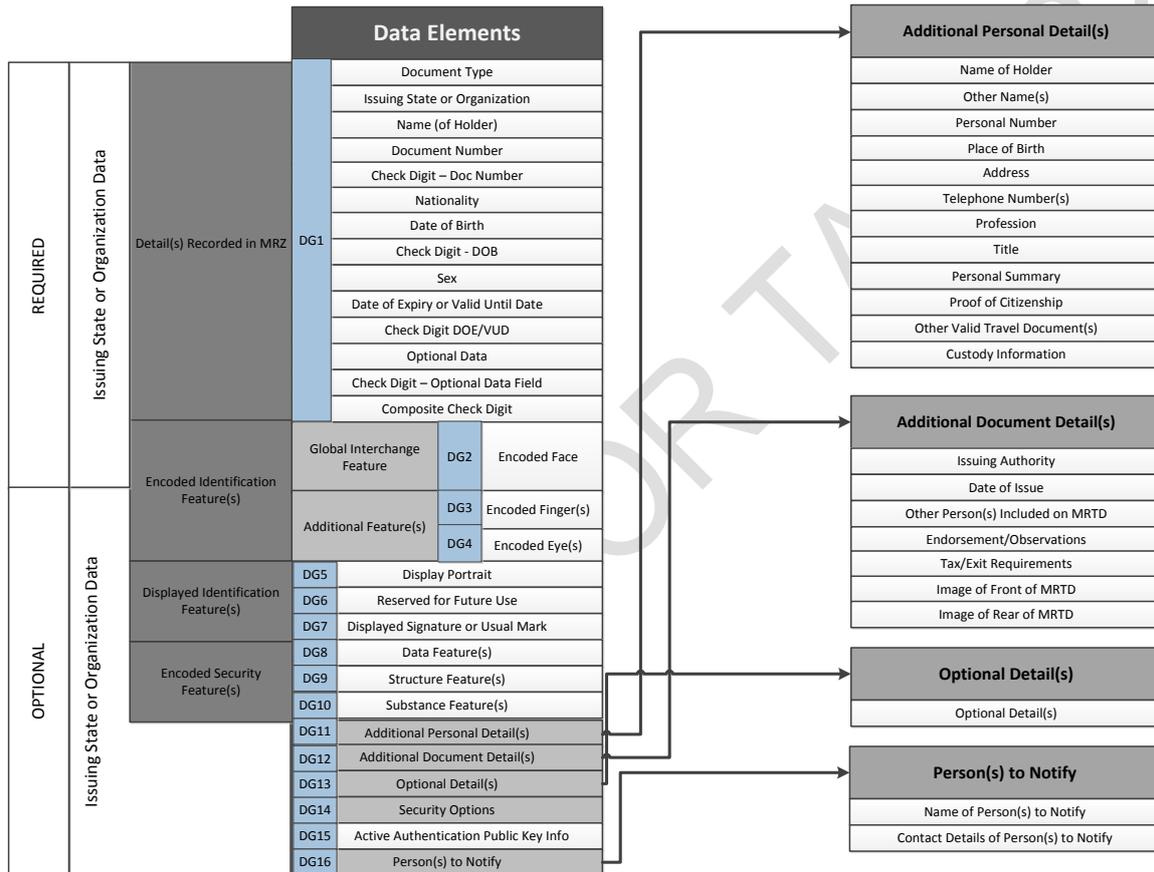


Figure 1: Data Group Reference Numbers Assigned to the LDS

The LDS is considered to be a single cohesive entity containing the number of groupings of Data Elements recorded in the optional capacity expansion technology at the time of machine reading.

The LDS has been designed with sufficient flexibility that it can be applied to all types of eMRTDs. Within the figures and tables which follow, some data items are only applicable to machine readable visas and to machine readable passports or require a different presentation in relation to these documents.

Within the LDS, logical groupings of related Data Elements have been established. These logical groupings are referred to as Data Groups.

Each Data Group is assigned a reference number. Figure 1 identifies the reference number assigned to each Data Group, for example, “DG2” identifies Data Group 2, Encoded Identification Feature(s) for the face of the holder of the eMRTD (i.e. facial biometric details).

3 APPLICATION PROFILE FOR THE CONTACTLESS IC

3.1 Minimum Requirements for Interoperability.

The following SHALL be the minimum requirements for interoperability of proximity contactless IC-based eMRTDs:

- [ISO/IEC 14443-1], [ISO/IEC 14443-2], [ISO/IEC 14443-3], [ISO/IEC 14443-4] including all associated amendments, and corrigendum;
- [ISO/IEC 10373-6] test specification compliant including all associated amendments and corrigendum;
- Type A or Type B signal interface;
- Support for a file structure as defined by [ISO/IEC 7816-4] for variable length transparent files;
- Support for one or more applications and appropriate [ISO/IEC 7816-4] commands as specified in Doc 9303
- Application Family Identifier (AFI) is 0xE1 (eMRTD). CRC_B of Application Identifier (AID: 0xA0000002471001) SHALL be 0xF35E. .

3.2 Electrical Characteristics

The radio frequency power and signal interface SHALL be as defined in [ISO/IEC14443-3]. A minimum of 424 kilo bits per second transmission speed is advised.

3.3 Physical Characteristics

It is recommended that the size of the coupling antenna area be in accordance with [ISO/IEC 14443-1] Class 1 (ID-1 antenna size) only.

3.4 Data Storage Capacity of the Contactless IC

The data storage capacity of the contactless IC is at the discretion of the Issuing State but SHALL be a minimum of 32 kB. This minimum capacity is necessary to store the mandatory stored facial image (typically 15 to 20 kB), the MRZ data, and the necessary elements for securing the data. The storage of additional facial, fingerprint, and/or iris images may require a significant increase in data storage capacity. There is no maximum contactless IC data capacity specified.

In the event that a State's PKI infrastructure is not available to sign eMRTD data as part of personalization, and the issuance of the document(s) cannot be delayed, it is RECOMMENDED that the eMRTD contactless IC be left blank and be locked. The eMRTD SHOULD contain an appropriate endorsement on this. This is expected to be an exceptional circumstance.

3.5 Storage of Other Data

A State MAY use the storage capacity of the contactless IC in an eMRTD to expand the machine readable data capacity of the eMRTD beyond that defined for global interoperability. This can be for such purposes as providing machine readable access to identity document information (e.g. birth certificate details), stored personal identity confirmation (biometrics) and/or document authenticity verification details.

3.6 Minimum Data Items To Be Stored In The LDS

The minimum mandatory items of data to be stored in the LDS on the contactless IC SHALL be a duplication of the machine readable zone data in Data Group 1 and the holder's facial image in Data Group 2. In addition, the IC in a compliant eMRTD SHALL contain the Document Security Object (EF.SOD) that is required to validate the integrity of data created by the issuer. These data items are stored in a Dedicated File (DF) known as the eMRTD Application, and specified in the LDS. The Document Security Object (EF.SOD) consists of the hashes of the Data Groups used.

3.7 Initialization, Anticollision, and Transmission Protocol According to ISO/IEC 14443

3.7.1 Transmission Protocol

The eMRTD SHALL support half-duplex transmission protocol defined in [ISO/IEC14443-4]. The eMRTD SHALL support either Type A or Type B transmission protocols.

3.7.2 Request Command and Answer to Request

The contactless IC SHALL respond to Request Command Type A (REQA) or Request Command Type B (REQB) with Answer to Request Type A (ATQA) or Answer to Request Type B (ATQB), as appropriate.

3.7.3 Random vs Fixed Identifier for the Contactless IC

The eMRTD may serve as a “beacon” in which the contactless IC emits a Unique Identifier (UID) for Type A, and PUPI for Type B when initially activated. This might allow identification of the Issuing Authority. [ISO/IEC 14443] allows the choice of the option whether the eMRTD presents a fixed identifier, assigned uniquely for only that eMRTD, or a random number, which is different at each start of the communication dialogue. Some Issuing States prefer to implement a unique number for security reasons or any other reason. Other issuers give greater preference to concerns about data privacy and the possibility to track persons due to fixed IC identifiers.

Choosing the one or the other option does not decrease interoperability since a reader terminal when compliant with ISO/IEC 14443 will understand both methods. The use of random IC identifiers is RECOMMENDED, but States MAY choose to apply unique UIDs for Type A or unique PUPIs for Type B.

3.8 Command Set

All commands, formats, and their return codes are defined in [ISO/IEC 7816-4]. The minimum set of commands to be supported by the eMRTD MUST be as follows:

SELECT
READ BINARY

It is recognized that additional commands will be required to establish the correct security environment, and implement the optional security provisions identified in Doc 9303-11. Implementation of the mechanisms specified in Doc 9303-11 requires support of the following additional commands:

GET CHALLENGE;
EXTERNAL AUTHENTICATE;
INTERNAL AUTHENTICATE;
MANAGE SECURITY ENVIRONMENT;
GENERAL AUTHENTICATE.

Further details on command protocols can be found in Doc 9303-11.

3.8.1 SELECT

The eMRTD supports two structure selection methods that are file identifier and short EF identifier. Readers support at least one of the two methods. The file identifier and Short File Identifier is REQUIRED for the contactless IC operating system, but OPTIONAL for the reader.

3.8.2 READ BINARY

The support of the READ BINARY command with an odd INS byte by an eMRTD is CONDITIONAL. The eMRTD SHALL support this command variant if it supports data groups with 32 768 bytes or more.

3.9 Command Formats and Parameter Options

3.9.1 Application Selection

Applications have to be selected either by their file identifier or their application name. After the selection of an application, the file within this application can be accessed.

Note: Application names have to be unique. Therefore selection of an application using the application name can be done from wherever needed.

3.9.1.1 Selection of Master File

Table 1: Selection of MF

CLA	INS	P1	P2	Lc	Data	Le
00	A4	00	0C	Empty	Empty	Empty

Note: It is RECOMMENDED that the SELECT MF command not be used.

3.9.1.2 Selection of application by application identifier

An application SHALL be selected by use of the DF Name. The parameters for the APDU command are shown below:

Table 2: SELECT Application command

CLA	INS	P1	P2	Lc	Data	Le
00	A4	04	0C	Var.	AID	–

The first [ISO/IEC7816-4] instruction is “select application”, with the code 0x00A4040C07A0000002471001. Every eMRTD application supports the select command.

3.9.2 EF Selection Using SELECT command

Files have to be selected by their file identifier. When files are selected by File Identifier, it has to be assured that the application the files are stored within has previously been selected.

Table 3: SELECT File command

CLA	INS	P1	P2	Lc	Data	Le
00	A4	02	0C	02	FileID	–

The eMRTD SHALL support the SELECT command with file identifier as specified in Table 3. The inspection system SHALL support at least one of the following methods:

- The SELECT command with file identifier as specified in Table 3
- The READ BINARY command with even INS byte and SFI as specified in Table 5.

3.9.3 Reading Data From EF (READ BINARY)

There are two methods to read data from the eMRTD: by selecting the file and then reading the data, or by reading the data directly using the Short File Identifier. Support for Short File Identifier is REQUIRED for the eMRTD. It is therefore RECOMMENDED that inspection systems use Short File Identifier.

3.9.3.1 Reading data of a selected file (transparent file)

Table 4: READ BINARY command

CLA	INS	P1	P2	Lc	Data	Le
00	B0	Offset MSB	Offset LSB	–	–	MaxRet

3.9.3.2 Reading data using Short File Identifier (transparent file)

Table 5: READ BINARY command with Short File Identifier

CLA	INS	P1	P2	Lc	Data	Le
00	B0	SFI	Offset LSB	–	–	MaxRet

3.9.4 Extended Lc/Le Support

It is RECOMMENDED that any eMRTD and eMRTD reader implementation support both single Lc/Le field (1 byte) and extended Lc/Le field (2 or 3 bytes).

3.9.5 EFs Larger than 32 767 Bytes

The maximum size of an EF is normally 32 767 bytes, but some contactless ICs support larger files. A different READ BINARY parameter option and command format is required to access the data area when the offset is greater than 32 767. This format of command should be used after the length of the template has been determined and the need to access the data in the extended data area has been determined. For example, if the data area contains multiple biometric data objects, it may not be necessary to read the entire data area. Once the offset for the data area is greater than 32 767, this command format shall be used. The offset is placed in the command field rather than in the parameters P1 and P2.

Table 6: Command Format for Efs Larger Than 32 767 Bytes

CLA	INS	P1	P2	Lc	Data	Le	Remark
00	B1	00	00	Var.	Offset TLV encoded	00	Reading files greater than 32 767 bytes

Both Length and Value fields of BER-TLV data object are variable length and can be encoded in different ways (see [ISO/IEC 7816-4]: "BER-TLV length fields").

For performance reasons, communication between the eMRTD and the terminal should be kept as short as possible. Therefore Length field and Value field in the BER-TLV data object SHOULD be as short as possible. This applies not only for Offset data objects in Odd INS READ BINARY commands but also for all other BER-TLV data objects exchanged between the eMRTD and the terminal.

Examples for encoded Offset in Data-field:

- Offset: 0x0001 is encoded as Tag=0x54 Length=0x01 Value=0x01;
- Offset: 0xFFFF is encoded as Tag= 0x54 Length=0x02 Value=0xffff.

The subsequent READ BINARY commands shall specify the offset in the Data field. The final READ BINARY command should request the remaining data area.

The Le byte contains either 0x00 or number of bytes containing extended TL and V.

For some purposes, B1 and the traditional B0 READ Binary commands could not overlap. In other words, B0 only should be used to read the first 32 767 bytes and B1 from 32K upward. For others there could be a small overlap of 256 bytes around the 32 767 threshold to allow a smoother transition between B0 and B1. For this latter group, B1 could be used right from the beginning of the file, i.e. with an offset starting from 0 to allow the same command to be used to read the full content. With respect to [ISO/IEC 7816-4], there are no constraints specified on the offset value when bit 1 of INS is set to 1 to allow a broader use.

The odd INS byte is not to be used by the inspection system if the size of an EF is 32 767 bytes or less.

4 FILE STRUCTURE SPECIFICATIONS

Information in an eMRTD is stored in a file system defined in [ISO/IEC 7816-4]. The file system is organized hierarchically into dedicated files (DFs) and elementary files (EFs). Dedicated files (DFs) contain elementary files or other dedicated files. An optional master file (MF) may be the root of the file system. See Figure 2 for a graphical representation of the file structure.

Note 1: The need for a master file is determined by the choice of operating systems and optional access conditions

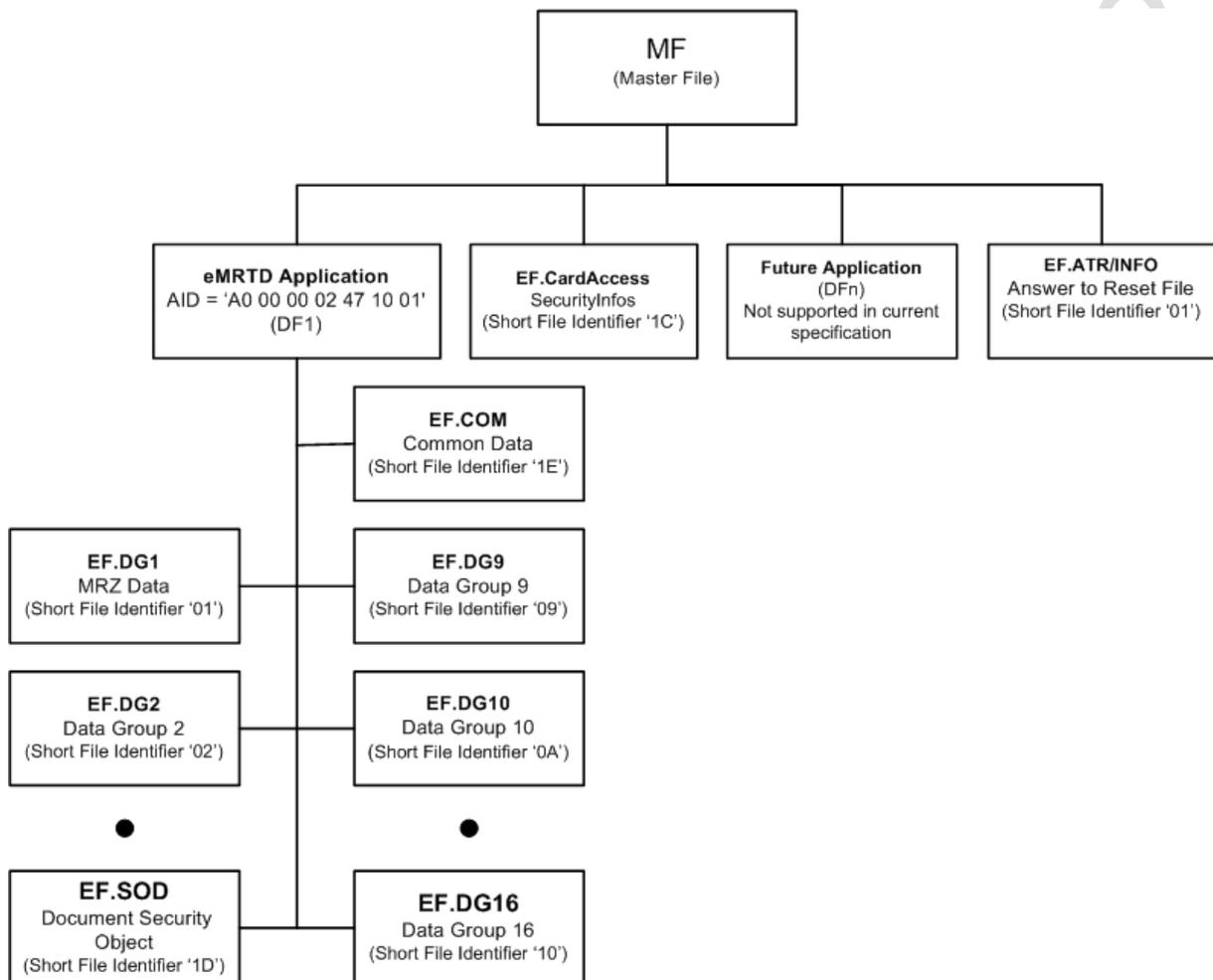


Figure 2: File Structure Summary

4.1 Application Selection - DF

The eMRTDs SHALL support at least one application as follows:

- The application SHALL consist of data recorded by the Issuing State or organization Data Groups 1 through to 16 together with the Document Security Object (EF.SOD)
- The Document Security Object (EF.SOD) consists of the hash values as defined in Doc 9303-11 and Doc 9303-12 for the Data Groups in use, and is needed to validate the integrity of data created by the issuer and stored in the eMRTD Application.

In addition, Issuing States or organizations may wish to add other applications. The file structure SHALL accommodate such additional applications, but the specifics of such applications are outside the scope of Doc 9303.

The eMRTD application SHALL be selected by use of the Application Identification (AID) as a reserved DF name. The AID SHALL consist of the Registered Application Identifier assigned by ISO according to [ISO/IEC 7816-5] and a Proprietary Application Identifier Extension (PIX) as specified within this document:

- The Registered Application Identifier is 0xA000000247;
- The issuer stored data application SHALL use PIX = 0x1001;
- The full AID of the eMRTD application is 'A0 00 00 02 47 10 01'.

4.2 Data Groups

Within each application there may be a number of Data Groups sometimes referred to as Elementary Files (EFs). The Issuing State or organization application may have up to 16 Data Groups. Data Group 1 (DG1), the machine readable zone (MRZ) and Data Group 2, the encoded face, are REQUIRED. All other Data Groups are OPTIONAL. All Data Groups are in the form of data templates and have individual ASN.1 Tags.

Each Data Group consists of a series of data objects within a template. Each Data Group SHALL be stored in a separate Elementary File (EF). Individual data objects from the Data Group can be retrieved directly after the relative position within the transparent file has been determined.

4.3 Data Elements Encoding Rules

The files contain the Data Elements as data objects within a template. The structure and coding of data objects are defined in [ISO/IEC 7816-4] and [ISO/IEC 7816-6]. Each data object has an identification Tag that is specified in hexadecimal coding (for example, 0x5A). The tags defined in this section use the coexistent coding option. Each data object has a unique Tag, a length and a value. The data objects that may be present in a file are identified as mandatory (M) or optional (O). Whenever possible inter-industry Tags are used. Note that the specific definition and format of some Tags have been changed to make them relevant for the eMRTD application. As examples:

- Tag 0x5A is defined as Document Number rather than Primary Account Number and has the format F9N rather than V19N;
- Tag 0x5F20, Cardholder name, has been redefined as "Name of holder" with length of up to 39 characters, encoded per Doc 9303 format;
- Tag 0x65 is defined as the Displayed Portrait rather than Cardholder Related Data;
- As needed, additional Tags have been defined within the 0x5F01 through 0x5F7F range.

4.3.1 Data Elements Encoding Normative Note

There is a mismatch between the LDS (version 1.7 and 1.8) specifications and [ISO/IEC 8825-1] (BER/DER encoding rules) where in [ISO/IEC 8825-1] States for tags with a number ranging from zero to 30 (inclusive), the identifier octets shall comprise a single octet encoded as follows:

- bit 8 and bit 7 shall be encoded to represent the class of the tag;
- bit 6 shall be a zero or a one;
- bits 5 to bit 1 shall encode the number of the tag as a binary integer with bit 5 as the most significant bit.

This means that (for instance) the tag for the version number of the LDS specification should be defined as tag 0x41 = 0x01000001b:

- where 01 means application class (bits 8 and 7);

- where 0 means that it is a primitive (bit 6);
- where 00001 is the encoding of tag number 1 (bits 5-1).

In Doc 9303 the tag for the version number of the LDS specification is defined as tag 0x5F01=0x0101111100000001b:

- where 01 means Application class;
- where 0 means that it is a primitive (not constructed);
- where 11111 means that the tag number is encoded in the next bytes;
- where 0 means that it is the last byte encoding the tag number;
- where 0000001 is the encoding of tag number 1.

This counts for all TAGs from zero to 30 (inclusive):

- 0x5F01, 0x5F08, 0x5F09, 0x5F0A, 0x5F0B, 0x5F0C, 0x5F0E, 0x5F0F, 0x5F10, 0x5F11, 0x5F12, 0x5F13, 0x5F14, 0x5F15, 0x5F16, 0x5F17, 0x5F18, 0x5F19, 0x5F1A, 0x5F1B, 0x5F1C, 0x5F1D, 0x5F1E.

Implementers should be aware of this mismatch and follow the specifications as set out in Doc 9303. One should however note that:

- eMRTD implementations cannot be created using a generator based on ASN.1;
- ASN.1/BER parsers may return an error instead of correctly parsing EF.COM;
- The hash over EF.COM cannot be re-created by decoding the EF.COM structure and encoding it again afterwards.

4.3.2 Data Element Presense Map (DEPM)

A concept of presence maps is used with a number of Data Groups that contain a series of subordinate Data Elements which may be included at the discretion of the State or organization making the recording. These presence maps, called Data Element Presence Maps (DEPM) are located at the start of those specific Data Groups that allow optional expansion.

A DEPM contains information to enable a receiving State or approved receiving organization to determine which Data Elements are present in the Data Group.

The DEPM consists of a list of tags consistent with the convention for identifying Data Elements recorded in eMRTDs in which each Tag identifies if a specific Data Element is recorded in the Data Group. This form of DEPM is encoded as a tag list within the relevant Data Group.

4.3.3 Length Encoding Rules for ASN.1 BER TLV Data Object

The definite form of ANS.1 length encoding as defined in [ISO/IEC 8825-1] MUST be used.

Table 7: Length Encoding Rules

Range	number of bytes	1st byte	2nd byte	3rd byte
0 to 127	1	binary value	None	None
128 to 255	2	81	binary value	None
256 to 65 535	3	82	binary value MSB LSB	

4.4 Normative Tags Used in LDS Context

Table 8: Normative Tags Summary

Tag	Definition	Where Used
02	Integer	Biometric and display templates
5C	Tag list	EF.COM and numerous other files
5F01	LDS Version Number	EF.COM
5F08	Date of birth (truncated)	MRZ
5F09	Compressed image (ANSI/NIST-ITL 1-2000)	Displayed finger

Tag	Definition	Where Used
5F0A	Security features — Encoded Data	Security features (details TBD)
5F0B	Security features — Structure	Security features (details TBD)
5F0C	Security features	Security features (details TBD)
5F0E	Full name, in national characters	Additional personal details
5F0F	Other names	Additional personal details
5F10	Personal number	Additional personal details
5F11	Place of birth	Additional personal details
5F12	Telephone	Additional personal details
5F13	Profession	Additional personal details
5F14	Title	Additional personal details
5F15	Personal summary	Additional personal details
5F16	Proof of citizenship (10918 image)	Additional personal details
5F17	Other valid TD Numbers	Additional personal details
5F18	Custody information	Additional personal details
5F19	Issuing Authority	Additional document details
5F1A	Other people on document	Additional document details
5F1B	Endorsements/Observations	Additional document details
5F1C	Tax/Exit requirements	Additional document details
5F1D	Image of document front	Additional document details
5F1E	Image of document rear	Additional document details
5F1F	MRZ Data Elements	MRZ data objects
5F26	Date of issue	Additional document details
5F2B	Date of birth (8 digit)	Additional personal details
5F2E	Biometric data block	Biometric data
5F36	Unicode Version Level	EF.COM
5F40	Compressed image template	Displayed portrait
5F42	Address	Additional personal details
5F43	Compressed image template	Displayed signature or mark
5F50	Date data recorded	Person to notify
5F51	Name of person	Name of person to notify
5F52	Telephone	Telephone number of person to notify
5F53	Address	Address of person to notify
5F55	Date and time document personalized	Additional document details
5F56	Serial number of personalization system	Additional document details
60	Common Data Elements	EF.COM
61	Template for MRZ Data Group	
63	Template for finger biometric Data Group	
65	Template for digitized facial image	
67	Template for digitized signature or usual mark	
68	Template for machine assisted security — Encoded data	
69	Template for machine assisted security — Structure	
6A	Template for machine assisted security — Substance	

Tag	Definition	Where Used
6B	Template for additional personal details	
6C	Template for additional document details	
6D	Optional details	
6E	Reserved for future use	
70	Person to notify	
75	Template for facial biometric Data Group	
76	Template for iris (eye) biometric template	
77	EF.SO _D (EF for Document Security Object)	
7F2E	Biometric data block (enciphered)	
7F60	Biometric information template	
7F61	Biometric information group template	
8x	Context specific tags	CBEFF
90	Enciphered hash code	Authenticity/Integrity code
A0	Context specific constructed data objects	Additional personal details
Ax or Bx	Repeating template, where x defines occurrence	Biometric header

4.4.1 Tags for Intermediate Processing (Informative)

Table 9: Intermediate Tags

Tag	Definition	Where Used
53	Optional data	Part of MRZ
59	Date of expiry	Part of MRZ
5A	Document number	Part of MRZ
5F02	Check digit — Optional data (TD3 only)	Part of MRZ
5F03	Document type	Part of MRZ
5F04	Check digit — Doc number	Part of MRZ
5F05	Check digit — Date of birth	Part of MRZ
5F06	Check digit — Expiry date	Part of MRZ
5F07	Check digit — Composite	Part of MRZ
5B	Name of document holder	Part of MRZ
5F28	Issuing State or organization	Part of MRZ
5F2B	Date of birth	Part of MRZ
5F2C	Nationality	Part of MRZ
5F35	Sex	Part of MRZ
5F57	Date of birth (6 digit)	Part of MRZ

4.4.1.1 Tags reserved for future use (normative)

Table 10: RFU Tags

Tag	Definition	Where Used
5F44	Country of entry/exit	Travel records
5F45	Date of entry/exit	Travel records
5F46	Port of entry/exit	Travel records
5F47	Entry/Exit indicator	Travel records
5F48	Length of stay	Travel records

Tag	Definition	Where Used
5F49	Category (classification)	Travel records
5F4A	Inspector reference	Travel records
5F4B	Entry/Exit indicator	Travel records
71	Template for electronic visas	
72	Template for border crossing schemes	
73	Template for travel record Data Group	

4.5 LDS Versioning

Future upgrades to the organization of the eMRTD LDS have been anticipated and will be addressed through publication of amendments to the specifications by ICAO. A version number will be assigned to each upgrade to ensure that receiving States and approved receiving organizations will be able to accurately decode all versions of the LDS.

4.5.1 LDS Version 1.7

LDS Version 1.7 MUST implement Document Security Object EF.SOD version V0 as found in section 5 of this document.

4.5.2 LDS Version 1.8

LDS Version 1.8 MUST implement Document Security Object EF.SOD version V1 as found in section 5 of this document.

5 ELEMENTARY FILES

5.1 Header and Data Group Presence Information EF.COM (REQUIRED)

EF.COM is located in the eMRTD application (Short File Identifier = 0x1E) and contains LDS version information, Unicode version information and a list of the Data Groups that are present for the application. The eMRTD application must have only one file EF.COM that contains the common information for the application.

The Data Elements that may occur in this template are as follows:

Table 11: EF.COM Normative Tags

Tag	L	Value		
60	Var	application level information		
		Tag	L	Value
		5F01	04	LDS Version number with format aabb, where aa defines the version of the LDS and bb defines the update level.
		5F36	06	Unicode Version number with format aabbcc, where aa defines the major version, bb defines the minor version and cc defines the release level.
		5C	Var	Tag list. List of all Data Groups present.

A Header and Data Group Presence Map SHALL be included. The header SHALL contain the following information which enables a receiving State or approved receiving organization to locate and decode the various Data Groups and Data Elements contained within the block of data recorded by the Issuing State or organization.

5.1.1 LDS Version Number

The LDS version number defines the format version of the LDS. The exact format to be used for storing this value will be defined section 6 of this document. standardized format for an LDS Version Number is "aabb", where:

- "aa" = number (01-99) identifying the major version of the LDS (i.e. significant additions to the LDS);
- "bb" = number (01-99) identifying the minor version of the LDS;

5.1.2 UNICODE Version Number

The Unicode version number identifies the coding method used when recording alpha, numeric and special characters, including national characters. The exact format to be used for storing this value will be defined in Section 6 of this document. The standardized format for a Unicode version number is "aabbcc", where:

- "aa" = number identifying the major version of the Unicode specification (i.e. significant additions to the specification, published as a book);
- "bb" = number identifying the minor version of the Unicode specification (i.e. character additions or more significant normative changes, published as a technical report and;
- "cc" = number identifying the update version of the Unicode specification (i.e. any other changes to normative or important informative portions of the specification that could change programme behavior. These changes are reflected in new Unicode character database files and an update page).For historical reasons, the numbering within each of the fields (i.e. a, b, c) is not necessarily consecutive.

The Universal Character Set (UCS) MUST comply with [ISO/IEC 10646]

5.2 Document Security Object EF.SOb (REQUIRED)

In addition to the LDS Data Groups, the contactless IC also contains a Document Security Object stored in EF.SOb. This object is digitally signed by the Issuing State and contains hash values of the LDS contents.

Table 12: EF.SOD Tags

Tag	L	Value
77	Var	Document Security Object

There are 2 versions of the Document Security Object EF.SOD currently available. It is REQUIRED that either EF.SOD V0 or EF.SOD V1 is implemented. Only 1 EF.SOD is allowed.

5.2.1 Document Security Object EF.SOD Version V0 LDS v1.7 (REQUIRED)

The Document Security Object V0 for the LDS v1.7 does not contain the LDS and Unicode version information:

```
LDSSecurityObject ::= SEQUENCE {
    version LDSSecurityObjectVersion,
    hashAlgorithm DigestAlgorithmIdentifier,
    dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
    DataGroupHash
```

5.2.2 SignedData Type for SOD V0

The Document Security Object is implemented as a SignedData Type, as specified in [RFC 3369]. All security objects SHALL be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

- Note 1: m REQUIRED — the field SHALL be present
 Note 2: x do not use — the field SHOULD NOT be populated
 Note 3: o optional — the field MAY be present
 Note 4: c choice — the field content is a choice from alternatives

Table 13: Signed Data Type for SOD V0

Value		Comments
SignedData		
Version	m	Value = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-mrtd-security-ldsSecurityObject
eContent	m	The encoded contents of an ldsSecurityObject.
Certificates	o	States may choose to include the Document Signer Certificate (CDS) which can be used to verify the signature in the signerInfos field.
Crls	x	It is recommended that States do not use this field.
signerInfos	m	It is recommended that States only provide 1 signerInfo within this field.
SignerInfo	m	
Version	m	The value of this field is dictated by the sid field. See RFC3369 Doc 9303-12 for rules regarding this field.
Sid	m	
issuerandSerialNumber	c	It is recommended that States support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	Producing States may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by receiving States except to verify the signature value.
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value and any associated parameters.
Signature	m	The result of the signature generation process.

Value		Comments
unsignedAttrs	o	Producing States may wish to use this field, but it is not recommended and receiving States may choose to ignore them.

5.2.3 ASN.1 Profile LDS Document Security Object for SO_D VO

```
LDSSecurityObject {iso(1) identified-organization(3) icao(ccc)
mrttd(1) security(1) ldsSecurityObject(1)}
```

```
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
-- Imports from RFC 3280 [PROFILE],
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
id-mod(0) id-pkix1-explicit(18) }
```

```
-- Constants
```

```
ub-DataGroups INTEGER ::= 16
```

```
-- Object Identifiers
```

```
id-icao OBJECT IDENTIFIER ::= {2.23.136}
id-icao-mrttd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrttd-security OBJECT IDENTIFIER ::= {id-icao-mrttd 1}
id-icao-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrttd-
security 1}
```

```
-- LDS Security Object
```

```
LDSSecurityObjectVersion ::= INTEGER {V0(0)}
```

```
DigestAlgorithmIdentifier ::= AlgorithmIdentifier
```

```
LDSSecurityObject ::= SEQUENCE {
    version LDSSecurityObjectVersion,
    hashAlgorithm DigestAlgorithmIdentifier,
    dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
    DataGroupHash }
```

```
DataGroupHash ::= SEQUENCE {
    dataGroupNumber DataGroupNumber,
    dataGroupHashValue OCTET STRING }
```

```
DataGroupNumber ::= INTEGER {
    dataGroup1 (1),
    dataGroup2 (2),
    dataGroup3 (3),
    dataGroup4 (4),
    dataGroup5 (5),
    dataGroup6 (6),
    dataGroup7 (7),
    dataGroup8 (8),
    dataGroup9 (9),
    dataGroup10 (10),
    dataGroup11 (11),
    dataGroup12 (12),
```

```

dataGroup13      (13),
dataGroup14      (14),
dataGroup15      (15),
dataGroup16      (16) }
END

```

Note: The field `dataGroupValue` contains the calculated hash over the complete contents of the Data Group EF, specified by `dataGroupNumber`.

5.2.4 Document Security Object EF.SO_D V1 LDS v1.8 (REQUIRED)

The Document Security Object V1 for the LDS v1.8 has been extended with a signed attribute, containing the LDS and Unicode version information:

```

LDSecurityObject ::= SEQUENCE {
    version LDSecurityObjectVersion,
    hashAlgorithm DigestAlgorithmIdentifier,
    dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
    DataGroupHash
    ldsVersionInfo LDSVersionInfo OPTIONAL
    -- If present, version MUST be V1 }

LDSVersionInfo ::= SEQUENCE {
    ldsVersion PRINTABLE STRING
    unicodeVersion PRINTABLE STRING }

```

5.2.5 SignedData Type for SO_D V1

The Document Security Object is implemented as a SignedData Type, as specified in [RFC 3369], Cryptographic Message Syntax (CMS), August 2002. All security objects MUST be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

- Note 1: m* *REQUIRED — the field SHALL be present*
Note 2: x *do not use — the field SHOULD NOT be populated*
Note 3: o *optional — the field MAY be present*
Note 4: c *choice — the field content is a choice from alternatives*

Table 14: Signed Data Type for SO_D V0

Value		Comments
SignedData		
Version	m	Value = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-mrtd-security-ldsSecurityObject
eContent	m	The encoded contents of an ldsSecurityObject.
Certificates	m	States may choose to include the Document Signer Certificate (C _{DS}) which can be used to verify the signature in the signerInfos field.
Crls	x	It is recommended that States do not use this field.
signerInfos	m	It is recommended that States only provide 1 signerInfo within this field.
SignerInfo	m	
Version	m	The value of this field is dictated by the sid field. See RFC3369 Doc 9303-12 for rules regarding this field.
Sid	m	
issuerandSerialNumber	c	It is recommended that States support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	

Value		Comments
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	Producing States may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by receiving States except to verify the signature value.
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value and any associated parameters.
Signature	m	The result of the signature generation process.
unsignedAttrs	o	Producing States may wish to use this field, but it is not recommended and receiving States may choose to ignore them.

5.2.6 ASN.1 Profile LDS Document Security Object for SO_D V1

```

LDSSecurityObject {iso(2) identified-organization(23) icao(136)
mrtd(1) security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Imports from RFC 3280 [PROFILE]
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
id-mod(0) id-pkix1-explicit(18) }

-- Constants

ub-DataGroups INTEGER ::= 16

-- Object Identifiers

id-icao OBJECT IDENTIFIER ::= {2.23.136}
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-mrtd-security-ldsSecurityObject OBJECT IDENTIFIER ::=
{idicao-
mrtd-security 1}

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {V0(0), V1(1)}
-- If LDSSecurityObjectVersion is V1, ldsVersionInfo MUST be present
}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

LDSSecurityObject ::= SEQUENCE {
    version LDSSecurityObjectVersion,
    hashAlgorithm DigestAlgorithmIdentifier,
    dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
    DataGroupHash
    ldsVersionInfo LDSVersionInfo OPTIONAL
    -- If present, version MUST be V1 }

DataGroupHash ::= SEQUENCE {
    dataGroupNumber DataGroupNumber,

```

```

dataGroupHashValue OCTET STRING }

DataGroupNumber ::= INTEGER {
    dataGroup1 (1),
    dataGroup2 (2),
    dataGroup3 (3),
    dataGroup4 (4),
    dataGroup5 (5),
    dataGroup6 (6),
    dataGroup7 (7),
    dataGroup8 (8),
    dataGroup9 (9),
    dataGroup10 (10),
    dataGroup11 (11),
    dataGroup12 (12),
    dataGroup13 (13),
    dataGroup14 (14),
    dataGroup15 (15),
    dataGroup16 (16)}

LDSVersionInfo ::= SEQUENCE {
    ldsVersion PRINTABLE STRING
    unicodeVersion PRINTABLE STRING }
END

```

Note: The field `dataGroupValue` contains the calculated hash over the complete contents of the Data Group EF, specified by `dataGroupNumber`.

5.3 EF.CardAccess (CONDITIONAL)

EF.CardAccess is a transparent elementary file contained in the master file and is conditionally required if the optional PACE access control as defined in Doc 9303-11 is invoked. A full description of SecurityInfos for PACE can be found in Doc 9303-11.

5.3.1 Storage On The Contactless IC

The eMRTD IC SHALL provide `SecurityInfos` in a transparent elementary file CardAccess contained in the master file.

Table 15: EF.CardAccess Storage on the IC

File Name	EF.CardAccess
File ID	0x011C
Short File ID	0x1C
Read Access	ALWAYS
Write Access	NEVER
Size	Variable
Content	DER encoded <code>SecurityInfos</code> See Doc 9303-11

6 DATA ELEMENTS FORMING DATA GROUPS 1 THROUGH 16

Data Groups 1 (DG1) through 16 (DG16) individually consist of a number of mandatory, optional, and conditional Data Elements. The specified order of Data Elements within the Data Group SHALL be followed. Each Data Group SHALL be stored in one transparent EF. Addressing EFs SHALL be by Short File Identifier as shown in Table 16. The EFs SHALL have file names for these files that SHALL be according to the number n, EF.DGn, where n is the Data Group number.

Table 16: Mandatory and optional Data Elements that combine to form the structure of Data Groups 1 (DG1) through 16 (DG16).

Data Group	EF Name	Short File Identifier	FID	Tag
Common	EF.COM	1E	01 1E	60
DG1	EF.DG1	01	01 01	61
DG2	EF.DG2	02	01 02	75
DG3	EF.DG3	03	01 03	63
DG4	EF.DG4	04	01 04	76
DG5	EF.DG5	05	01 05	65
DG6	EF.DG6	06	01 06	66
DG7	EF.DG7	07	01 07	67
DG8	EF.DG8	08	01 08	68
DG9	EF.DG9	09	01 09	69
DG10	EF.DG10	0A	01 0A	6A
DG11	EF.DG11	0B	01 0B	6B
DG12	EF.DG12	0C	01 0C	6C
DG13	EF.DG13	0D	01 0D	6D
DG14	EF.DG14	0E	01 0E	6E
DG15	EF.DG15	0F	01 0F	6F
DG16	EF.DG16	10	01 10	70
Document Security Object	EF.SO _D	1D	01 1D	77
Common	EF.CARDACCESS	1C	01 1C	
Common	EF.ATR/INFO			

6.1 DATA GROUP 1 - Machine Readable Zone Information (REQUIRED)

The Data Elements of Data Group 1 (DG1) are intended to reflect the entire contents of the MRZ whether it contains actual data or filler characters. Details on the implementation of the MRZ are dependent on the type of eMRTD (TD1, TD2, or TD3 formats).

This EF contains the REQUIRED machine readable zone (MRZ) information for the document in template 0x61. The template contains one data object, the MRZ in data object 0x5F1F. The MRZ data object is a composite Data Element, identical to the OCR-B MRZ information printed on the document.

Table 17: Data Group 1 Tags

Tag	L	Value		
61	Var			
		Tag	L	Value
		5F1F	F	The MRZ data object as a composite Data Element. (REQUIRED) (The Data Element contains all mandatory fields from Document Type through to Composite check digit)

6.1.1 DATA GROUP 1 – EF.DG1 Data Elements for TD1 Size eMRTD

This section describes the Data Elements that may be present in Data Group 1 (DG1). Storage, ordering, and coding requirements of Data Group 1 is intended to be exactly the same as found in the printed MRZ and described in Doc 9303-3 and Doc 9303-5. Data Elements and their format within each Data Group area for TD1 shall be as in the following table:

Note: A = Alpha character [A..Z], N = Numeric character [0..9], S = Special character ['<'], F = fixed-length field.

Table 18: Data Elements for TD1 format

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
01	M	Document code	2	F	A,S
02	M	Issuing State or organization	3	F	A,S
03	M	Document number (Nine most significant characters)	9	F	A,N,S
04	M	Check digit — Document number or filler character (<) indicating document number exceeds nine characters	1	F	N,S
05	M	Optional data and/or in the case of a Document Number exceeding 9 characters, least significant characters of document number plus document number check digit plus filler character	15	F	A,N,S

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
06	M	Date of birth	6	F	N,S
07	M	Check digit — Date of birth	1	F	N
08	M	Sex	1	F	A,S
09	M	Date of Expiry	6	F	N
10	M	Check digit — Date of expiry	1	F	N
11	M	Nationality	3	F	A,S
12	M	Optional data	11	F	A,N,S
13	M	Composite check digit	1	F	N
14	M	Name of holder	30	F	A,N,S

6.1.2 DATA GROUP 1 – EF.DG1 Data Elements for TD2 Size eMRTD

This section describes the Data Elements that may be present in Data Group 1 (DG1). Storage, ordering, and coding requirements of Data Group 1 intended to be exactly the same as found in the printed MRZ and described in 9303-3 and Doc 9303-6. Data Elements and their format within each Data Group area for TD2 shall be as in the following table:

Note: A = Alpha character [A..Z], N = Numeric character [0..9], S = Special character ['<'], F = fixed-length field.

Table 19: Data Elements for TD2 format

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
01	M	Document code	2	F	A,S
02	M	Issuing State or organization	3	F	A,S
03	M	Name of holder	31	F	A,N,S
04	M	Document number (Nine principal characters)	9	F	A,N,S
05	M	Check digit	1	F	N,S
06	M	Nationality	3	F	A,S
07	M	Date of birth	6	F	N,S
08	M	Check digit	1	F	N
09	M	Sex	1	F	A,S
10	M	Date of expiry	6	F	N
11	M	Check digit	1	F	N
12	M	Optional data plus filler character	7	F	A,N,S
13	M	Composite Check Digit - MRZ line 2	1	F	N

6.1.3 DATA GROUP 1 – EF.DG1 Data Elements for TD3 Size eMRTD

This section describes the Data Elements that may be present in Data Group 1 (DG1). Storage, ordering and coding requirements of Data Group 1 intended to be exactly the same as found in the printed MRZ and described in Doc 9303-3 and Doc 9303-4. Data Elements and their format within each Data Group area for TD3 shall be as in the following table:

Note: A = Alpha character [A..Z], N = Numeric character [0..9], S = Special character ['<'], F = fixed-length field.

Table 20: Data Elements for TD3 format

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
01	M	Document code	2	F	A,S
02	M	Issuing State or organization	3	F	A,S
03	M	Name of holder	39	F	A,S
04	M	Document number	9	F	A,N,S
05	M	Check digit — Document number	1	F	N,S
06	M	Nationality	3	F	A,S
07	M	Date of birth	6	F	N,S
08	M	Check digit — Date of birth	1	F	N
09	M	Sex	1	F	A,S
10	M	Date of expiry	6	F	N
11	M	Check digit — Date of expiry or valid until date	1	F	N
12	M	Optional data	14	F	A,N,S
13	M	Check digit	1	F	N
14	M	Composite check digit	1	F	N

6.2 DATA GROUP 2 - Encoded Identification Features – Face (REQUIRED)

Data Group 2 (DG2) represents the globally interoperable biometric for machine assisted identity confirmation with machine readable travel documents, which SHALL be an image of the face of the holder as an input to a face recognition system. If there is more than one recording, the most recent internationally interoperable encoding SHALL be the first entry.

Table 21: Data Group 2 Tags.

Tag	L	Value
75	Var	See Biometric encoding of EF.DG2

6.2.1 Biometric Encoding of EF.DG2

DG2 MUST use the Biometric Information Template (BIT) group template with nested BITs specified in [ISO/IEC 7816-11], which allows the possibility to store multiple biometric templates and are in harmony with the Common Biometric Exchange File Format (CBEFF). The biometric sub-header defines the type of biometric that is present and the specific biometric feature. The nested option of ISO/IEC [7816-11]

is always to be used, even for encodings of a single biometric template. The latter case is indicated by numbering with n=1.

Each nested template has the following structure:

Table 22: Data Group 2: Biometric Encoding Tags

Tag	L	Value		
7F61	Var	Biometric Information Group Template		
		Tag	L	Value
		02	01	Integer — Number of instances of this type of biometric
		7F60	Var	1st Biometric Information Template
			Tag	L
			A1	Var
				Biometric Header Template (BHT)
			Tag	L
				Value
			80	02
				ICAO header version 0101 (Optional) — Version of the CBEFF patron header format
			81	01-03
				Biometric type (Optional)
			82	01
				Biometric subtype Optional for DG2
			83	07
				Creation date and time (Optional)
			85	08
				Validity period (from through) (Optional)
			86	02
				Creator of the biometric reference data (PID) (Optional)
			87	02
				Format owner (REQUIRED)
			88	02
				Format type (REQUIRED)
			5F2E or 7F2E	Var
				Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).
		Tag	L	
		7F60	Var	2nd Biometric Information Template
			Tag	L
			A1	Var
				Biometric Header Template (BHT)
			Tag	L
				Value
			80	02
				ICAO header version '0101' (Optional) — Version of the CBEFF patron header format
			81	01-03
				Biometric type (Optional)
			82	01
				Biometric subtype Optional for DG2
			83	07
				Creation date and time (Optional)
			85	08
				Validity period (from through) (Optional)
			86	04
				Creator of the biometric reference data (PID) (Optional)
			87	02
				Format owner (REQUIRED)
			88	02
				Format type (REQUIRED)
			5F2E or 7F2E	Var
				Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).

The default OID of CBEFF is used. The OID data object (tag 0x06) just under Biometric Information Template (BIT, tag 0x7F60) specified in [ISO/IEC 7816-11] is not included in this structure. Likewise the tag allocation authority is not specified in the structure.

To facilitate interoperability, the first biometric recorded in each Data Group SHALL be encoded as per [ISO/IEC19794-5].

6.2.2 DATA GROUP 2 – EF.DG2 Data Elements

This section describes the Data Elements that may be present in Data Group 2 (DG2): Data Elements and their format within each Data Group area SHALL be as in the following tables:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 23: Data Elements for DG2

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M	Number of face biometric encodings recorded	1	F	N	1 to 9 identifying number of unique encodings of data on the face.
02	M	Header		Var	A,N	Data Element may recur as defined by DE 01.
03	M	Face biometric data encoding(s)		Var	A,N,S, B	Data Element may recur as defined by DE 01.

6.3 DATA GROUP 3 - Additional Identification Feature - Finger(s) (OPTIONAL)

ICAO recognizes that Member States may elect to use fingerprint recognition as additional biometric technologies in support of machine assisted identity confirmation, which SHALL be encoded as Data Group 3 (DG3).

Table 24: Data Group 3 Tags

Tag	L	Value
63	Var	See Biometric encoding of EF.DG3

6.3.1 Biometric Encoding of EF.DG3

EF.DG3 MUST use the Biometric Information Template (BIT) group template with nested BITs specified in [ISO/IEC 7816-11], which allows the possibility to store multiple biometric templates and are in harmony with the Common Biometric Exchange File Format (CBEFF). The biometric sub-header defines the type of biometric that is present and the specific biometric feature. The nested option of ISO/IEC [7816-11] MUST be used, even for encodings of a single biometric template. The latter case is indicated by numbering with n=1. The number of instances in DG3 can be '0...n'.

Each nested template has the following structure:

Table 25: Data Group 3 Nested Tags

Tag	L	Value		
7F61	Var	Biometric Information Group Template		
		Tag	L	Value
		02	01	Integer — Number of instances of this type of biometric
		7F60	Var	1st Biometric Information Template
			Tag	L
			A1	Var
				Biometric Header Template (BHT)
			Tag	L
			80	02
				ICAO header version '0101' (Optional) — Version of the CBEFF patron header format
			81	01-03
				Biometric type (Optional)
			82	01
				Biometric subtype REQUIRED for DG3
			83	07
				Creation date and time (Optional)
			85	08
				Validity period (from through) (Optional)
			86	02
				Creator of the biometric reference data (PID) (Optional)
			87	02
				Format owner (REQUIRED)
			88	02
				Format type (REQUIRED)
			5F2E or 7F2E	Var
				Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).
		Tag	L	
		7F60	X	2nd Biometric Information Template
			Tag	L
			A1	Var
				Biometric Header Template (BHT)
			Tag	L
			80	02
				ICAO header version '0101' (Optional) — Version of the CBEFF patron header format
			81	01-03
				Biometric type (Optional)
			82	01
				Biometric subtype REQUIRED for DG3
			83	07
				Creation date and time (Optional)
			85	08
				Validity period (from through) (Optional)
			86	04
				Creator of the biometric reference data (PID) (Optional)
			87	02
				Format owner (REQUIRED)
			88	02
				Format type (REQUIRED)
			5F2E or 7F2E	Var
				Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).

The default OID of CBEFF is used. The OID data object (tag 0x06) just under Biometric Information Template (BIT, tag 0x7F60) specified in [ISO/IEC 7816-11] is not included in this structure. Likewise the tag allocation Authority is not specified in the structure.

To facilitate interoperability, the first biometric recorded in each Data Group SHALL be encoded as per [ISO/IEC19794-5].

6.3.2 DATA GROUP 3 – EF.DG3 Data Elements

This section describes the Data Elements that may be present in Data Group 3 (DG3) Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 26: Data Elements for DG3

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If encoded finger(s) feature recorded)	Number of finger(s) biometric encodings recorded	1	F	N	0 to n identifying number of unique encodings of data on the finger(s).
02	M (If encoded finger(s) feature recorded)	Header		Var	B	Data Element may recur as defined by DE 01.
03	M (If encoded finger(s) feature recorded)	Finger biometric data encoding(s)		Var	A,N,S, B	Data Element may recur as defined by DE 01.

6.3.2.1 Biometric sub-type encoding

The biometric header template tags and their assigned values are the minimum each implementation shall support as shown in the following table. Each single biometric information template has the following structure:

Table 27: Encoding of sub-features scheme for the encoding of sub-features: CBEFF

b8	b7	b6	b5	b4	b3	b2	b1	Biometric Sub-type
0	0	0	0	0	0	0	0	No information given
						0	1	Right
						1	0	Left
		0	0	0				No meaning
		0	0	1				Thumb
		0	1	0				Pointer
		0	1	1				Middle
		1	0	0				Ring
		1	0	1				Little
X	X	X						Reserved for future use

6.3.2.2 Encoding of zero instance

States, not issuing eMRTDs with fingerprints SHOULD NOT not populate DG3. Data Group 3 of this structure has the drawback that it will result in a static DG3 hash in the SO_D for all eMRTDs where the biometric features are not present and populated at the time of eMRTD issuance but the DG3 is declared. For interoperability purposes States supporting fingerprints in their eMRTDs MUST store an empty Biometric Information Group Template in cases where no fingerprints are available at the time of eMRTD issuance. The template counter denotes a value of 0x00 in this case.

It is RECOMMENDED to add tag 0x53 with issuer defined content (e.g. a random number).

Table 28: Encoding zero instances

Tag	L	Value				
63	Var	LDS element				
		Tag	L	Value		
		7F 61	03	Biometric Information Group Template		
			02	01	00	Defines that there are no Biometric Information Templates stored in this Data Group.
		53	Var	Issuer defined content (e.g. a random number).		

6.3.2.3 Encoding of one instance

In cases where only one fingerprint is available, the single instance MUST be encoded in the following manner (example for DG3 – fingerprint):

Table 29: Encoding one instance

Tag	L	Value						
63	aa	LDS element where aa is the total length of the entire LDS data content						
		Tag	L	Value				
		7F 61	bb	Biometric Information Group Template, where bb is the total length of the entire Group Template content.				
			02	01	01	Defines the total number of fingerprints stored as Biometric Information Templates that follow.		
			7F 60	cc	First biometric information template where cc is the total length of the entire BIT			
				A1	dd	Biometric Header Template, where dd is the total length of the BHT		
					81	01	08	Biometric type "Fingerprint"
					82	01	0A	Biometric subtype "left pointer finger"
					87	02	01 01	Format Owner JTC 1 SC 37
					88	02	00 07	Format Type [ISO/IEC 19794-4]
					Note that the BHT may contain additional optional elements. Of course, this fingerprint can either be a left or right finger depending on the available image.			
			5F 2E	ee	Biometric Data Block where ee is total length of the encoded [ISO/IEC 19794-4] structure. The Biometric Data Block MUST contain exactly one fingerprint image.			

6.3.2.4 Encoding of more than one instance

To achieve interoperability each feature MUST be stored in an individual Biometric Information Template. The feature position MUST be specified within the CBEFF biometric subtype if this information is available. The following table contains a worked example for the CBEFF encoding of an interoperable DG 3 element with two fingerprint images.

Table 30: Encoding greater than one instance

Tag	L	Value						
63	aa	LDS element where aa is the total length of the entire LDS data content						
		Tag	L	Value				
		7F 61	bb	Biometric Information Group Template, where bb is the total length of the entire Group Template content.				
			02	01	02	Defines the total number of fingerprints stored as Biometric Information Templates that follow.		
			7F 60	cc	First biometric information template where cc is the total length of the entire BIT			
				A1	Dd	Biometric Header Template, where dd is the total length of the BHT		
					81	01	08	Biometric type "Fingerprint"
					82	01	0A	Biometric subtype "left pointer finger"
					87	02	01 01	Format Owner JTC 1 SC 37
					88	02	00 07	Format Type [ISO/IEC 19794-4]
					Note that the BHT may contain additional optional elements. It is also possible that the order of fingerprints (left/right) is different.			

				5F 2E	ee	Biometric Data Block where ee is total length of the encoded [ISO/IEC 19794-4] structure. The Biometric Data Block MUST contain exactly one fingerprint image.		
			7F 60	ff	Second biometric information template where ff is the total length of the entire BIT			
				A1	Gg	Biometric Header Template, where gg is the total length of the BHT		
					81	01	08	Biometric type "Fingerprint"
					82	01	09	Biometric subtype "right pointer finger"
					87	02	01 01	Format Owner JTC 1 SC 37
					88	02	00 07	Format Type [ISO/IEC 19794-4]
					Note that the BHT may contain additional optional elements. It is also possible that the order of fingerprints (left/right) is different.			
				5F 2E	Hh	Biometric Data Block where hh is total length of the encoded [ISO/IEC 19794-4] structure. The Biometric Data Block MUST contain exactly one fingerprint image.		

6.4 DATA GROUP 4 - Additional Identification Feature –Iris(es) (OPTIONAL)

ICAO recognizes that member States may elect to use iris recognition as additional biometric technologies in support of machine assisted identity confirmation, which SHALL be encoded as Data Group 4 (DG4).

Table 31: Data Group 4 Tags

Tag	L	Value
76	Var	See Biometric encoding of EF.DG4

6.4.1 Biometric Encoding of EF.DG4

DG4 MUST use the Biometric Information Template (BIT) group template with nested BITs specified in [ISO/IEC 7816-11], which allows the possibility to store multiple biometric templates and are in harmony with the Common Biometric Exchange File Format (CBEFF). The biometric sub-header defines the type of biometric that is present and the specific biometric feature. The nested option of ISO/IEC [7816-11] MUST be used, even for encodings of a single biometric template. The latter case is indicated by numbering with n=1. The number of instances in DG4 can be '0...n'

Each nested template has the following structure:

Table 32: Data Group 4 Nested Tags

Tag	L	Value
7F61	Var	Biometric Information Group Template
		Tag L Value
		02 1 Integer — Number of instances of this type of biometric
		7F60 var 1st Biometric Information Template
		Tag L
		A Var Biometric Header Template (BHT)
		Tag L Value
		80 02 ICAO header version '0101' (Optional) — Version of the CBEFF patron header format
		81 01-03 Biometric type (Optional)
		82 01 Biometric sub-type, REQUIRED for DG4
		83 07 Creation date and time (Optional)
		85 08 Validity period (from through) (Optional)

Tag	L	Value				
				86	02	Creator of the biometric reference data (PID) (Optional)
				87	02	Format owner (REQUIRED)
				88	02	Format type (REQUIRED)
			5F2E or 7F2E	Var		Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).
		Tag	L			
		7F60	var	2nd Biometric Information Template		
		Tag	L			
		A1	Var	Biometric Header Template (BHT)		
				Tag	L	Value
				80	02	ICAO header version '0101' (Optional) — Version of the CBEFF patron header format
				81	01-03	Biometric type (Optional)
				82	01	Biometric subtype (REQUIRED for DG4)
				83	07	Creation date and time (Optional)
				85	08	Validity period (from through) (Optional)
				86	04	Creator of the biometric reference data (PID) (Optional)
				87	02	Format owner (REQUIRED)
				88	02	Format type (REQUIRED)
			5F2E or 7F2E	Var		Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).

The default OID of CBEFF is used. The OID data object (tag 0x06) just under Biometric Information Template (BIT, tag 0x7F60) specified in [ISO/IEC 7816-11] is not included in this structure. Likewise the tag allocation authority is not specified in the structure.

To facilitate interoperability, the first biometric recorded in each Data Group SHALL be encoded as per [ISO/IEC 19794-5].

6.4.2 DATA GROUP 4 – EF.DG4 Data Elements

This section describes the Data Elements that may be present in Data Group (DG4) Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 33: Data Elements for DG4

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M, if encoded eye(s) feature included	Number of eye biometric encodings recorded	1	F	N	1 to 9 identifying number of unique encodings of data on the eye(s).
02	M, if encoded eye(s) feature included	Header		Var	B	Data Element may recur as defined by DE 01.
03	M, if encoded eye(s) feature included	Eye biometric data encoding(s)		Var	A,N,S, B	Data Element may recur as defined by DE 01.

6.4.2.1 Biometric sub-type encoding

The biometric header template tags and their assigned values are the minimum each implementation SHALL support as shown in the following table. Each single biometric information template has the following structure:

Table 34: Encoding of sub-features scheme for the encoding of sub-features: CBEFF

b8	b7	b6	b5	b4	b3	b2	b1	Biometric Sub-type
0	0	0	0	0	0	0	0	No information given
						0	1	Right
						1	0	Left
		0	0	0				Reserved for future use
		0	0	1				Reserved for future use
		0	1	0				Reserved for future use
		0	1	1				Reserved for future use
		1	0	0				Reserved for future use
		1	0	1				Reserved for future use
X	X	X						Reserved for future use

6.4.2.2 Encoding of zero instance

States, not issuing eMRTDs with irises SHOULD NOT not populate DG4. Data Group 4 of this structure has the drawback that it will result in a static DG4 hash in the SO_D for all eMRTDs where the biometric features are not present and populated at the time of eMRTD issuance but the DG4 is declared. For interoperability purposes States supporting irises in their eMRTDs MUST store an empty Biometric Information Group Template in cases where no irises are available at the time of eMRTD issuance. The template counter denotes a value of 0x00 in this case.

It is RECOMMENDED to add Tag 0x53 with issuer defined content (e.g. a random number).

Table 35: Encoding zero instances

Tag	L	Value				
76	Var	LDS element				
		Tag	L	Value		
		7F 61	03	Biometric Information Group Template		
			02	01	00	Defines that there are no Biometric Information Templates stored in this Data Group.
		53	Var	Issuer defined content (e.g. a random number).		

6.4.2.3 Encoding of one instance

In cases where only one iris is available, the single instance MUST be encoded.

6.4.2.4 Encoding of more than one instance

To achieve interoperability each feature MUST be stored in an individual Biometric Information Template. The feature position MUST be specified within the CBEFF biometric subtype if this information is available.

6.5 DATA GROUP 5 - Displayed Portrait (OPTIONAL)

Data Elements assigned to Data Group 5 (DG5) SHALL be as follows:

Table 36: Data Group 5 Tags

Tag	L	Value		
65	Var			
		Tag	L	Value
		02	Var	Number of instances of this type of displayed image (REQUIRED in first template. Not used in succeeding templates.)
		5F40	Var	Displayed portrait

The following format owners are recognized for the specified type of displayed image.

Table 37: DG5 Formats

Displayed Image	Format Owner
Displayed Facial Image	[ISO/IEC 10918], JFIF option

6.5.1 DATA GROUP 5 – EF.DG5 Data Elements (Optional)

This section describes the Data Elements that may be present in Data Group 5 (DG5). Data Elements and their format within Data Group 5 SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 38: Data Elements for DG5

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If displayed portrait recorded)	Number of displayed portraits recorded	1	F	N	1 to 9 identifying number of unique recordings of displayed portrait.
02	M (If displayed portrait recorded)	Displayed portrait representation(s)		Var	A,N	Data Element may recur as defined by DE 01.
	M (If displayed portrait recorded)	Number of bytes in representation of displayed portrait	5	F	N	00001 to X9, identifying number of bytes in representation of displayed portrait immediately following.
	M (If displayed portrait recorded)	Representation of displayed portrait		Var	A,N,S, B	Formatted as per [ISO/IEC 10918-1] or [ISO/IEC 15444].

Note: Data Element 02 SHALL be encoded as defined in [ISO/IEC 10918], using the JFIF option or [ISO/IEC 15444] using JPEG 2000 image coding system.

6.6 DATA GROUP 6 - Reserved for Future Use

Data Elements assigned to Data Group 6 (DG6) SHALL be as follows:

Table 39: Data Group 6 Tags

Tag	L	Value
66	Var	

6.6.1 DATA GROUP 6 – EF.DG6 Data Elements

The data elements for Data Group 6 (DG6) are reserved for future use.

6.7 DATA GROUP 7 - Displayed Signature or Usual Mark (OPTIONAL)

Data Elements assigned to Data Group 7 (DG7) SHALL be as follows:

Table 40: Data Group 7 Tags

Tag	L	Value		
67	Var			
		Tag	L	Value
		02	Var	Number of instances of this type of displayed image (REQUIRED in first template. Not used in succeeding templates.)
		5F43	Var	Displayed Signature

The following format owners are recognized for the specified type of displayed image:

Table 41: DG7 Formats

Displayed Image	Format Owner
Displayed Signature/usual mark	[ISO/IEC 10918], JFIF option

6.7.1 DATA GROUP 7 - EF.DG7 Data Elements (OPTIONAL)

This section describes the Data Elements that may be present in Data Group 7 (DG7). Data Elements and their format within each Data Group 7 SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 42: Data Elements for DG7

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If displayed signature or usual mark recorded)	Number of displayed signature or usual marks	1	F	N	1 to 9 identifying number of unique recordings of displayed signature or usual mark.
02	M (If displayed signature or usual mark recorded)	Displayed signature or usual mark representation		Var	A,N,S, B	Data Element may recur as defined by DE 01. Formatted as per [ISO/IEC 10918-1] or [ISO/IEC 15444].

Note: Data Element 02 SHALL be encoded as defined in [ISO/IEC 10918], using the JFIF option, or [ISO/IEC 15444] using JPEG 2000 image coding system.

6.8 DATA GROUP 8 - Data Feature(s) (OPTIONAL)

This Data Group has yet to be defined. Until then, they are available for temporary proprietary usage. This Data Element could use a structure similar to that for biometric templates. Machine assisted security feature verification and encoded detail(s). Data Elements combining to form Data Group 8 (DG8) SHALL be as follows:

Table 43: Data Group 8 Tags

Tag	L	Value		
68	var	To Be Defined		
		Tag	L	Value
		02	1	Integer — Number of instances of this type of template (REQUIRED in first template. Not used in succeeding templates.)
			var	Header Template. Details to be defined.

6.8.1 DATA GROUP 8 – EF.DG8 Data Elements

This section describes the Data Elements that may be present in Data Group 8 (DG8). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 44: Data Elements for DG8

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If this encoded feature is used)	Number of data feature(s)	1	F	N	1 to 9, identifying number of unique encodings of data feature(s) (embraces DE 02 through DE 04).
02	M (If this encoded feature is used)	Header (to be defined)	1			Header details to be defined.
03	M (If this encoded feature is used)	Data feature(s) data	999 Max	Var	A,N,S, B	Format defined at the discretion of Issuing State or organization.

6.9 DATA GROUP 9 - Structure Feature(s) (OPTIONAL)

This Data Group has yet to be defined. Until then, it is available for temporary proprietary use. These Data Elements could use a structure similar to that for biometric templates..Data Elements combining to form Data Group 9 (DG9) SHALL be as follows:

Table 45: Data Group 9 Tags

Tag	L	Value		
69	Var	To Be Defined		
		Tag	L	Value
		02	01	Integer — Number of instances of this type of template (REQUIRED in first template. Not used in succeeding templates.)
			X	Header Template. Details to be defined.

6.9.1 DATA GROUP 9 – EF.DG9 Data Elements

Data Group 9 (DG9) Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 46: Data Elements for DG9

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If this encoded feature is used)	Number of structure feature(s)	1	F	N	1 to 9, identifying number of unique encodings of structure feature(s) (embraces DE 02 through DE 04).
02	M (If this encoded feature is used)	Header (to be defined)			N	Header details to be defined
03	M (If this encoded feature is used)	Structure feature(s) data		Var		

6.10 DATA GROUP 10 - Substance Feature(s) (OPTIONAL)

This Data Group has yet to be defined. Until then, it is available for temporary proprietary usage. These Data Elements could use a structure similar to that for biometric templates. Data Elements combining to form Data Group 10 (DG10) SHALL be as follows:

Table 47: Data Group 10 Tags

Tag	L	Value		
6A	var			
		Tag	L	Value
		02	01	Integer — Number of instances of this type of template (REQUIRED in first template. Not used in succeeding templates.)
			Var	To Be Defined.

6.10.1 DATA GROUP 10 – EF.DG10 Data Elements

This section describes the Data Elements that may be present in Data Group 10 (DG10). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 48: Data Elements for DG10

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If this encoded feature is used)	Number of substance feature(s) recorded	1	F	N	1 to 9, identifying number of unique encodings of substance feature(s) (embraces DE 02 through DE 04).
02	M (If this encoded feature is used)	Header (to be defined)	TBD	TBD	N	Details to be defined.
03	M (If this encoded feature is used)	Substance feature(s) data	999 Max	Var	A,N,S, B	Format defined at the discretion of Issuing State or Organization.

6.11 DATA GROUP 11 - Additional Personal Detail(s) (OPTIONAL)

This Data Group is used for additional details about the document holder. Since all of the Data Elements within this group are optional, a Tag list is used to define those present. Data Elements combining to form Data Group 11 (DG11) SHALL be as follows:

Note: This template may contain non-Latin characters.

Table 49: Data Group 11 Tags

Tag	L	Value		
6B	Var			
		Tag	L	Value
		5C	Var	Tag list with list of Data Elements in the template.
		5F0E	Var	Full name of document holder in national characters. Encoded per Doc 9303 rules.
		A0	Var	Content-specific class
				Tag L Value
			02 01	Number of other names

Tag	L	Value				
				5F0F	Var	Other name formatted per Doc 9303. The data object repeats as many times as indicated in number of other names (data object with tag'02')
		Tag	L	Value		
		5F10	Var			Personal number
		5F2B	08			Full date of birth yyymmdd
		5F11	Var			Place of birth. Fields separated by '<'
		5F42	Var			Permanent address. Fields separated by '<'
		5F12	Var			Telephone
		5F13	Var			Profession
		5F14	Var			Title
		5F15	Var			Personal summary
		5F16	Var			Proof of citizenship. Compressed image per [ISO/IEC 10918]
		5F17	Var			Other valid TD numbers. Separated by '<'
		5F18	Var			Custody information

6.11.1 DATA GROUP 11 – EF.DG11 Data Elements

This section describes the Data Elements that may be present in Data Group 11 (DG11). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note 1: Data Element 11 SHALL be encoded as defined in [ISO/IEC 10918], using the JFIF option or [ISO/IEC 15444] using JPEG 2000 image coding system.

Note 2: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 50: Data Elements for DG11

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	O	Name of holder (in full)	99 Max	Var	B	Filler characters (<) inserted as per MRZ. No fillers inserted at end of line. Truncation not permitted.
02	O	Other name(s)	99 Max	Var	B	Filler characters (<) inserted as per MRZ. No fillers inserted at end of line. Truncation not permitted.
03	O	Personal number	99 Max	Var	A,N,S	Free-form text.
04	O	Full date of birth	8	F	B	CCYYMMDD
05	O	Place of birth	99 Max	Var	B	Free-form text.
06	O	Address	99 Max	Var	A,N,S, B	Free-form text.
07	O	Telephone	99 Max	Var	N,S	Free-form text.
08	O	Profession	99 Max	Var	B	Free-form text.
09	M, if DE 08 included	Title	99 Max	Var	B	Free-form text.
10	M, if DE 09 included	Personal summary	99 Max	Var	B	Free-form text.
11	M, if DE 10 included	Proof of citizenship		Var	A,N,S, B	Image of citizenship document formatted as per [ISO/IEC 10918-1]
12	O	Other valid travel document(s) Travel document number	99 Max	Var	A,N,S, B	Free-form text, separated by <.
13	O	Custody information	999 Max	Var	B	Free-form text.

Note: In case, the month (MM) or the day (DD) are unknown, the interoperable way to indicate this in DG11 is to set the respective characters to '00'. In case, the century and the year (CCYY) are unknown, the interoperable way to indicate this in DG11 is to set the respective characters to '0000'.

Issuer-assigned dates must always be used consistently.

6.12 DATA GROUP 12 - Additional Document Detail(s) (OPTIONAL)

This Data Group is used for additional information about the document. All Data Elements within this group are optional.

Table 51: Data Group 12 Tags

Tag	L	Value				
6C	Var					
		Tag	L	Value		
		5C	Var	Tag list with list of Data Elements in the template		
		5F19	Var	Issuing Authority		
		5F26	08	Date of issue. yyymmdd		
		A0	Var	Content-specific class		
				Tag	L	Value
				02	01	Number of other persons
				5F1A	Var	Name of other person formatted per Doc 9303 rules. The data object repeats as many times as indicated in number of other names DE02 (data object with tag'02').
		Tag	L	Value		
		5F1B	Var	Endorsements, observations		
		5F1C	Var	Tax/Exit requirements		
		5F1D	Var	Image of front of document. Image per ISO/IEC 10918		
		5F1E	Var	Image of rear of document. Image per ISO/IEC 10918		
		5F55	0E	Date and time of document personalization yyymmddhhmmss		
		5F56	Var	Serial number of personalization system		

It is RECOMMENDED that Inspection Systems support both 8 bytes ASCII and BCD date/time encoding.

6.12.1 DATA GROUP 12 – EF.DG12 Data Elements

This section describes the Data Elements that may be present in Data Group 12 (DG12). Data Elements and their format within each Data Group SHALL be as in the following table:

Note 1: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Note 2: Data Elements 07 and 08 SHALL be encoded as defined in [ISO/IEC 10918], using the JFIF option or [ISO/IEC 15444] using JPEG 2000 image coding system.

Table 52: Data Elements for DG12

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	O	Issuing Authority	99 Max	Var	B	Free-form text.
02	O	Date of issue	8	F	N	Date of issue of document; i.e. YYYYMMDD.
03	O	Other person(s) details	99 Max	Var	B	Free-form text (Only valid with MRV).
04	O	Endorsement(s)/ Observation(s)	99 Max	Var	B	Free-form text.
05	O	Tax/Exit requirements	99 Max	Var	B	Free-form text.
06	O	Image of front of MRTD		Var	A,N,S, B	Formatted as per [ISO/IEC 10918-1]
07	O	Image of rear of MRTD		Var	A,N,S, B	Formatted as per [ISO/IEC 10918-1]
08	O	Personalization Time	14	F	N	ccyymmddhhmmss
09	O	Personalization device serial number	99 max	Var	A,N,S	Free format.

6.13 DATA GROUP 13 - Optional Details(s) (OPTIONAL)

Data Elements combining to form Data Group 13 (DG13) are at the discretion of the Issuing State or organization and SHALL be as follows;

Table 53: Data Group 13 Tags

Tag	L	Value
'6D'	Var	

6.13.1 DATA GROUP 13 – EF.DG13 Data Elements

Data Elements and their format within Data Group 13 are at the discretion of the Issuing State

6.14 DATA GROUP 14 - Security Options (CONDITIONAL)

Data Group contains security options for additional security mechanisms. For details see Doc 9303-11..

Table 54: Data Group 14 Tags

Tag	L	Value
6 ^E	Var	Refer to Doc 9303-10 Data Group 14 SecurityInfos

6.14.1 DATA GROUP14 – EF.DG14 Data Elements

This section describes the Data Elements that may be present in Data Group 14 (DG14). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 55: Data Elements for DG14

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
	O	SecurityInfos		Var	B	Refer to Doc 9303-10 Data Group 14 SecurityInfos as defined in 6.14.2

6.14.2 DATA GROUP 14 SecurityInfos

The following generic ASN.1 data structure SecurityInfos allows various implementations of security options for secondary biometrics. For interoperability reasons, it is RECOMMENDED that this data structure be provided by the eMRTD chip in DG14 to indicate supported security protocols. The data structure is specified as follows:

```

SecurityInfos ::= SET of SecurityInfo

SecurityInfo ::= SEQUENCE {
    protocol          OBJECT IDENTIFIER,
    requiredData     ANY DEFINED BY protocol,
    optionalData     ANY DEFINED BY protocol OPTIONAL
}
    
```

The elements contained in a SecurityInfo data structure have the following meaning:

- The object identifier protocol identifies the supported protocol;
- The open type requiredData contains protocol specific mandatory data;
- The open type optionalData contains protocol specific optional data.

6.15 DATA GROUP 15 - Active Authentication Public Key Info (CONDITIONAL)

This OPTIONAL Data Group contains the Active Authentication Public Key and is REQUIRED when implementing the optional Active Authentication chip authentication as described in Doc 9303-11.

Table 56: Data Group 15 Tags

Tag	L	Value
6F	var	Refer to Doc 9303-11

6.15.1 DATA GROUP 15 – EF.DG15 Data Elements

This section describes the Data Elements that may be present in Data Group 15 (DG15). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 57: Data Elements for DG15

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
	O	ActiveAuthenticationPublicKeyInfo		Var	B	See Doc 9303-11

6.16 DATA GROUP 16 - Person(s) to Notify (OPTIONAL)

This Data Group lists emergency notification information. It is encoded as a series of templates using the Tag 'Ax' designation. DG16 (as all other Data Groups) should not be updated after issuance; DG16 is represented by a hash value in the SO_D and the SO_D is only signed once at issuance.

Table 58: Data Group 16 Tags

Tag	L	Value
70	Var	

Tag	L	Value		
		Tag	L	Value
		02	01	Number of templates (occurs only in first template)
		Ax	Var	Start of template, where x (x=1,2,3...) increments for each occurrence
5F50	04			Date data recorded
5F51	Var			Name of person
5F52	Var			Telephone
5F53	Var			Address

6.16.1 DATA GROUP 16 – EF.DG16 Data Elements

This section describes the Data Elements that may be present in Data Group 16 (DG16). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 59: Data Elements for DG16

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M, if DG 16 included	Number of persons identified	2	F	N	Identifies number of persons included in the Data Group.
02	M, if DG 16 included	Date details recorded	8	F	N	Date notification date recorded; Format = CCYYMMDD.
03	M, if DG 16 included	Name of person to notify Primary and secondary identifiers		Var	B	Filler characters (<) inserted as per MRZ. Truncation not permitted.
04	M, if DE 03 included	Telephone number of person to notify		Var	N,S	Telephone number in international form (country code and local number).
05	M	Address of person to notify		Var	B	Free-form text.

A.3 EF.DG2 to EF.DG2 Biometric Templates

DG2 to DG4 use the nested off-card option of [ISO/IEC 7816-11] for having the possibility to store multiple biometric templates of a kind, which are in harmony with the Common Biometric Exchange File Format (CBEFF), [NISTR 6529a]. The biometric sub-header defines the type of biometric that is present and the specific biometric feature

Example: One signed, facial biometric with the biometric data block length of 12 642 bytes ('3162' bytes), encoded using a device with a PID of '00 01 00 01', using format type '00 04' owned by template provider '00 0A' was captured on 15 March 2002 (no UTC offset) and is valid from 1 April 2002 through 31 March 2007. ICAO patron template Version 1.0 is being used.

The total length of the template is 12 704 bytes. The template is stored starting at the beginning of EF.DG2 (SFID 02).

```
'75' '82319EC'
  '7F61' '823199'
    '02' '01' '01'
    '7F60' '823191'
      'A1' '26'
        '80' '02' '0101'
        '81' '01' '02'
        '83' '07' '20020315133000'
        '85' '08' '2002040120070331'
        '86' '04' '00010001'
        '87' '02' '000A'
        '88' '02' '0004'
    '5F2E' '823162' '... 12642 bytes of biometric data ...'
```

A.4 EF.DG5 to EF.DG7 Displayed Image Templates

Note 1: one EF for each DG

Example: Image template with the displayed image data length of 2 000 bytes. The length of the template is 2 008 bytes ('07D8').

```
'65' '8207D8'
  '02' '01' '1'
  '5F40' '8207D0' '....2000 bytes of image data ...'
```

A.5 EF.DG11 Additional Personal Details

The following example shows the following personal details: Full name (John J Smith), Place of birth (Anytown, MN), Permanent address (123 Maple Rd, Anytown, MN), Telephone number 1-612-555-1212 and Profession (Travel Agent). The length of the template is 99 bytes ('63').

```
'6B' '63'
  '5C' '0A' '5F0E' '5F11' '5F42' '5F12' '5F13'
  '5F0E' '0D' SMITH<<JOHN<J
  '5F11' '0A' ANYTOWN<MN
  '5F42' '17' 123 MAPLE RD<ANYTOWN<MN
  '5F12' '0E' 1-612-555-1212
  '5F13' '0C' TRAVEL<AGENT
```

A.6 EF.DG12 Additional Document Details

The following example contains the Issuing Authority (United States of America), the date of issue (31 May 2002), one other person included on the document (Brenda P Smith). The length of the template is 64 bytes ('40').

'6C' '45'

'5C' '06' '5F19' '5F26' '5F1A'
 '5F19' '18' UNITED STATES OF AMERICA
 '5F26' '08' 20020531
 '0A' '15'
 '02' '01' '01'
 '5F1A' '0F' SMITH<<BRENDA<P

A.7 EF.DG16 Person(s) To Notify

Example with two entries: Charles R Smith of Anytown, MN and Mary J Brown of Ocean Breeze, CA. The length of the template is 162 bytes ('A2').

'70' '81A2'

'02' '01' 2
 'A1' '4C'
 '5F50' '08' 20020101
 '5F51' '10' SMITH<<CHARLES<R
 '5F52' '0B' 19525551212
 '5F53' '1D' 123 MAPLE RD<ANYTOWN<MN<55100
 'A2' '4F'
 '5F50' '08' 20020315
 '5F51' '0D' BROWN<<MARY<J
 '5F52' '0B' 14155551212
 '5F53' '23' 49 REDWOOD LN<OCEAN BREEZE<CA<94000

REFERENCES (NORMATIVE)

- [ISO/IEC 14443-1] ISO/IEC 14443-1:2008, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1: Physical Characteristics*
- [ISO/IEC 14443-1/Amd 1] ISO/IEC 14443-1:2008/Amd 1:2012, *Additional PICC classes*
- [ISO/IEC 14443-2] ISO/IEC 14443-2:2010, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio Frequency Power and Signal Interface*
- [ISO/IEC 14443-2/Amd 1] ISO/IEC 14443-2:2010/Amd 1:2011, *Limits of electromagnetic disturbance levels parasitically generated by the PICC*
- [ISO/IEC 14443-2 /Amd 2] ISO/IEC 14443-2:2010/Amd 2:2012, *Additional PICC classes*
- [ISO/IEC 14443-2 /Amd 3] ISO/IEC 14443-2:2010/Amd 3:2012, *Bits rates of fc/8, fc/4 and fc/2*
- [ISO/IEC 14443-3] ISO/IEC 14443-3:2011, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and Anticollision*
- [ISO/IEC 14443-3 /Amd 1] ISO/IEC 14443-3:2011/Amd 1:2011, *Electromagnetic disturbance handling and single-size unique identifier*
- [ISO/IEC 14443-3 /Amd 2] ISO/IEC 14443-3:2011/Amd 2:2012, *Bit rates of fc/8, fc/4 and fc/2, frame size from 512 bytes to 4 096 bytes and minimum TR0*
- [ISO/IEC 14443-4] ISO/IEC 14443-4:2008, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol*
- [ISO/IEC 14443-4 /Amd 1] ISO/IEC 14443-4:2008/Amd 1:2012, *Exchange of additional parameters*
- [ISO/IEC 14443-4 /Amd 2] ISO/IEC 14443-4:2008/Amd 2:2012, *Bit rates of fc/8, fc/4 and fc/2, protocol activation of PICC Type A and frame size from 512 bytes to 4 096 bytes*
- [ISO/IEC 10373-6] ISO/IEC 10373-6:2011, *Identification cards – Test methods – Part 6: Proximity cards*
- [ISO/IEC 10373-6 /Amd 1] ISO/IEC 10373-6:2011/Amd 1:2012, *Additional PICC classes*
- [ISO/IEC 10373-6 /Amd 2] ISO/IEC 10373-6:2011/Amd 2:2012, *Test methods for electromagnetic disturbance*
- [ISO/IEC 10373-6 /Amd 3] ISO/IEC 10373-6:2011/Amd 3:2012, *Exchange of additional parameters, block numbering, unmatched AFI and TR2*
- [ISO/IEC 10373-6 /Amd 4] ISO/IEC 10373-6:2011/Amd 4:2012, *Bit rates of fc/8, fc/4 and fc/2 and frame size from 512 to 4096 bytes*
- [ISO/IEC 10373-6 /Amd 7] ISO/IEC 10373-6:2011/Amd 7:2010, *Identification cards – Test methods – Part 6: Proximity cards – Test methods for ePassport Readers*
- [ISO/IEC 7816-2] ISO/IEC 7816-2: 2007, *Identification cards – Integrated Circuit cards – Part 2: Cards with contacts – Dimensions and location of the contacts*
- [ISO/IEC 7816-4] ISO/IEC 7816-4: 2013, *Identification cards – Integrated Circuit cards – Part 4: Organization, security and commands for interchange*
- [ISO/IEC 7816-5] ISO/IEC 7816-5: 2004, *Identification cards – Integrated Circuit cards – Part 5: Registration of application providers*
- [ISO/IEC 7816-6] ISO/IEC 7816-6: 2004, *Identification cards – Integrated Circuit cards – Part 6: Interindustry data elements for interchange (Defect report included)*
- [ISO/IEC 7816-11] ISO/IEC 7816-11: 2004, *Identification cards – Integrated Circuit cards – Part 11: Personal verification through biometric methods*
- [ISO/IEC 8825-1] ISO/IEC 8825-1:2008, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguishing Encoding Rules (DER)*
- [ISO/IEC 19794-4] ISO/IEC 19794-4:2011, *Information technology -- Biometric data interchange formats -- Part 4: Finger image data*
- [ISO/IEC 19794-5] ISO/IEC 19794-5:2011, *Information technology -- Biometric data interchange formats -- Part 5: Face image data*
- [ISO/IEC 10646] ISO/IEC 10646:2012, *Information technology – Universal Coded Character Set (UCS)*
- [RFC 3369] Cryptographic Message Syntax 2002
- [ISO/IEC 10918-1] ISO/IEC 10918-1:1994, *Information technology -- Digital compression and coding of continuous-tone still images: Requirements and guidelines*
- [ISO/IEC 15444] ISO/IEC 15444-n, *JPEG 2000 image coding system*
- [ISO/IEC 19785] ISO/IEC 19785-n, *Information technology -- Common Biometric Exchange Formats Framework*

Doc 9303



Machine Readable Travel Documents

Part 11
Security Mechanisms for Machine Readable Travel Documents

Approved by the Secretary General
and published under his authority

Seventh Edition — Revision 1 — 2014

International Civil Aviation Organization

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

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

Doc 9303, Machine Readable Travel Documents
ISBN xxx-xx-xxxx-xxx-x

© ICAO 2014

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 TO DOC 9303-11, 7TH EDITION

Revision	Date	Description
01	xx-xx-2014	Initial release of the 7 th edition

DRAFT_4 FOR TAG_22

TABLE OF CONTENTS

1	SCOPE	6
2	ASSUMPTIONS AND NOTATIONS	7
2.1	Notations.....	7
3	SECURING ELECTRONIC DATA	8
4	ACCESS TO THE CONTACTLESS IC	10
4.1	Compliant Configurations.....	10
4.2	Chip Access Procedure.....	11
4.3	Basic Access Control	12
4.4	Password Authenticated Connection Establishment	14
5	AUTHENTICATION OF DATA	22
5.1	Passive Authentication.....	22
6	AUTHENTICATION OF THE CONTACTLESS IC	24
6.1	Active Authentication.....	24
7	ADDITIONAL ACCESS CONTROL MECHANISMS	27
7.1	Extended Access Control for Additional Biometrics.....	27
7.2	Encryption of Additional Biometrics	27
8	INSPECTION SYSTEM	28
8.1	Basic Access Control	28
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
9	COMMON SPECIFICATIONS	30
9.1	Information on Supported Protocols	30
9.2	Public Key Data Objects	33
9.3	Standardized Domain Parameters.....	34
9.4	Key Agreement Algorithms	35
9.5	Key Derivation Mechanism	35
9.6	Secure Messaging	36
APPENDIX A	ENTROPY OF MRZ-DERIVED ACCESS KEYS (INFORMATIVE)	41
APPENDIX B	POINT ENCODING FOR THE ECDH-INTEGRATED MAPPING (INFORMATIVE)	42
B.1	High-level Description of the Point Encoding Method.....	42
B.2	Implementation for Affine Coordinates.....	42
B.3	Implementation for Jacobian Coordinates	43
APPENDIX C	WORKED EXAMPLE: BASIC ACCESS CONTROL (INFORMATIVE)	44
C.1	Compute Keys from Key Seed (K_{seed}).....	44
C.2	Derivation of Document Basic Access Keys (K_{Enc} and K_{MAC})	45
C.3	Authentication and Establishment of Session Keys.....	46
C.4	Secure Messaging	48
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

F.1 ECDH based example..... 55
F.2 DH based example..... 62
APPENDIX G WORKED EXAMPLE: PACE – INTEGRATED MAPPING (INFORMATIVE)..... 70
G.1 ECDH based example..... 70
G.2 DH based example..... 72
REFERENCES (NORMATIVE)..... 75

DRAFT_4 FOR TAG_22

1 SCOPE

The seventh edition of Doc 9303 represents a restructuring of the ICAO specifications for Machine Readable Travel Documents. Without incorporating substantial modifications of the specifications, in this new edition Doc 9303 has been reformatted into a set of specifications for Size 1 Machine Readable Official Travel Document (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 11 of Doc 9303 is based on Doc 9303 Part 1 Machine Readable Passports, Volume 2 Specifications for Electronically Enabled with Biometric Identification Capability, Sixth edition – 2006 and Doc 9303 Part 3 Machine Readable Official Travel Documents, Volume 2 Specifications for Electronically Enabled MRTDs with Biometric Identification Capability, Third edition – 2008.

This Part 11 provides specifications to enable States and suppliers to implement cryptographic security features for electronic machine readable travel documents (“eMRTDs”) offering contactless IC read-only access. Cryptographic protocols are specified to:

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

Additional access control to sensitive data (i.e. secondary biometrics) is not specified in this edition of Doc 9303, but national schemes to protect these data are allowed. An interoperable specification is foreseen for future editions of Doc 9303.

The authentication of the data stored on the contactless IC is the basic security feature to enable the use of the IC for manual and/or automated inspection. This feature is therefore **REQUIRED**.

Implementation of a protocol to prevent skimming of the data stored on the contactless IC and to prevent eavesdropping on the communication between IC and terminal is **RECOMMENDED**.

Implementation of the other protocols is **OPTIONAL**, allowing the Issuing State or organization to decide on the necessary set of security features according to national regulations/demands.

This Part should be read in conjunction with the following Parts of Doc 9303:

- Part 1 – Introduction;
- Part 10 – Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless IC; and
- Part 12 – Public Key Infrastructure for Machine Readable Travel Documents.

2 ASSUMPTIONS AND NOTATIONS

It is assumed that the reader of this document is familiar with the concepts and mechanisms offered by public key cryptography and public key infrastructures.

Whilst the use of public key cryptography techniques adds some complexity to the implementation of eMRTDs, such techniques add value in that they will provide front-line border control points with an additional measure to determine the authenticity of the eMRTD. It is assumed that the use of such a technique is not the sole measure for determining authenticity and it SHOULD NOT be relied upon as a single determining factor.

In the event that the data from the contactless IC cannot be used, for instance as a result of a certificate revocation or an invalid signature verification, or if the contactless IC was left intentionally blank (see Doc 9303-10), the eMRTD is not necessarily invalidated. In such cases a receiving State MAY rely on other document security features for validation purposes.

2.1 Notations

The following notations are used to denote cryptographic primitives in an algorithm independent way:

- Encryption of clear text S with symmetric key K : $E(K, S)$;
- Decryption of cipher text C with symmetric key K : $D(K, C)$;
- Computing a Message Authentication Code with symmetric key K over message M : $MAC(K, M)$;
- Key agreement based on asymmetric key pairs (SK, PK) and (SK', PK') and domain parameters D : $KA(SK, PK', D) / KA(SK', PK, D)$;
- Key derivation from a shared secret S : $KDF(S)$.

3 SECURING ELECTRONIC DATA

Besides Passive Authentication by digital signatures, States MAY choose additional security, using more complex ways of securing the contactless IC and its data.

Accessing an eMRTD comprises the following steps:

1. Gain access to the contactless IC of the eMRTD (section 4)
2. Authentication of Data (section 5)
3. Authentication of the Chip (section 6)
4. Additional Access Control Mechanisms (section 7)
5. Reading Data (see Doc 9303-10)

Different protocols are available for the different steps. The exact configuration of an eMRTD is chosen by the Issuing State or organization. The options given in *Table 1* can be suitably combined to achieve additional security according to the requirements of Issuers.

Table 1: Securing Electronic Data (Summary)

Method	Contact-less IC	Inspection System	Benefits	Note
BASELINE SECURITY METHOD				
Passive Authentication (Section 5.1)	m	m	Proves that the contents of the SO _D and the LDS are authentic and not changed.	Does not prevent an exact copy or IC substitution. Does not prevent unauthorized access. Does not prevent skimming.
ADVANCED SECURITY METHODS				
Comparison of conventional MRZ(OCR-B) and IC-based MRZ(LDS)	n/a	o	Proves that contactless IC's content and physical eMRTD belong together.	Adds (minor) complexity. Does not prevent an exact copy of contactless IC and conventional document.
Active Authentication (Section 6.1)	o	o	Prevents copying the SO _D and proves that it has been read from the authentic contactless IC. Proves that the contactless IC has not been substituted.	Does not prevent unauthorized access. Adds complexity.
Basic Access Control (BAC) (Section 4.3)	r/c (see also 4.1)	m (see also 4.1)	Prevents skimming and misuse. Prevents eavesdropping on the communications between eMRTD and inspection system (when used to set up encrypted session channel).	Does not prevent an exact copy or IC substitution (requires also copying of the conventional document). Adds complexity.
Password Authenticated Connection Establishment (PACE) (Section 4.4)	r (see also 4.1)	r (see also 4.1)		
Extended Access Control (Section 7.1)	o	o	Prevents unauthorized access to additional biometrics. Prevents skimming of	Requires additional key management. Does not prevent an exact copy or IC substitution

Method	Contact-less IC	Inspection System	Benefits	Note
			additional biometrics.	(requires also copying of the conventional document). Adds complexity.
Data Encryption (Section 7.2)	o	o	Secures additional biometrics. Does not require processor-ICs.	Requires complex decryption key management. Does not prevent an exact copy or IC substitution. Adds complexity.
m = REQUIRED, r = RECOMMENDED, o = OPTIONAL, c = CONDITIONAL, n/a = not applicable.				

Note: See section 4 for details on compliant configurations of contactless ICs with respect to the implementation of Basic Access Control and Password Authenticated Connection Establishment.

Implementation of advanced security methods as listed in *Table 1* does not affect ICAO compliance.

4 ACCESS TO THE CONTACTLESS IC

Adding a contactless IC without access control to a MRTD introduces two new attack possibilities:

- the data stored in the contactless IC can be electronically read without authorizing this reading of the document (skimming); and
- the unencrypted communication between a contactless IC and a reader can be eavesdropped within a distance of several metres.

While there are physical measures possible against skimming (e.g. shielding using a metal mesh in the cover of a passport booklet), these do not address eavesdropping. Therefore, it is understood that Issuing States or organizations SHOULD choose to implement a Chip Access Control mechanism, i.e. an access control mechanism that in effect requires the knowledge of the bearer of the eMRTD that the data stored in the contactless IC is being read in a secure way. This Chip Access Control mechanism prevents skimming as well as eavesdropping.

A contactless IC that is protected by a Chip Access Control mechanism denies access to its contents unless the inspection system can prove that it is authorized to access the contactless IC. This proof is given in a cryptographic protocol, where the inspection system proves knowledge of the information derived from the data page.

The inspection system MUST be provided with this information prior to being able to read the contactless IC. The information has to be retrieved optically/visually from the eMRTD (e.g. from the MRZ). It also MUST be possible for an inspector to enter this information manually in the inspection system in case machine-reading of the information is not possible.

Assuming that the information from the data page cannot be obtained from an unviewed document (e.g. since they are derived from the optically read MRZ), it is accepted that the eMRTD was knowingly handed over for inspection. Due to the encryption of the channel, eavesdropping on the communication would require a considerable effort.

This section defines two mechanisms for Chip Access Control:

- Basic Access Control (BAC, section 4.3), which is purely based on symmetric cryptography; and
- Password Authenticated Connection Establishment (PACE, section 4.4), which employs asymmetric cryptography to provide higher entropy session keys.

See also APPENDIX A for additional information on the strength of session keys.

4.1 Compliant Configurations

The following configurations are compliant to this specification:

- eMRTD chips implementing no Chip Access Control (“plain eMRTDs”);
- eMRTD chips implementing BAC only;
- eMRTD chips implementing PACE *and* BAC;
- Starting 01/01/2018, eMRTD chips implementing PACE only.

Note: For global interoperability, States MUST NOT implement PACE without implementing Basic Access Control until 31/12/2017. Inspection Systems SHOULD implement and use PACE if provided by the eMRTD chip.

BAC may become deprecated in the future. In this case PACE will become the default access control mechanism.

Compliant inspection systems MUST support all compliant eMRTD configurations. If an eMRTD supports both PACE and BAC, the inspection system SHALL use either BAC or PACE but not both in the same session.

4.2 Chip Access Procedure

The chip access procedure to authenticate the inspection system consists of the following steps. If PACE is not supported by the inspection system, steps 1 and 2 are skipped.

Step 1. Read EF.CardAccess

If PACE is supported by the eMRTD, the eMRTD chip MUST provide the parameters to be used for PACE in the file EF.CardAccess.

If EF.CardAccess is available, the inspection system SHALL read the file EF.CardAccess (cf. Section 9.1.5) to determine the parameters (i.e. symmetric ciphers, key agreement algorithms, domain parameters, and mappings) supported by the eMRTD chip. The inspection system may select any of those parameters.

If the file EF.CardAccess is not available or does not contain parameters for PACE, the inspection system SHOULD try to read the eMRTD with Basic Access Control (skip to Step 4).

Step 2. PACE

(CONDITIONAL)

This step is RECOMMENDED if PACE is supported by the eMRTD chip.

- The inspection system SHOULD derive the key K_{π} from the MRZ. It MAY use the CAN instead of the MRZ if the CAN is known to the inspection system.
- The eMRTD chip SHALL accept the MRZ as passwords for PACE. It MAY additionally accept the CAN.
- The inspection system and the eMRTD chip mutually authenticate using K_{π} and derive session keys K_{SEnc} and K_{SMAC} .

If successful, the eMRTD chip performs the following:

- It SHALL start Secure Messaging.
- It SHALL grant access to less-sensitive data (e.g. DG1, DG2, DG14, DG15, etc. and the Document Security Object – for the definition of “sensitive data” see Doc 9303-1).
- It SHALL restrict access rights to require Secure Messaging.

Step 3. Select eMRTD Application

(REQUIRED)

Step 4. Basic Access Control

(CONDITIONAL)

This step is REQUIRED if Chip Access Control is enforced by the eMRTD chip and PACE has not been used. If PACE was successfully performed or if the eMRTD does not enforce Chip Access Control, this step is skipped.

- The inspection system SHOULD derive the Document Basic Access Keys (K_{Enc} and K_{MAC}) from the MRZ.

- The inspection system and the eMRTD chip mutually authenticate using the Document Basic Access Keys and derive session keys KS_{Enc} and KS_{MAC} .

If successful, the eMRTD chip performs the following:

- It SHALL start Secure Messaging.
- It SHALL grant access to less-sensitive data (e.g. DG1, DG2, DG14, DG15, etc. and the Document Security Object).
- It SHALL restrict access rights to require Secure Messaging.

The inspection system MUST verify the authenticity of the contents of the file EF.CardAccess (see above) using DG14.

4.3 Basic Access Control

4.3.1 Protocol Specification

Authentication and Key Establishment is provided by a three pass challenge-response protocol according to [ISO/IEC 11770-2] Key Establishment Mechanism 6 using 3DES [FIPS 46-3] as block cipher. A cryptographic checksum according to [ISO/IEC 9797-1] MAC Algorithm 3 is calculated over and appended to the ciphertexts. The modes of operation described in section 4.3.3 MUST be used. Exchanged nonces MUST be of size 8 bytes, exchanged keying material MUST be of size 16 bytes. The IFD and the contactless IC MUST NOT use distinguishing identifiers as nonces.

In more detail, IFD and IC SHALL perform the following steps:

- 1) The IFD requests a challenge RND.IC by sending the GET CHALLENGE command. The IC generates and responds with a nonce RND.IC.
- 2) The IFD performs the following operations:
 - a) Generate a nonce RND.IFD and keying material K.IFD.
 - b) Generate the concatenation $S = \text{RND.IFD} \parallel \text{RND.IC} \parallel \text{K.IFD}$.
 - c) Compute the cryptogram $E_{IFD} = E(K_{Enc}, S)$.
 - d) Compute the checksum $M_{IFD} = \text{MAC}(K_{MAC}, E_{IFD})$.
 - e) Send an EXTERNAL AUTHENTICATE command with mutual authenticate function using the data $E_{IFD} \parallel M_{IFD}$.
- 3) The IC performs the following operations:
 - a) Check the checksum M_{IFD} of the cryptogram E_{IFD} .
 - b) Decrypt the cryptogram E_{IFD} .
 - c) Extract RND.IC from S and check if IFD returned the correct value.
 - d) Generate keying material K.IC.
 - e) Generate the concatenation $R = \text{RND.IC} \parallel \text{RND.IFD} \parallel \text{K.IC}$.
 - f) Compute the cryptogram $E_{IC} = E(K_{Enc}, R)$.
 - g) Compute the checksum $M_{IC} = \text{MAC}(K_{MAC}, E_{IC})$.
 - h) Send the response using the data $E_{IC} \parallel M_{IC}$.
- 4) The IFD performs the following operations:
 - a) Check the checksum M_{IC} of the cryptogram E_{IC} .
 - b) Decrypt the cryptogram E_{IC} .
 - c) Extract RND.IFD from R and check if IC returned the correct value.
- 5) The IFD and the IC derive session keys KS_{Enc} and KS_{MAC} using the key derivation mechanism described in section 9.5.4 with $(K.IC \text{ xor } K.IFD)$ as key seed..

4.3.2 Inspection Process

When an eMRTD with Basic Access Control is offered to the inspection system, optically or visually read information is used to derive the Document Basic Access Keys (K_{Enc} and K_{MAC}) to gain access to the

contactless IC and to set up a secure channel for communications between the eMRTD's contactless IC and the inspection system.

An eMRTD's contactless IC that supports Basic Access Control MUST respond to unauthenticated read attempts, i.e. read attempts sent without Secure Messaging (including selection of (protected) files in the LDS), with "Security status not satisfied" (0x6982) once the Secure Channel is established. If the IC receives a plain SELECT, i.e. without Secure Messaging applied, in the Secure Channel, the IC SHALL abort the Secure Channel. When a plain SELECT is sent before the Secure Channel is established, or when the Secure Channel has been aborted, both 0x6982 and 0x9000 MAY be returned by the IC, i.e. are ICAO compliant responses.

To authenticate the inspection system the following steps MUST be performed:

- 1) The inspection system reads the "MRZ_information". The "MRZ_information" consists of the concatenation of Document Number, Date of Birth and Date of Expiry, including their respective check digits, as described in Doc 9303-4, Doc 9303-5 or Doc 9303-6 for document form factors TD3, TD1 and TD2, respectively, from the MRZ using an OCR-B reader. Alternatively, the required information can be typed in; in this case it SHALL be typed in as it appears in the MRZ. The most significant 16 bytes of the SHA-1 hash of this "MRZ_information" are used as key seed to derive the Document Basic Access Keys using the key derivation mechanism described in section 9.5.2.
- 2) The inspection system and the eMRTD's contactless IC mutually authenticate and derive session keys. The authentication and key establishment protocol described above MUST be used.
- 3) After a successful execution of the authentication protocol both the IFD and the IC compute session keys K_{SEnc} and K_{SMAC} using the key derivation mechanism described in section 9.5.4 with $(K.IC \text{ xor } K.IFD)$ as key seed. All subsequent communication MUST be protected by Secure Messaging as described in section 9.6.

4.3.3 Cryptographic Specifications

4.3.3.1 Encryption of Challenge and Response

Two key 3DES in CBC mode with zero IV (i.e. 0x00 00 00 00 00 00 00 00) according to [ISO/IEC 11568-2] SHALL be used for computation of E_{IFD} and E_{IC} . Padding for the input data MUST NOT be used when performing the EXTERNAL AUTHENTICATE command.

4.3.3.2 Authentication of Challenge and Response

The cryptographic checksums M_{IFD} and M_{IC} SHALL be calculated using [ISO/IEC 9797-1] MAC algorithm 3 with block cipher DES, zero IV (8 bytes), and [ISO/IEC 9797-1] padding method 2. The MAC length MUST be 8 bytes.

4.3.4 Application Protocol Data Units

Basic Access Control is performed using the commands GET CHALLENGE and EXTERNAL AUTHENTICATE with mutual authenticate function. The commands SHALL be encoded as specified in [ISO/IEC 7816-4].

4.3.4.1 GET CHALLENGE

Command		
CLA		Context specific
INS	0x84	GET CHALLENGE
P1/P2	0x0000	--
Data		<i>Absent</i>

Response		
Data	Random Nonce	
Status Bytes	0x9000	<i>Normal processing</i> Random Nonce successfully generated and transmitted
	Other	<i>Operating system dependent error</i> Nonce could not be returned

4.3.4.2 EXTERNAL AUTHENTICATE

Command			
CLA		Context specific	
INS	0x82	EXTERNAL AUTHENTICATE	
P1/P2	0x0000	--	
Data		Command data $E_{IFD} M_{IFD}$	REQUIRED
Response			
Data		Response data $E_{IC} M_{IC}$	REQUIRED
Status Bytes	0x9000	<i>Normal processing</i> The protocol has been performed successfully.	
	Other	<i>Operating system dependent error</i> The protocol failed.	

4.4 Password Authenticated Connection Establishment

PACE is a password authenticated Diffie-Hellman key agreement protocol that provides secure communication and password-based authentication of the eMRTD chip and the inspection system (i.e. eMRTD chip and inspection system share the same password π).

PACE establishes Secure Messaging between an eMRTD chip and an inspection system based on weak (short) passwords. It enables the eMRTD chip to verify that the inspection system is authorized to access stored data and has the following features:

- Strong session keys are provided independent of the strength of the password.
- The entropy of the password(s) used to authenticate the inspection system can be very low (e.g. 6 digits are sufficient in general).

PACE uses keys K_{π} derived from passwords with a key derivation function \mathbf{KDF}_{π} (cf. section 9.5.3). For globally interoperable machine readable travel documents the following two passwords and corresponding keys are available:

- **MRZ:** The key K_{π} defined by $K_{\pi} = \mathbf{KDF}_{\pi}(\text{MRZ})$ is REQUIRED. It is derived from the Machine Readable Zone (MRZ) similar to Basic Access Control, i.e. the key is derived from the Document Number, the Date of Birth and the Date of Expiry.
- **CAN:** The key K_{π} defined by $K_{\pi} = \mathbf{KDF}_{\pi}(\text{CAN})$ is OPTIONAL. It is derived from the Card Access Number (CAN). The CAN is a number printed on the *front side* of the datapage.

Note: In contrast to the MRZ (Document Number, Date of Birth, Date of Expiry) the CAN has the advantage that it can easily be typed in manually.

4.4.1 Protocol Specification

The inspection system reads the parameters for PACE supported by the eMRTD chip from the file EF.CardAccess (cf. Section 9.1.5) and selects the parameters to be used, followed by the protocol execution.

The following commands SHALL be used:

- READ BINARY as specified in Doc 9303-10;
- MSE:SET AT (MANAGE SECURITY ENVIRONMENT command with SET Authentication Template function) as specified in Section 4.4.4.1;
- The following steps SHALL be performed by the inspection system and the eMRTD chip using a chain of General Authenticate commands as specified in Section 4.4.4.2:
 - 1) The eMRTD chip randomly and uniformly chooses a nonce s , encrypts the nonce to $z = \mathbf{E}(K_\pi, s)$, where $K_\pi = \mathbf{KDF}_\pi(\pi)$ is derived from the shared password π , and sends the ciphertext z to the inspection system.
 - 2) The inspection system recovers the plaintext $s = \mathbf{D}(K_\pi, z)$ with the help of the shared password π .
 - 3) Both the eMRTD chip and the inspection system perform the following steps:
 - a) They exchange additional data required for the mapping of the nonce:
 - i. For the generic mapping the eMRTD chip and the inspection system exchange ephemeral key public keys.
 - ii. For the integrated mapping the inspection system sends an additional nonce to the eMRTD chip.
 - b) They compute the ephemeral domain parameters $D = \mathbf{Map}(D_{IC}, s, \dots)$ as described in Section 4.4.3.3.
 - c) They perform an anonymous Diffie-Hellman key agreement (cf. section 9.4) based on the ephemeral domain parameters and generate the shared secret $K = \mathbf{KA}(SK_{IC}, PK_{PCD}, D) = \mathbf{KA}(SK_{PCD}, PK_{IC}, D)$.
 - d) During Diffie-Hellman key agreement, the IC and the inspection system SHOULD check that the two public keys PK_{IC} and PK_{PCD} differ.
 - e) They derive session keys $KS_{MAC} = \mathbf{KDF}_{MAC}(K)$ and $KS_{Enc} = \mathbf{KDF}_{Enc}(K)$ as described in Section 9.5.1.
 - f) They exchange and verify the authentication token $T_{PCD} = \mathbf{MAC}(KS_{MAC}, PK_{IC})$ and $T_{IC} = \mathbf{MAC}(KS_{MAC}, PK_{PCD})$ as described in Section 4.4.3.4.

A simplified version of the protocol is also shown in the figure below.

IC (chip)		PCD (Inspection system)
Static domain parameters D_{IC}		
Choose random nonce s		
Compute $z = \mathbf{E}(K_\pi, s)$	$\leftarrow z \rightarrow$	
	\leftarrow additional data for Map \rightarrow	Compute $s = \mathbf{D}(K_\pi, z)$
$D = \mathbf{Map}(D_{IC}, s, \dots)$		$D = \mathbf{Map}(D_{IC}, s, \dots)$
Choose random ephemeral key pair (SK_{IC}, PK_{IC}, D)	$\leftarrow PK_{IC}, PK_{PCD} \rightarrow$	Choose random ephemeral key pair (SK_{PCD}, PK_{PCD}, D)
Check $PK_{IC} \neq PK_{PCD}$		Check $PK_{IC} \neq PK_{PCD}$
$K = \mathbf{KA}(SK_{IC}, PK_{PCD}, D)$		$K = \mathbf{KA}(SK_{PCD}, PK_{IC}, D)$
Compute $T_{IC} = \mathbf{MAC}(KS_{MAC}, PK_{PCD})$	$\leftarrow T_{IC}, T_{PCD} \rightarrow$	Compute $T_{PCD} = \mathbf{MAC}(KS_{MAC}, PK_{IC})$

Verify T_{PCD} Verify T_{IC}

Figure 1: Password Authenticated Connection Establishment

4.4.2 Security Status

An eMRTD chip that supports PACE SHALL respond to unauthenticated read attempts (including selection of (protected) files in the LDS) with “Security status not satisfied” (0x6982).

Note: This specification is more restrictive than the corresponding specification for BAC-only eMRTDs.

If PACE was successfully performed then the eMRTD chip has verified the used password. Secure Messaging is started using the derived session keys KS_{MAC} and KS_{Enc} .

4.4.3 Cryptographic Specifications

This section contains the cryptographic details of the specification.

Particular algorithms are selected by the issuer of the eMRTD. The inspection system MUST support all combinations described in the following. The eMRTD chip MAY support more than one combination of algorithms.

4.4.3.1 DH

For PACE with DH the respective algorithms and formats from section 9.4 and the following table MUST be used.

Table 2: Algorithms and formats for DH

OID	Mapping	Sym. Cipher	Key-length	Secure Messaging	Auth. Token
id-PACE-DH-GM-3DES-CBC-CBC	Generic	3DES	112	CBC / CBC	CBC
id-PACE-DH-GM-AES-CBC-CMAC-128	Generic	AES	128	CBC / CMAC	CMAC
id-PACE-DH-GM-AES-CBC-CMAC-192	Generic	AES	192	CBC / CMAC	CMAC
id-PACE-DH-GM-AES-CBC-CMAC-256	Generic	AES	256	CBC / CMAC	CMAC
id-PACE-DH-IM-3DES-CBC-CBC	Integrated	3DES	112	CBC / CBC	CBC
id-PACE-DH-IM-AES-CBC-CMAC-128	Integrated	AES	128	CBC / CMAC	CMAC
id-PACE-DH-IM-AES-CBC-CMAC-192	Integrated	AES	192	CBC / CMAC	CMAC
id-PACE-DH-IM-AES-CBC-CMAC-256	Integrated	AES	256	CBC / CMAC	CMAC

4.4.3.2 ECDH

For PACE with ECDH the respective algorithms and formats from section 9.4 and the following table MUST be used.

Only prime curves with uncompressed points SHALL be used. The standardized domain parameters described in section 9.3 SHOULD be used.

Table 3: Algorithms and formats for ECDH

OID	Mapping	Sym. Cipher	Keylen	Secure Messaging	Auth. Token
id-PACE-ECDH-GM-3DES-CBC-CBC	Generic	3DES	112	CBC / CBC	CBC
id-PACE-ECDH-GM-AES-CBC-CMAC-128	Generic	AES	128	CBC / CMAC	CMAC

id-PACE-ECDH-GM-AES-CBC-CMAC-192	Generic	AES	192	CBC / CMAC	CMAC
id-PACE-ECDH-GM-AES-CBC-CMAC-256	Generic	AES	256	CBC / CMAC	CMAC
id-PACE-ECDH-IM-3DES-CBC-CBC	Integrated	3DES	112	CBC / CBC	CBC
id-PACE-ECDH-IM-AES-CBC-CMAC-128	Integrated	AES	128	CBC / CMAC	CMAC
id-PACE-ECDH-IM-AES-CBC-CMAC-192	Integrated	AES	192	CBC / CMAC	CMAC
id-PACE-ECDH-IM-AES-CBC-CMAC-256	Integrated	AES	256	CBC / CMAC	CMAC

4.4.3.3 Encrypting and Mapping Nonces

The eMRTD chip SHALL randomly and uniformly select the nonce s as a binary bit string of length l , where l is a multiple of the block size in bits of the respective block cipher $E()$ chosen by the eMRTD chip.

- The nonce s SHALL be encrypted in CBC mode according to [ISO/IEC 10116] using the key $K_\pi = \text{KDF}_\pi(\pi)$ derived from the password π and IV set to the all-0 string.
- The nonce s SHALL be converted to a random generator using an algorithm-specific mapping function **Map**.
- For the Integrated Mapping the additional nonce t SHALL be selected randomly and uniformly as a binary bit string of length k and sent in clear. In this case k is the key size in bits of the respective block cipher $E()$ and l SHALL be the smallest multiple of the block size of $E()$ such that $l \geq k$.

To map the nonce s or the nonces s, t into the cryptographic group either the generic mapping or the integrated mapping, respectively, SHALL be used.

ECDH Mapping

Let G and \hat{G} be the static and an ephemeral base point on the elliptic curve.

Generic Mapping

The function **Map**: $G \rightarrow \hat{G}$ is defined as $\hat{G} = s \times G + H$, where H in $\langle G \rangle$ is chosen such that $\log_G H$ is unknown. The point H SHALL be calculated by an anonymous Diffie-Hellman Key Agreement [TR-03111].

Note: The key agreement algorithm ECKA prevents small subgroup attacks by using compatible cofactor multiplication.

Integrated Mapping

The function **Map**: $G \rightarrow \hat{G}$ is defined as $\hat{G} = f_G(\mathbf{R}_p(s,t))$, where $\mathbf{R}_p()$ is a pseudo-random function that maps octet strings to elements of $GF(p)$ and $f_G()$ is a function that maps elements of $GF(p)$ to $\langle G \rangle$. The random nonce t SHALL be chosen randomly by the inspection system and sent to the eMRTD chip. The pseudo-random function $\mathbf{R}_p()$ is described below. The function $f_G()$ is defined in [BCIMRT2010]. An informative description is given in APPENDIX B.

DH Mapping

Let g and \hat{g} be the static and an ephemeral generator.

Generic Mapping

The function **Map**: $g \rightarrow \hat{g}$ is defined as $\hat{g} = g^s \times h$, where h in $\langle g \rangle$ is chosen such that $\log_g h$ is unknown. The group element h SHALL be calculated by an anonymous Diffie-Hellman Key Agreement.

Note: The public key validation method described in [RFC 2631] MUST be used to prevent small subgroup attacks.

Integrated Mapping

The function **Map**: $g \rightarrow \hat{g}$ is defined as $\hat{g} = f_g(R_p(s,t))$, where $R_p()$ is a pseudo-random function that maps octet strings to elements of $GF(p)$ and $f_g()$ is a function that maps elements of $GF(p)$ to $\langle g \rangle$. The random nonce t SHALL be chosen randomly by the inspection system and sent to the eMRTD chip. The pseudo-random function $R_p()$ is described below. The function $f_g()$ is defined as $f_g(x) = x^a \bmod p$, and $a = (p-1)/q$ is the cofactor. Implementations MUST check that $\hat{g} \neq 1$.

Pseudo-random Number Mapping

The function $R_p(s,t)$ is a function that maps octet strings s (of bit length l) and t (of bit length k) to an element $\text{int}(x_1 || x_2 || \dots || x_n) \bmod p$ of $GF(p)$. The function $R_p(s,t)$ is specified in the Figure below.

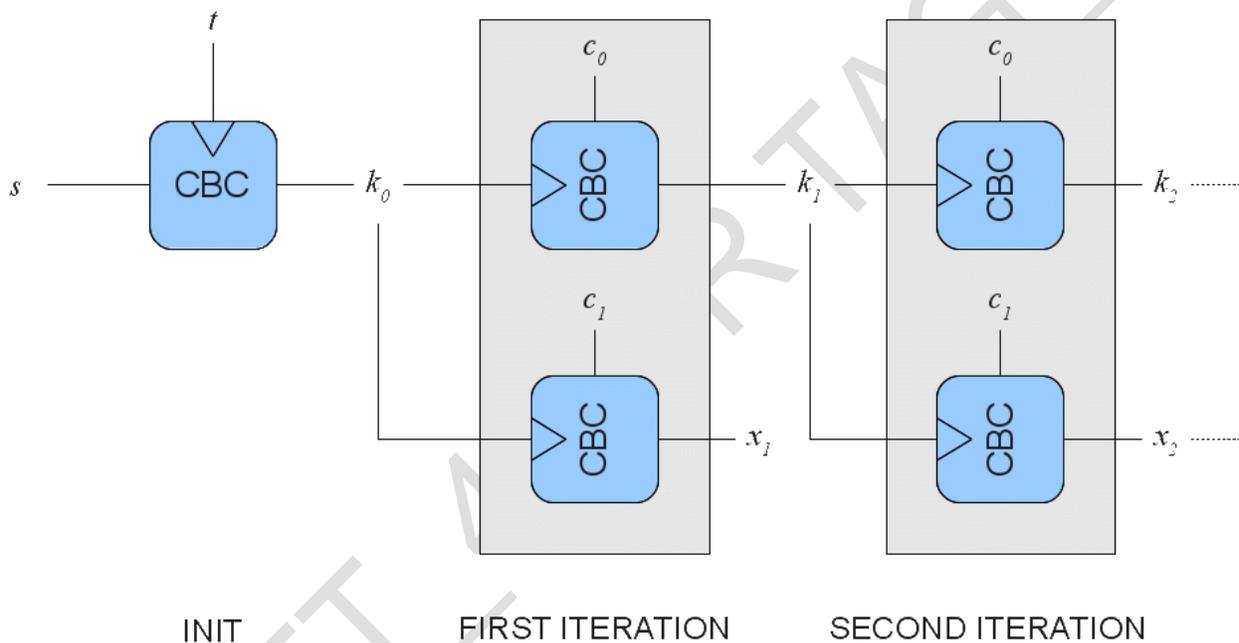


Figure 2: Pseudo-random number mapping

The construction is based on the respective block cipher $E()$ in CBC mode according to [ISO/IEC 10116] with $IV=0$, where k is the key size (in bits) of $E()$. Where required, the output k_i MUST be truncated to key size k . The value n SHALL be selected as smallest number, such that $n \cdot l \geq \log_2 p + 64$.

Note: The truncation is only necessary for AES-192: Use octets 1 to 24 of k_i ; additional octets are not used. In case of DES, k is considered to be equal to 128 bits, and the output of $R(s,t)$ shall be 128 bits.

The constants c_0 and c_1 are defined as follows:

- For 3DES and AES-128 ($l=128$):
 - $c_0=0xa668892a7c41e3ca739f40b057d85904$
 - $c_1=0xa4e136ac725f738b01c1f60217c188ad$
- For AES-192 and AES-256 ($l=192$):

- C₀=
0xd463d65234124ef7897054986dca0a174e28df758cbaa03f240616414d5a1676
- C₁=
0x54bd7255f0aaf831bec3423fcf39d69b6cbf066677d0faae5aadd99df8e53517

4.4.3.4 Authentication Token

The authentication token SHALL be computed over a public key data object (cf. Section 9.2) containing the object identifier as indicated in MSE:Set AT (cf. Section 4.4.4.1), and the received ephemeral public key (i.e. excluding the domain parameters, cf. Section 9.2.3) using an authentication code and the key K_{SMAC} derived from the key agreement.

Note: Padding is performed internally by the message authentication code.

3DES

3DES [FIPS 46-3] SHALL be used in Retail-mode according to [ISO/IEC 9797-1] MAC algorithm 3 / padding method 2 with block cipher DES and IV=0.

AES

AES [FIPS 197] SHALL be used in CMAC-mode [SP 800-38B] with a MAC length of 8 bytes.

4.4.4 Application Protocol Data Units

The following sequence of commands SHALL be used to implement PACE:

1. MSE:SET AT
2. GENERAL AUTHENTICATE

4.4.4.1 MSE:SET AT

The command MSE:SET AT is used to select and initialize the PACE protocol.

Command			
CLA		Context specific	
INS	0x22	MANAGE SECURITY ENVIRONMENT	
P1/P2	0xC1A4	Set Authentication Template for mutual authentication	
Data	0x80	<i>Cryptographic mechanism reference</i> Object Identifier of the protocol to select (value only, Tag 0x06 is omitted).	REQUIRED
	0x83	<i>Reference of a public key / secret key</i> The password to be used is indicated as follows: 0x01: MRZ_information 0x02: CAN	REQUIRED
	0x84	<i>Reference of a private key / Reference for computing a session key</i> This data object is REQUIRED to indicate the identifier of the domain parameters to be used if the domain parameters are ambiguous, i.e. more than one set of domain parameters is available for PACE.	CONDITIONAL
Response			
Data	–	Absent	

Status Bytes	0x9000	<i>Normal processing</i> The protocol has been selected and initialized.
	0x6A80	<i>Incorrect parameters in the command data field</i> Algorithm not supported or initialization failed.
	0x6A88	<i>Referenced data not found</i> The referenced data (i.e. password or domain parameter) is not available.
	other	<i>Operating system dependent error</i> The initialization of the protocol failed.

Note: Some operating systems accept the selection of an unavailable key and return an error only when the key is used for the selected purpose.

4.4.4.2 GENERAL AUTHENTICATE

A chain of General Authenticate commands is used to perform the PACE protocol.

Command			
CLA		Context specific.	
INS	0x86	GENERAL AUTHENTICATE	
P1/P2	0x0000	Keys and protocol implicitly known	
Data	0x7C	<i>Dynamic Authentication Data</i> Protocol specific data objects	REQUIRED
Response			
Data	0x7C	<i>Dynamic Authentication Data</i> Protocol specific data objects as described in Section 4.4.5.	REQUIRED
Status Bytes	0x9000	<i>Normal processing</i> The protocol (step) was successful.	
	0x6300	Authentication failed The protocol (step) failed.	
	0x6A80	<i>Incorrect parameters in command data field</i> Provided data is invalid.	
	other	<i>Operating system dependent error</i> The protocol (step) failed.	

4.4.4.3 Command Chaining

Command chaining MUST be used for the GENERAL AUTHENTICATE command to link the sequence of commands to the execution of the protocol. Command chaining MUST NOT be used for other purposes unless clearly indicated by the chip. For details on command chaining see [ISO/IEC 7816-4].

4.4.5 Exchanged Data

The protocol specific data objects SHALL be exchanged in a chain of GENERAL AUTHENTICATE commands, with protocol specific command and response data encapsulated in a Dynamic Authentication data object (see section 4.4.4.2) with context specific tags as shown in the table below:

Table 4: Exchanged data for PACE

Step	Description	Protocol Command Data	Protocol Response Data
------	-------------	-----------------------	------------------------

1.	Encrypted Nonce	-	Absent ¹	0x80	Encrypted Nonce
2.	Map Nonce	0x81	Mapping Data	0x82	Mapping Data
3.	Perform Key Agreement	0x83	Ephemeral Public Key	0x84	Ephemeral Public Key
4.	Mutual Authentication	0x85	Authentication Token	0x86	Authentication Token

4.4.5.1 Encrypted Nonce

The encrypted nonce (cf. Section 4.4.3.3) SHALL be encoded as octet string.

4.4.5.2 Mapping Data

The exchanged data is specific to the used mapping:

Generic Mapping

The ephemeral public keys (cf. Section 4.4.3.3 and Section 9.2.3) SHALL be encoded as elliptic curve point (ECDH) or unsigned integer (DH).

Integrated Mapping

The nonce t SHALL be encoded as octet string.

Note: The context specific data object 0x82 SHALL be empty for the Integrated Mapping.

4.4.5.3 Public Keys

The public keys SHALL be encoded as described in Section 9.2.3.

4.4.5.4 Authentication Token

The authentication token (cf. Section 4.4.3.4) SHALL be encoded as octet string.

¹ This implies an empty Dynamic Authentication Data Object

5 AUTHENTICATION OF DATA

In addition to the LDS Data Groups, the contactless IC also contains a Document Security Object (SO_D). This object is digitally signed by the Issuing State or organization and contains hash representations of the LDS contents (see Doc 9303-10).

An inspection system, containing the Document Signer Public Key (K_{PuDS}) of each State, or having read the Document Signer Certificate (C_{DS}) from the eMRTD, will be able to verify the Document Security Object (SO_D). In this way, through the contents of the Document Security Object (SO_D), the contents of the LDS are authenticated.

This verification mechanism does not require processing capabilities of the contactless IC in the eMRTD. Therefore it is called “Passive Authentication” of the contactless IC’s contents.

Passive Authentication proves that the contents of the Document Security Object (SO_D) and LDS are authentic and not changed. It does not prevent exact copying of the contactless IC’s content or chip substitution.

Therefore Passive Authentication SHOULD be supported by an additional physical inspection of the eMRTD.

5.1 Passive Authentication

5.1.1 Inspection Process

The inspection system performs the following steps:

1. The inspection system SHALL read the Document Security Object (SO_D) (which MUST contain the Document Signer Certificate (C_{DS}), see also Doc 9303-10) from the contactless IC.
2. The inspection system SHALL build and validate a certification path from a Trust Anchor to the Document Signer Certificate used to sign the Document Security Object (SO_D) according to Doc 9303-12.
3. The inspection system SHALL use the verified Document Signer Public Key (K_{PuDS}) to verify the signature of the Document Security Object (SO_D).
4. The inspection system MAY read relevant Data Groups from the contactless IC.
5. The inspection system SHALL ensure that the contents of the Data Group are authentic and unchanged by hashing the contents and comparing the result with the corresponding hash value in the Document Security Object (SO_D).

The following additional checks are considered Best Practice:

1. The inspection system or the inspection officer SHOULD check the presence of a DocumentTypeExtension in the Document Signer Certificate.
 - If yes, the inspection system SHOULD check the consistency of the DocumentTypeExtension, the Document Type from Data Group 1 and the Document Type from the visual MRZ (see 9303-12, -10 and -3, respectively).
 - If no, the inspection system SHOULD check that the KeyUsage of the Document Signer Certificate is set to digitalSignature and that the Document Signer Certificate contains no ExtendedKeyUsage-Extension (see Doc 9303-12).
2. The inspection system or the inspection officer SHOULD check the consistency of the country codes from:

- the Subject-field and, if present, the SubjectAltName of the Document Signer Certificate;
- the Subject-field and, if present, the SubjectAltName of the Trust Anchor (CSCA certificate);
- the Data Group 1 as read from the contactless IC; and
- the visual MRZ.

Additionally, the inspection system or the inspection officer MAY compare the contents of Data Group 1 to the visual MRZ (see Doc 9303-12, -10 and -3, respectively).

3. The inspection system SHOULD verify that the Issuing Date of the eMRTD is included in the Private Key Usage Period contained in the Document Signer Certificate (see Doc 9303-12).

The biometric information can now be used to perform the biometrics verification with the person who offers the eMRTD.

DRAFT_4 FOR TAG_2

6 AUTHENTICATION OF THE CONTACTLESS IC

An Issuing State or organization MAY choose to protect its eMRTDs against chip substitution. This can be done by implementing an Active Authentication mechanism.

If supported, the Active Authentication mechanism MUST ensure that the contactless IC has not been substituted, by means of a challenge-response protocol between the inspection system and the eMRTD's contactless IC.

For this purpose the contactless IC contains its own Active Authentication Key pair (KPr_{AA} and KPu_{AA}). A hash representation of Data Group 15 (Public Key (KPu_{AA}) info) is stored in the Document Security Object (SO_D) and therefore authenticated by the issuer's digital signature. The corresponding Private Key (KPr_{AA}) is stored in the contactless IC's secure memory.

By authenticating the visual MRZ (through the hashed MRZ in the Document Security Object (SO_D)) in combination with the challenge response, using the eMRTD's Active Authentication Key Pair (KPr_{AA} and KPu_{AA}), the inspection system verifies that the Document Security Object (SO_D) has been read from the genuine contactless IC, stored in the genuine eMRTD.

Active Authentication requires processing capabilities of the eMRTD's contactless IC.

6.1 Active Authentication

Active Authentication authenticates the contactless IC by signing a challenge sent by the IFD with a private key only known to the IC.

6.1.1 Protocol Specification

Active Authentication is performed using the [ISO/IEC 7816-4] INTERNAL AUTHENTICATE command.

If Active Authentication is performed after Secure Messaging was established, all commands and responses MUST be transmitted as Secure Messaging APDUs according to section 9.6.

In more detail, IFD (inspection system) and IC (eMRTD's contactless IC) perform the following steps:

1. The IFD generates a nonce RND_{IFD} and sends it to the IC using the INTERNAL AUTHENTICATE command.
2. The IC performs the following operations:
 - a) Generate the message M ;
 - b) Calculate $h(M)$;
 - c) Compute the signature σ and send the response to the IFD.
3. The IFD verifies the response on the sent INTERNAL AUTHENTICATE command and checks if the IC returned the correct value.

6.1.2 Cryptographic Specifications

6.1.2.1 Nonce

The input is a nonce (RND_{IFD}) that MUST be 8 bytes.

Note: Nonces MUST NOT be reused, e.g. the nonce used for BAC/PACE MUST NOT be reused for Active Authentication.

6.1.2.2 RSA

The IC SHALL compute a signature, when an integer factorization based mechanism is used, according to [ISO/IEC 9796-2] Digital Signature scheme 1.

In the following k denotes the length of key for signature generation and L_h the length of the output of the hash function H used during signature generation. The trailer field option 1 MUST be used (and t set to 1) if SHA-1 is used during signature generation, trailer field option 2 MUST be used otherwise (and t set to 2).

The message M to be signed SHALL be the concatenation of M_1 and M_2 , where M_1 MUST be a nonce of length $c - 4$ bits (RND.IC) generated by the eMRTD, where c (the *capacity of the signature*) is given by $c = k - L_h - (8 \times t) - 4$, and M_2 is RND.IFD generated by the Inspection System.

The result of the signature computation MUST be a signature σ without the non-recoverable message part M_2 .

eMRTDs SHOULD implement the signature generation scheme specified in [ISO/IEC 9796-2] paragraph B.6 and SHOULD NOT make use of the signature generation scheme specified in [ISO/IEC 9796-2] paragraph B.4. eMRTDs SHALL NOT implement other signature generation schemes.

Inspection systems SHALL implement the signature generation scheme specified in [ISO/IEC 9796-2] paragraph B.6 and SHOULD implement the signature generation scheme specified in [ISO/IEC 9796-2] paragraph B.4.

6.1.2.3 ECDSA

For ECDSA, the plain signature format according to [TR-03111] SHALL be used. Only prime curves with uncompressed points SHALL be used. A hash algorithm, whose output length is of the same length or shorter than the length of the ECDSA key in use, SHALL be used.

The message M to be signed is the nonce RND.IFD provided by the Inspection System.

6.1.3 Application Protocol Data Units

Active Authentication is performed by a single invocation of the INTERNAL AUTHENTICATE command as specified in [ISO/IEC 7816-4].

Command			
CLA		Context specific	
INS	0x88	INTERNAL AUTHENTICATE	
P1/P2	0x0000	--	
Data		RND.IFD	REQUIRED
Response			
Data		Signature σ generated by the IC	REQUIRED
Status Bytes	0x9000	<i>Normal processing</i> The protocol has been performed successfully.	
	Other	<i>Operating system dependent error</i> The protocol failed.	

6.1.4 Active Authentication Keys

The Active Authentication Key Pairs (KPr_{AA} and KPu_{AA}) SHALL be generated in a secure way.

Both the Active Authentication Public Key (KPu_{AA}) and the Active Authentication Private Key (KPr_{AA}) are stored in the eMRTD's contactless IC. After that, no Key Management is applicable for these keys.

Note: It should be noted that when using key lengths exceeding 1848 bits in Active Authentication with Secure Messaging, Extended Length APDUs MUST be supported by the eMRTD chip and the Inspection System.

Issuing States or organizations SHALL choose appropriate key lengths offering protection against attacks for the life time of the eMRTD. Suitable cryptographic catalogues SHOULD be taken into account.

6.1.5 Active Authentication Public Key Info

The Active Authentication Public Key is stored in the LDS Data Group 15. The format of the structure (SubjectPublicKeyInfo) is specified in [RFC 5280]. All security objects MUST be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

```
ActiveAuthenticationPublicKeyInfo ::= SubjectPublicKeyInfo
```

```
SubjectPublicKeyInfo ::= SEQUENCE {  
    algorithm AlgorithmIdentifier,  
    subjectPublicKey BIT STRING }
```

```
AlgorithmIdentifier ::= SEQUENCE {  
    algorithm OBJECT IDENTIFIER,  
    parameters ANY DEFINED BY algorithm OPTIONAL }
```

6.1.6 Inspection Process

When an eMRTD with Data Group 15 is offered to the inspection system, the Active Authentication mechanism MAY be performed to ensure that the data are read from the genuine contactless IC and that the contactless IC and data page belong to each other.

The inspection system and the contactless IC perform the following steps:

1. The entire MRZ is read visually from the eMRTD (if not already read as part of the Basic Access Control procedure) and compared with the MRZ value in Data Group 1. Since the authenticity and integrity of Data Group 1 have been checked through Passive Authentication, similarity ensures that the visual MRZ is authentic and unchanged.
2. Passive Authentication has also proven the authenticity and integrity of Data Group 15. This ensures that the Active Authentication Public Key (KP_{UAA}) is authentic and unchanged.
3. To ensure that the Document Security Object (SO_D) is not a copy, the inspection system uses the eMRTD's Active Authentication Key pair (KPr_{AA} and KPu_{AA}) in a challenge-response protocol with the eMRTD's contactless IC as described above.

After a successful challenge-response protocol, it is proven that the Document Security Object (SO_D) belongs to the data page, the contactless IC is genuine and contactless IC and data page belong to each other.

7 ADDITIONAL ACCESS CONTROL MECHANISMS

The personal data stored in the contactless IC as defined to be the mandatory minimum for global interoperability are the MRZ and the digitally stored image of the bearer's face. Both items can also be seen (read) visually after the eMRTD has been opened and offered for inspection.

Besides the digitally stored image of the face as the primary biometric for global interoperability, ICAO has endorsed the use of digitally stored images of fingers and/or irises in addition to the face. For national or bilateral use, States MAY choose to store templates and/or MAY choose to limit access or encrypt this data, as to be decided by States themselves.

Access to this more sensitive personal data SHOULD be more restricted. This can be accomplished in two ways: extended access control or data encryption. Although these options are mentioned in this Section, ICAO is not proposing or specifying any specifications or practices in these areas at this time.

7.1 Extended Access Control for Additional Biometrics

The Extended Access Control mechanism is OPTIONAL. For Extended Access Control a Document Extended Access Key set is used instead of the Document Basic Access Keys (K_{Enc} and K_{MAC}).

Defining the (IC-individual) Document Extended Access Key set is up to the implementing State. The Document Extended Access Key set MAY consist of either symmetric keys, e.g. derived from the MRZ and a National Master key, or an asymmetric key pair with a corresponding card verifiable certificate.

Extended Access Control requires processing capabilities of the eMRTD's contactless IC.

The implementation of the protection of the additional biometrics depends on the State's internal specifications or the bilaterally agreed specifications between States sharing this information.

7.2 Encryption of Additional Biometrics

Restricting access to the additional biometrics MAY also be done by encrypting them. To be able to decrypt the encrypted data, the inspection system MUST be provided with a decryption key. Defining the encryption/decryption algorithm and the keys to be used is up to the implementing State and is outside the scope of this document.

The implementation of the protection of the additional biometrics depends on the State's internal specifications or the bilaterally agreed specifications between States sharing this information.

8 INSPECTION SYSTEM

In order to support the required functionality and the defined options that can be implemented on eMRTDs that will be offered, the inspection system will have to meet certain pre-conditions.

8.1 Basic Access Control

Inspection systems supporting Basic Access Control MUST meet the following pre-conditions:

1. The inspection system is equipped with means to acquire the MRZ from the data page to derive the Document Basic Access Keys (K_{ENC} and K_{MAC}) from the eMRTD.
2. The inspection system's software supports the protocol described in section 4.3, in the case that an eMRTD with Basic Access Control is offered to the system, including the encryption of the communication channel with Secure Messaging.

8.2 Password Authenticated Connection Establishment

Inspection systems supporting PACE MUST meet the following pre-conditions:

1. The inspection system is equipped with means to acquire the MRZ and/or the CAN from the data page.
2. The inspection system's software supports the protocol described in section 4.4, in the case that an eMRTD with PACE is offered to the system, including the encryption of the communication channel with Secure Messaging.

8.3 Passive Authentication

To be able to perform a passive authentication of the data stored in the eMRTDs contactless IC, the inspection system needs to have knowledge of key information of the Issuing States or organizations:

1. Of each Issuing State or organization, the Country Signing CA Certificate (C_{CSCA}) or the relevant information extracted from the certificate SHALL be securely stored in the inspection system.
2. Alternatively, of each Issuing State or organization, the Document Signer Certificates (C_{DS}) or the relevant information extracted from the certificates SHALL be securely stored in the inspection system.

Before using a Country Signing CA Public Key of an Issuing State of organization trust in this key MUST be established by the receiving State or organization.

Before using a Document Signer Certificate (C_{DS}) for verification of a SO_D , the inspection system SHALL verify its digital signature, using the Country Signing CA Public Key ($K_{PU_{CSCA}}$).

Additionally, inspection systems SHALL have access to verified revocation information.

8.4 Active Authentication

Support of Active Authentication by inspection systems is OPTIONAL.

If the inspection system supports Active Authentication, it is REQUIRED that the inspection system has the ability to read the visual MRZ.

If the inspection system supports Active Authentication, the inspection system's software SHALL support the Active Authentication protocol described in section 6.1.

8.5 Extended Access Control to Additional Biometrics

The implementation of the protection of the optional additional biometrics depends on the State's internal specifications or the bilaterally agreed specifications between States sharing this information.

8.6 Decryption of Additional Biometrics

The implementation of the protection of the optional additional biometrics depends on the State's internal specifications or the bilaterally agreed specifications between States sharing this information.

DRAFT_4 FOR TAG_22

9 COMMON SPECIFICATIONS

9.1 Information on Supported Protocols

The ASN.1 data structure `SecurityInfos` SHALL be provided by the eMRTD chip to indicate supported security protocols. The data structure is specified as follows:

```
SecurityInfos ::= SET OF SecurityInfo

SecurityInfo ::= SEQUENCE {
    protocol      OBJECT IDENTIFIER,
    requiredData  ANY DEFINED BY protocol,
    optionalData  ANY DEFINED BY protocol OPTIONAL
}
```

The elements contained in a `SecurityInfo` data structure have the following meaning:

- The object identifier `protocol` identifies the supported protocol.
- The open type `requiredData` contains protocol specific mandatory data.
- The open type `optionalData` contains protocol specific optional data.

Security Infos for PACE

To indicate support for PACE `SecurityInfos` may contain the following entries:

- At least one `PACEInfo` using a standardized domain parameter MUST be present.
- For each supported set of explicit domain parameters a `PACEDomainParameterInfo` MUST be present.

Security Infos for Active Authentication

If ECDSA based signature algorithm is used for Active Authentication by the eMRTD chip, the `SecurityInfos` MUST contain the following `SecurityInfo` entry:

- `ActiveAuthenticationInfo`

Security Infos for Other Protocols

`SecurityInfos` may contain additional entries indicating support for other protocols. The inspection system may discard any unknown entry.

9.1.1 PACEInfo

This data structure provides detailed information on an implementation of PACE.

- The object identifier `protocol` SHALL identify the algorithms to be used (i.e. key agreement, symmetric cipher and MAC).
- The integer `version` SHALL identify the version of the protocol. Only version 2 is supported by this specification.

- The integer `parameterId` is used to indicate the domain parameter identifier. It **MUST** be used if the eMRTD chip uses standardized domain parameters (cf. Section 9.3) or provides multiple explicit domain parameters for PACE.

```

PACEInfo ::= SEQUENCE {
  protocol    OBJECT IDENTIFIER(
    id-PACE-DH-GM-3DES-CBC-CBC |
    id-PACE-DH-GM-AES-CBC-CMAC-128 |
    id-PACE-DH-GM-AES-CBC-CMAC-192 |
    id-PACE-DH-GM-AES-CBC-CMAC-256 |
    id-PACE-ECDH-GM-3DES-CBC-CBC |
    id-PACE-ECDH-GM-AES-CBC-CMAC-128 |
    id-PACE-ECDH-GM-AES-CBC-CMAC-192 |
    id-PACE-ECDH-GM-AES-CBC-CMAC-256 |
    id-PACE-DH-IM-3DES-CBC-CBC |
    id-PACE-DH-IM-AES-CBC-CMAC-128 |
    id-PACE-DH-IM-AES-CBC-CMAC-192 |
    id-PACE-DH-IM-AES-CBC-CMAC-256 |
    id-PACE-ECDH-IM-3DES-CBC-CBC |
    id-PACE-ECDH-IM-AES-CBC-CMAC-128 |
    id-PACE-ECDH-IM-AES-CBC-CMAC-192 |
    id-PACE-ECDH-IM-AES-CBC-CMAC-256),
  version    INTEGER, -- MUST be 2
  parameterId INTEGER OPTIONAL
}

```

9.1.2 PACEDomainParameterInfo

This data structure is **REQUIRED** if the eMRTD chip provides explicit domain parameters for PACE of the eMRTD chip and **MUST** be omitted otherwise.

- The object identifier `protocol` **SHALL** identify the type of the domain parameters (i.e. DH or ECDH).
- The sequence `domainParameter` **SHALL** contain the domain parameters.
- The integer `parameterId` **MAY** be used to indicate the local domain parameter identifier. It **MUST** be used if the eMRTD chip provides multiple explicit domain parameters for PACE.

```

PACEDomainParameterInfo ::= SEQUENCE {
  protocol    OBJECT IDENTIFIER(
    id-PACE-DH-GM |
    id-PACE-ECDH-GM |
    id-PACE-DH-IM |
    id-PACE-ECDH-IM),
  domainParameter AlgorithmIdentifier,
  parameterId  INTEGER OPTIONAL
}

```

The domain parameters for PACE **MUST** be provided as `AlgorithmIdentifier`. The data structure `AlgorithmIdentifier` is defined as follows:

```

AlgorithmIdentifier ::= SEQUENCE {
  algorithm OBJECT IDENTIFIER,
  parameters ANY DEFINED BY algorithm OPTIONAL
}

```

The object identifier algorithm **SHALL** be `dhpublicnumber` or `ecPublicKey` for DH or ECDH, respectively.

```
dhpublicnumber OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1
}

ecPublicKey OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) ansi-x962(10045) keyType(2) 1
}
```

Details on the `parameters` can be found in [X9.42] and [TR-03111].

Note: The eMRTD chip MAY support more than one set of explicit domain parameters (i.e. the chip may support different algorithms and/or key lengths). In this case the identifier MUST be disclosed in the corresponding `PACEDomainParameterInfo`.

Domain parameters contained in `PACEDomainParameterInfo` are unprotected and may be insecure. Using insecure domain parameters for PACE will leak the used password. eMRTD chips **MUST** support at least one set of standardized domain parameters as specified in section 9.3. Inspection systems **MUST NOT** use explicit domain parameters provided by the eMRTD chip unless those domain parameters are explicitly known to be secure by the inspection systems.

Ephemeral public keys **MUST** be exchanged as plain public key values. More information on the encoding can be found in Section 9.2.3.

9.1.3 PACE Object Identifier

The object identifiers used for PACE are contained in the subtree of `bsi-de`:

```
bsi-de OBJECT IDENTIFIER ::= {
  itu-t(0) identified-organization(4) etsi(0)
  reserved(127) etsi-identified-organization(0) 7
}
```

The following Object Identifier **SHALL** be used:

```
id-PACE OBJECT IDENTIFIER ::= {
  bsi-de protocols(2) smartcard(2) 4
}
```

<code>id-PACE-DH-GM</code>	OBJECT IDENTIFIER ::= {id-PACE 1}
<code>id-PACE-DH-GM-3DES-CBC-CBC</code>	OBJECT IDENTIFIER ::= {id-PACE-DH-GM 1}
<code>id-PACE-DH-GM-AES-CBC-CMAC-128</code>	OBJECT IDENTIFIER ::= {id-PACE-DH-GM 2}
<code>id-PACE-DH-GM-AES-CBC-CMAC-192</code>	OBJECT IDENTIFIER ::= {id-PACE-DH-GM 3}
<code>id-PACE-DH-GM-AES-CBC-CMAC-256</code>	OBJECT IDENTIFIER ::= {id-PACE-DH-GM 4}
<code>id-PACE-ECDH-GM</code>	OBJECT IDENTIFIER ::= {id-PACE 2}
<code>id-PACE-ECDH-GM-3DES-CBC-CBC</code>	OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 1}
<code>id-PACE-ECDH-GM-AES-CBC-CMAC-128</code>	OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 2}
<code>id-PACE-ECDH-GM-AES-CBC-CMAC-192</code>	OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 3}
<code>id-PACE-ECDH-GM-AES-CBC-CMAC-256</code>	OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 4}
<code>id-PACE-DH-IM</code>	OBJECT IDENTIFIER ::= {id-PACE 3}
<code>id-PACE-DH-IM-3DES-CBC-CBC</code>	OBJECT IDENTIFIER ::= {id-PACE-DH-IM 1}
<code>id-PACE-DH-IM-AES-CBC-CMAC-128</code>	OBJECT IDENTIFIER ::= {id-PACE-DH-IM 2}
<code>id-PACE-DH-IM-AES-CBC-CMAC-192</code>	OBJECT IDENTIFIER ::= {id-PACE-DH-IM 3}
<code>id-PACE-DH-IM-AES-CBC-CMAC-256</code>	OBJECT IDENTIFIER ::= {id-PACE-DH-IM 4}

```

id-PACE-ECDH-IM                OBJECT IDENTIFIER ::= {id-PACE 4}
id-PACE-ECDH-IM-3DES-CBC-CBC   OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 1}
id-PACE-ECDH-IM-AES-CBC-CMAC-128 OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 2}
id-PACE-ECDH-IM-AES-CBC-CMAC-192 OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 3}
id-PACE-ECDH-IM-AES-CBC-CMAC-256 OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 4}

```

9.1.4 ActiveAuthenticationInfo

If ECDSA based signature algorithm is used for Active Authentication by the eMRTD chip, the SecurityInfos in LDS Data Group 14 of the eMRTD chip MUST contain following SecurityInfo entry:

```

ActiveAuthenticationInfo ::= SEQUENCE {
    protocol id-icao-mrtd-security-aaProtocolObject
    version INTEGER -- MUST be 1
    signatureAlgorithm OBJECT IDENTIFIER
}

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

```

For signatureAlgorithm, the object identifiers defined in [TR-03111] SHALL be used.

Note: The Object Identifier id-icao-mrtd-security is defined in Doc 9303-10.

9.1.5 Storage on the Chip

- The file EF.CardAccess (see Doc 9303-10) SHALL contain the relevant SecurityInfos that are required for PACE:
 - PACEInfo
 - PACEDomainParameterInfo
- The full set of SecurityInfos (including SecurityInfos contained in EF.CardAccess not specified in Doc 9303) SHALL additionally be stored in DG14 of the eMRTD Application (see Doc 9303-10).

Note: While the authenticity of SecurityInfos stored in DG14 is protected by Passive Authentication, the file EF.CardAccess is unprotected.

9.2 Public Key Data Objects

A public key data object is a constructed BER TLV structure containing an object identifier and several context specific data objects nested within the cardholder public key template '7F49'.

- The object identifier is application specific and refers not only to the public key format (i.e. the context specific data objects) but also to its usage.
- The context-specific data objects are defined by the object identifier and contain the public key value and the domain parameters.

The format of public keys data objects used in this specification is described below.

9.2.1 Diffie Hellman Public Keys

The data objects contained in a DH public key are shown below. The order of the data objects is fixed.

Table 5: Data objects for DH public keys

Data Object	Notation	Tag	Type
Object Identifier		0x06	Object Identifier
Prime modulus	P	0x81	Unsigned Integer
Order of the subgroup	Q	0x82	Unsigned Integer
Generator	G	0x83	Unsigned Integer
Public Value	Y	0x84	Unsigned Integer

9.2.2 Elliptic Curve Public Keys

The data objects contained in an EC public key are shown below. The order of the data objects is fixed, CONDITIONAL domain parameters MUST be either all present, except the cofactor, or all absent as follows:

Table 6: Data objects for ECDH public keys

Data Object	Notation	Tag	Type
Object Identifier		0x06	Object Identifier
Prime modulus	P	0x81	Unsigned Integer
First coefficient	A	0x82	Unsigned Integer
Second coefficient	B	0x83	Unsigned Integer
Base point	G	0x84	Elliptic Curve Point
Order of the base point	R	0x85	Unsigned Integer
Public point	Y	0x86	Elliptic Curve Point
Cofactor	F	0x87	Unsigned Integer

9.2.3 Ephemeral Public Keys

For ephemeral public keys the format and the domain parameters are already known. Therefore, only the plain public key value, i.e. the public value y for Diffie-Hellman public keys and the public point Y for Elliptic Curve Public Keys, is used to convey the ephemeral public key in a context specific data object.

9.3 Standardized Domain Parameters

The standardized domain parameters IDs described in the table below SHALL be used. Explicit domain parameters provided by `PACEDomainParameterInfo` MUST NOT use those IDs reserved for standardized domain parameters.

Table 7: Standardized domain parameters

ID	Name	Size (bit)	Type	Reference
0	1024-bit MODP Group with 160-bit Prime Order Subgroup	1024/160	GFP	[RFC 5114]
1	2048-bit MODP Group with 224-bit Prime Order Subgroup	2048/224	GFP	[RFC 5114]
2	2048-bit MODP Group with 256-bit Prime Order Subgroup	2048/256	GFP	[RFC 5114]
3-7	RFU			
8	NIST P-192 (secp192r1)	192	ECP	[RFC 5114], [FIPS 186-4]
9	BrainpoolP192r1	192	ECP	[RFC 5639]
10	NIST P-224 (secp224r1) *	224	ECP	[RFC 5114], [FIPS 186-4]
11	BrainpoolP224r1	224	ECP	[RFC 5639]
12	NIST P-256 (secp256r1)	256	ECP	[RFC 5114], [FIPS 186-4]
13	BrainpoolP256r1	256	ECP	[RFC 5639]
14	BrainpoolP320r1	320	ECP	[RFC 5639]
15	NIST P-384 (secp384r1)	384	ECP	[RFC 5114], [FIPS 186-4]
16	BrainpoolP384r1	384	ECP	[RFC 5639]
17	BrainpoolP512r1	512	ECP	[RFC 5639]
18	NIST P-521 (secp521r1)	521	ECP	[RFC 5114], [FIPS 186-4]
19-31	RFU			

* This curve cannot be used with the Integrated Mapping.

9.4 Key Agreement Algorithms

This specification supports Diffie-Hellman and Elliptic Curve Diffie-Hellman key agreement as summarized in the following table:

Table 8: Key agreement algorithms

Algorithm / Format	DH	ECDH
Key Agreement Algorithm	[PKCS#3]	ECKA [TR-03111]
X.509 Public Key Format	[X9.42]	[TR-03111]
TLV Public Key Format	TLV, cf. Section 9.2.1	TLV, cf. Section 9.2.2
Ephemeral Public Key Validation	[RFC 2631]	[TR-03111]

9.5 Key Derivation Mechanism

9.5.1 Key Derivation Function

The key derivation function $KDF(K,c)$, is defined as follows:

Input: The following inputs are required:

- The shared secret value K (REQUIRED)
- A 32-bit, big-endian integer counter c (REQUIRED)

Output: An octet string keydata.

Actions: The following actions are performed:

- $keydata = H(K || c)$

- Output octet string keydata

The key derivation function $\mathbf{KDF}(K,c)$ requires a suitable hash function denoted by $\mathbf{H}()$, i.e the bit-length of the hash function SHALL be greater or equal to the bit-length of the derived key. The hash value SHALL be interpreted as big-endian byte output.

Note: The shared secret K is defined as an octet string. If the shared secret is generated with ECKA [TR-03111], the x -coordinate of the generated point SHALL be used.

9.5.1.1 3DES

To derive 128-bit (112-bit excluding parity bits) 3DES [FIPS 46-3] keys the hash function SHA-1 [FIPS 180-2] SHALL be used and the following additional steps MUST be performed:

- Use octets 1 to 8 of keydata to form keydataA and octets 9 to 16 of keydata to form keydataB; additional octets are not used.
- Adjust the parity bits of keydataA and keydataB to form correct DES keys (OPTIONAL).

9.5.1.2 AES

To derive 128-bit AES [FIPS 197] keys the hash function SHA-1 [FIPS 180-2] SHALL be used and the following additional step MUST be performed:

- Use octets 1 to 16 of keydata; additional octets are not used.

To derive 192-bit and 256-bit AES [FIPS 197] keys SHA-256 [FIPS 180-2] SHALL be used. For 192-bit AES keys the following additional step MUST be performed:

- Use octets 1 to 24 of keydata; additional octets are not used.

9.5.2 Document Basic Access Keys

The computation of two key 3DES keys from a key seed (K) is used in the establishment of the Document Basic Access Keys $K_{Enc} = \mathbf{KDF}(K,1)$ and $K_{MAC} = \mathbf{KDF}(K,2)$.

9.5.3 PACE

Let $\mathbf{KDF}_{\pi}(\pi) = \mathbf{KDF}(f(\pi),3)$ be a key derivation function to derive encryption keys from a password π . The encoding of passwords, i.e. $K = f(\pi)$ is specified below:

Table 9: Password encodings

Passwort	Encoding
MRZ	SHA-1(Serial Number Date of Birth Date of Expiry)
CAN	[ISO/IEC 8859-1] encoded character string

9.5.4 Secure Messaging Keys

Keys for encryption and authentication are derived with $\mathbf{KDF}_{Enc}(K) = \mathbf{KDF}(K,1)$ and $\mathbf{KDF}_{MAC}(K) = \mathbf{KDF}(K,2)$ respectively, from a shared secret K .

9.6 Secure Messaging

Secure Messaging is based on either 3DES [FIPS 46-3] or AES [FIPS 197] in encrypt-then-authenticate mode, i.e. data is padded, encrypted and afterwards the formatted encrypted data is input to the authentication calculation. The session keys SHALL be derived using the key derivation function described in section 9.5.1.

Note: Padding is always performed by the secure messaging layer, therefore the underlying message authentication code needs not to perform any internal padding.

9.6.1 Send Sequence Counter

An unsigned integer SHALL be used as Send Sequence Counter (SSC). The bitsize of the SSC SHALL be equal to the blocksize of the block cipher used for Secure Messaging, i.e. 64 bit for 3DES and 128 bit for AES.

The SSC SHALL be increased every time before a command or response APDU is generated, i.e. if the starting value is x , in the first command the value of the SSC is $x+1$. The value of SSC for the first response is $x+2$.

If Secure Messaging is restarted, the SSC is used as follows:

- The commands used for key agreement are protected with the old session keys and old SSC. This applies in particular for the response of the last command used for session key agreement.
- The Send Sequence Counter is set to its new start value, see section 9.6.4.3 for 3DES/ section 9.6.5.3 for AES.
- The new session keys and the new SSC are used to protect subsequent commands/responses.

9.6.2 Message Structure of SM APDUs

The SM Data Objects (see [ISO/IEC 7816-4]) MUST be used in the following order:

- Command APDU: [DO'85' or DO'87'] [DO'97'] DO'8E'.
- Response APDU: [DO'85' or DO'87'] [DO'99'] DO'8E'.

All SM Data Objects MUST be encoded in BER TLV as specified in [ISO/IEC 7816-4]. The command header MUST be included in the MAC calculation, therefore the class byte CLA = 0x0C MUST be used.

The actual value of Lc will be modified to Lc' after application of Secure Messaging. If required, an appropriate data object may optionally be included into the APDU data part in order to convey the original value of Lc.

Figure 3: shows the transformation of an unprotected command APDU to a protected command APDU in the case *Data* and *Le* are available. If no *Data* is available, leave building DO '87' out. If *Le* is not available, leave building DO '97' out. To avoid ambiguity it is RECOMMENDED not to use an empty value field of Le Data Object (see also Section 10.4 of [ISO/IEC 7816-4]).

Figure 4: shows the transformation of an unprotected response APDU to a protected response APDU in case *Data* is available. If no *Data* is available, leave building DO '87' out.

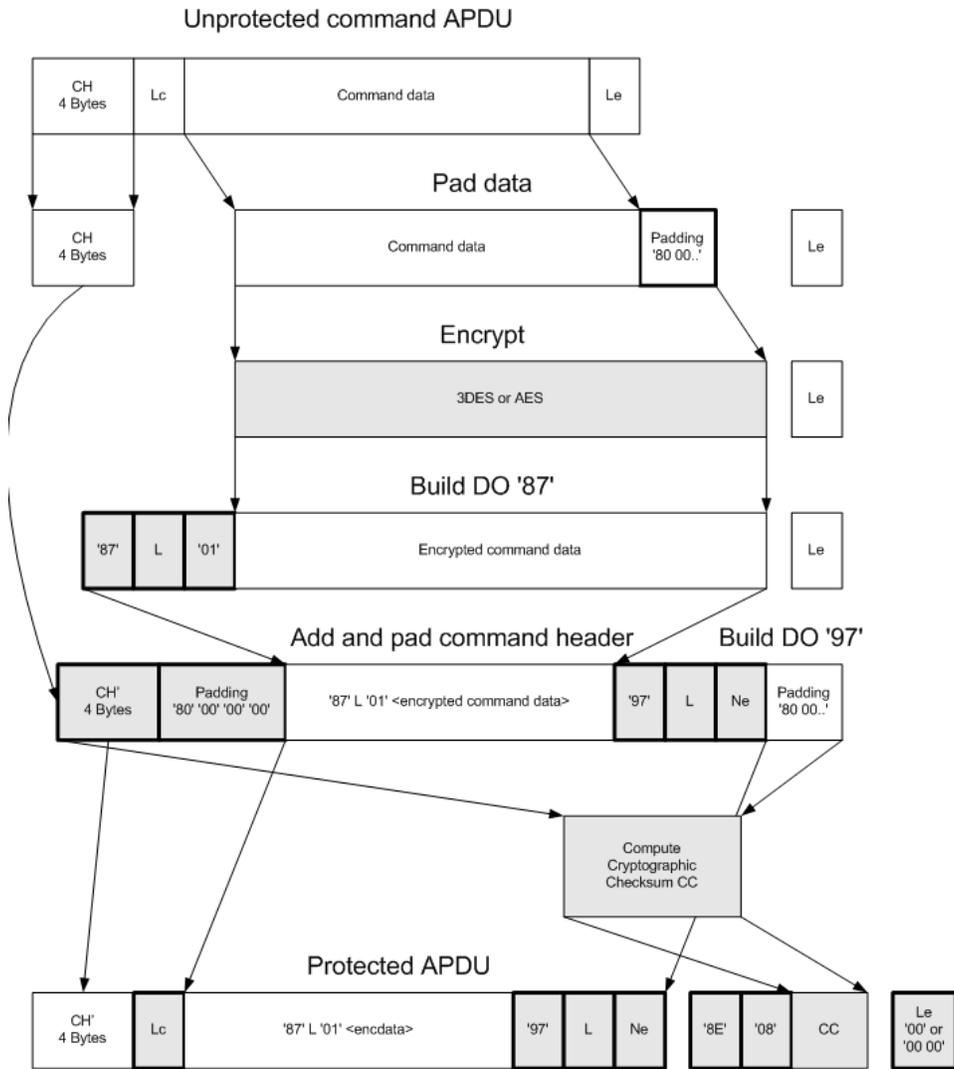


Figure 3: Computation of a SM command APDU for even INS Byte

DRAFT

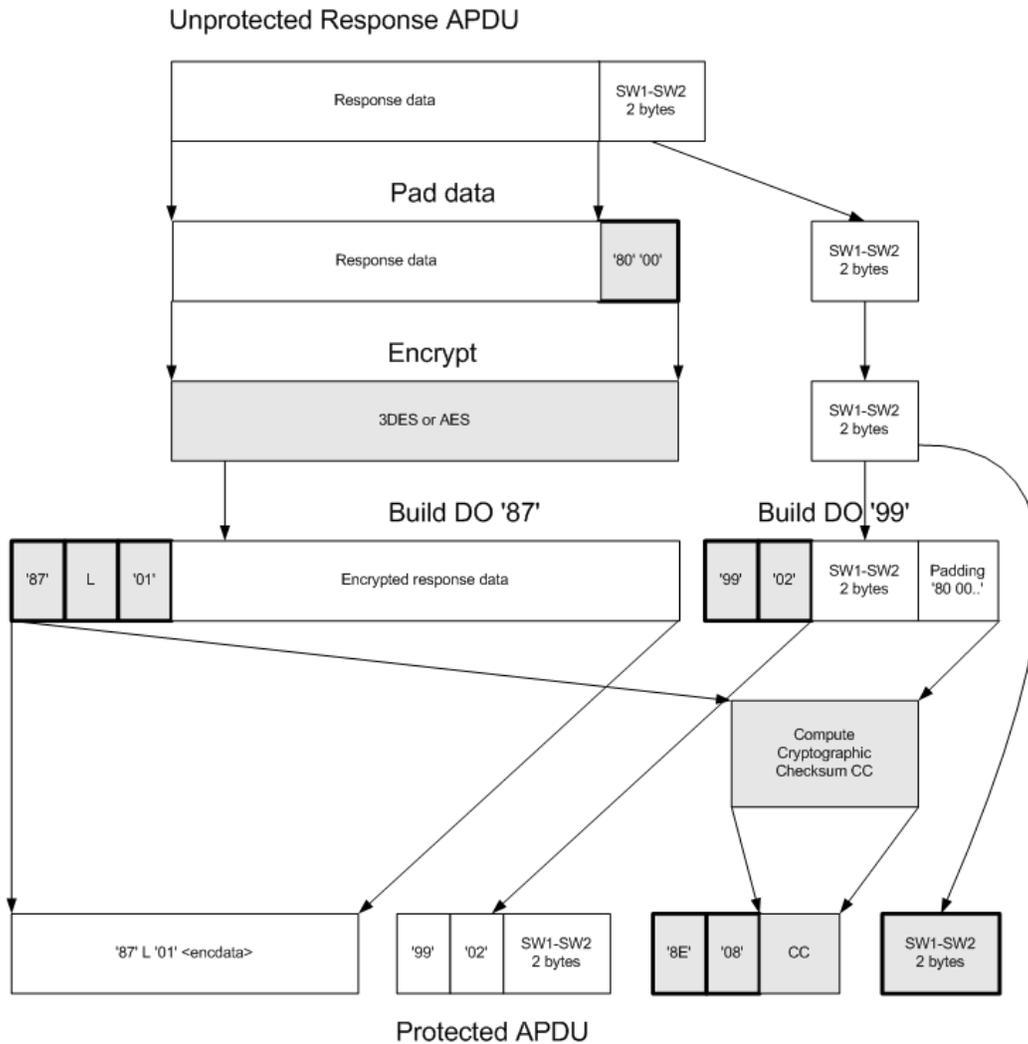


Figure 4: Computation of a SM response APDU for even INS Byte

9.6.3 SM Errors

Abortion of the Secure Channel for the eMRTD application occurs when:

- the contactless IC is de-powered; or
- the contactless IC recognizes an SM error while interpreting a command. In this case the status bytes must be returned without SM.

If Secure Messaging is aborted, the eMRTD chip SHALL delete the stored session keys and reset the terminal's access rights.

Note: There MAY be other circumstances in which the contactless IC aborts the session. It is not feasible to provide a complete list of such circumstances.

9.6.4 3DES Modes of Operation

9.6.4.1 Encryption

Two key 3DES in CBC mode with zero IV (i.e. 0x00 00 00 00 00 00 00 00) according to [ISO/IEC 11568-2] is used. Padding according to [ISO/IEC 9797-1] padding method 2 is used.

9.6.4.2 Message Authentication

Cryptographic checksums are calculated using [ISO/IEC 9797-1] MAC algorithm 3 with block cipher DES, zero IV (8 bytes), and [ISO/IEC 9797-1] padding method 2. The MAC length MUST be 8 bytes.

After a successful authentication the datagram to be MACed MUST be prepended by the Send Sequence Counter.

9.6.4.3 Send Sequence Counter

For Secure Messaging following BAC, the Send Sequence Counter SHALL be initialized by concatenating the four least significant bytes of RND.IC and RND.IFD, respectively:

$$\text{SSC} = \text{RND.IC (4 least significant bytes)} \parallel \text{RND.IFD (4 least significant bytes)}.$$

In all other cases, the SSC SHALL be initialized to zero (i.e. 0x00 00 00 00 00 00 00 00).

9.6.5 AES Modes of Operation

9.6.5.1 Encryption

For message encryption AES [FIPS 197] SHALL be used in CBC-mode according to [ISO/IEC 10116] with key KS_{Enc} and $\text{IV} = \text{E}(\text{KS}_{\text{Enc}}, \text{SSC})$.

9.6.5.2 Message Authentication

For message authentication AES SHALL be used in CMAC-mode [SP 800-38B] with KS_{MAC} with a MAC length of 8 bytes. The datagram to be authenticated SHALL be prepended by the Send Sequence Counter.

9.6.5.3 Send Sequence Counter

The Send Sequence Counter SHALL be initialized to zero (i.e. 0x00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00).

APPENDIX A ENTROPY OF MRZ-DERIVED ACCESS KEYS (INFORMATIVE)

Due to its simplicity Basic Access Control turned out to be a very successful protocol and it is implemented in almost every eMRP.

The security provided by Basic Access Control is limited by the design of the protocol. The Document Basic Access Keys (K_{ENC} and K_{MAC}) are generated from printed data with very limited randomness. The data that is used for the generation of the keys are Document Number, Date of Birth, and Date of Expiry. As a consequence the resulting keys have a relatively low entropy and are cryptographically weak. The actual entropy mainly depends on the type of the Document Number. For 10 year valid travel document the **maximum** strength of the keys is approximately:

- 56 Bit for a numeric Document Number ($365^2 * 10^{12}$ possibilities)
- 73 Bit for an alphanumeric Document Number ($365^2 * 36^9 * 10^3$ possibilities)

Especially in the second case this estimation requires the Document Number to be randomly and uniformly chosen which is usually not the case. Depending on the knowledge of the attacker, the actual entropy of the Document Basic Access Key may be lower, e.g. if the attacker knows all Document Numbers in use or is able to correlate Document Numbers and Dates of Expiry.

There is no straightforward way to strengthen Basic Access Control as its limitations are inherent to the design of the protocol based on symmetric (“secret key”) cryptography. A cryptographically strong access control mechanism must (additionally) use asymmetric (“public key”) cryptography.

Password Authenticated Connection Establishment (PACE) was designed to overcome this problem. It employs asymmetric cryptography to establish session keys, whose strength is independent of the entropy of the used password. If PACE is implemented with elliptic curve cryptography with 256 Bit curves and AES-128 (a common choice), the session keys have 128 Bit entropy.

Two types of attacks must be distinguished:

- Skimming: this is an online attack, i.e. the attacker tries to access the contactless IC in real time, e.g. by guessing the password. If the protocol used to protect the contactless IC has no cryptographic weakness, the success probability of the attacker is given by the time the attacker has access to the IC, the duration of a single attempt to guess the password, and the entropy of the passport.
- Eavesdropping: this is an offline attack, i.e. the attacker tries to decrypt intercepted communication without access to the contactless IC. If the protocol used to establish the session keys has no cryptographic weakness, the success probability is given by the strength of the session keys and the computing power available to the attacker.

For further information see [Keesing2009] for a general discussion on entropy of session keys and a comparison of BAC and PACE, and [BFK2009] for a cryptographic analysis of PACE.

APPENDIX B POINT ENCODING FOR THE ECDH-INTEGRATED MAPPING (INFORMATIVE)

B.1 High-level Description of the Point Encoding Method

The algorithm takes as inputs the curve parameters (a, b, p, f) where (a, b) are the curve coefficients, p is the characteristic of the prime field over which the curve

$$E : y^2 \equiv x^3 + ax + b \pmod{p}$$

is defined. The order of E is always of the form fq for some prime q and f is called the co-factor. PACE v2 requires the generation of a point that belongs to the q -subgroup of E that we denote by $E[q]$. The point encoding also takes as input a number t such that

$$0 < t < p$$

and returns, in constant time, a point that belongs to $E[q]$. As described in [BCIMRT2010], point encoding comes in two flavors, depending on the coordinate system preferred by the implementation:

- A first implementation, described in Section B.2 outputs the elliptic curve point in affine coordinates (x, y) ;
- An alternate implementation, presented in Section B.3, outputs the same point in Jacobian coordinates (X, Y, Z) .

Irrespective of which option is taken, the generated point is identical in the sense that

$$x = XZ^2 \pmod{p} \text{ and } y = YZ^3 \pmod{p}$$

and the implementation of the subsequent phase of PACE v2 (the elliptic curve Diffie-Hellman key exchange phase) can therefore take advantage of using the option that best fits the interface of the cryptographic API that performs elliptic-curve operations.

As noted hereafter, point encoding for affine coordinates roughly requires two modular exponentiations modulo p whereas point encoding for Jacobian coordinates only requires a single one.

Note that for the two available implementations, point encoding explicitly requires that $p \equiv 3 \pmod{4}$.

B.2 Implementation for Affine Coordinates

The algorithm is implemented as follows:

Inputs: curve parameters (a, b, p, f) and t such that $0 < t < p$

Output: a point (x, y) in the prime-order subgroup $E[q]$ of E

1. Compute $\alpha = -t^2 \pmod{p}$
2. Compute $X_2 = -ba^{-1}(1+(\alpha+\alpha^2)^{-1}) \pmod{p}$
3. Compute $X_3 = \alpha X_2 \pmod{p}$
4. Compute $h_2 = (X_2)^3 + a X_2 + b \pmod{p}$
5. Compute $h_3 = (X_3)^3 + a X_3 + b \pmod{p}$
6. Compute $U = t^3 h_2 \pmod{p}$
7. Compute $A = (h_2)^{p-1-(p+1)/4} \pmod{p}$
8. If $A^2 h_2 = 1 \pmod{p}$ define $(x, y) = (X_2, A h_2 \pmod{p})$

9. Otherwise define $(x, y) = (X_3, A U \bmod p)$
10. Output $(x, y) = [f](x, y)$.

Implementation Notes

Neglecting modular multiplications and additions, the execution time of the above implementation is dominated by two modular exponentiations:

- Step 2 can be rewritten

$$X_2 = -ba^{-1}(1+(a+\alpha^2)^{-1}) = -b(1+a+\alpha^2)(a+\alpha^2)^{p-2} \bmod p$$

which essentially amounts to a modular exponentiation with exponent $p-2$;

- Step 7 is a modular exponentiation with exponent $p-1-(p+1)/4$.

Note: Step 10 requires a scalar multiplication by the co-factor f . For many curves, the co-factor is equal to 1 so that this scalar multiplication can be avoided.

B.3 Implementation for Jacobian Coordinates

The algorithm is implemented as follows:

Inputs: curve parameters (a, b, p, f) and t such that $0 < t < p$

Output: a point (X, Y, Z) in the prime-order subgroup $E[q]$ of E

1. Compute $\alpha = -t^2 \bmod p$
2. Compute $Z = a(\alpha + \alpha^2) \bmod p$
3. Compute $X_2 = -bZ(1 + \alpha + \alpha^2) \bmod p$
4. Compute $X_3 = \alpha X_2 \bmod p$
5. Compute $h_2 = (X_2)^3 + a X_2 Z^4 + b Z^6 \bmod p$
6. Compute $h_3 = (X_3)^3 + a X_3 Z^4 + b Z^6 \bmod p$
7. Compute $U = -\alpha t h_2 \bmod p$
8. Compute $A = (h_2)^{p-1-(p+1)/4} \bmod p$
9. If $A^2 h_2 = 1 \bmod p$ define $(X, Y, Z) = (X_2, A h_2 \bmod p, Z)$
10. Otherwise define $(X, Y, Z) = (X_3, A U \bmod p, Z)$
11. Output $(X, Y, Z) = [f](X, Y, Z)$.

Implementation Notes

Neglecting modular multiplications and additions, the execution time of the above implementation is dominated by the single modular exponentiation of Step 7. Therefore, it is expected to be roughly twice faster than the implementation for affine coordinates.

Note: The scalar multiplication in Step 10 can be completely avoided when the co-factor f is equal to 1.

APPENDIX C WORKED EXAMPLE: BASIC ACCESS CONTROL (INFORMATIVE)

C.1 Compute Keys from Key Seed (K_{seed})

This section provides an example for derivation of 3DES keys from a seed value K_{seed} . This procedure will be used as a “subroutine” in the examples for Basic Access Control.

Input:

$K_{seed} = '239AB9CB282DAF66231DC5A4DF6BFBAE'$

Compute encryption key ($c = '00000001'$):

1. Concatenate K_{seed} and c :
 $D = '239AB9CB282DAF66231DC5A4DF6BFBAE00000001'$
2. Calculate the SHA-1 hash of D :
 $H_{SHA-1}(D) = 'AB94FCEDF2664EDFB9B291F85D7F77F27F2F4A9D'$
3. Form DES keys K_a and K_b , intended to be used as first and second key for 3DES (i.e. the 3DES key is the concatenation of K_a and K_b):
 $K_a = 'AB94FCEDF2664EDF'$
 $K_b = 'B9B291F85D7F77F2'$
4. Adjust parity bits:
 $K_a = 'AB94FDECF2674FDF'$
 $K_b = 'B9B391F85D7F76F2'$

Compute MAC computation key ($c = '00000002'$):

1. Concatenate K_{seed} and c :
 $D = '239AB9CB282DAF66231DC5A4DF6BFBAE00000002'$
2. Calculate the SHA-1 hash of D :
 $H_{SHA-1}(D) = '7862D9ECE03C1BCD4D77089DCF131442814EA70A'$
3. Form keys K_a and K_b :
 $K_a = '7862D9ECE03C1BCD'$
 $K_b = '4D77089DCF131442'$
4. Adjust parity bits:
 $K_a = '7962D9ECE03D1ACD'$
 $K_b = '4C76089DCE131543'$

3. Calculate the SHA-1 hash of 'MRZ_information':
 $H_{\text{SHA-1}}(\text{MRZ_information}) = \text{'239AB9CB282DAF66231DC5A4DF6BFBAEDF477565'}$
4. Take the most significant 16 bytes to form the K_{seed} :
 $K_{\text{seed}} = \text{'239AB9CB282DAF66231DC5A4DF6BFBAE'}$
5. Calculate the basic access keys (K_{Enc} and K_{MAC}) according to section 9.5.2/Appendix C.1:
 $K_{\text{Enc}} = \text{'AB94FDECF2674FDFB9B391F85D7F76F2'}$
 $K_{\text{MAC}} = \text{'7962D9ECE03D1ACD4C76089DCE131543'}$

C.3 Authentication and Establishment of Session Keys

This section provides an example for performing Basic Access Control.

Inspection system:

1. Request an 8 byte random number from the eMRTD's contactless IC:

Command APDU:				
CLA	INS	P1	P2	Le
00	84	00	00	08

Response APDU:	
Response data field	SW1-SW2
RND.IC	9000

$\text{RND.IC} = \text{'4608F91988702212'}$

2. Generate an 8 byte random and a 16 byte random:
 $\text{RND.IFD} = \text{'781723860C06C226'}$
 $\text{K}_{\text{IFD}} = \text{'0B795240CB7049B01C19B33E32804F0B'}$
3. Concatenate RND.IFD, RND.IC and K_{IFD} :
 $\text{S} = \text{'781723860C06C2264608F919887022120B795240CB7049B01C19B33E32804F0B'}$
4. Encrypt S with 3DES key K_{Enc} :
 $\text{E}_{\text{IFD}} = \text{'72C29C2371CC9BDB65B779B8E8D37B29ECC154AA56A8799FAE2F498F76ED92F2'}$
5. Compute MAC over E_{IFD} with 3DES key K_{MAC} :
 $\text{M}_{\text{IFD}} = \text{'5F1448EEA8AD90A7'}$
6. Construct command data for EXTERNAL AUTHENTICATE and send command APDU to the eMRTD's contactless IC:
 $\text{cmd_data} = \text{'72C29C2371CC9BDB65B779B8E8D37B29ECC154AA56A8799FAE2F498F76ED92F25F1448EEA8AD90A7'}$

Command APDU:

CLA	INS	P1	P2	Lc	Command data field	Le
00	82	00	00	28	cmd_data	28

eMRTD's contactless IC:

1. Decrypt and verify received data and compare RND.IC with response on GET CHALLENGE.
2. Generate a 16 byte random:
 $K_{IC} = \text{'0B4F80323EB3191CB04970CB4052790B'}$
3. Calculate XOR of K_{IFD} and K_{IC} :
 $K_{seed} = \text{'0036D272F5C350ACAC50C3F572D23600'}$
4. Calculate session keys (KS_{Enc} and KS_{MAC}) according to section 9.5.1/Appendix C.1:
 $KS_{Enc} = \text{'979EC13B1CBFE9DCD01AB0FED307EAE5'}$
 $KS_{MAC} = \text{'F1CB1F1FB5ADF208806B89DC579DC1F8'}$
5. Calculate send sequence counter:
 $SSC = \text{'887022120C06C226'}$
6. Concatenate RND.IC, RND.IFD and K_{IC} :
 $R = \text{'4608F91988702212781723860C06C2260B4F80323EB3191CB04970CB4052790B'}$
7. Encrypt R with 3DES key K_{Enc} :
 $E_{IC} = \text{'46B9342A41396CD7386BF5803104D7CEDC122B9132139BAF2EEDC94EE178534F'}$
8. Compute MAC over E_{IC} with 3DES key K_{MAC} :
 $M_{IC} = \text{'2F2D235D074D7449'}$
9. Construct response data for EXTERNAL AUTHENTICATE and send response APDU to the inspection system:
 $resp_data = \text{'46B9342A41396CD7386BF5803104D7CEDC122B9132139BAF2EEDC94EE178534F2F2D235D074D7449'}$

Response APDU:	
Response data field	SW1-SW2
resp_data	9000

Inspection system:

1. Decrypt and verify received data and compare received RND.IFD with generated RND.IFD.
2. Calculate XOR of K_{IFD} and K_{IC} :
 $K_{seed} = \text{'0036D272F5C350ACAC50C3F572D23600'}$
3. Calculate session keys (KS_{Enc} and KS_{MAC}) according to section 9.5.1/Appendix C.1:
 $KS_{Enc} = \text{'979EC13B1CBFE9DCD01AB0FED307EAE5'}$
 $KS_{MAC} = \text{'F1CB1F1FB5ADF208806B89DC579DC1F8'}$
4. Calculate send sequence counter:

SSC = '887022120C06C226'

C.4 Secure Messaging

After authentication and establishment of the session keys, the inspection system selects the EF.COM (File ID = '011E') and reads the data using secure messaging. The calculated KS_{Enc} , KS_{MAC} and SSC (previous steps 3 and 4 of the inspection system) will be used.

First the EF.COM will be selected, then the first four bytes of this file will be read so that the length of the structure in the file can be determined and after that the remaining bytes are read.

1. Select EF.COM

Unprotected command APDU:

CLA	INS	P1	P2	Lc	Command data field
00	A4	02	0C	02	01 1E

- a. Mask class byte and pad command header:
CmdHeader = '0CA4020C80000000'
- b. Pad data:
Data = '011E800000000000'
- c. Encrypt data with KS_{Enc} :
EncryptedData = '6375432908C044F6'
- d. Build DO'87':
DO87 = '8709016375432908C044F6'
- e. Concatenate CmdHeader and DO'87':
M = '0CA4020C800000008709016375432908C044F6'
- f. Compute MAC of M:
 - i. Increment SSC with 1:
SSC = '887022120C06C227'
 - ii. Concatenate SSC and M and add padding:
N = '887022120C06C2270CA4020C80000000
8709016375432908C044F68000000000'
 - iii. Compute MAC over N with KS_{MAC} :
CC = 'BF8B92D635FF24F8'
- g. Build DO'8E':
DO8E = '8E08BF8B92D635FF24F8'
- h. Construct and send protected APDU:
ProtectedAPDU = '0CA4020C158709016375432908C0
44F68E08BF8B92D635FF24F800'
- i. Receive response APDU of eMRTD's contactless IC:
RAPDU = '990290008E08FA855A5D4C50A8ED9000'
- j. Verify RAPDU CC by computing MAC of DO'99':
 - i. Increment SSC with 1:
SSC = '887022120C06C228'

- ii. Concatenate SSC and DO'99' and add padding:
K = '887022120C06C2289902900080000000'
- iii. Compute MAC with KS_{MAC} :
CC' = 'FA855A5D4C50A8ED'
- iv. Compare CC' with data of DO'8E' of RAPDU.
'FA855A5D4C50A8ED' == 'FA855A5D4C50A8ED' ? YES.

2. Read Binary of first four bytes:

Unprotected command APDU:

CLA	INS	P1	P2	Le
00	B0	00	00	04

- a. Mask class byte and pad command header:
CmdHeader = '0CB0000080000000'
- b. Build DO'97':
DO97 = '970104'
- c. Concatenate CmdHeader and DO'97':
M = '0CB0000080000000970104'
- d. Compute MAC of M:
 - i. Increment SSC with 1:
SSC = '887022120C06C229'
 - ii. Concatenate SSC and M and add padding:
N = '887022120C06C2290CB00000
80000009701048000000000'
 - iii. Compute MAC over N with KS_{MAC} :
CC = 'ED6705417E96BA55'
- e. Build DO'8E':
DO8E = '8E08ED6705417E96BA55'
- f. Construct and send protected APDU:
ProtectedAPDU = '0CB00000D9701048E08ED6705417E96BA5500'
- g. Receive response APDU of eMRTD's contactless IC:
RAPDU = '8709019FF0EC34F992265199029000
8E08AD55CC17140B2DED9000'
- h. Verify RAPDU CC by computing MAC of concatenation DO'87' and DO'99':
 - i. Increment SSC with 1:
SSC = '887022120C06C22A'
 - ii. Concatenate SSC, DO'87' and DO'99' and add padding:
K = '887022120C06C22A8709019F
F0EC34F99226519902900080'
 - iii. Compute MAC with KS_{MAC} :
CC' = 'AD55CC17140B2DED'
 - iv. Compare CC' with data of DO'8E' of RAPDU:
'AD55CC17140B2DED' == 'AD55CC17140B2DED' ? YES.
- i. Decrypt data of DO'87' with KS_{Enc} :
DecryptedData = '60145F01'

- j. Determine length of structure:
 $L = '14' + 2 = 22$ bytes

3. Read Binary of remaining 18 bytes from offset 4:

Unprotected command APDU:

CLA	INS	P1	P2	Le
00	B0	00	04	12

- a. Mask class byte and pad command header:
 $\text{CmdHeader} = '0CB0000480000000'$
- b. Build DO'97':
 $\text{DO97} = '970112'$
- c. Concatenate CmdHeader and DO'97':
 $\text{M} = '0CB0000480000000970112'$
- d. Compute MAC of M:
 - Increment SSC with 1:
 $\text{SSC} = '887022120C06C22B'$
 - Concatenate SSC and M and add padding:
 $\text{N} = '887022120C06C22B0CB00004800000009701128000000000000'$
 - Compute MAC over N with KS_{MAC} :
 $\text{CC} = '2EA28A70F3C7B535'$
- e. Build DO'8E':
 $\text{DO8E} = '8E082EA28A70F3C7B535'$
- f. Construct and send protected APDU:
 $\text{ProtectedAPDU} = '0CB000040D9701128E082EA28A70F3C7B53500'$
- g. Receive response APDU of eMRTD's contactless IC:
 $\text{RAPDU} = '871901FB9235F4E4037F2327DCC8964F1F9B8C30F42C8E2FFF224A990290008E08C8B2787EAEA07D749000'$
- h. Verify RAPDU CC by computing MAC of concatenation DO'87' and DO'99':
 - Increment SSC with 1:
 $\text{SSC} = '887022120C06C22C'$
 - Concatenate SSC, DO'87' and DO'99' and add padding:
 $\text{K} = '887022120C06C22C871901FB9235F4E4037F2327DCC8964F1F9B8C30F42C8E2FFF224A99029000'$
 - Compute MAC with KS_{MAC} :
 $\text{CC}' = 'C8B2787EAEA07D74'$
 - Compare CC' with data of DO'8E' of RAPDU:
 $'C8B2787EAEA07D74' == 'C8B2787EAEA07D74' ? \text{YES.}$
- i. Decrypt data of DO'87' with KS_{Enc} :
 $\text{DecryptedData} = '04303130365F36063034303030305C026175'$

RESULT:

EF.COM data = '60145F0104303130365F36063034303030305C026175'

APPENDIX D WORKED EXAMPLE: PASSIVE AUTHENTICATION (INFORMATIVE)

- Step 1: Read the Document Security Object (SO_D) (optionally containing the Document Signer Certificate (C_{DS})) from the contactless IC.
- Step 2: Read the Document Signer (DS) from the Document Security Object (SO_D).
- Step 3: The inspection system verifies SO_D by using Document Signer Public Key (KPU_{DS}).
- Step 4: The inspection system verifies C_{DS} by using the Country Signing CA Public Key (KPU_{CSCA}).

If both verifications in step 3 and 4 are correct, then this ensures that the contents of SO_D can be trusted and can be used in the inspection process.

- Step 5: Read the relevant Data Groups from the LDS.
- Step 6: Calculate the hashes of the relevant Data Groups.
- Step 7: Compare the calculated hashes with the corresponding hash values in the SO_D.

If the hash values in step 7 are identical, this ensures that the contents of the Data Group are authentic and unchanged.

APPENDIX E WORKED EXAMPLE: ACTIVE AUTHENTICATION (INFORMATIVE)

This worked example uses the following settings:

1. Integer factorization-based mechanism: RSA
 2. Modulus length (k): 1 024 bits (128 bytes)
 3. Hash algorithm: SHA-1
- Inspection system:

Step 1. Generate an 8 byte random:
RND.IFD = 'F173589974BF40C6'

Step 2. Construct command for internal authenticate and send command APDU to the eMRTD's contactless IC:

Command APDU

CLA	INS	P1	P2	Lc	Command data field	Le
00	88	00	00	08	RND.IFD	00

eMRTD's contactless IC:

- Step 3. Determine M_2 from incoming APDU:
 $M_2 = \text{'F173589974BF40C6'}$
- Step 4. Create the trailer:
 $T = \text{'BC'}$ (i.e. SHA-1)
 t (length of T in octets) = 1
- Step 5. Determine lengths:
a. $c = k - L_h - 8t - 4 = 1024 - 160 - 8 - 4 = 852$ bits
b. $L_{M1} = c - 4 = 848$ bits
- Step 6. Generate nonce M_1 of length L_{M1} :
 $M_1 = \text{'9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8'}$
- Step 7. Create M:
 $M = M_1 | M_2 = \text{'9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8F173589974BF'}$

40C6'

Step 8. Calculate SHA-1 digest of M:
 $H = \text{SHA-1}(M) = \text{'C063AA1E6D22FBD976AB0FE73D94D2D9C6D88127'}$

Step 9.² Construct the message representative:
 $F = \text{'6A'} \parallel M_1 \parallel H \parallel T =$
 $\text{'6A9D2784A67F8E7C659973EA1AEA25D95B6C8F91E5002F369F0FBDCE8A3CEC1991B543F1696546C5524CF23A5303CD6C98599F40B79F377B5F3A1406B3B4D8F96784D23AA88DB7E1032A405E69325FA91A6E86F5C71AEA978264C4A207446DAD4E7292E2DCDA3024B47DA8C063AA1E6D22FBD976AB0FE73D94D2D9C6D88127BC'}$

Step 10. Encrypt F with the Active Authentication Private Key to form the signature:
 $S = \text{'756B683B036A6368F4A2EB29EA700F96E26100AFC0809F60A91733BA29CAB3628CB1A017190A85DADE83F0B977BB513FC9C672E5C93EFEBBE250FE1B722C7CEE F35D26FC8F19219C92D362758FA8CB0FF68CEF320A8753913ED25F69F7CEE7726923B2C43437800BBC9BC028C49806CF2E47D16AE2B2CC1678F2A4456EF98FC9'}$

Step 11. Construct response data for INTERNAL AUTHENTICATE and send response APDU to the inspection system:

Response APDU:

Response data field	SW1-SW2
S	9000

Inspection system:

Step 12. Decrypt the signature with the public key:
 $F = \text{'6A9D2784A67F8E7C659973EA1AEA25D95B6C8F91E5002F369F0FBDCE8A3CEC1991B543F1696546C5524CF23A5303CD6C98599F40B79F377B5F3A1406B3B4D8F96784D23AA88DB7E1032A405E69325FA91A6E86F5C71AEA978264C4A207446DAD4E7292E2DCDA3024B47DA8C063AA1E6D22FBD976AB0FE73D94D2D9C6D88127BC'}$

Step 13. Determine hash algorithm by trailer T*:
 $T = \text{'BC'}$ (i.e. SHA-1)

2. Since the known part (RND.IFD) is not returned, but must be appended by the IFD itself, Partial Recovery applies ('6A').

Step 14. Extract digest:

```
D = `C063AA1E6D22FBD976AB0FE73D94D2D9
C6D88127`
```

Step 15. Extract M_1 :

```
M1 = `9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8`
```

Step 16. Header indicates partial recovery but signature has modulus length so concatenate M_1 with known M_2 (i.e. RND.IFD):

```
M* = `9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8F173589974BF
40C6`
```

Step 17. Calculate SHA-1 digest of M^* :

```
D* = `C063AA1E6D22FBD976AB0FE73D94D2D9
C6D88127`
```

Step 18. Compare D and D^* :

D is equal to D^* so verification successful.

APPENDIX F WORKED EXAMPLE: PACE – GENERIC MAPPING (INFORMATIVE)

This Appendix provides two worked examples for the PACE protocol as defined in Section 4.4 using the generic mapping. The first example is based on ECDH while the second one uses DH. All numbers contained in the tables are noted hexadecimal.

In both examples, the MRZ is used as password. This also leads to the same symmetric key K_{π} . The relevant data fields of the MRZ including the check digits are:

- Serial Number: T220001293;
- Date of Birth: 6408125;
- Date of Expiry: 1010318.

Hence, the encoding K of the MRZ and the derived encryption key K_{π} are

K	7E2D2A41 C74EA0B3 8CD36F86 3939BFA8 E9032AAD
K_{π}	89DED1B2 6624EC1E 634C1989 302849DD

F.1 ECDH based example

This example is based on ECDH applying the standardized BrainpoolP256r1 domain parameters (see [RFC 5639]).

The first section introduces the corresponding `PACEInfo`. Subsequently, the exchanged APDU's including all generated nonces and ephemeral keys are listed and examined.

Elliptic Curve Parameters

Using standardized domain parameters, all information required to perform PACE are given by the data structure `PACEInfo`. In particular, no `PACEDomainParameterInfo` is needed.

<code>PACEInfo</code>	3012060A 04007F00 07020204 02020201 0202010D
-----------------------	--

The detailed structure of `PACEInfo` is itemized in the following table.

<i>Tag</i>	<i>Length</i>	<i>Value</i>	<i>ASN.1 Type</i>	<i>Comment</i>
30	12		SEQUENCE	<code>PACEInfo</code>
06	0A	04 00 7F 00 07 02 02 04 02 02	OBJECT IDENTIFIER	PACE with ECDH, generic mapping and AES 128 session keys
02	01	02	INTEGER	Version 2
02	01	0D	INTEGER	Brainpool P256r1 Standardized Domain Parameters

For convenience, an ASN.1 encoding of the BrainpoolP256r1 domain parameters is given below.

<i>Tag</i>	<i>Length</i>	<i>Value</i>	<i>ASN.1 Type</i>	<i>Comment</i>
------------	---------------	--------------	-------------------	----------------

30	81 EC		SEQUENCE	Domain parameter
06	0A	2A 86 48 CE 3D 02 01	OBJECT IDENTIFIER	Algorithm id-ecPublicKey
30	81 E0		SEQUENCE	Domain Parameter
02	01	01	INTEGER	Version
30	2C		SEQUENCE	Underlying field
06	07	2A 86 48 CE 3D 01 01	OBJECT IDENTIFIER	Prime field
02	21	00 A9 FB 57 DB A1 EE A9 BC 3E 66 0A 90 9D 83 8D 72 6E 3B F6 23 D5 26 20 28 20 13 48 1D 1F 6E 53 77	INTEGER	Prime p
30	44		SEQUENCE	Curve equation
04	20	7D 5A 09 75 FC 2C 30 57 EE F6 75 30 41 7A FF E7 FB 80 55 C1 26 DC 5C 6C E9 4A 4B 44 F3 30 B5 D9	OCTET STRING	Parameter a
04	20	26 DC 5C 6C E9 4A 4B 44 F3 30 B5 D9 BB D7 7C BF 95 84 16 29 5C F7 E1 CE 6B CC DC 18 FF 8C 07 B6	OCTET STRING	Parameter b
04	41		OCTET STRING	Group generator G
		04	-	Uncompressed point
		8B D2 AE B9 CB 7E 57 CB 2C 4B 48 2F FC 81 B7 AF B9 DE 27 E1 E3 BD 23 C2 3A 44 53 BD 9A CE 32 62	-	x-coordinate
		54 7E F8 35 C3 DA C4 FD 97 F8 46 1A 14 61 1D C9 C2 77 45 13 2D ED 8E 54 5C 1D 54 C7 2F 04 69 97	-	y-coordinate
02	21	00 A9 FB 57 DB A1 EE A9 BC 3E 66 0A 90 9D 83 8D 71 8C 39 7A A3 B5 61 A6 F7 90 1E 0E 82 97 48 56 A7	INTEGER	Group order n
02	01	01	INTEGER	Cofactor f

Application flow of the ECDH-based example

To initialize PACE, the terminal sends the command MSE:AT to the chip.

T>C :	00 22 C1 A4 0F 80 0A 04 00 7F 00 07 02 02 04 02 02 83 01 01
C>T :	90 00

Here, T>C is an abbreviation for an APDU sent from terminal to chip while C>T denotes the corresponding response sent by the chip to the terminal. The encoding of the command is explained in the next table.

Command				
CLA	00		Plain	
INS	22		Manage security environment	
P1/P2	C1 A4		Set Authentication Template for mutual authentication	
L_c	0F		Length of data field	
Data	Tag	Length	Value	Comment
	80	0A	04 00 7F 00 07 02 02 04 02 02	Cryptographic mechanism: PACE with ECDH, generic mapping and AES128 session keys
	83	01	01	Password: MRZ
Response				
Status Bytes	90 00		Normal operation	

Encrypted Nonce

Next, the chip randomly generates the nonce s and encrypts it by means of K_r .

Decrypted Nonce s	3F00C4D3 9D153F2B 2A214A07 8D899B22
Encrypted Nonce z	95A3A016 522EE98D 01E76CB6 B98B42C3

The encrypted nonce is queried by the terminal.

T>C :	10 86 00 00 02 7C 00 00
C>T :	7C 12 80 10 95 A3 A0 16 52 2E E9 8D 01 E7 6C B6 B9 8B 42 C3 90 00

The encoding of the command APDU and the corresponding response can be found in the following table.

Command				
CLA	10		Command chaining	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	02		Length of data	
Data	Tag	Length	Value	Comment
	7C	00	-	Absent
L_e	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment

	7C	12		Dynamic Authentication Data
	80	10	95 A3 A0 16 52 2E E9 8D 01 E7 6C B6 B9 8B 42 C3	Encrypted Nonce
Status Bytes	90 00		Normal operation	

Map Nonce

The nonce is mapped to an ephemeral group generator via generic mapping. The required randomly chosen ephemeral keys are also collected in the next table.

Terminal's Private Key	7F4EF07B 9EA82FD7 8AD689B3 8D0BC78C F21F249D 953BC46F 4C6E1925 9C010F99
Terminal's Public Key	7ACF3EFC 982EC455 65A4B155 129EFBC7 4650DCBF A6362D89 6FC70262 E0C2CC5E, 544552DC B6725218 799115B5 5C9BAA6D 9F6BC3A9 618E70C2 5AF71777 A9C4922D
Chip's Private Key	498FF497 56F2DC15 87840041 839A8598 2BE7761D 14715FB0 91EFA7BC E9058560
Chip's Public Key	824FBA91 C9CBE26B EF53A0EB E7342A3B F178CEA9 F45DE0B7 0AA60165 1FBA3F57, 30D8C879 AAA9C9F7 3991E61B 58F4D52E B87A0A0C 709A49DC 63719363 CCD13C54
Shared secret H	60332EF2 450B5D24 7EF6D386 8397D398 852ED6E8 CAF6FFEE F6BF85CA 57057FD5, 0840CA74 15BAF3E4 3BD414D3 5AA4608B 93A2CAF3 A4E3EA4E 82C9C13D 03EB7181
Mapped generator \tilde{G}	8CED63C9 1426D4F0 EB1435E7 CB1D74A4 6723A0AF 21C89634 F65A9AE8 7A9265E2, 8C879506 743F8611 AC33645C 5B985C80 B5F09A0B 83407C1B 6A4D857A E76FE522

The following APDU's are exchanged by terminal and chip to map the nonce.

T>C :	10 86 00 00 45 7C 43 81 41 04 7A CF 3E FC 98 2E C4 55 65 A4 B1 55 12 9E FB C7 46 50 DC BF A6 36 2D 89 6F C7 02 62 E0 C2 CC 5E 54 45 52 DC B6 72 52 18 79 91 15 B5 5C 9B AA 6D 9F 6B C3 A9 61 8E 70 C2 5A F7 17 77 A9 C4 92 2D 00
C>T :	7C 43 82 41 04 82 4F BA 91 C9 CB E2 6B EF 53 A0 EB E7 34 2A 3B F1 78 CE A9 F4 5D E0 B7 0A A6 01 65 1F BA 3F 57 30 D8 C8 79 AA A9 C9 F7 39 91 E6 1B 58 F4 D5 2E B8 7A 0A 0C 70 9A 49 DC 63 71 93 63 CC D1 3C 54 90 00

The structure of the ADPU's can be described as follows:

Command		
CLA	10	Command chaining

INS	86	General Authenticate		
P1/P2	00 00	Keys and protocol implicitly known		
L_c	45	Length of data		
Data	Tag	Length	Value	Comment
	7C	43	-	Dynamic Authentication Data
	81	41		Mapping Data
			04	Uncompressed Point
			7A CF 3E FC 98 2E ... C2 CC 5E	x-coordinate
			54 45 52 DC B6 72 ... C4 92 2D	y-coordinate
L_e	00	Expected maximal byte length of the response data field is 256		
Response				
Data	Tag	Length	Value	Comment
	7C	43		Dynamic Authentication Data
	82	41		Mapping Data
			04	Uncompressed Point
			82 4F BA 91 C9 CB ... BA 3F 57	x-coordinate
			30 D8 C8 79 AA A9 ... D1 3C 54	y-coordinate
Status Bytes	90 00	Normal operation		

Perform Key Agreement

In the third step, chip and terminal perform an anonymous ECDH key agreement using the new domain parameters determined by the ephemeral group generator \tilde{G} of the previous step. Only the x-coordinate is required as shared secret since the KDF only uses the first coordinate to derive the session keys.

Terminal's Private Key	A73FB703 AC1436A1 8E0CFA5A BB3F7BEC 7A070E7A 6788486B EE230C4A 22762595
Terminal's Public Key	2DB7A64C 0355044E C9DF1905 14C625CB A2CEA487 54887122 F3A5EF0D 5EDD301C, 3556F3B3 B186DF10 B857B58F 6A7EB80F 20BA5DC7 BE1D43D9 BF850149 FBB36462
Chip's Private Key	107CF586 96EF6155 053340FD 633392BA 81909DF7 B9706F22 6F32086C 7AFF974A
Chip's Public Key	9E880F84 2905B8B3 181F7AF7 CAA9F0EF B743847F 44A306D2 D28C1D9E C65DF6DB, 7764B222 77A2EDDC 3C265A9F 018F9CB8 52E111B7 68B32690 4B59A019 3776F094
Shared Secret	28768D20 701247DA E81804C9 E780EDE5 82A9996D B4A31502 0B273319 7DB84925

The key agreement is performed as follows:

T>C :	10 86 00 00 45 7C 43 83 41 04 2D B7 A6 4C 03 55 04 4E C9 DF 19 05 14 C6 25 CB A2 CE A4 87 54 88 71 22 F3 A5 EF 0D 5E DD 30 1C 35 56 F3 B3 B1 86 DF 10 B8 57 B5 8F 6A 7E B8 0F 20 BA 5D C7 BE 1D 43 D9 BF 85 01 49 FB B3 64 62 00
C>T :	7C 43 84 41 04 9E 88 0F 84 29 05 B8 B3 18 1F 7A F7 CA A9 F0 EF B7 43 84 7F 44 A3 06 D2 D2 8C 1D 9E C6 5D F6 DB 77 64 B2 22 77 A2 ED DC 3C 26 5A 9F 01 8F 9C B8 52 E1 11 B7 68 B3 26 90 4B 59 A0 19 37 76 F0 94 90 00

The encoding of the key agreement is examined in the following table:

Command				
CLA	10	Command chaining		
INS	86	General Authenticate		
P1/P2	00 00	Keys and protocol implicitly known		
L_c	45	Length of data		
Data	Tag	Length	Value	Comment
	7C	43	-	Dynamic Authentication Data
	83	41		Terminal's Ephemeral Public Key
			04	Uncompressed Point
			2D B7 A6 4C 03 55 ... DD 30 1C	x-coordinate
			35 56 F3 B3 B1 86 ... B3 64 62	y-coordinate
L_e	00	Expected maximal byte length of the response data field is 256		
Response				
Data	Tag	Length	Value	Comment
	7C	43		Dynamic Authentication Data
	84	41		Chip's Ephemeral Public Key
			04	Uncompressed Point
			9E 88 0F 84 29 05 ... 5D F6 DB	x-coordinate
			77 64 B2 22 77 A2 ... 76 F0 94	y-coordinate
Status Bytes	90 00	Normal operation		

By means of the KDF, the AES 128 session keys KS_{ENC} and KS_{MAC} are derived from the shared secret. These are

KS_{Enc}	F5F0E35C 0D7161EE 6724EE51 3A0D9A7F
KS_{MAC}	FE251C78 58B356B2 4514B3BD 5F4297D1

Mutual Authentication

The authentication tokens are derived by means of KS_{MAC} using

Input Data for T_{PCD}	7F494F06 0A04007F 00070202 04020286 41049E88 0F842905 B8B3181F 7AF7CAA9 F0EFB743 847F44A3 06D2D28C 1D9EC65D F6DB7764 B22277A2 EDDC3C26 5A9F018F 9CB852E1 11B768B3 26904B59 A0193776 F094
Input Data for T_{IC}	7F494F06 0A04007F 00070202 04020286 41042DB7 A64C0355 044EC9DF 190514C6 25CBA2CE A4875488 7122F3A5 EF0D5EDD 301C3556 F3B3B186 DF10B857 B58F6A7E B80F20BA 5DC7BE1D 43D9BF85 0149FBB3 6462

as input. The encoding of the input data is shown below

Tag	Length	Value	ASN.1 Type	Comment
7F49	4F		PUBLIC KEY	Input data for T_{PCD}
06	0A	04 00 7F 00 07 02 02 04 02 02	OBJECT IDENTIFIER	PACE with ECDH, generic mapping and AES 128 session keys
86	41		ELLIPTIC CURVE POINT	Chip's Ephemeral Public Point
		04		Uncompressed Point
		9E 88 0F 84 29 ... 5D F6 DB		x-coordinate
		77 64 B2 22 77 ... 76 F0 94		y-coordinate

Tag	Length	Value	ASN.1 Type	Comment
7F49	4F		PUBLIC KEY	Input data for T_{PICC}
06	0A	04 00 7F 00 07 02 02 04 02 02	OBJECT IDENTIFIER	PACE with ECDH, generic mapping and AES 128 session keys
86	41		ELLIPTIC CURVE POINT	Terminal's Ephemeral Public Point
		04		Uncompressed Point
		2D B7 A6 4C 03 ... DD 30 1C		x-coordinate
		35 56 F3 B3 B1 ... B3 64 62		y-coordinate

The computed authentication tokens are:

T _{PCD}	C2B0BD78 D94BA866
T _{IC}	3ABB9674 BCE93C08

Finally, these tokens are exchanged and verified.

T>C :	00 86 00 00 0C 7C 0A 85 08 C2 B0 BD 78 D9 4B A8 66 00
C>T :	7C 0A 86 08 3A BB 96 74 BC E9 3C 08 90 00

F.2 DH based example

The second example is based on DH using the 1024-bit MODP Group with 160-bit Prime Order Subgroup specified by [RFC 5114]. The parameters of the group are:

Prime p	B10B8F96 A080E01D DE92DE5E AE5D54EC 52C99FBC FB06A3C6 9A6A9DCA 52D23B61 6073E286 75A23D18 9838EF1E 2EE652C0 13ECB4AE A9061123 24975C3C D49B83BF ACCBDD7D 90C4BD70 98488E9C 219A7372 4EFFD6FA E5644738 FAA31A4F F55BCCC0 A151AF5F 0DC8B4BD 45BF37DF 365C1A65 E68CFDA7 6D4DA708 DF1FB2BC 2E4A4371
Subgroup Generator g	A4D1CBD5 C3FD3412 6765A442 EFB99905 F8104DD2 58AC507F D6406CFF 14266D31 266FEA1E 5C41564B 777E690F 5504F213 160217B4 B01B886A 5E91547F 9E2749F4 D7FBD7D3 B9A92EE1 909D0D22 63F80A76 A6A24C08 7A091F53 1DBF0A01 69B6A28A D662A4D1 8E73AFA3 2D779D59 18D08BC8 858F4DCE F97C2A24 855E6EEB 22B3B2E5
Prime Order q of g	F518AA87 81A8DF27 8ABA4E7D 64B7CB9D 49462353

The first section introduces the PACEInfo. Subsequently, the exchanged APDU's including all generated nonces and ephemeral keys are listed and examined.

Diffie Hellman Parameters

The relevant information for PACE is given by the data structure PACEInfo.

PACEInfo	3012060A 04007F00 07020204 01020201 02020100
----------	--

The detailed structure of PACEInfo is:

Tag	Length	Value	ASN.1 Type	Comment
30	12		SEQUENCE	PACEInfo

06	0A	04 00 7F 00 07 02 02 04 01 02	OBJECT IDENTIFIER	OID: PACE with DH, generic mapping and AES 128 session keys
02	01	02	INTEGER	Version 2
02	01	00	INTEGER	Standardized 1024-bit Group specified by RFC 5114

Application flow of the DH-based example

To initialize PACE, the terminal sends the command MSE:AT to the chip.

T>C :	00 22 C1 A4 0F 80 0A 04 00 7F 00 07 02 02 04 01 02 83 01 01
C>T :	90 00

The encoding of the command is described in the next table.

Command				
CLA	00	Plain		
INS	22	Manage security environment		
P1/P2	C1 A4	Set Authentication Template for mutual authentication		
L_c	0F	Length of data field		
Data	Tag	Length	Value	Comment
	80	0A	04 00 7F 00 07 02 02 04 01 02	OID: Cryptographic mechanism: PACE with DH, generic mapping and AES128
	83	01	01	Password: MRZ
Response				
Status Bytes	90 00	Normal operation		

Encrypted Nonce

Next, the terminal queries a nonce from the chip.

Decrypted Nonce s	FA5B7E3E 49753A0D B9178B7B 9BD898C8
Encrypted Nonce z	854D8DF5 827FA685 2D1A4FA7 01CDDCA

The communication looks as follows.

T>C :	10 86 00 00 02 7C 00 00
C>T :	7C 12 80 10 85 4D 8D F5 82 7F A6 85 2D 1A 4F A7 01 CD DD CA 90 00

The encoding of the command APDU and the corresponding response is described in the following table.

Command

CLA	10	Command chaining		
INS	86	General Authenticate		
P1/P2	00 00	Keys and protocol implicitly known		
L_c	02	Length of data		
Data	Tag	Length	Value	Comment
	7C	00	-	Absent
L_e	00	Expected maximal byte length of the response data field is 256		
Response				
Data	Tag	Length	Value	Comment
	7C	12		Dynamic Authentication Data
	80	10	85 4D 8D F5 82 7F A6 85 2D 1A 4F A7 01 CD DD CA	Encrypted Nonce
Status Bytes	90 00	Normal operation		

Map Nonce

By means of the generic mapping, the nonce is mapped to an ephemeral group generator. For that purpose, the following ephemeral keys are randomly generated by terminal and chip.

Terminal's Private Key	24C3C0E0 A3280ECB 943345D9 DC2A7B72 539FDA6F FDF99AB7 B6CDDDD1 BE425AF3 D02C4ED0 CDD73EBB 4B2EDF8C 07FB3A35 903F72B8 4F3771F4 EBF4952 0D61A8F7 C7FB8C9E 2ABC24BF 4FF9D8DD F381A193 80C85B62 3AB02ACB F6D220F5 12BF4065 8322AD20 9AC0BF9E 6F8DB602 D5197D25 2BF6D148 510CA1B7 40AF0F99 F33CA5F1
Terminal's Public Key	23FB3749 EA030D2A 25B278D2 A562047A DE3F01B7 4F17A154 02CB7352 CA7D2B3E B71C343D B13D1DEB CE9A3666 DBCFC920 B49174A6 02CB4796 5CAA73DC 702489A4 4D41DB91 4DE9613D C5E98C94 160551C0 DF86274B 9359BC04 90D01B03 AD54022D CB4F57FA D6322497 D7A1E28D 46710F46 1AFE710F BBBC5F8B A166F431 1975EC6C
Chip's Private Key	4EC025E4 0C6D10B2 AAF6FCAC 98C4244F 57481A49 61F3ADC3 72A95E40 E0CC3555 F73CCFC6 5E9DB956 DD61B143 E0C7DC51 9E7DD8ED D8E3E46A 094CF226 4FD193D0 BC4BC05C DE6CA443 19C2439F D04A4644 3C8D0494 487F6F2F E9AC8BE9 B9EE16A3 D242668C BA4FFD42 EEAC3650 9E16B4D1 E6E8EE00 25FF8244 B190F57D 441EC328
Chip's Public Key	78879F57 225AA808 0D52ED0F C890A4B2 5336F699 AA89A2D3 A189654A F70729E6 23EA5738 B26381E4 DA19E004 706FACE7 B235C2DB F2F38748 312F3C98 C2DD4882 A41947B3 24AA1259 AC22579D B93F7085

	655AF308 89DBB845 D9E6783F E42C9F24 49400306 254C8AE8 EE9DD812 A804C0B6 6E8CAFC1 4F84D825 8950A91B 44126EE6
Shared secret H	5BABEBEF 5B74E5BA 94B5C063 FDA15F1F 1CDE9487 3EE0A5D3 A2FCAB49 F258D07F 544F13CB 66658C3A FEE9E727 389BE3F6 CBBBD321 28A8C21D D6EEA3CF 7091CDDF B08B8D00 7D40318D CCA4FFBF 51208790 FB4BD111 E5A968ED 6B6F08B2 6CA87C41 0B3CE0C3 10CE104E ABD16629 AA48620C 1279270C B0750C0D 37C57FFF E302AE7F
Mapped generator \tilde{g}	7C9CBFE9 8F9FBDDA 8D143506 FA7D9306 F4CB17E3 C71707AF F5E1C1A1 23702496 84D64EE3 7AF44B8D BD9D45BF 6023919C BAA027AB 97ACC771 666C8E98 FF483301 BFA4872D EDE9034E DFACB708 14166B7F 36067682 9B826BEA 57291B5A D69FBC84 EF1E7790 32A30580 3F743417 93E86974 2D401325 B37EE856 5FFCDEE6 18342DC5

The following APDU's are exchanged by terminal and chip to map the nonce.

T>C :	10 86 00 00 86 7C 81 83 81 81 80 23 FB 37 49 EA 03 0D 2A 25 B2 78 D2 A5 62 04 7A DE 3F 01 B7 4F 17 A1 54 02 CB 73 52 CA 7D 2B 3E B7 1C 34 3D B1 3D 1D EB CE 9A 36 66 DB CF C9 20 B4 91 74 A6 02 CB 47 96 5C AA 73 DC 70 24 89 A4 4D 41 DB 91 4D E9 61 3D C5 E9 8C 94 16 05 51 C0 DF 86 27 4B 93 59 BC 04 90 D0 1B 03 AD 54 02 2D CB 4F 57 FA D6 32 24 97 D7 A1 E2 8D 46 71 0F 46 1A FE 71 0F BB BC 5F 8B A1 66 F4 31 19 75 EC 6C 00
C>T :	7C 81 83 82 81 80 78 87 9F 57 22 5A A8 08 0D 52 ED 0F C8 90 A4 B2 53 36 F6 99 AA 89 A2 D3 A1 89 65 4A F7 07 29 E6 23 EA 57 38 B2 63 81 E4 DA 1 9E0 04 70 6F AC E7 B2 35 C2 DB F2 F3 87 48 31 2F 3C 98 C2 DD 48 82 A4 19 47 B3 24 AA 12 59 AC 22 57 9D B9 3F 70 85 65 5A F3 08 89 DB B8 45 D9 E6 78 3F E4 2C 9F 24 49 40 03 06 25 4C 8A E8 EE 9D D8 12 A8 04 C0 B6 6E 8C AF C1 4F 84 D8 25 89 50 A9 1B 44 12 6E E6 90 00

The structure of the ADPU's can be described as follows:

Command				
CLA	10	Command chaining		
INS	86	General Authenticate		
P1/P2	00 00	Keys and protocol implicitly known		
L_c	86	Length of data		
Data	Tag	Length	Value	Comment
	7C	81 83	-	Dynamic Authentication Data
	81	81 80	23 FB 37 49 EA 03 ... 75 EC 6C	Mapping Data
L_e	00	Expected maximal byte length of the response data field is 256		

Response				
Data	Tag	Length	Value	Comment
	7C	81 83		Dynamic Authentication Data
	82	81 80	ED 0F C8 90 A4 B2 ... 12 6E E6	Mapping Data
Status Bytes	90 00		Normal operation	

Perform Key Agreement

Subsequently, chip and terminal perform an anonymous DH key agreement using the new domain parameters determined by the ephemeral group generator \tilde{g} of the previous step.

Terminal's Private Key	4BD0E547 40F9A028 E6A515BF DAF96784 8C4F5F5F FF65AA09 15947FFD 1A0DF2FA 6981271B C905F355 1457B7E0 3AC3B806 6DE4AA40 6C1171FB 43DD939C 4BA16175 103BA3DE E16419AA 248118F9 0CC36A3D 6F4C3736 52E0C3CC E7F0F1D0 C5425B36 00F0F0D6 A67F004C 8BBA33F2 B4733C72 52445C1D FC4F1107 203F71D2 EFB28161
Terminal's Public Key	00907D89 E2D425A1 78AA81AF 4A7774EC 8E388C11 5CAE6703 1E85EECE 520BD911 551B9AE4 D04369F2 9A02626C 86FBC674 7CC7BC35 2645B616 1A2A42D4 4EDA80A0 8FA8D61B 76D3A154 AD8A5A51 786B0BC0 71470578 71A92221 2C5F67F4 31731722 36B7747D 1671E6D6 92A3C7D4 0A0C3C5C E397545D 015C175E B5130551 EDBC2EE5 D4
Chip's Private Key	020F018C 7284B047 FA7721A3 37EFB7AC B1440BB3 0C5252BD 41C97C30 C994BB78 E9F0C5B3 2744D840 17D21FFA 6878396A 6469CA28 3EF5C000 DAF7D261 A39AB886 0ED4610A B5343390 897AAB5A 7787E4FA EFA0649C 6A94FDF8 2D991E8E 3FC332F5 142729E7 040A3F7D 5A4D3CD7 5CBEE1F0 43C1CAD2 DD484FEB 4ED22B59 7D36688E
Chip's Public Key	075693D9 AE941877 573E634B 6E644F8E 60AF17A0 076B8B12 3D920107 4D36152B D8B3A213 F53820C4 2ADC79AB 5D0AEEC3 AEFB9139 4DA476BD 97B9B14D 0A65C1FC 71A0E019 CB08AF55 E1F72900 5FBA7E3F A5DC4189 9238A250 767A6D46 DB974064 386CD456 743585F8 E5D90CC8 B4004B1F 6D866C79 CE0584E4 9687FF61 BC29AEA1
Shared Secret	6BABC7B3 A72BCD7E A385E4C6 2DB2625B D8613B24 149E146A 629311C4 CA6698E3 8B834B6A 9E9CD718 4BA8834A FF5043D4 36950C4C 1E783236 7C10CB8C 314D40E5 990B0DF7 013E64B4 549E2270 923D06F0 8CFF6BD3 E977DDE6 ABE4C31D 55C0FA2E 465E553E 77BDF75E 3193D383 4FC26E8E

	B1EE2FA1 E4FC97C1 8C3F6CFF FE2607FD
--	-------------------------------------

The key agreement is performed as follows:

T>C :	10 86 00 00 86 7C 81 83 83 81 80 90 7D 89 E2 D4 25 A1 78 AA 81 AF 4A 77 74 EC 8E 38 8C 11 5C AE 67 03 1E 85 EE CE 52 0B D9 11 55 1B 9A E4 D0 43 69 F2 9A 02 62 6C 86 FB C6 74 7C C7 BC 35 26 45 B6 16 1A 2A 42 D4 4E DA 80 A0 8F A8 D6 1B 76 D3 A1 54 AD 8A 5A 51 78 6B 0B C0 71 47 05 78 71 A9 22 21 2C 5F 67 F4 31 73 17 22 36 B7 74 7D 16 71 E6 D6 92 A3 C7 D4 0A 0C 3C 5C E3 97 54 5D 01 5C 17 5E B5 13 05 51 ED BC 2E E5 D4 00
C>T :	7C 81 83 84 81 80 07 56 93 D9 AE 94 18 77 57 3E 63 4B 6E 64 4F 8E 60 AF 17 A0 07 6B 8B 12 3D 92 01 07 4D 36 15 2B D8 B3 A2 13 F5 38 20 C4 2A DC 79 AB 5D 0A EE C3 AE FB 91 39 4D A4 76 BD 97 B9 B1 4D 0A 65 C1 FC 71 A0 E0 19 CB 08 AF 55 E1 F7 29 00 5F BA 7E 3F A5 DC 41 89 92 38 A2 50 76 7A 6D 46 DB 97 40 64 38 6C D4 56 74 35 85 F8 E5 D9 0C C8 B4 00 4B 1F 6D 86 6C 79 CE 05 84 E4 96 87 FF 61 BC 29 AE A1 90 00

Command				
CLA	10	Command chaining		
INS	86	General Authenticate		
P1/P2	00 00	Keys and protocol implicitly known		
L_c	86	Length of data		
Data	Tag	Length	Value	Comment
	7C	81 83	-	Dynamic Authentication Data
	83	81 80	90 7D 89 E2 D4 25 ... 2E E5 D4	Terminal's Ephemeral Public Key
L_e	00	Expected maximal byte length of the response data field is 256		
Response				
Data	Tag	Length	Value	Comment
	7C	81 83		Dynamic Authentication Data
	84	81 80	07 56 93 D9 AE 94 ... 29 AE A1	Chip's Ephemeral Public Key
Status Bytes	90 00	Normal operation		

The AES 128 session keys KS_{Enc} and KS_{MAC} are derived from the shared secret using the KDF.

KS_{Enc}	2F7F46AD CC9E7E52 1B45D192 FAFA9126
KS_{MAC}	805A1D27 D45A5116 F73C5446 9462B7D8

Mutual Authentication

The authentication tokens are constructed from the following input data.

Input Data for T_{PCD}	7F49818F 060A0400 7F000702 02040102 84818007 5693D9AE 94187757 3E634B6E 644F8E60 AF17A007 6B8B123D 9201074D 36152BD8 B3A213F5 3820C42A DC79AB5D 0AEEC3AE FB91394D A476BD97 B9B14D0A 65C1FC71 A0E019CB 08AF55E1 F729005F BA7E3FA5 DC418992 38A25076 7A6D46DB 97406438 6CD45674 3585F8E5 D90CC8B4 004B1F6D 866C79CE 0584E496 87FF61BC 29AEA1
Input Data for T_{IC}	7F49818F 060A0400 7F000702 02040102 84818090 7D89E2D4 25A178AA 81AF4A77 74EC8E38 8C115CAE 67031E85 EECE520B D911551B 9AE4D043 69F29A02 626C86FB C6747CC7 BC352645 B6161A2A 42D44EDA 80A08FA8 D61B76D3 A154AD8A 5A51786B 0BC07147 057871A9 22212C5F 67F43173 172236B7 747D1671 E6D692A3 C7D40A0C 3C5CE397 545D015C 175EB513 0551EDBC 2EE5D4

The encoding of the input data is shown below

Tag	Length	Value	ASN.1 Type	Comment
7F49	81 8F		PUBLIC KEY	Input data for T_{PCD}
06	0A	04 00 7F 00 07 02 02 04 01 02	OBJECT IDENTIFIER	PACE with DH, generic mapping and AES 128 session keys
84	81 80	07 56 93 D9 AE ... 29 AE A1	UNSIGNED INTEGER	Chip's Ephemeral Public Key

Tag	Length	Value	ASN.1 Type	Comment
7F49	81 8F		PUBLIC KEY	Input data for T_{PICC}
06	0A	04 00 7F 00 07 02 02 04 01 02	OBJECT IDENTIFIER	PACE with DH, generic mapping and AES 128 session keys
84	81 80	90 7D 89 E2 D4 ... 2E E5 D4	UNSIGNED INTEGER	Terminal's Ephemeral Public Key

The computed authentication tokens are

T_{PCD}	B46DD9BD 4D98381F
T_{IC}	917F37B5 C0E6D8D1

Finally, these tokens are exchanged and verified.

$T > C$:	00 86 00 00 0C 7C 0A 85 08 B4 6D D9 BD 4D 98 38 1F 00
$C > T$:	7C 1B 86 08 91 7F 37 B5 C0 E6 D8 D1 87 0F 44 45 54 45 53 54 43 56 43 41 30 30 30 30 33

Command				
CLA	00		Plain	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	0C		Length of data	
Data	Tag	Length	Value	Comment
	7C	0A	-	Dynamic Authentication Data
	85	08	B4 6D D9 BD 4D 98 38 1F	Terminal's Authentication Token
L_e	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	0A		Dynamic Authentication Data
	86	08	91 7F 37 B5 C0 E6 D8 D1	Chip's Authentication Token
Status Bytes	90 00		Normal operation	

APPENDIX G WORKED EXAMPLE: PACE – INTEGRATED MAPPING (INFORMATIVE)

This section provides two examples for the PACE protocol with Integrated Mapping. The first one is based on Elliptic Curve Diffie-Hellman (ECDH) and the second one on Diffie-Hellman (DH). The MRZ-derived key K from the previous Example is used.

G.1 ECDH based example

This example is based on the BrainpoolP256r1 elliptic curve. The block cipher used in this example is AES-128. For reminder, the curve parameters are the following:

Prime p	A9FB57DB A1EEA9BC 3E660A90 9D838D72 6E3BF623 D5262028 2013481D 1F6E5377
Parameter a	7D5A0975 FC2C3057 EEF67530 417AFFE7 FB8055C1 26DC5C6C E94A4B44 F330B5D9
Parameter b	26DC5C6C E94A4B44 F330B5D9 BBD77CBF 95841629 5CF7E1CE 6BCCDC18 FF8C07B6
x-coordinate of the group generator G	8BD2AEB9 CB7E57CB 2C4B482F FC81B7AF B9DE27E1 E3BD23C2 3A4453BD 9ACE3262
y-coordinate of the group generator G	547EF835 C3DAC4FD 97F8461A 14611DC9 C2774513 2DED8E54 5C1D54C7 2F046997
Group order n	A9FB57DB A1EEA9BC 3E660A90 9D838D71 8C397AA3 B561A6F7 901E0E82 974856A7
Cofactor f	01

The encryption key is the following:

K_{\square}	591468CD A83D6521 9CCCB856 0233600F
---------------	-------------------------------------

Encrypted Nonce

A nonce s is randomly chosen by the chip and encrypted using K_{\square} . The encrypted nonce z is then sent to the terminal.

Decrypted Nonce s	2923BE84 E16CD6AE 529049F1 F1BBE9EB
Encrypted Nonce z	143DC40C 08C8E891 FBED7DED B92B64AD

Map Nonce

A nonce t is randomly chosen and sent in clear. t and s are then used to compute the Integrated Mapping. First, the pseudo-random function R_p , derived from AES, is applied to s and t . Then, the point encoding f_G is used on the result to compute the Mapped Generator $\hat{G}=f_G(R_p(s,t))$.

Nonce t	5DD4CBFC 96F5453B 130D890A 1CDBAE32
Pseudo-random $R(s,t)$	E4447E2D FB3586BA C05DDB00 156B57FB B2179A39 49294C97 25418980 0C517BAA 8DA0FF39 7ED8C445 D3E421E4 FEB57322

$R_p(s,t)$	A2F8FF2D F50E52C6 599F386A DCB595D2 29F6A167 ADE2BE5F 2C3296AD D5B7430E
x-coordinate of the Mapped Generator \hat{G}	8E82D315 59ED0FDE 92A4D049 8ADD3C23 BABA94FB 77691E31 E90AEA77 FB17D427
y-coordinate of the Mapped Generator \hat{G}	4C1AE14B D0C3DBAC 0C871B7F 36081693 64437CA3 0AC243A0 89D3F266 C1E60FAD

Perform Key Agreement

The chip and the terminal perform an anonymous Diffie-Hellman key agreement using their secret keys and the mapped generator \hat{G} . The shared secret K is the x-coordinate of agreement.

Chip's private key SK_{ic}	107CF586 96EF6155 053340FD 633392BA 81909DF7 B9706F22 6F32086C 7AFF974A
Chip's public key PK_{ic}	67F78E5F 7F768608 2B293E8D 087E0569 16D0F74B C01A5F89 57D0DE45 691E51E8 932B69A9 62B52A09 85AD2C0A 271EE6A1 3A8ADDDC D1A3A994 B9DED257 F4D22753
Terminal's private key SK_{PCD}	A73FB703 AC1436A1 8E0CFA5A BB3F7BEC 7A070E7A 6788486B EE230C4A 22762595
Terminal's public key PK_{PCD}	89CBA23F FE96AA18 D824627C 3E934E54 A9FD0B87 A95D1471 DC1C0ABF DCD640D4 6755DE9B 7B778280 B6BEBD57 439ADFEB 0E21FD4E D6DF4257 8C13418A 59B34C37
Shared secret K	4F150FDE 1D4F0E38 E95017B8 91BAE171 33A0DF45 B0D3E18B 60BA7BEA FDC2C713

Using the specifications from [1], the session keys K_{Enc} and K_{MAC} are derived from K using the hash function SHA-1: $K_{Enc} = \text{SHA-1}(K || 0x00000001)$ and $K_{MAC} = \text{SHA-1}(K || 0x00000002)$. Then, only the first 16 octets of the digest are used with the following result:

K_{Enc}	0D3FEB33 251A6370 893D62AE 8DAAF51B
K_{MAC}	B01E89E3 D9E8719E 586B50B4 A7506E0B

Mutual Authentication

The authentication tokens are computed using a CMAC on the following inputs with the key K_{MAC} .

Input data for T_{ic}	7F494F06 0A04007F 00070202 04040286 410489CB A23FFE96 AA18D824 627C3E93 4E54A9FD 0B87A95D 1471DC1C 0ABFDCD6 40D46755 DE9B7B77 8280B6BE BD57439A DFEB0E21 FD4ED6DF 42578C13 418A59B3 4C37
Input data for T_{PCD}	7F494F06 0A04007F 00070202 04040286 410467F7 8E5F7F76 86082B29 3E8D087E 056916D0 F74BC01A 5F8957D0 DE45691E 51E8932B 69A962B5 2A0985AD 2C0A271E E6A13A8A DDDCD1A3 A994B9DE D257F4D2 2753

The corresponding authentication tokens are:

T_{IC}	75D4D96E 8D5B0308
T_{PCD}	450F02B8 6F6A0909

G.2 DH based example

This example is based on the 1024-bit MODP Group with 160-bit Prime Order Subgroup. The block cipher used in this example is AES-128.

The group parameters are:

Prime p	B10B8F96 A080E01D DE92DE5E AE5D54EC 52C99FBC FB06A3C6 9A6A9DCA 52D23B61 6073E286 75A23D18 9838EF1E 2EE652C0 13ECB4AE A9061123 24975C3C D49B83BF ACCBDD7D 90C4BD70 98488E9C 219A7372 4EFFD6FA E5644738 FAA31A4F F55BCCC0 A151AF5F 0DC8B4BD 45BF37DF 365C1A65 E68CFDA7 6D4DA708 DF1FB2BC 2E4A4371
Subgroup generator g	A4D1CBD5 C3FD3412 6765A442 EFB99905 F8104DD2 58AC507F D6406CFF 14266D31 266FEA1E 5C41564B 777E690F 5504F213 160217B4 B01B886A 5E91547F 9E2749F4 D7FBD7D3 B9A92EE1 909D0D22 63F80A76 A6A24C08 7A091F53 1DBF0A01 69B6A28A D662A4D1 8E73AFA3 2D779D59 18D08BC8 858F4DCE F97C2A24 855E6EEB 22B3B2E5
Prime order q of g	F518AA87 81A8DF27 8ABA4E7D 64B7CB9D 49462353

The following encryption key is used:

K_{\square}	591468CD A83D6521 9CCCB856 0233600F
---------------	-------------------------------------

Encrypted Nonce

A nonce s is randomly chosen by the chip and encrypted using K_{\square} . The encrypted nonce z is then sent to the terminal.

Decrypted Nonce s	FA5B7E3E 49753A0D B9178B7B 9BD898C8
Encrypted Nonce z	9ABB8864 CA0FF155 1E620D1E F4E13510

Map Nonce

A nonce t is randomly chosen and sent in clear. t and s are then used to compute the Integrated Mapping. First, the pseudo-random function R_p , derived from AES, is applied to s and t. Then, the point encoding f_g is used on the result.

Nonce t	B3A6DB3C 870C3E99 245E0D1C 06B747DE
Pseudo-random $R(s,t)$	EAB98D13 E0905295 2AA72990 7C3C9461 84DEA0FE 74AD2B3A F506F0A8 3018459C 38099CD1 F7FF4EA0 A078DB1F AC136550 5E3DC855 00EF95E2 0B4EEF2E 88489233 BEE0546B 472F994B 618D1687 02406791 DEEF3CB4 810932EC 278F3533 FDB860EB 4835C36F A4F1BF3F A0B828A7 18C96BDE

	88FBA38A 3E6C35AA A1095925 1EB5FC71 0FC18725 8995944C 0F926E24 9373F485
$R_p(s,t)$	A0C7C50C 002061A5 1CC87D25 4EF38068 607417B6 EE1B3647 3CFB800D 2D2E5FA2 B6980F01 105D24FA B22ACD1B FA5C8A4C 093ECDFA FE6D7125 D42A843E 33860383 5CF19AFA FF75EFE2 1DC5F6AA 1F9AE46C 25087E73 68166FB0 8C1E4627 AFED7D93 570417B7 90FF7F74 7E57F432 B04E1236 819E0DFE F5B6E77C A4999925 328182D2
Mapped Generator $\hat{g} = f_g(R_p(s,t))$	1D7D767F 11E333BC D6DBAEF4 0E799E7A 926B9697 3550656F F3C83072 6D118D61 C276CDCC 61D475CF 03A98E0C 0E79CAEB A5BE2557 8BD4551D 0B109032 36F0B0F9 76852FA7 8EEA14EA 0ACA87D1 E91F688F E0DFF897 BBE35A47 2621D343 564B262F 34223AE8 FC59B664 BFEDFA2B FE7516CA 5510A6BB B633D517 EC25D4E0 BBAA16C2

Perform Key Agreement

The chip and the terminal perform an anonymous Diffie-Hellman key agreement using their secret keys and the mapped generator \hat{g} .

Chip's private key SK_{ic}	020F018C 7284B047 FA7721A3 37EFB7AC B1440BB3 0C5252BD 41C97C30 C994BB78 E9F0C5B3 2744D840 17D21FFA 6878396A 6469CA28 3EF5C000 DAF7D261 A39AB886 0ED4610A B5343390 897AAB5A 7787E4FA EFA0649C 6A94FDF8 2D991E8E 3FC332F5 142729E7 040A3F7D 5A4D3CD7 5CBEE1F0 43C1CAD2 DD484FEB 4ED22B59 7D36688E
Chip's public key PK_{ic}	928D9A0F 9DBA450F 13FC859C 6F290D1D 36E42431 138A4378 500BEB4E 0401854C FF111F71 CB6DC1D0 335807A1 1388CC8E AA87B079 07AAD9FB A6B169AF 6D8C26AF 8DDDC39A DC3AD2E3 FF882B84 D23E9768 E95A80E4 746FB07A 9767679F E92133B4 D379935C 771BD7FB ED6C7BB4 B1708B27 5EA75679 524CDC9C 6A91370C C662A2F3
Terminal's private key SK_{PCD}	4BD0E547 40F9A028 E6A515BF DAF96784 8C4F5F5F FF65AA09 15947FFD 1A0DF2FA 6981271B C905F355 1457B7E0 3AC3B806 6DE4AA40 6C1171FB 43DD939C 4BA16175 103BA3DE E16419AA 248118F9 0CC36A3D 6F4C3736 52E0C3CC E7F0F1D0 C5425B36 00F0F0D6 A67F004C 8BBA33F2 B4733C72 52445C1D FC4F1107 203F71D2 EFB28161
Terminal's public key PK_{PCD}	0F0CC629 45A80292 51FB7EF3 C094E12E C68E4EF0 7F27CB9D 9CD04C5C 4250FAE0 E4F8A951 557E929A EB48E5C6 DD47F2F5 CD7C351A 9BD2CD72 2C07EDE1 66770F08 FFCB3702 62CF308D D7B07F2E 0DA9CAAA 1492344C 85290691 9538C98A 4BA4187E 76CE9D87 832386D3 19CE2E04 3C3343AE AE6EDBA1 A9894DC5 094D22F7 FE1351D5
Shared secret K	419410D6 C0A17A4C 07C54872 CE1CBCEB 0A2705C1 A434C8A8 9A4CFE41 F1D78124 CA7EC52B DE7615E5 345E48AB 1ABB6E7D 1D59A57F 3174084D 3CA45703 97C1F622

	28BDFDB2 DA191EA2 239E2C06 0DBE3BBC 23C2FCD0 AF12E0F9 E0B99FCF 91FF1959 011D5798 B2FCBC1F 14FCC24E 441F4C8F 9B08D977 E9498560 E63E7FFA B3134EA7
--	--

The session keys K_{Enc} and K_{MAC} are derived from K using the hash function SHA-1: $K_{Enc} = \text{SHA-1}(K || 0x00000001)$ and $K_{MAC} = \text{SHA-1}(K || 0x00000002)$. Then, only the first 16 octets of the digest are used with the following result:

K_{Enc}	01AFC10C F87BE36D 8179E873 70171F07
K_{MAC}	23F0FBD0 5FD6C7B8 B88F4C83 09669061

Mutual Authentication

The authentication tokens are computed using a CMAC on the following inputs with the key K_{MAC} .

Input data for T_{IC}	7F49818F 060A0400 7F000702 02040302 8481800F 0CC62945 A8029251 FB7EF3C0 94E12EC6 8E4EF07F 27CB9D9C D04C5C42 50FAE0E4 F8A95155 7E929AEB 48E5C6DD 47F2F5CD 7C351A9B D2CD722C 07EDE166 770F08FF CB370262 CF308DD7 B07F2E0D A9CAAA14 92344C85 29069195 38C98A4B A4187E76 CE9D8783 2386D319 CE2E043C 3343AEAE 6EDBA1A9 894DC509 4D22F7FE 1351D5
Input data for T_{PCD}	7F49818F 060A0400 7F000702 02040302 84818092 8D9A0F9D BA450F13 FC859C6F 290D1D36 E4243113 8A437850 0BEB4E04 01854CFF 111F71CB 6DC1D033 5807A113 88CC8EAA 87B07907 AAD9FBA6 B169AF6D 8C26AF8D DDC39ADC 3AD2E3FF 882B84D2 3E9768E9 5A80E474 6FB07A97 67679FE9 2133B4D3 79935C77 1BD7FBED 6C7BB4B1 708B275E A7567952 4CDC9C6A 91370CC6 62A2F3

The corresponding authentication tokens are:

T_{IC}	C2F04230 187E1525
T_{PCD}	55D61977 CBF5307E

REFERENCES (NORMATIVE)

- [X9.42] ANSI: X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, 1999
- [ISO/IEC 7816-4] ISO/IEC 7816-4:2013 Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange
- [ISO/IEC 8859-1] ISO/IEC 8859-1:1998 Information Technology — 8-bit single-byte-coded graphic character sets — Part 1: Latin alphabet No. 1
- [ISO/IEC 9796-2] ISO/IEC 9796-2:2010 Information Technology — Security Techniques — Digital Signature Schemes giving message recovery — Part 2: Integer factorisation based mechanisms
- [ISO/IEC 9797-1] ISO/IEC 9797-1:2011 Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher
- [ISO/IEC 10116] ISO/IEC 10116:2006 Information technology – Security techniques – Modes of operation for an n-bit block cipher
- [ISO/IEC 11568-2] ISO/IEC 11568-2:2012 Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle
- [ISO/IEC 11770-2] ISO/IEC 11770-2:2008 Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques
- [FIPS 46-3] NIST FIPS PUB 46-3, Data Encryption Standard (DES), 1999
- [FIPS 180-2] NIST FIPS PUB 180-2, Secure hash standard (and Change Notice to include SHA-224), 2002
- [FIPS 186-4] NIST FIPS PUB 186-4, Digital Signature Standard (DSS), 2013
- [FIPS 197] NIST FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), 2001
- [SP 800-38B] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
- [RFC 2631] Rescorla, Eric: RFC 2631 Diffie-Hellman key agreement method, 1999
- [RFC 5114] Lepinski, Matt; Kent, Stephen: RFC 5114 Additional Diffie-Hellman Groups for Use with IETF Standards, 2008
- [RFC 5280] D. Cooper, S. Santesson, S. Farrell, S. Boyen, R. Housley, W. Polk, RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2008
- [RFC 5639] Lochter, Manfred; Merkle, Johannes: RFC 5639 Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010
- [TR-03111] BSI: Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, 2012
- [PKCS#3] RSA Laboratories, PKCS#3: Diffie-Hellman key-agreement standard, 1993

- [Keesing2009] J. Bender, D. Kügler: Introducing the PACE solution, in: Keesing Journal of Documents & Identity, Issue 30, Keesing, 2009.
- [BFK2009] J. Bender, M. Fischlin, D. Kügler: Security Analysis of the PACE Key-Agreement Protocol, in: Proceedings ISC 2009, LNCS volume 5735, Springer, 2009.
- [BCIMRT2010] Brier, Eric; Coron, Jean-Sébastien; Icart, Thomas; Madore, David; Randriam, Hugues; and Tibouch, Mehdi, Efficient Indifferentiable Hashing into Ordinary Elliptic Curves, Advances in Cryptology – CRYPTO 2010, Springer-Verlag, 2010

DRAFT_4 FOR TAG_22

Doc 9303



Machine Readable Travel Documents

**Part 12
Public Key Infrastructure for Machine Readable Travel Documents**

Approved by the Secretary General
and published under his authority

Seventh Edition - Revision 1 - 2014

International Civil Aviation Organization

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

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

Doc 9303, Machine Readable Travel Documents
Order Number: xxxx
ISBN xxx-xx-xxxx-xxx-x

© ICAO 2014

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 TO DOC 9303-12, 7TH EDITION

Revision	Date	Description
01	xx-xx-2014	Initial release of the 7 th edition

DRAFT_4 FOR TAG_22

TABLE OF CONTENTS

1	SCOPE	2
2	OVERVIEW OF THE PUBLIC KEY INFRASTRUCTURE	3
3	ROLES AND RESPONSIBILITIES	4
3.1	Country Signing Certification Authority	4
3.2	Document Signer	5
3.3	Inspection System	5
3.4	Master List Signer	5
4	KEY MANAGEMENT	6
4.1	Document Signer Keys and certificates	6
4.2	CSCA Keys and Certificates	7
4.3	Certificate Revocation	8
4.4	Cryptographic Algorithms	9
5	DISTRIBUTION MECHANISMS	10
5.1	PKD Distribution Mechanism	11
5.2	Bilateral Exchange Distribution Mechanism	11
5.3	Master List Distribution Mechanism	11
6	PKI TRUST AND VALIDATION	13
6.1	Trust Anchor Management	13
6.2	Certificate/CRL Validation and Revocation Checking	14
7	CERTIFICATE AND CRL PROFILES	15
7.1	Certificate Profiles	15
7.2	CRL Profile	22
8	CSCA MASTER LIST STRUCTURE	24
8.1	SignedData Type	24
8.2	ASN.1 Master List Specification	24
	APPENDIX A - LIFETIMES (INFORMATIVE)	26
A.1	Example 1	26
A.2	Example 2	26
A.3	Example 3	26
	APPENDIX B – CERTIFICATE & CRL PROFILE REFERENCE TEXT (INFORMATIVE)	27
	APPENDIX C – EARLIER CERTIFICATE PROFILES (INFORMATIVE)	34
	APPENDIX D – RFC 5280 VALIDATION COMPATIBILITY (INFORMATIVE)	37
D.1	Steps Relevant to eMRTD	37
D.2	Steps not Required by eMRTD	40
D.3	Modifications required to process CRLs	40
	REFERENCES (NORMATIVE)	41

1 SCOPE

The seventh edition of Doc 9303 represents a restructuring of the ICAO specifications for Machine Readable Travel Documents. Without incorporating substantial modifications of 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) size documents, 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 12 of Doc 9303 is based on Doc 9303 Part 1 Machine Readable Passports, Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability, Sixth edition – 2006 and Doc 9303 Part 3 Machine Readable Official Travel Documents, Volume 2 Specifications for Electronically Enabled MRTDs with Biometric Identification Capability, Third edition – 2008.

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.

Doc 9303-12 should be read in conjunction with:

- Doc 9303-10 – Logical Data Structure (LDS) for storage of biometrics and other data in the contactless IC; and
- Doc 9303-11 – Security Protocols.

2 OVERVIEW OF THE PUBLIC KEY INFRASTRUCTURE

The eMRTD Public Key Infrastructure (PKI) enables the creation, and subsequent verification of digital signatures on eMRTD objects, including the Document Security Object (SO_D) to ensure the signed data is authentic and has not been modified. Revocation of a certificate, failure of the certification path validation procedure or failure of digital signature verification does not on its own cause an eMRTD to be considered invalid. Such a failure means that the electronic verification of the integrity and authenticity of the LDS data has failed and other non-electronic mechanisms could then be used to make that determination as part of the overall inspection of the eMRTD.

The eMRTD PKI is much simpler than more generic multi-application PKIs such as the Internet PKI defined in [RFC 5280]. In the eMRTD PKI, each Issuing State/Authority establishes a single Certification Authority (CA) that issues all certificates directly to end-entities, including Document Signers. These CAs are referred to as Country Signing Certification Authorities (CSCA). There are no other CAs in the infrastructure. Receiving States establish trust directly in the keys/certificates of each Issuing State or organization's CSCA.

The eMRTD PKI is based on generic PKI standards including [X.509] and [RFC 5280]. Those base PKI standards define a large set of optional features and complex trust relationships among CAs that are not relevant to the eMRTD application. A profile of those standards, tailored to the eMRTD application is specified in this Part of Doc 9303. Some of the unique aspects of the eMRTD application include:

- There is precisely one CSCA per Issuing State;
- Certification paths include precisely one certificate (e.g. Document Signer);
- Signature verification must be possible 5-10 years after creation;
- CSCA name change is supported; and
- CSCA Link certificates are not processed as intermediate certificates in a certification path.

For the most part, the eMRTD PKI infrastructure is compliant with [RFC 5280]. However, the fact that CSCAs can undergo a name change imposes unique requirements on the eMRTD PKI that are incompatible with some of **the CRL validation** procedures defined in [RFC 5280]. These differences have been kept to a minimum and are clearly identified.

This Part 12 of Doc 9303 specifies the eMRTD PKI profile including:

- Roles and responsibilities of entities in the infrastructure;
- Cryptographic algorithms and key management;
- Certificate and CRL content;
- Certificate and CRL distribution mechanisms; and
- Certification path validation.

3 ROLES AND RESPONSIBILITIES

The authenticity and integrity of data stored on eMRTDs is protected by Passive Authentication. This security mechanism is based on digital signatures and consists of the following PKI entities:

- **Country Signing CA (CSCA):** Each Issuing State/Authority establishes a single CSCA as its national trust point in the context of eMRTDs. The CSCA issues public key certificates for one or more (national) Document Signers and optionally for other end-entities such as Master List Signers. The CSCA also issues periodic Certificate Revocation Lists (CRL) indicating whether any of the issued certificates have been revoked.
- **Document Signers (DS):** A Document Signer digitally signs data to be stored on eMRTDs; this signature is stored on the eMRTD in a Document Security Object.
- **Inspection Systems (IS):** An Inspection System verifies the digital signature, including certification path validation to verify the authenticity and integrity of the electronic data stored on the eMRTD as part of Passive Authentication.
- **Master List Signers:** A Master List Signer is an optional entity that digitally signs a list of CSCA certificates (domestic and foreign) in support of the bilateral distribution mechanism for CSCA certificates.

The secure facilities to generate key pairs SHALL be under the control of the Issuing State or organization. Each key pair includes a 'private' key and a 'public' key. The private keys and associated systems or facilities SHALL be well protected from any outside or unauthorized access through inherent design and hardware security facilities.

While the CSCA certificate remains relatively static, a large number of Document Signer certificates will be created over time.

The CSCA of each Issuing State or organization acts as the trust point for the Receiving State. The Issuing State or organization distributes its own CSCA public key to Receiving States in the form of a certificate. The Receiving State establishes that this certificate (and certified key) are "trusted" through out-of-band means, and stores a "Trust Anchor" for that trusted key/certificate. These CSCA certificates SHALL be self-signed certificates issued directly by the CSCA. CSCA certificates MUST NOT be subordinate or cross certificates in a larger PKI infrastructure. CSCA self-issued link certificates may also be issued to help the Receiving State in establishing trust in a new CSCA key/certificate following a key-rollover.

Note: In some States there is a requirement that a centralized Controller of Certification Authority (CCA) be the supreme authority to publish self-signed certificates for all applications. In these cases, a possible solution is for the CSCA to create a self-signed certificate (satisfying the ICAO 9303 requirements) and have that certificate countersigned by the CCA (satisfying the State's own CCA requirement). However, these countersigned certificates are not part of the eMRTD PKI and would not be distributed to Receiving States.

3.1 Country Signing Certification Authority

It is RECOMMENDED that CSCA key pairs (KP_{UCSCA} , KP_{CSCA}) be generated and stored in a highly protected, off-line CA infrastructure.

The CSCA private key (KP_{CSCA}) is used to sign Document Signer certificates (C_{DS}), other certificates and CRLs.

Country Signing Certification Authority certificates (C_{CSCA}) are used to validate Document Signer certificates, Master List Signer certificates, CRLs and other certificates issued by the CSCA.

All certificates and CRLs MUST comply with the profiles specified in Section 7 and MUST be distributed using the distribution mechanisms as specified in Section 5.

For PKD participants, each CSCA certificate (C_{CSCA}) MUST also be forwarded to the PKD (for the purpose of validation of Document Signer certificates (C_{DS})).

CRLs MUST be issued on a periodic basis as specified in Section 4.

3.2 Document Signer

It is RECOMMENDED that Document Signer key pairs (K_{PuDS} , K_{PrDS}) be generated and stored in a highly protected infrastructure.

The Document Signer private key (K_{PrDS}) is used to sign Document Security Objects (SO_D).

Document Signer certificates (C_{DS}) are used to validate Document Security Objects (SO_D).

Each Document Signer certificate (C_{DS}) MUST comply with the certificate profile defined in Section 7 and MUST be stored in the contactless IC of each eMRTD that was signed with the corresponding DS private key (See Doc 9303-10 for details). This ensures that the Receiving State has access to the Document Signer certificate relevant to each eMRTD.

Document Signer certificates of PKD participants should also be forwarded to ICAO for publication in the ICAO Public Key Directory (PKD).

3.3 Inspection System

Inspection Systems perform Passive Authentication to ensure the integrity and authenticity of the data stored on the eMRTD contactless IC. As part of that process, Inspection Systems MUST perform certification path validation as indicated in Section 6.

3.4 Master List Signer

The Master List Signer private key is used to sign CSCA Master Lists.

Master List Signer certificates are used to validate CSCA Master Lists.

4 KEY MANAGEMENT

Issuing States or organizations SHALL have at least two key pair types:

- Country Signing CA key pair; and
- Document Signer key pair.

Issuing States or organizations MAY have additional key pair types:

- Master List Signer key pair

The Country Signing CA, Document Signer, and Master List Signer public keys are issued using [X.509] certificates. The public keys contained in CSCA certificates are used to verify the CSCA signature on issued certificates (Document Signer, Master List Signer and CSCA) and on issued CRLs. The public keys contained in Document Signer certificates are used to verify digital signatures created with the corresponding private key by the subject Document Signer on Document Security Objects (SO_D). The public keys contained in Master List certificates are used to verify the digital signature on Master Lists.

For Master List Signer and Communications keys and certificates, the private key lifetime and the certificate validity period are left to the discretion of the Issuing State or organization.

Both the CSCA certificates and Document Signer certificates are associated with a private key usage and a public key validity period as outlined in Table 1.

Table 1: Key Usage and Validity

	Use of Private Key	Public Key Validity (assuming 10 year valid passports)
Country Signing CA	3-5 years	13-15 years
Document Signer	Up to 3 months ¹	approx. 10 years
Master List Signer	Discretion of Issuing State or organization	Discretion of Issuing State or organization
Communication	Discretion of Issuing State or organization	Discretion of Issuing State or organization

4.1 Document Signer Keys and certificates

The usage period of a Document Signer private key is much shorter than the validity period of the DS certificate for the corresponding public key.

4.1.1 Document Signer Public Key Validity

The lifetime, i.e. the certificate validity period, of the Document Signer public key is determined by concatenating the following two periods:

- The length of time the corresponding private key will be used to issue eMRTDs, with;
- The longest validity period of any eMRTD issued under that key².

The Document Signer certificate (C_{DS}) SHALL be valid for this total period to enable the authenticity of eMRTDs to be verified. However the corresponding private key SHOULD only be used to issue documents for a limited period; once the last document it was used to issue has expired, the public key is no longer required.

¹ Note the corresponding `privateKeyUsage` extension in DS certificate might be slightly longer to allow for overlap or production requirements.

² Some Issuing States or organizations may issue eMRTDs before they become valid, for instance on a change of name upon marriage. In these situations, the "longest validity period of any eMRTD" includes the actual validity of the eMRTD (e.g. 10 years) plus the maximum time between when the eMRTD is issued and the time it becomes valid.

4.1.2 Document Signer Private Key Issuing Period

When deploying their systems Issuing States or organizations may wish to take into account the number of documents that will be signed by any one individual Document Signer private key.

An Issuing State or organization may deploy one or more Document Signers, each with its own unique key pair, that are active at any given time.

In order to minimize business continuity costs in the event of a Document Signer certificate being revoked, an Issuing State or organization that issues a large number of eMRTDs per day may wish to:

- Use a very short private key usage period; and/or
- Deploy several concurrent Document Signers that are active at the same time, each with its own unique private key and public key certificate.

An Issuing State or organization that issues a small number of eMRTDs per day may choose to deploy a single Document Signer and may also be comfortable with a slightly longer private key usage period.

Regardless of the number of eMRTDs issued per day, or number of Document Signers active at the same time, it is RECOMMENDED that the maximum period any Document Signer private key is used to sign eMRTDs be three months.

Once the last document signed with a given private key has been produced it is RECOMMENDED that Issuing States or organizations erase the private key in an auditable and accountable manner.

4.2 CSCA Keys and Certificates

The usage period of a CSCA private key is much shorter than the validity period of the CSCA certificate for the corresponding public key.

4.2.1 Country Signing CA Public Key Validity

The lifetime, i.e. the certificate validity, of the CSCA public key is determined by concatenating the following periods:

- The length of time the corresponding CSCA private key will be used to sign Document Signer certificates (C_{DS}); and,
- The key lifetime of Document Signer public key certificates (See 4.1.1)

4.2.2 Country Signing CA Private Key Issuing Period

The usage period for the CSCA private key to sign certificates and CRLs is a delicate balance among the following factors:

- In the unlikely event of an Issuing State or organization Country Signing Private CA Key being compromised, then the validity of all eMRTDs issued using Document Signer Keys whose certificates were signed by the compromised CSCA private key is called into doubt. Consequently Issuing States or organizations MAY wish to keep the issuing period quite short;
- Keeping the issuing period very short, however, leads to having a very large number of CSCA public keys valid at any one time. This can lead to more complex certificate management within the border processing systems.

It is therefore RECOMMENDED that an Issuing State or organization's CSCA key pair be replaced every three to five years.

4.2.3 Country Signing CA Re-key

CSCA keys provide the trust points in the whole system and without these the system would collapse. Therefore Issuing States or organizations SHOULD plan the replacement of their CSCA key pair carefully. Once the issuance period for the initial CSCA private signing key has elapsed, an Issuing State or organization will always have at least two CSCA certificates (C_{CSCA}) valid at any one time.

Issuing States or organizations MUST notify Receiving States that a CSCA key rollover is planned. This notification MUST be provided 90 days in advance of the key rollover. Once the key rollover has occurred the new CSCA certificate (certifying the new CSCA public key) is distributed to Receiving States.

If the CSCA certificate is a new self-signed certificate, authentication of that certificate should be done using an out-of-band method.

When a CSCA key rollover occurs a certificate **MUST** be issued that links the new key to the old key to provide a secure transition for relying parties. Generally this is achieved through the issuance of a self-issued-certificate where the issuer and subject fields are identical but the key used to verify the signature represents the old key pair and the certified public key represents the new key pair. These CSCA Link certificates need not be verified using an out-of-band method as the signature on the CSCA Link certificate is verified using an already trusted public key for that CSCA. Master Lists can also be used to distribute CSCA Link and CSCA self-signed root certificates.

Issuing States or organizations should refrain from using their new CSCA private key for the first two days after the CSCA key rollover, to ensure the corresponding new CSCA public key certificate has been distributed successfully.

Issuing States or organizations **MUST** use the newest CSCA private key for signing certificates, including Document Signer certificates, and for signing CRLs.

4.3 Certificate Revocation

Issuing States or organizations may need to revoke certificates in case of an incident (like a key compromise).

All CSCAs **MUST** produce periodic revocation information in the form of Certificate Revocation Lists (CRL).

CSCAs **MUST** issue at least one CRL every 90 days, even if no certificates have been revoked since the previous CRL was issued. CRLs **MAY** be issued more frequently than every 90 days but not more frequently than every 48 hours.

If a certificate is revoked, a CRL indicating that revocation **MUST** be distributed within 48 hours.

Only certificates can be revoked, not Document Security Objects. The use of Certificate Revocation Lists (CRLs) is limited to notifications of revoked certificates that had been issued by the CSCA that issued the CRL (including revocation notices for CSCA certificates, DS certificates and Master List Signer certificates).

Partitioned CRLs are not used in the eMRTD application. All certificates revoked by a CSCA, including DS certificates, CSCA certificates, and Master List Signer certificates are listed on the same CRL. Although the CRL is always signed with the newest (current) CSCA private signing key, the CRL includes revocation notices for certificates signed with that same private key as well as certificates signed with earlier CSCA private signing keys.

4.3.1 Revocation of CSCA Certificates

Revocation of a CSCA certificate is both extreme and difficult. Upon informing a Receiving State that a CSCA certificate has been revoked, all other certificates signed using the corresponding CSCA private key are effectively revoked.

Where a CSCA link certificate has been signed using an old CSCA private to certify a new CSCA public key (see "Country Signing Re-key" in 4.2), revoking the old CSCA certificate **SHALL** also revoke the new CSCA certificate.

If a CSCA certificate needs to be revoked, the CSCA may issue a CRL signed with the private key that corresponds to the public key being revoked, as this is the only key users of the CRL will be able to verify at that time. The CSCA public key should be considered valid only for the purpose of verifying that CRL signature. Once a CRL user has verified the CRL signature the CSCA private signing key is considered compromised and the certificate revoked for all future verifications.

To issue new documents the Issuing State or organization **MUST** revert to bootstrapping its authentication process from the beginning, by issuing a new CSCA Root certificate, distributing that

certificate to Receiving States, and supporting out-of-band confirmation that the certificate received by each Receiving State is in fact the current authentic CSCA certificate.

4.3.2 Revocation of Other Certificates

When an Issuing State or organization wishes to revoke a Document Signer, Master List Signer, or communication certificate, it does not need to wait until the `nextUpdate` period in the current CRL is due to issue a new CRL. It is RECOMMENDED that a new CRL be issued within a 48-hour period of revocation notification.

4.4 Cryptographic Algorithms

An Issuing State or organization MUST support the same algorithm for use in their CSCA and Document Signing keys, although different key sizes may be required depending on the algorithm selected.

Issuing States or organizations SHALL choose appropriate key lengths offering protection against attacks. Suitable cryptographic catalogues SHOULD be taken into account.

Receiving States MUST support all algorithms at points where they wish to validate the signature on eMRTDs.

For use in their CSCA, Document Signing keys and, where applicable, Document Security Objects Issuing States or organizations SHALL support one of the algorithms below.

4.4.1 RSA

Those Issuing States or organizations implementing the RSA algorithm for signature generation and verification of certificates and the Document Security Object (SO_D) SHALL use [RFC 4055]. [RFC 4055] specifies two signature mechanisms, RSASSA-PSS and RSASSA-PKCS1_v15. It is RECOMMENDED that Issuing States or organizations generate signatures according to RSASSA-PSS, but Receiving States MUST also be prepared to verify signatures according to RSASSA-PKCS1_v15.

4.4.2 Digital Signature Algorithm (DSA)

Those Issuing States or organizations implementing DSA for signature generation or verification SHALL use [FIPS 186-4].

4.4.3 Elliptic Curve DSA

Those Issuing States or organizations implementing ECDSA for signature generation or verification SHALL use [X9.62] or [ISO/IEC 15946]. The elliptic curve domain parameters used to generate the ECDSA key pair MUST be described explicitly in the parameters of the public key, i.e. parameters MUST be of type `ECParameters` (no named curves, no implicit parameters) and MUST include the optional co-factor. `ECPoints` MUST be in uncompressed format.

It is RECOMMENDED that the guideline [TR 03111] be followed.

4.4.4 Hashing Algorithms

SHA-224, SHA-256, SHA-384 and SHA-512, are the only permitted hashing algorithms. See [FIPS 180-2].

5 DISTRIBUTION MECHANISMS

PKI objects need to be distributed to the Receiving States. A number of different distribution mechanisms are used, depending on the type of object and operational requirements. It is important to note that distribution of these objects does NOT establish trust in those objects, or the private/public keys associated with them. Mechanisms for establishing trust are specified in Section 6.

The objects that need to be distributed from Issuing States or organizations to Receiving States include:

- CSCA certificates;
- Document Signer certificates;
- CRLs (null and non-null);
- Master List Signer certificates; and
- Master Lists.

The distribution mechanisms used in the eMRTD PKI include:

- PKD;
- Bilateral exchange;
- Master Lists; and
- eMRTD contactless IC.

A primary and secondary distribution mechanism is specified for each object as outlined in Table 2 below.

Table 2: Primary & Secondary Distribution

	CSCA Certificates	Document Signer Certificates	CRLs (Null & Non-null)	Master List Signer Certificates	Master Lists
Primary	Bilateral	eMRTD contactless IC	Bilateral	Master Lists	PKD / Bilateral
Secondary	Master Lists	PKD	PKD		

Operationally, Receiving States are not obliged to use both the primary and secondary source. In the daily operation of an inspection system, it is at the inspecting authority's discretion whether to use the primary or the secondary source. If authority Receiving State uses the secondary source for a certificate or CRL in its daily operations, it should be prepared to support the primary source as well.

Issuing States or organizations need to plan their key pair rollover strategies for both CSCA keys and Document Signer keys in order to enable propagation of certificates and CRLs into Receiving States' border control systems in a timely manner. Ideally propagation will occur within 48 hours, but some Receiving States may have remote and poorly connected border outposts to which it may take more time for certificates and CRLs to propagate out. Receiving States SHOULD make every effort to distribute these certificates and CRLs to all border stations within 48 hours.

Issuing States or organizations should expect that CSCA certificates (C_{CSCA}) will be propagated by Receiving States within 48 hours.

Issuing States or organizations ensure the timely propagation of Document Signer certificates (C_{DS}) by including the Document Signer certificate (C_{DS}) within the Document Security Object (SO_D). They should expect that Document Signer certificates (C_{DS}) published in the PKD will also be propagated to border stations within 48 hours.

Receiving States SHOULD make every attempt whether electronically or by other means to act upon CRLs, including those CRLs issued under exceptional circumstances.

Timely propagation of Master List Signer certificates (C_{DS}) is ensured by including them within each Master List.

5.1 PKD Distribution Mechanism

ICAO provides a Public Key Directory (PKD) service. This service SHALL accept PKI objects, including certificates, CRLs and Master Lists, from PKD participants, store them in a directory, and make them accessible to all Receiving States.

CSCA certificates (C_{CSCA}) are not stored individually as part of the ICAO PKD service. However, they may be present in the PKD if they are contained on Master Lists.

Each Document Signer certificate (C_{DS}) remains in the PKD until its certificate validity period has expired, regardless of whether the corresponding private key is still in use.

Certificates, CRLs and Master Lists stored in the PKD by all PKD participants SHALL be made available to all parties (including non PKD participants) that need this information for validating the authenticity and integrity of digitally stored eMRTD data.

5.1.1 PKD Upload

Only PKD participants MAY upload certificates, CRLs and Master Lists to the PKD. All certificates and CRLs MUST comply with the profiles in Section 7. All Master Lists MUST comply with the specification in Section 8.

The PKD consists of a “Write Directory” and a “Read Directory”. PKD participants SHALL use the Lightweight Directory Access Protocol (LDAP) protocol to upload their objects to the Write Directory. Once the digital signature has been verified on an object, and other due diligence checks completed, the object is published in the Read Directory.

5.1.2 PKD Download

Read access to all certificates, CRLs and Master Lists published in the PKD SHALL be available to PKD participants and non-participants. Access control SHALL NOT be implemented for PKD read access.

It is the Receiving State’s responsibility to distribute objects downloaded from the PKD to its Inspection Systems and to maintain a current CRL cache along with the certificates necessary to verify the signatures on eMRTD data.

5.2 Bilateral Exchange Distribution Mechanism

For CRLs and CSCA certificates (C_{CSCA}), the primary distribution channel is bilateral exchange between Issuing States or organizations and Receiving States. Bilateral exchange can also be used to distribute Master Lists.

The specific technology used for that bilateral exchange may vary depending on the policies of each Issuing State or organization that has a need to distribute their certificates CRLs and Master Lists, as well as the policies of each Receiving State that needs access to those objects. Some examples of technologies that may be used in bilateral exchange include:

- Diplomatic courier/pouch;
- Email exchange;
- Download from website associated with the issuing CSCA; and
- Download from LDAP server associated with the issuing CSCA.

This is not an exhaustive list and other technologies may also be used.

5.3 Master List Distribution Mechanism

Master Lists are a supporting technology for the bilateral distribution scheme. As such, distribution of CSCA certificates via Master Lists is a subset of the bilateral distribution scheme.

A Master List is a digitally signed list of the CSCA certificates that are ‘trusted’ by the Receiving State that issued the Master List. CSCA self-signed Root certificates and CSCA Link certificates may be included in a Master List. The structure and format of a Master List is defined in Section 8. Publication of a Master List enables other Receiving States to obtain a set of CSCA certificates from a single

source (the Master List issuer) rather than establish a direct bilateral exchange agreement with each of the Issuing Authorities or organizations represented on that list.

A Master List Signer is authorized by a CSCA to compile, digitally sign, and issue Master Lists. Master Lists **MUST NOT** be signed and issued directly by a CSCA itself. Master List Signer certificates **MUST** comply with the certificate profile defined in Section 7.

Before issuing a Master List the issuing Master List Signer **SHOULD** extensively validate the CSCA certificates to be countersigned, including ensuring that the certificates indeed belong to the identified CSCAs. The procedures used for this out-of-band validation **SHOULD** be reflected in the published certificate policies of the CSCA that issued the Master List Signer certificate.

Each Master List **MUST** include the Master List Signer's certificate that will be used to verify the signature on that Master List as well as the CSCA certificates of the CSCA that issued that Master List Signer certificate.

If new CSCA certificates have been received by a Receiving State, and its validation procedures have been completed, it is **RECOMMENDED** that a new Master List be compiled and issued.

Use of a Master List does enable more efficient distribution of CSCA certificates for some Receiving States. However a Receiving State making use of Master Lists **MUST** still determine its own policies for establishing trust in the certificates contained on that list (see Section 6 for details).

DRAFT - 4 FOR TRIP 2019

6 PKI TRUST AND VALIDATION

In the eMRTD PKI environment, the Inspection Systems in Receiving States act in the role of PKI relying parties. Successful verification of the digital signature on the Document Security Object of an eMRTD ensures the authenticity and integrity of the data stored on the contactless IC of that eMRTD. That signature verification process requires that the relying party establish that the Document Signer public key used to verify the signature is itself 'trusted'.

The various distribution mechanisms defined in Section 5 allow Receiving States to gain access to the certificates and CRLs that they need to verify digital signatures in question. However, these distribution schemes do not establish trust in those certificates, CRLs or the public keys that will be used to verify signatures on those certificates and CRLs.

The public keys contained in CSCA certificates (C_{CSCA}) are used to verify the digital signature on certificates (including Document Signer and Master List Signer certificates) and CRLs. Therefore, to accept an eMRTD from another Issuing State, the Receiving State MUST already have placed into some form of trust store, accessible by their border control system, a trusted copy of the Issuing State or organization CSCA certificate (C_{CSCA}), or other form of Trust Anchor information for that CSCA public key as derived from the certificate.

It is a Receiving State's responsibility to establish trust in the CSCA certificates (C_{CSCA}) and store the certificates (or information from the certificates) as Trust Anchors, in a secure way for use by their border inspection systems.

6.1 Trust Anchor Management

As specified in [RFC 5280] a Trust Anchor must be established that can be used to anchor the validation procedure for a given Document Signer, Master List Signer or other type of certificate.

Each Trust Anchor is comprised of a trusted public key, and associated metadata. Trust Anchors MUST include, as a minimum:

- The trusted public key and any associated key parameters;
- The public key algorithm;
- The name of the key owner; and
- The value of the `SubjectAltName` extension of the CSCA certificate containing the ICAO assigned 3 letter code of the Issuing Authority or organization. Although this is not used in the certification path or CRL validation procedures, it is used in Passive Authentication defined in Doc 9303-11.

In the eMRTD application, a separate Trust Anchor is established for each public key of a given CSCA. For the initial public key obtained from a CSCA, trust MUST be established through an out-of-band mechanism. For example, if a CSCA certificate was downloaded from server associated with the CSCA, out-of-band communication (e.g. phone or email) could be used to verify that the downloaded certificate is in fact the authentic certificate for that CSCA. Also, the relying party might analyse the policies, procedures and practices of the issuing CSCA to determine whether they are secure enough to satisfy the local requirements for use of certificates. Once an initial Trust Anchor is established for a given CSCA, the process could be simplified for subsequent keys for that same CSCA. If the CSCA issues a CSCA Link certificate, then out-of-band communication with the CSCA to verify the authenticity of the new certificate could be skipped because the already trusted public key for that same CSCA is used to verify the signature on that CSCA link certificate.

Trust Anchor information may be stored as a trusted copy of the CSCA certificate itself, or in some other trusted format.

Because signatures on certificates issued by CSCAs need to be verifiable long after that CSCA has updated its key pair, a Receiving State will typically have more than one Trust Anchor for the same CSCA at any one time. If a CSCA has undergone a name change, some of these Trust Anchors will contain the old CSCA name and others will contain the new name.

6.2 Certificate/CRL Validation and Revocation Checking

As part of the process of verifying the authenticity and integrity of data objects in the eMRTD application (e.g. Document Security Objects, Master Lists, etc.) a Receiving State:

- Validates the certificate used to verify the signature on the data object (e.g. Document Signer Certificate, Master List Signer certificate, etc.);
- Validates the CRL that is used to check the revocation status of the certificate in question; and
- Processes the CRL to verify the revocation status of the certificate in question.

Sample algorithms for these processes are available, such as those specified in [RFC 5280]. Receiving States need not implement the specific algorithm defined in RFC 5280, but **MUST** provide functionality equivalent to the external behavior resulting from this procedure. Any algorithm may be used by a particular implementation as long as it derives the correct result.

Appendix D provides guidance for Receiving State that choose to base their algorithm on that specified in [RFC 5280].

DRAFT_4 FOR TAG_22

7 CERTIFICATE AND CRL PROFILES

Issuing States or organizations **MUST** issue certificates and CRLs that conform to the profiles specified below. All certificates and CRLs **MUST** be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them. The profiles for CSCA and DS certificates that were included in the 6th edition of this specification differ in some areas from the current profiles. Inspection Systems **MUST** be capable of handling certificates that were issued in accordance with those earlier profiles (See Appendix C) as well as the current profiles.

These profiles are based on the requirement that each Issuing State or organization or entity **SHALL** create a single CSCA for the purpose of signing all Doc 9303 compliant eMRTDs.

Certificate profiles are defined in Section 7.1 for the following certificate types:

Profiles are specified for the following certificate types:

- Country Signing CA;
- Document Signer;
- CSCA Master List Signer certificates; and
- Communications - even though it is not strictly needed today. This is a future proofing step. these certificates may be used for access to the PKD or for LDAP/EMAIL/ HTTP communications between countries. It is recommended to position this under the CSCA.

The CRL profile is defined in Section 7.2.

The profiles use the following terminology for presence requirements of each of the components/extensions:

- m mandatory – the field **MUST** be present
- x do not use – the field **MUST NOT** be present
- o optional – the field **MAY** be present

The profiles use the following terminology for criticality requirements of extensions that may/must be included:

- c critical – receiving applications **MUST** be able to process this extension.
- nc non-critical - receiving applications that do not understand this extension **MAY** ignore it.

Some of the requirements identified in these profiles are inherited from the referenced base profiles (e.g. RFC 5280). For convenience, the relevant text from the base profile that covers the specific requirement is duplicated in a table in Appendix B.

7.1 Certificate Profiles

Table 3 defines the certificate profile requirements for the fields of the certificate body. Table 4 defines the requirements for certificate extensions.

Table 3: Certificate Fields Profile

Certificate Component	Presence	Comments
Certificate	m	
TBSCertificate	m	see next part of the table
signatureAlgorithm	m	value inserted here dependent on algorithm selected
signatureValue	m	value inserted here dependent on algorithm selected
TBSCertificate		
version	m	MUST be v3
serialNumber	m	MUST be positive integer and maximum 20 Octets MUST use 2's complement encoding and be represented in the smallest number of octets
signature	m	value inserted here MUST be the same as that in signatureAlgorithm component of Certificate sequence

Certificate Component	Presence	Comments
issuer	m	countryName and serialNumber, if present, MUST be PrintableString Other attributes that have DirectoryString syntax MUST be either PrintableString or UTF8String countryName MUST be Upper Case See 7.1.1 for naming conventions
validity	m	MUST terminate with Zulu (Z) Seconds element MUST be present Dates through 2049 MUST be in UTCTime UTCTime MUST be represented as YYMMDDHHMMSSZ Dates in 2050 and beyond MUST be in GeneralizedTime. GeneralizedTime MUST NOT have fractional seconds GeneralizedTime MUST be represented as YYYYMMDDHHMMSSZ
subject	m	countryName and serialNumber, if present, MUST be PrintableString Other attributes that have DirectoryString syntax MUST be either PrintableString or UTF8String countryName MUST be Upper Case countryName in issuer and subject fields MUST match See 7.1.1 for naming conventions
subjectPublicKeyInfo	m	
issuerUniqueID	x	
subjectUniqueID	x	
extensions	m	See next table on which extensions should be present Default values for extensions MUST NOT be encoded

Table 4: Certificate Extensions Profile

Extension name	CSCA Self-Signed Root		CSCA Link		Docu ment Signer		Master List Signer		Comm unication		Comments
	Presence	Criticality	Presence	Criticality	Presence	Criticality	Presence	Criticality	Presence	Criticality	
<i>Table 1:</i>											
<i>Table 2: Authority KeyIdentifier</i>	o	nc	m	nc	m	nc	m	nc	m	nc	
keyIdentifier	m		m		m		m		m		
authorityCertIssuer	o		o		o		o	<i>Tab</i>	o	<i>Tab</i>	

Extension name	CSCA Self-Signed Root		CSCA Link		Docu ment Signer		Master List Signer		Comm unication		Comments
	o	nc	m	nc	o	nc	o	nc	o	nc	
authorityCertSerialNumber	o		o		o		o		o		
Table 7: SubjectKeyIdentifier	m	nc	m	nc	o	nc	o	nc	o	nc	
Table 9: subjectKeyIdentifier	Tab	Tab	Ta	Tab	Ta		m	Tab	Ta	Tab	
Table 18: KeyUsage	m	c	m	c	m	c	m	c	m	c	
digitalSignature	x		x		m		m		o		Some communication certificates (e.g. TLS certificates) require that the keyUsage bits be set in accordance with the particular cipher suite used. Some cipher suites do, and some do not require the digitalSignature bit to be set.
nonRepudiation	x		x		x		x		x		
keyEncipherment	x		x		x		x	Tab	o	Tab	
dataEncipherment	x		x		x		x	Tab	x	Tab	
keyAgreement	x		x		x		x	Tab	o	Tab	
keyCertSign	m		m		x		x	Tab	x	Tab	
cRLSign	m		m		x		x	Tab	x	Tab	
encipherOnly	x		x		x		x	Tab	x	Tab	
decipherOnly	x		x		x		x	Tab	x	Tab	
PrivateKeyUsagePeriod	m	nc	m	nc	m	nc	o	nc	o	nc	
notBefore	o		o		o		o		o		At least one of notBefore or notAfter MUST be present MUST be encoded as generalizedTime
notAfter	o		o		o		o		o		
CertificatePolicies	o	nc	o	nc	o	nc	o	nc	o	nc	
PolicyInformation	m		m		m		m		m		
policyIdentifier	m		m		m		m		m		
policyQualifiers	o		o		o		o		o		
PolicyMappings	x		x		x		x		x		See Note 1
SubjectAltName	m	nc	m	nc	m	nc	m	nc	m	nc	See 7.1.2
IssuerAltName	m	nc	m	nc	m	nc	m	nc	m	nc	See 7.1.2
SubjectDirectoryAttributes	x		x		x		x		x		
Basic Constraints	m	c	m	c	x		x	Tab	x		
ca	m		m		x		x	Tab	x	Tab	
PathLenConstraint	m		m		x		x		x		MUST always be '0'
NameConstraints	x		x		x		x		x		See Note 1
PolicyConstraints	x		x		x		x		x		See Note 1
ExtKeyUsage	x		x		x		m	c	m	c	See 7.1.3
CRLDistributionPoints	m	nc	m	nc	m	nc	m	nc	o	nc	
distributionPoint	m		m		m		m		m		MUST be ldap, http or https

Extension name	CSCA Self-Signed Root		CSCA Link		Docu ment Signer		Master List Signer		Comm unication		Comments
											See 7.1.4
reasons	x		x		x		x		x		
cRLIssuer	x		x		x		x		x		
InhibitAnyPolicy	x		x		x		x		x		See Note1
FreshestCRL	x		x		x		x		x		See Note 2
privateInternetExtensions	o	nc	o	nc	o	nc	o	nc	o	nc	See Note 3
NameChange	o	nc	o	nc	x		x		x		See 7.1.5
DocumentType	x		x		m	nc	x		x		See 7.1.6
Netscape Certificate Type	x		x		x		x		x		See Note 4
other private extensions	o	nc	o	nc	o	nc	o	nc	o	nc	

Note 1: The extension, by definition, can only appear in intermediate CA certificates (certificates issued by one CA to another CA). Intermediate CA certificates are not used in the eMRTD PKI. Therefore this extension is prohibited from eMRTD certificates.

Note 2: The freshest CRL extension is used to point to a delta CRL. Delta CRLs are not supported in the eMRTD PKI. Therefore this extension is prohibited.

Note 3: There are two Private Internet Extensions (Authority Information Access and Subject Information Access) defined in RFC 5280 that are used to point to information about the issuer or subject of a certificate. These extensions are not required in the eMRTD PKI. However as they do not impact interoperability, and are non-critical, they may optionally be included in eMRTD certificates.

Note 4: The Netscape Certificate Type extension can be used to limit the purposes for which a certificate can be used. The extKeyUsage and basicConstraints extensions are now the standard extensions for those purposes and are used in the eMRTD application. Because of the potential conflict between values in the standard extensions and in the Netscape proprietary extension, the Netscape extension is prohibited.

7.1.1 Issuer and Subject Field Requirements

The following naming and addressing conventions for Issuer and Subject fields are REQUIRED.

- `countryName`. MUST be present. The value contains a country code that MUST follow the format of two letter country codes, specified in [ISO 3166-1]
- `commonName`. MUST be present.

Other attributes MAY also be included at the discretion of the Issuing State or organization.

7.1.2 Issuer and Subject Alternative Name Requirements

Because the functions served by alternative names in the eMRTD application are specific to this application, and different from those defined for the Internet PKI in [RFC 5280], values in the Subject Alternative Name extension of eMRTD certificates do not generally unambiguously identify the certificate subject.

In the eMRTD application, alternative names serve the following two functions.

The first function is to provide contact information for the subject and/or issuer of the certificate. For that purpose it SHOULD include at least one of the following:

- `rfc822Name`;
- `dNSName`; or
- `uniformResourceIdentifier`.

The second function is to provide a directory string made of ICAO assigned country codes. For this purpose certificates issued using this profile MUST additionally include a directory name that is constructed as follows:

- `localityName` that contains the ICAO country code as it appears in the MRZ; and
- if this country code does not uniquely define the Issuing State or organization, the attribute `stateOrProvinceName` SHALL be used to indicate the ICAO assigned three letter code for the Issuing State or organization.
- Other attributes are not permitted.

In CSCA self-signed Root certificates, the `IssuerAltName` and `SubjectAltName` extensions MUST be identical. In CSCA Link certificates, the values MAY be different. For example, if a change has occurred with the `rfc822Name` of the CSCA immediately prior to issuance of a CSCA Link certificate, the `IssuerAltName` extension would contain the old `rfc822Name` and the `SubjectAltName` extension would contain the new `rfc822Name`. Any subsequent CSCA Link certificates would contain the new `rfc822Name` in both extensions.

7.1.3 Extended Key Usage Extension Requirements

The Object Identifier (OID) that must be included in the `extendedKeyUsage` extension for Master List Signer certificates is 2.23.136.1.1.3. For communication certificates the value of this extension depends on the communication protocol used (see RFC 5280, section 4.2.1.12).

7.1.4 CRL Distribution Points Extension Requirements

CSCAs may publish their CRL in several places including the PKD, their own website, etc.

For CRLs that are published in locations other than the PKD (e.g. website or local LDAP server), the values that are to be included in this extension are under the control of the CSCA issuing the certificates and the CRL in question.

For CRLs submitted to the PKD, PKD participants MAY include two URL values for their CRL using the following template (replace “CountryCode” with the Issuing State or organization ICAO assigned 3 letter code). If this country code does not uniquely identify the Issuing State or organization, the entry will be created by appending the symbol “_” to the three letter country code in the MRZ, and then the ICAO assigned three letter code for the Issuing State or organization which uniquely identifies the Issuing State or organization:

```
https://pkddownload1.icao.int/CRLs/CountryCode.crl  
https://pkddownload2.icao.int/CRLs/CountryCode.crl
```

This is a mandatory extension and revocation status checks are a mandatory part of the validation procedure. Therefore at least one value MUST be populated.

- The PKD values may be the only values in the extension;
- There may be additional values (e.g. a CSCA may also choose to publish their CRL on a website and include a pointer to that source); or
- A CSCA may also choose to include only a single value (e.g. a pointer to their website as a source) even if they also submit their CRL to the PKD.

The following examples illustrate the PKD values that would be populated in certificates issued by the Issuing Authority for Singapore and for Hong Kong:

Singapore PKD example:

```
https://pkddownload1.icao.int/CRLs/SGP.crl  
https://pkddownload2.icao.int/CRLs/SGP.crl
```

Hong Kong example:

```
https://pkddownload1.icao.int/CRLs/CHN_HKG.crl  
https://pkddownload2.icao.int/CRLs/CHN_HKG.crl
```

7.1.5 Name Change Extension

When a CSCA key rollover occurs a certificate **MUST** be issued that links the old public key to the new public key to provide a secure transition for relying parties. Generally this is achieved through the issuance of a self-issued certificate where the issuer and subject fields are identical but the key used to verify the signature represents the old key pair and the certified public key represents the new key pair.

It is **RECOMMENDED** that CSCAs do not change their Distinguished Name (DN) unnecessarily as there is an adverse impact on relying parties (they must retain both the old and new names as valid CSCAs for the same Issuing State or organization until all eMRPs signed under the old name have expired). However, if a name change is necessary, this **MUST** be conveyed to relying parties through the issuance of a CSCA Link certificate where the `issuer` field contains the old name and the `subject` field contains the new name. This CSCA Link certificate also conveys a key rollover where the key used to verify the signature represents the old key pair and the certified public key represents the new key pair. Certificates that convey both a CSCA name change and a key rollover for that CSCA **MUST** include the `NameChange` extension to identify the certificate as such. This has no effect on `PathLengthConstraint`; it remains '0'.

In addition, the `NameChange` extension **MAY** also be included in the new CSCA self signed certificate created upon the change of the CSCA DN. In such a self-signed CSCA Root certificate both the issuer and subject fields contain the new DN. Unlike the CSCA self-issued link certificate, containing both the old and new DN for the CSCA, inclusion of the `NameChange` extension in a CSCA self-signed Root certificate simply indicates that a name change has occurred and does not link the old DN to the new one.

A CSCA **MUST NOT** re-use certificate serial numbers. Each certificate issued by a CSCA, regardless of whether that CSCA has undergone a name change or not, **MUST** be unique.

ASN.1 for Name Change extension:

```
nameChange  EXTENSION ::= {
    SYNTAX          NULL
    IDENTIFIED BY   id-icao-mrtd-security-extensions-nameChange}

id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 6}
id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER ::=
{id-icao-
mrtd-security-extensions 1}
```

7.1.6 Document Type Extension

The `DocumentType` extension **MUST** be used to indicate the document types, as they appear in the MRZ, that the corresponding Document Signer is allowed to produce. This extension **MUST** always be set to non-critical.

ASN.1 for Document Type List extension:

```
documentTypeList  EXTENSION ::= {
    SYNTAX          DocumentTypeListSyntax
    IDENTIFIED BY   id-icao-mrtd-security-extensions-
documentTypeList}

DocumentTypeListSyntax ::= SEQUENCE {
    version          DocumentTypeListVersion,
    docTypeList     SET OF DocumentType }

DocumentTypeListVersion ::= INTEGER {v0(0)}
```

```
-- Document Type as contained in MRZ, e.g. "P" or "ID" where a  
-- single letter denotes all document types starting with that letter  
DocumentType ::= PrintableString(1..2)
```

```
id-icao-mrtd-security-extensions-documentTypeList OBJECT  
IDENTIFIER ::= {id-icao-mrtd-security-extensions 2}
```

DRAFT_4 FOR TAG_22

7.2 CRL Profile

Table 5 defines the CRL profile requirements for the fields of the CRL body. Table 6 defines the CRL profile requirements for CRL and CRL Entry extensions.

Table 5: CRL Fields Profile

Certificate List Component	CSCA CRL	Comments
CertificateList	m	
tBSCertList	m	See next part of the table
signatureAlgorithm	m	Value inserted here dependent on algorithm selected
signatureValue	m	Value inserted here dependent on algorithm selected
tBSCertList		
version	m	MUST be v2
signature	m	value inserted here MUST be the same as that in signatureAlgorithm component of CertificateList sequence
issuer	m	countryName and serialNumber, if present, MUST be PrintableString Other attributes that have DirectoryString syntax MUST be either PrintableString or UTF8String countryName MUST be Upper Case
thisUpdate	m	MUST terminate with Zulu (Z) Seconds element MUST be present Dates through 2049 MUST be in UTCTime UTCTime MUST be represented as YYMMDDHHMMSSZ Dates in 2050 and beyond MUST be in GeneralizedTime. GeneralizedTime MUST NOT have fractional seconds GeneralizedTime MUST be represented as YYYYMMDDHHMMSSZ
nextUpdate	m	MUST terminate with Zulu (Z) Seconds element MUST be present Dates through 2049 MUST be in UTCTime UTCTime MUST be represented as YYMMDDHHMMSSZ Dates in 2050 and beyond MUST be in GeneralizedTime. GeneralizedTime MUST NOT have fractional seconds GeneralizedTime MUST be represented as YYYYMMDDHHMMSSZ
revokedCertificates	m	If present, MUST NOT be empty

Certificate List Component	CSCA CRL	Comments
crlExtensions	m	See next table on which extensions should be present Default values for extensions MUST NOT be encoded

Table 6: CRL & CRL Entry Extensions Profile

Extension Name	CSCA CRL	Criticality	Comments
CRL Extensions			
authorityKeyIdentifier	m	nc	This MUST be the same value as the subjectKeyIdentifier field in the CRL Issuer's certificate.
keyIdentifier	m		
authorityCertIssuer	o		
authorityCertSerialNumber	o		
issuerAlternativeName	o	nc	See Note 1
cRLNumber	m	nc	MUST be non-negative integer and maximum 20 Octets MUST use 2's complement encoding and be represented in the smallest number of octets
deltaCRLIndicator	x		
issuingDistributionPoint	x		
freshestCRL	x		
CRL Entry Extensions			
reasonCode	x		
holdInstructionCode	x		
invalidityDate	x		
certificateIssuer	x		

Note 1: If a CSCA has undergone a name change, this extension MAY be included in CRLs issued following the CSCA name change. If present, the value(s) in this extension MUST be identical to the issuer field of certificates issued by the CSCA under that previous name. Once all certificates issued under a previous CSCA name have expired, that CSCA name can be excluded from subsequent CRLs. Inspection Systems are not required to process this extension. Given that ICAO 9303 dictates a single CSCA per country, the countryName component of the issuer field is sufficient to uniquely identify the CSCA. The latest public key of that CSCA is used to verify the signature of the CRL. Since a CSCA issues a single CRL, this CRL covers all certificates issued with that countryName. In addition to that mandatory check, an optional check that the issuer field of the certificate is equal to the issuer field of the CRL or one of the values of the issuerAltName extension in the CRL MAY also be done.

Note 2: It is possible that the CRL contains other revocation information, for example concerning system operator or registration authority certificates.

8 CSCA MASTER LIST STRUCTURE

Master Lists are implemented as instances of the `ContentInfo` Type, as specified in [RFC 5652]. The `ContentInfo` MUST contain a single instance of the `SignedData` Type as profiled below. No other data types are included in the `ContentInfo`. All Master Lists MUST be produced in DER format to preserve the integrity of the signatures within them.

8.1 SignedData Type

The processing rules in [RFC 5652] apply.

The specification of Master List structure uses the following terminology for presence requirements of each field.

- m mandatory – the field MUST be present
- r recommended - the field SHOULD be present
- x do not use – the field MUST NOT be present
- o optional – the field MAY be present

Table 7: Master List

Value		Comments
<code>SignedData</code>		
<code>version</code>	m	Value = v3
<code>digestAlgorithms</code>	m	
<code>encapContentInfo</code>	m	
<code>eContentType</code>	m	<code>id-icao-cscaMasterList</code>
<code>eContent</code>	m	The encoded contents of an <code>cscaMasterList</code>
<code>certificates</code>	m	The Master List Signer certificate MUST be included and the CSCA certificate, which can be used to verify the signature in the <code>signerInfos</code> field SHOULD be included.
<code>crls</code>	x	
<code>signerInfos</code>	m	It is RECOMMENDED that States only provide 1 <code>signerinfo</code> within this field.
<code>SignerInfo</code>	m	
<code>version</code>	m	The value of this field is dictated by the <code>sid</code> field. See [RFC 5652] for rules regarding this field
<code>sid</code>	m	
<code>subjectKeyIdentifier</code>	r	It is RECOMMENDED that this field be supported rather than <code>issuerandSerialNumber</code> .
<code>digestAlgorithm</code>	m	The algorithm identifier of the algorithm used to produce the hash value over <code>encapsulatedContent</code> and <code>SignedAttrs</code> .
<code>signedAttrs</code>	m	Additional attributes may be included. However these do not have to be processed by Receiving States except to verify the signature value. <code>signedAttrs</code> MUST include signing time (see [PKCS #9]).
<code>signatureAlgorithm</code>	m	The algorithm identifier of the algorithm used to produce the signature value, and any associated parameters.
<code>signature</code>	m	The result of the signature generation process.
<code>unsignedAttrs</code>	o	Although this field MAY be included, Receiving States may choose to ignore it.

8.2 ASN.1 Master List Specification

`CscaMasterList`

```
{ iso-itu-t(2) international-organization(23) icao(136) mrt(1)
security(1) masterlist(2)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

    -- Imports from RFC 5280 [PROFILE], Appendix A.1
    Certificate
        FROM PKIX1Explicit88
            { iso(1) identified-organization(3) dod(6)
              internet(1) security(5) mechanisms(5) pkix(7)
              mod(0) pkix1-explicit(18) };

    -- CSCA Master List

CscMasterListVersion ::= INTEGER {v0(0)}

CscMasterList ::= SEQUENCE {
    version          CscMasterListVersion,
    certList        SET OF Certificate }

-- Object Identifiers

id-icao-cscMasterList OBJECT IDENTIFIER ::=
    {id-icao-mrt-security 2}
id-icao-cscMasterListSigningKey OBJECT IDENTIFIER ::=
    {id-icao-mrt-security 3}

END
```

APPENDIX A - LIFETIMES (INFORMATIVE)

The following examples illustrate calculation of private key usage periods and public key certificate validity for various scenarios as described in Section 4.

A.1 Example 1

The first example illustrates a scenario where eMRTDs are valid for five years. Because a relatively large number of eMRTDs are issued per day, the policy is to keep private key usage periods and public key certificate validity to a minimum. For this example, the minimum private key usage period for Document Signer certificates is 1 month.

Item	Usage/Validity Period
eMRTD Validity	5 years
Document Signer private key usage period	1 month
Document Signer certificate validity	5 years + 1 month
CSCA private key usage period	3 years
CSCA certificate validity	8 years + 1 month

The consequences of this example are that by the time the first CSCA certificate becomes invalid at least 36 Document Signer certificates will have been issued (one corresponding to each private key that has a one-month usage period). In the last few months before the first CSCA certificate becomes invalid, there will be at least 2 additional CSCA certificates issued (one corresponding to each private key that has a 3 year usage period).

A.2 Example 2

The second example illustrates a scenario where eMRTDs are valid for ten years. The policy is to keep private key usage periods and public key certificate validity to an average length.

Item	Usage/Validity Period
eMRTD Validity	10 years
Document Signer private key usage period	2 months
Document Signer certificate validity	10 years + 2 months
CSCA private key usage period	4 years
CSCA certificate validity	14 years + 2 months

The consequences of this example are by the time the first CSCA certificate becomes invalid at least 24 Document Signer certificates will have been issued (one corresponding to each private key that has a 2 month usage period). In the last few months before the first CSCA certificate becomes invalid, there will be at least 3 additional CSCA certificates issued (one corresponding to each private key that has a 4 year usage period).

A.3 Example 3

The final example illustrates a scenario where eMRTDs are valid for ten years and the policy is to use the maximum private key usage periods and public key certificate validity.

Item	Usage/Validity Period
eMRTD Validity	10 years
Document Signer private key usage period	3 months
Document Signer certificate validity	10 years + 3 months
CSCA private key usage period	5 years
CSCA certificate validity	15 years + 3 months

The consequences of this example are by the time the first CSCA certificate becomes invalid at least 20 Document Signer certificates will have been issued (one corresponding to each private key that has a 3 month usage period). In the last few months before the first CSCA certificate becomes invalid, there will be at least 3 additional CSCA certificates issued (one corresponding to each private key that has a 5 year usage period).

APPENDIX B – CERTIFICATE & CRL PROFILE REFERENCE TEXT (INFORMATIVE)

The certificate and CRL profiles defined in Section 7 are based on definitions and base profile requirements specified in referenced documents. Brief excerpts of some relevant sections from these source documents (as of the time of writing) are replicated in the tables below. These excerpts are provided to assist the reader in understanding the background for some of the requirements specified in the eMRTD certificate and CRL profiles. They are not intended to be relied on instead of the referenced documents. In all cases, to obtain the full specification of the referenced component/extension and to obtain the most current specification, the actual referenced documents MUST be used.

Table 8: Certificate Fields and Extensions

Component / Extension	Reference	Relevant Excerpts
Certificate	RFC 5280 - 4.1.1	
TBSCertificate	RFC 5280 - 4.1.1.1	
signatureAlgorithm	RFC 5280 - 4.1.1.2	
signatureValue	RFC 5280 - 4.1.1.3	
TBSCertificate	RFC 5280 - 4.1.2	
version	RFC 5280 - 4.1.2.1	When extensions are used, as expected in this profile, version MUST be 3 (value is 2).
serialNumber	RFC 5280 - 4.1.2.2	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA (i.e., the issuer name and serial number identify a unique certificate). CAs MUST force the serialNumber to be a non-negative integer. Given the uniqueness requirements above, serial numbers can be expected to contain long integers. Certificate users MUST be able to handle serialNumber values up to 20 octets. Conformant CAs MUST NOT use serialNumber values longer than 20 octets.
	X.690 - 8.3.2	If the contents octets of an integer value encoding consist of more than one octet, then the bits of the first octet and bit 8 of the second octet: a) shall not all be ones; and b) shall not all be zero. NOTE – These rules ensure that an integer value is always encoded in the smallest possible number of octets.
	X.690 - 8.3.3	The contents octets shall be a two's complement binary number equal to the integer value, and consisting of bits 8 to 1 of the first octet, followed by bits 8 to 1 of the second octet,

		followed by bits 8 to 1 of each octet in turn up to and including the last octet of the contents octets.
signature	RFC 5280 - 4.1.1.2	This field MUST contain the same algorithm identifier as the signatureAlgorithm field in the sequence Certificate.
issuer	RFC 5280 – Appendix A.1	X520countryName ::= PrintableString (SIZE (2)) X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))
	RFC 5280 – 4.1.2.4	CAs conforming to this profile MUST use either the PrintableString or UTF8String encoding of DirectoryString.
	ISO 3166-1	
validity	RFC 5280 - 4.1.2.5	Both notBefore and notAfter may be encoded as UTCTime or GeneralizedTime. CAs conforming to this profile MUST always encode certificate validity dates through the year 2049 as UTCTime. Certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime.
(if encoded as UTCTime)	X.690 – 11.8.1	The encoding shall terminate with "Z", as described in the ITU-T X.680 ISO/IEC 8824-1 clause on UTCTime.
	X.690 – 11.8.2	The seconds element shall always be present.
(if encoded as GeneralizedTime)	X.690 – 11.7.1	The encoding shall terminate with a "Z", as described in the ITU-T Rec. X.680 ISO/IEC 8824-1 clause on GeneralizedTime.
	X.690 – 11.7.2	The seconds element shall always be present.
	RFC 5280 – 4.1.2.5.2	GeneralizedTime values MUST NOT include fractional seconds. For the purposes of this profile, GeneralizedTime values MUST be expressed Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero.
subject	RFC 5280 – Appendix A.1	X520countryName ::= PrintableString (SIZE (2)) X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))
	RFC 5280 – 4.1.2.6	CAs conforming to this profile MUST use either the PrintableString or UTF8String encoding of DirectoryString.
subjectPublicKeyInfo	RFC 5280 - 4.1.2.7	
issuerUniqueID	RFC 5280 -	CAs conforming to this profile MUST

	4.1.2.8	NOT generate certificates with unique identifiers.
subjectUniqueID	RFC 5280 - 4.1.2.8	CAs conforming to this profile MUST NOT generate certificates with unique identifiers.
extensions	X.690 – 11.5	The encoding of a set value or sequence value shall not include an encoding for any component value which is equal to its default value.
<i>Table 36: AuthorityKeyIdentifier</i>	RFC 5280 – 4.2.1.1	The keyIdentifier field of the authorityKeyIdentifier extension MUST be included in all certificates generated by conforming CAs to facilitate certification path construction. There is one exception. Where a CA distributes its public key in the form of a "self-signed" certificate, the authority key identifier MAY be omitted.
keyIdentifier		
authorityCertIssuer		
authorityCertSerialNumber		
<i>Table 37: SubjectKeyIdentifier</i>	RFC 5280 – 4.2.1.2	To facilitate certification path construction, this extension MUST appear in all conforming CA certificates, that is, all certificates including the basic constraints extension (section 4.2.1.9) where the value of cA is TRUE.
<i>Table 38: subjectKeyIdentifier</i>		
<i>Table 39: KeyUsage</i>	RFC 5280 – 4.2.1.3	The usage restriction might be employed when a key that could be used for more than one operation is to be restricted.
digitalSignature		The digitalSignature bit is asserted when the subject public key is used with a digital signature mechanism to support security services other than certificate signing (bit 5), or CRL signing (bit 6).
nonRepudiation		
keyEncipherment		
dataEncipherment		
keyAgreement		
keyCertSign		The keyCertSign bit is asserted when the subject public key is used for verifying a signature on public key certificates.
cRLSign		The cRLSign bit is asserted when the subject public key is used for verifying a signature on certificate revocation list (e.g., a CRL, delta CRL, or an ARL). This bit MUST be asserted in certificates that are used to verify signatures on CRLs.
encipherOnly		
decipherOnly		
PrivateKeyUsagePeriod	RFC 3280 –	CAs conforming to this profile MUST

	4.2.1.4	NOT generate certificates with private key usage period extensions unless at least one of the two components is present and the extension is non-critical.
notBefore		Where used, notBefore and notAfter are represented as GeneralizedTime and MUST be specified and interpreted as defined in section 4.1.2.5.2.
notAfter		
CertificatePolicies	RFC 5280 – 4.2.1.4	If this extension is critical, the path validation software MUST be able to interpret this extension (including the optional qualifier), or MUST reject the certificate.
PolicyInformation		
policyIdentifier		
policyQualifiers		
PolicyMappings	RFC 5280 – 4.2.1.5	
SubjectAltName	RFC 5280 – 4.2.1.6	
IssuerAltName	RFC 5280 – 4.2.1.7	
SubjectDirectoryAttributes	RFC 5280 – 4.2.1.8	
Basic Constraints	RFC 5280 – 4.2.1.9	The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate. Conforming CAs MUST include this extension in all CA certificates that contain public keys used to validate digital signatures on certificates and MUST mark the extension as critical in such certificates.
cA		The cA boolean indicates whether the certified public key belongs to a CA. If the cA boolean is not asserted, then the keyCertSign bit in the key usage extension MUST NOT be asserted.
PathLenConstraint		
NameConstraints	RFC 5280 – 4.2.1.10	
PolicyConstraints	RFC 5280 – 4.2.1.11	
ExtKeyUsage	RFC 5280 – 4.2.1.12	This extension indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension.
CRLDistributionPoints	RFC 5280 – 4.2.1.13	
distributionPoint		
reasons		
cRLIssuer		
InhibitAnyPolicy	RFC 5280 –	

	4.2.1.14	
FreshestCRL	RFC 5280 – 4.2.1.15	
privateInternetExtensions	RFC 5280 – 4.2.2	
NameChange		
DocumentType		
Netscape Certificate Type		
other private extensions		

Table 9: CRL Fields and Extensions

Component / Extension	Reference	Relevant Excerpts
CertificateList	RFC 5280 - 5.1.1	
tBSCertList	RFC 5280 - 5.1.1.1	
signatureAlgorithm	RFC 5280 - 5.1.1.2	
signatureValue	RFC 5280 - 5.1.1.3	
	RFC 5280 - 5.1.2	
version	RFC 5280 - 5.1.2.1	This optional field describes the version of the encoded CRL. When extensions are used, as required by this profile, this field MUST be present and MUST specify version 2 (the integer value is 1).
signature	RFC 5280 - 5.1.2.2	This field MUST contain the same algorithm identifier as the signature field in the sequence CertificateList.
issuer	RFC 5280 - Appendix A.1	X520countryName ::= PrintableString (SIZE (2)) X520serialNumber ::= PrintableString (SIZE 1..ub-serial-number))
	RFC 5280 5.1.2.3 and 4.1.2.4	CAs conforming to this profile MUST use either the PrintableString or UTF8String encoding of DirectoryString.
thisUpdate	RFC 5280 5.1.2.4	CRL issuers conforming to this profile MUST encode thisUpdate as UTCTime for dates through the year 2049. CRL issuers conforming to this profile MUST encode thisUpdate as GeneralizedTime for dates in the year 2050 or later.
(if encoded as UTCTime)	X.690 – 11.8.1	The encoding shall terminate with "Z", as described in the ITU-T X.680 ISO/IEC 8824-1 clause on UTCTime.
	X.690 – 11.8.2	The seconds element shall always be present.
(if encoded as GeneralizedTime)	X.690 – 11.7.1	The encoding shall terminate with a "Z", as described in the ITU-T Rec. X.680 ISO/IEC 8824-1 clause on GeneralizedTime.
	X.690 – 11.7.2	The seconds element shall always be present.
	RFC 5280 – 4.1.2.5.2	GeneralizedTime values MUST NOT include fractional seconds. For the purposes of this profile, GeneralizedTime values MUST be expressed Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of

Component / Extension	Reference	Relevant Excerpts
		seconds is zero.
nextUpdate	5.1.2.5	CRL issuers conforming to this profile MUST encode nextUpdate as UTCTime for dates through the year 2049. CRL issuers conforming to this profile MUST encode nextUpdate as GeneralizedTime for dates in the year 2050 or later.
(if encoded at UTCTime)	X.690 – 11.8.1	The encoding shall terminate with "Z", as described in the ITU-T X.680 ISO/IEC 8824-1 clause on UTCTime.
	X.690 – 11.8.2	The seconds element shall always be present.
(if encoded at GeneralizedTime)	X.690 – 11.7.1	The encoding shall terminate with a "Z", as described in the ITU-T Rec. X.680 ISO/IEC 8824-1 clause on GeneralizedTime.
	X.690 – 11.7.2	The seconds element shall always be present.
	RFC 5280 – 4.1.2.5.2	GeneralizedTime values MUST NOT include fractional seconds. For the purposes of this profile, GeneralizedTime values MUST be expressed Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero.
revokedCertificates	RFC 5280 - 5.1.2.6	When there are no revoked certificates, the revoked certificates list MUST be absent. Otherwise, revoked certificates are listed by their serial numbers.
crlExtensions	RFC 5280 - 5.2	Conforming CRL issuers are REQUIRED to include the authority key identifier (Section 5.2.1) and the CRL number (Section 5.2.3) extensions in all CRLs issued.
	X.690 – 11.5	The encoding of a set value or sequence value shall not include an encoding for any component value which is equal to its default value.
authorityKeyIdentifier	RFC 5280 - 5.2.1	Conforming CRL issuers MUST use the key identifier method, and MUST include this extension in all CRLs issued.
issuerAlternativeName	RFC 5280 - 5.2.2	
cRLNumber	RFC 5280 - 5.2.3	CRL issuers conforming to this profile MUST include this extension in all CRLs and MUST mark this extension as non-critical. CRLNumber ::= INTEGER (0..MAX) Given the requirements above, CRL numbers can be expected to contain long integers. CRL verifiers MUST be able to handle CRLNumber values up to 20 octets. Conforming CRL issuers MUST NOT use CRLNumber values longer than 20 octets.
	X.690 – 8.3.2	If the contents octets of an integer value encoding consist of more than one octet, then the bits of the first octet and bit 8 of the second octet: a) shall not all be ones; and b) shall not all be zero.

Component / Extension	Reference	Relevant Excerpts
		NOTE – These rules ensure that an integer value is always encoded in the smallest possible number of octets.
	X.690 – 8.3.3	The contents octets shall be a two's complement binary number equal to the integer value, and consisting of bits 8 to 1 of the first octet, followed by bits 8 to 1 of the second octet, followed by bits 8 to 1 of each octet in turn up to and including the last octet of the contents octets.
deltaCRLIndicator	RFC 5280 - 5.2.4	
issuingDistributionPoint	RFC 5280 - 5.2.5	
freshestCRL	RFC 5280 - 5.2.6	
reasonCode	RFC 5280 - 5.3.1	
holdInstructionCode	RFC 5280 - 5.3.2	
invalidityDate	RFC 5280 - 5.3.3	
certificateIssuer	RFC 5280 - 5.3.4	

APPENDIX C – EARLIER CERTIFICATE PROFILES (INFORMATIVE)

The certificate profiles in this Appendix were specified in the 6th edition of ICAO 9303. Although CSCAs MUST issue certificates that comply with the current profiles as specified in Section 7, the earlier profiles are included here for information only as certificates that were issued in compliance with the earlier profiles will be in circulation, and processed by Inspection Systems for several years.

Table 10: Certificate Body

Certificate Component	Section in RFC 3280	Country Signing CA Certificate	Document Signer Certificate	Comments
Certificate	4.1.1	m	m	
TBSertificate	4.1.1.1	m	m	See next part of the table
SignatureAlgorithm	4.1.1.2	m	m	Value inserted here dependent on algorithm selected
SignatureValue	4.1.1.3	m	m	Value inserted here dependent on algorithm selected
TBSertificate	4.1.2			
version	4.1.2.1	m	m	SHALL be v3
serialNumber	4.1.2.2	m	m	
signature	4.1.2.3	m	m	Value inserted here SHALL match the OID in signatureAlgorithm
issuer	4.1.2.4	m	m	See A1.5
validity	4.1.2.5	m	m	Implementations SHALL specify using UTC time until 2049 from then on using GeneralisedTime
subject	4.1.2.6	m	m	See A1.5
subjectPublicKeyInfo	4.1.2.7	m	m	
issuerUniqueID	4.1.2.8	x	x	
subjectUniqueID	4.1.2.8	x	x	
extensions	4.1.2.9	m	m	See next table on which extensions SHOULD be present

Table 11: Extensions

Extension name	Paragraph in RFC 3280	Country Signing CA Certificate	Document Signer Certificate	Comments
AuthorityKeyIdentifier	4.2.1.1	o	m	Mandatory in all certificates except for self-signed CSCA certificates
SubjectKeyIdentifier	4.2.1.2	m	o	
KeyUsage	4.2.1.3	mc	mc	This extension SHALL be marked CRITICAL
PrivateKeyUsagePeriod	4.2.1.4	o	o	This would be the issuing period of the private key
CertificatePolicies	4.2.1.5	o	o	
PolicyMappings	4.2.1.6	x	x	
SubjectAltName	4.2.1.7	x	x	
IssuerAltName	4.2.1.8	x	x	
SubjectDirectoryAttributes	4.2.1.9	x	x	
BasicConstraints	4.2.1.10	mc	x	This extension SHALL be marked CRITICAL

Extension name	Paragraph in RFC 3280	Country Signing CA Certificate	Document Signer Certificate	Comments
NameConstraints	4.2.1.11	x	x	
PolicyConstraints	4.2.1.12	x	x	
ExtKeyUsage	4.2.1.13	x	x	
CRLDistributionPoints	4.2.1.14	o	o	If Issuing States or organizations choose to use this extension they SHALL include the ICAO PKD as a distribution point. Implementations may also include relative CRL DPs for local purposes; these may be ignored by other Receiving States.
InhibitAnyPolicy	4.2.1.15	x	x	
FreshestCRL	4.2.1.16	x	x	
privateInternetExtensions	4.2.2	x	x	
other private extensions	N/A	o	o	If any private extension is included for national purposes then they SHALL NOT be marked. Issuing States or organizations are discouraged from including any private extensions.
AuthorityKeyIdentifier	4.2.1.1			
keyIdentifier		m	m	If this extension is used this field SHALL be supported as a minimum
authorityCertIssuer		o	o	See A1.5
authorityCertSerialNumber		o	o	
SubjectKeyIdentifier	4.2.1.2			
subjectKeyIdentifier		m	m	
KeyUsage	4.2.1.3			
digitalSignature		x	m	
nonRepudiation		x	x	
keyEncipherment		x	x	
dataEncipherment		x	x	
keyAgreement		x	x	
keyCertSign		m	x	
cRLSign		m	x	
encipherOnly		x	x	
decipherOnly		x	x	
BasicConstraints	4.2.1.10			
cA		m	x	TRUE for CA certificates
PathLenConstraint		m	x	0 for New CSCA certificate, 1 for Linked CSCA certificate
CRLDistributionPoints	4.2.1.14			
distributionPoint		m	x	
reasons		m	x	
cRLIssuer		m	x	
CertificatePolicies	4.2.1.5			
PolicyInformation				
policyIdentifier		m	m	

Extension name	Paragraph in RFC 3280	Country Signing CA Certificate	Document Signer Certificate	Comments
policyQualifiers		0	0	

DRAFT_4 FOR TAG_22

APPENDIX D – RFC 5280 VALIDATION COMPATIBILITY (INFORMATIVE)

This Appendix provides guidance to Receiving States wishing to use systems that implement the [RFC 5280] certification path and CRL validation algorithms.

The eMRTD PKI trust model is a subset of that covered by the validation procedures defined in [RFC 5280]. Section D.1 identifies the subset of steps from the [RFC 5280] definition that are required for the eMRTD application and provides the necessary inputs and initialization values and processes for certification path validation, CRL validation and revocation checking.

Section D.2 covers the remaining steps from the [RFC 5280] definition that are not relevant to the eMRTD application. The inputs and initialization values for certification path validation and CRL validation are provided. This guidance in this section is for use in situations where the tools implement the full [RFC 5280] algorithms, rather than just the subset described in D.1.

Section D.3 provides guidance to support the extension of [RFC 5280] based CRL processing to cover revocation checking after a CSCA has undergone a name change.

D.1 Steps Relevant to eMRTD

The eMRTD certification path validation procedure defined here is based on the procedure described in [RFC 5280]. The same terminology and process descriptions are used. The eMRTD certificate profiles restrict certification paths to a single certificate and prohibit use of many optional features that are used in other applications, such as the Internet PKI defined in [RFC 5280]. Path validation steps associated with these features are omitted from the eMRTD certification path validation procedure.

D.1.1 Certification Path Validation Procedure

D.1.1.1 Inputs

[RFC 5280] defines a set of 9 inputs to the path validation algorithm. Only the following 3 are relevant to the eMRTD application:

- certification path: A single certificate (e.g. the Document Signer certificate);
- current date/time; and
- Trust Anchor information, including:
 - trusted issuer name: If the Trust Anchor is in the form of a CSCA certificate, the trusted issuer name is the value of the Subject field of that certificate;
 - trusted public key algorithm: If the Trust Anchor is in the form of a CSCA certificate, the trusted public key algorithm is taken from the `SubjectPublicKeyInfo` field of that certificate;
 - trusted public key: If the Trust Anchor is in the form of a CSCA certificate, the trusted public key is taken from the `SubjectPublicKeyInfo` field of that certificate; and
 - trusted public key parameters: This is an optional input that is only included if the trusted public key algorithm requires parameters. If the Trust Anchor is in the form of a CSCA certificate, these parameters are taken from the `SubjectPublicKeyInfo` field of that certificate.

If an implementation requires that the additional 6 inputs be supplied, recommendations for these are provided in D.2.

There could be several Trust Anchors for the CSCA that issued the certificate being validated. Of these Trust Anchors, the one that **MUST** be used is the one that contains the public key that matches the value of the Authority Key Identifier extension in the certificate being validated.

D.1.1.2 Initialization

There are 11 state variables defined in [RFC 5280]. Only the following 5 are relevant to the eMRTD application:

- application: `max_path_length`: Initialize to “0”;
- working_issuer_name: Initialize to the value of the trusted issuer name;

- `working_public_key_algorithm`: Initialize to the value of the trusted public key algorithm;
- `working_public_key`: Initialize to the value of the trusted public key; and
- `working_public_key_parameters`: Initialize to the value of the trusted public key parameters.

If an implementation requires that the additional 6 variables be initialized, recommendations for these are provided in D.2.

D.1.1.3 Certificate Processing

eMRTD certificate processing steps are a subset of those defined in [RFC 5280]. The result of processing an eMRTD certificate using this simplified process will be consistent with the result using the full RFC 5280 algorithm. If the additional inputs and state variables are configured as described in D.2.

- a) Verify the basic certificate information. The certificate **MUST** satisfy each of the following:
 - The signature on the certificate can be verified using `working_public_key_algorithm`, the `working_public_key`, and the `working_public_key_parameters`;
 - The certificate validity period includes the current time;
 - At the current time, the certificate is not revoked (see 6.3 for details); and
 - The certificate issuer name is the `working_issuer_name`.
- b) Assign the certificate `subjectPublicKey` to `working_public_key`.
- c) If the `subjectPublicKeyInfo` field of the certificate contains an algorithm field with non-null parameters, assign the parameters to the `working_public_key_parameters` variable. If the `subjectPublicKeyInfo` field of the certificate contains an algorithm field with null parameters or parameters are omitted, compare the certificate `subjectPublicKey` algorithm to the `working_public_key_algorithm`. If the certificate `subjectPublicKey` algorithm and the `working_public_key_algorithm` are different, set the `working_public_key_parameters` to null.
- d) Assign the certificate `subjectPublicKey` algorithm to the `working_public_key_algorithm` variable.
- e) Recognize and process any other critical extensions present in the certificate.
- f) Process any other recognized non-critical extensions present in the certificate.

If any of the checks in step a) fail or if there are any unrecognized critical extensions in the certificate that cannot be processed, the path validation procedure fails. Otherwise the procedure succeeds.

D.1.1.4 Outputs

If path validation succeeds, the procedure terminates, returning a success indication together with the `working_public_key`, the `working_public_key_algorithm`, and the `working_public_key_parameters`.

If path validation fails, the procedure terminates, returning a failure indication and an appropriate reason.

D.1.2 CRL Validation and Revocation Checking

The CRL validation algorithm in [REC 5280] covers various types of CRLs including delta CRLs, partitioned CRLs, indirect CRLs etc. The CRL profile for the eMRTD application is very restrictive and prohibits use of any of these features. Use of the `issuingDistributionPoint` extension as well as all of the standardized CRL-entry extensions is also prohibited. As a result, CRL validation and revocation checking for the eMRTD application is relatively simple.

D.1.2.1 Inputs

[RFC 5280] defines 2 inputs to the CRL validation algorithm. Only the following 1 of these is relevant to the eMRTD application. If an implementation requires that the additional input be supplied, a recommendation for this is provided in D.2.

- certificate: certificate serial number and issuer name

D.1.2.2 Initialization

There are 3 state variables defined in [RFC 5280]. Only the following 1 of these is relevant to the eMRTD application. If an implementation requires that the additional 2 variables be initialized, recommendations for these are provided in D.2.

- cert_status : initialize to the value UNREVOKED

D.1.2.3 CRL Processing

All CRLs in the eMRTD application are complete CRLs that cover all current certificates issued by the CSCA that issued the CRL. There are no partitioned, delta or indirect CRLs. The steps in the CRL processing algorithm for the eMRTD application are:

- a) Obtain the current CRL for the CSCA that issued the certificate. If the CRL cannot be obtained, the cert_status variable is set to UNDETERMINED, and processing is stopped.
- b) Verify that the CRL issuer is the same CSCA that issued the certificate in question. Because there is a single CSCA in each country, and the eMRTD application is a closed application with Inspection Systems retaining a cache of CRLs that is unique to this application, verifying that the country name is the same in the issuer field of the CRL and the issuer field of the certificate is sufficient.
 - If the CSCA has not undergone a name change since the certificate was issued, the issuer field in the CRL and the issuer field in the certificate will be identical.
 - If the CSCA has undergone a name change since the certificate was issued, the country attribute of the name in the issuer field of the certificate and in the issuer field of the CRL will be the same, but some other attributes may be different.
 - If the relying party wishes to verify that substitution of some non eMRTD CRL has not happened, they may optionally verify that they have Trust Anchors for both CSCA names and that those Trust Anchors are for the same CSCA. If the CSCA has undergone a name change and has included to the optional issuerAltName extension in the CRL the relying party MAY optionally verify that the issuer field in the certificate is identical to one of the values in this extension.

If the CRL issuer is not the CSCA that issued the certificate, the cert_status variable is set to UNDETERMINED, and processing is stopped.

- c) Validate the certification path for the issuer of the CRL. Note that in the eMRTD application all CRLs are issued by CSCAs that are the Trust Anchors for the respective paths. Unlike the algorithm in [RFC 5280], the eMRTD application does NOT require that the Trust Anchor used to validate the CRL certification path be the same Trust Anchor that was used to validate the target certificate. However, if the Trust Anchors are different, they MUST both be Trust Anchors for the same CSCA. Unlike [RFC 5280], the eMRTD application has multiple Trust Anchors for a given CSCA that are valid at the same time. If the certification path cannot be successfully validated, the cert_status variable is set to UNDETERMINED, and processing is stopped.
- d) Verify the signature on the CRL. If the signature cannot be successfully verified, the cert_status variable is set to UNDETERMINED, and processing is stopped.
- e) Search for the certificate on the CRL. If an entry is found that matches the certificate issuer and serial number, then the cert_status variable is set to UNSPECIFIED.

D.1.2.4 Output

Return the cert_status. If steps a) b) c) or d) failed, the status will be UNDETERMINED. If the certificate was listed as revoked on the CRL, the status will be UNSPECIFIED. If CRL validation succeeded, but the certificate was not listed on the CRL, the status will be UNREVOKED.

D.2 Steps not Required by eMRTD

D.2.1 Certification Path Validation

Settings for additional inputs that are not relevant to eMRTD validation include:

- initial-policy-mapping-inhibit: Set to inhibit policy mapping;
- initial-any-policy-inhibit: Set to inhibit processing of the any-policy value;
- initial-permitted-subtrees: Set to permit all subtrees;
- initial-excluded-subtrees: Set to exclude no subtrees;
- initial-explicit-policy: This should NOT be set; and
- user-initial-policy-set: Set to the special value “any-policy”.

Initialization of state variables that are not relevant to the eMRTD application include:

- permitted_subtrees: Initialize to permit all subtrees;
- excluded_subtrees: Initialize to exclude no subtrees;
- inhibit_any_policy: If initial-any-policy-inhibit is set, initialize to “0”. Otherwise, set to the value 1 or any value greater than that;
- policy_mapping: Initialize to “0”;
- explicit_policy: Initialize to “2”; and
- valid_policy_tree: Initialize the valid_policy element to “anyPolicy”, the qualifier_set element to empty and the expected_policy_set to “anyPolicy”.

D.2.2 CRL Validation

Settings for additional inputs that are not relevant to eMRTD validation include:

- use-deltas: Set to prohibit use of deltas.

Initialization of state variables that are not relevant to the eMRTD application include:

- reasons_mask: Initialize to an empty set; and
- Interim_reasons_mask: Initialize to the special value “all-reasons”.

D.3 Modifications required to process CRLs

CRL validation systems that comply with the CRL validation procedure in [RFC 5280] are not intended to support environments where a CA has undergone a name change, such as the eMRTD application environment. Therefore these systems require some modification to handle this special case, as described below:

- a) In clause 6.3.3, step a) of the [RFC 5280] CRL validation procedure, the name in the distribution point field of the CRL Distribution Points extension of the certificate in question is used to update the local cache with the relevant CRL(s). For the eMRTD application, this step would need to be modified and only the `countryName` attribute of the distribution point field should be used to identify and obtain the appropriate CRL.
- b) In clause 6.3.3, step f) of the [RFC 5280] CRL validation procedure, there is a requirement that the same Trust Anchor be used to validate the certification path for the CRL issuer that was used to validate the target certificate. This is NOT a requirement for the eMRTD application because independent Trust Anchors are established for each public key of the CSCA.

The Trust Anchor used for validation of the CRL issuer will be the one for the CSCA’s public key that corresponds to the private key used to sign the CRL. The Trust Anchor used to validate the certification path for the target certificate may be for an earlier CSCA key pair.

REFERENCES (NORMATIVE)

- [FIPS 180-2] FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB) 180-2, *Secure Hash Standard*, August 2002
- [FIPS 186-4] FIPS 186-4, Federal Information Processing Standards Publication (FIPS PUB) 186-4, *Digital Signature Standard*, July 2013 (Supersedes FIPS PUB 186-3 dated June 2009).
- [ISO 3166-1] ISO/IEC 3166-1: 2006, Codes for the representation of names of countries and their subdivisions — Part 1: Country Codes
- [ISO/IEC 15946] ISO/IEC 15946: 2002, Cryptographic techniques based on elliptic curves
- [RFC 3280] RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002
- [RFC 4055] RFC 4055, J. Schaad, B. Kaliski, R. Housley, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, June 2005
- [RFC 5652] RFC 5652, R. Housley, Cryptographic Message Syntax, September 2009
- [RFC 5280] RFC 5280, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May, 2008
- [TR 03111] BSI TR-03111: Elliptic Curve Cryptography v 2.0 2012
- [X9.62] X9.62, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 7 January 1999
- [X.509] ITU-T X.509 | ISO/IEC 9594-8, 2008: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
- [X.690] ITU-T X.690 2008: Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)