ICAO

Doc 9303

Machine Readable Travel Documents

Seventh Edition, 2015

Part 1: Introduction

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

ICAO

Doc 9303

Machine Readable Travel Documents

Seventh Edition, 2015

Part 1: Introduction

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

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

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

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

AMENDMENTS

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

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by

TABLE OF CONTENTS

1. FOREWORD

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

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

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

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

2. SCOPE

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

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

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

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

3. GENERAL CONSIDERATIONS

3.1 ICAO's Leadership Role

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

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

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

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

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

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

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

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

3.2 Relative Costs and Benefits of Machine Readable Travel Documents

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

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

3.3 Operations

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

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

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

3.4 Note on the Supplement

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

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

3.5 Endorsement by ISO

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

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

4. DEFINITIONS AND REFERENCES

4.1 Acronyms

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

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

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

4.2 Terms and Definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.3 Key Words

Key words are used to signify requirements.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" used in capitalized form in Doc 9303 are to be interpreted as described in [RFC 2119]:

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

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

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

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

4.4 Object Identifiers

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

```
-- ICAO security framework
id-icao OBJECT IDENTIFIER ::= {2.23.136}

id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}

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


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


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

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


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


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

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


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

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

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


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

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

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

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

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

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

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

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

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

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

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

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

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

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


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

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

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

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

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

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

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

4.5 The Use of Notes

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

5. GUIDANCE ON THE USE OF DOC 9303

5.1 Doc 9303 Composition

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

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

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

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

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

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

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

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

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

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

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

Part 8 — Emergency Travel Documents
Reserved for future use.

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

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

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

Part 11 specifies cryptographic protocols to:

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

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

5.2 Relationship between MRTD Form Factors and relevant Doc 9303 Parts

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

Table 1-1. Form factors cross-reference table

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

6. REFERENCES (NORMATIVE)

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

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

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

— END —

ISBN 978-92-9249-790-3