ICAO

Doc 9303

Machine Readable Travel Documents

Seventh Edition, 2015

Part 9: Deployment of Biometric Identification and Electronic Storage of Data in MRTDs

Approved by and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION

ICAO

Doc 9303

Machine Readable Travel Documents

Seventh Edition, 2015

Part 9: Deployment of Biometric Identification
and Electronic Storage of Data in MRTDs

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

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

Downloads and additional information are available at www.icao.int/Security/FAL/TRIP

Doc 9303, *Machine Readable Travel Documents*
Part 9 — *Deployment of Biometric Identification and Electronic Storage of Data in MRTDs*
Order No.: 9303P9
ISBN 978-92-9249-797-2

DOCUMENT CHANGE RECORD

Doc 9303, Part 9

DATE	NO.	SECTION/PAGES AFFECTED	
6/12/16	1	Title	Revised "eMRTDs" to "MRTDs"
		Page 11	5.1 Characteristics of the Contactless IC — Added reference to ISO/IEC 14443 application profile
		Page 13	6. Test Methodologies for (e)MRTDS — Reference updated for ISO/IEC 18745-2
		Pages 13 and 14	7. References (Normative) — References updated for ISO/IEC 10373-6, 18745-2, 14443-1 to 4
		Appendix	Previous section A.1 (Location of the IC and its Associated Antenna) revised and moved to Doc 9303-10, Appendix B

TABLE OF CONTENTS

1. SCOPE 1

2. eMRTD 1

2.1 Conformance to Doc 9303 1
2.2 Validity Period for an eMRTD 1
2.3 Chip Inside Symbol 2
2.4 Warning regarding Care in Handling an eMRP 3

3. BIOMETRIC IDENTIFICATION 3

3.1 ICAO Vision on Biometrics 3
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 7

4.1 Primary Biometric: Facial Image 7
4.2 Optional Additional Biometrics 10

5. STORAGE OF THE BIOMETRIC AND OTHER DATA IN A LOGICAL FORMAT IN A CONTACTLESS IC 11

5.1 Characteristics of the Contactless IC 11
5.2 Logical Data Structure 12
5.3 Security and Privacy of the Stored Data 12

6. TEST METHODOLOGIES FOR (e)MRTDS 13

7. REFERENCES (NORMATIVE) 13

APPENDIX TO PART 9 — PROCESS FOR READING eMRTDS (INFORMATIVE) App-1

A.1 Precautions in eMRTD manufacture App-1
A.2 Reading both the OCR and the data on the IC App-1
A.3 Reading geometries App-1
A.4 Reading process App-2

1. SCOPE

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

This Part 9 of Doc 9303 is based on the Sixth Edition of Doc 9303 Part 1, Volume 2, Section II (2006), as well as the Third Edition of Doc 9303 Part 3, 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 IC 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 Part 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:

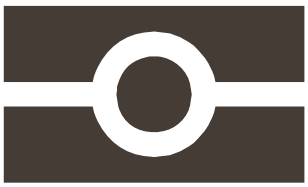


Figure 1. Chip Inside symbol

An electronic file of the symbol is available from the ICAO website. 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 an 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 I.

The image, as shown in Figure 1, 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 is 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.

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.

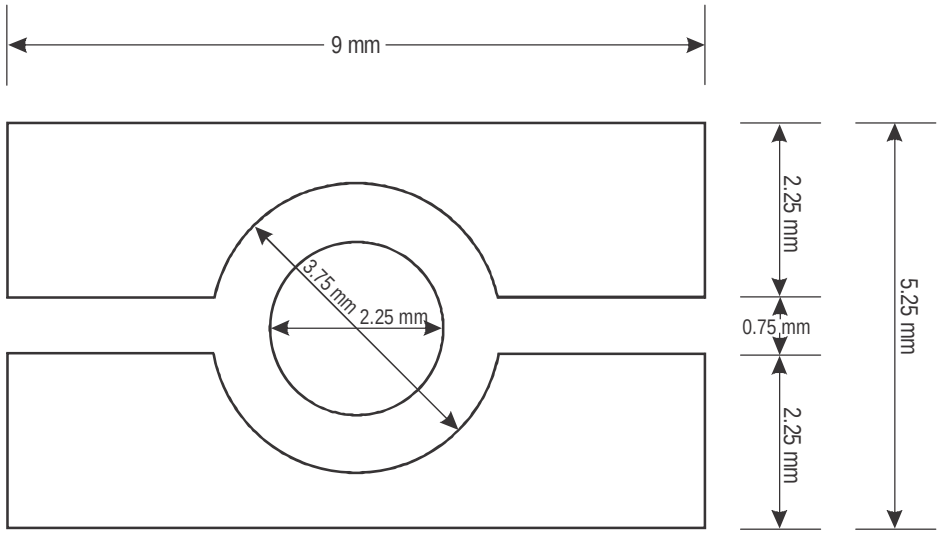


Figure 2. Dimensions of the symbol

Note.— 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).

2.4 Warning regarding Care in Handling an eMRP

It is suggested that a warning be placed in an obvious location on the book urging the holder of an eMRP to take care of the document. 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[1] 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.

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

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 facial 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 is 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.

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 his 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 JPEG 2000 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 to 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.

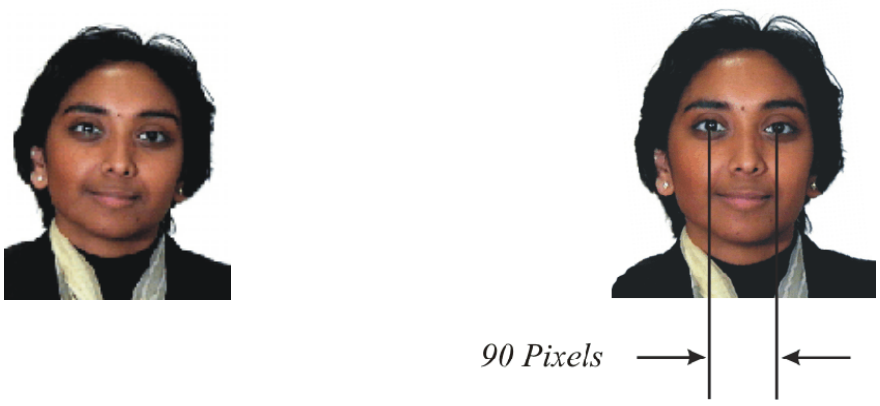
Figure 3. Cropping

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: Face 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.



Original image Token image (angled and resized)

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.

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]. An ISO/IEC 14443 application profile for MRTDs is provided in Doc 9303-10.

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 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 to, modified or deleted from the contactless IC. After issuance a locked contactless IC cannot be unlocked.

Public Key Infrastructure (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 incompliant with 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 cooperation 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 organizations 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 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

7. REFERENCES (NORMATIVE)

ICAO TR RF & PROTOCOL P3	RF Protocol and Application Test Standard for eMRTD — Part 3: Tests for Application Protocol and Logical Data Structure [2]
ICAO TR RF & PROTOCOL P4	RF Protocol and Application Test Standard for eMRTD — Part 4: Conformity Test for Inspection Systems [3]
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	ISO/IEC 10373-6:2016 Identification cards — Test methods — Part 6: Proximity cards
ISO/IEC 18745-2	ISO/IEC 18745-2:2016 Information technology — Test methods for machine readable travel documents (MRTD) and associated devices — Part 2: Test methods for the contactless interface
ISO/IEC 14443-1	ISO/IEC 14443-1:2016, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1: Physical characteristics

[2] to be converted into [ISO/IEC 18745-3]
[3] to be converted into [ISO/IEC 18745-4]

ISO/IEC 14443-2	ISO/IEC 14443-2:2016, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio frequency power and signal interface. *Note.— Latest revisions of ISO/IEC 14443-2 stipulate limits of EMD as REQUIRED. However eMRTDs issued to the field and in process do not necessarily conform to this new parameter. To maintain backwards compatibility for compliance the EMD limits referenced in ISO/IEC 14443-2 should remain as OPTIONAL for eMRTDs within Doc 9303.*
ISO/IEC 14443-3	ISO/IEC 14443-3:2016 (corrected version 2016-09-01), Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and anticollision
ISO/IEC 14443-4	ISO/IEC 14443-4:2016, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol
ISO/IEC 18745-1	ISO/IEC 18745-1:2014, Information technology -- Test methods for machine readable travel documents (MRTD) and associated devices -- Part 1: Physical test methods for passport books (durability)
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

— — — — — — — —

Appendix to Part 9

PROCESS FOR READING eMRTDS (INFORMATIVE)

A.1 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.2 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.3 READING GEOMETRIES

States shall therefore install reading equipment capable of handling MRPs of both geometries, preferably capable of reading both OCR and the IC. Figure 6 shows possible reader configurations, each capable of reading the OCR and the IC. The book is half opened and two antennas ensure that the IC is read irrespective of whether or not it faces the MRZ. 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.

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.

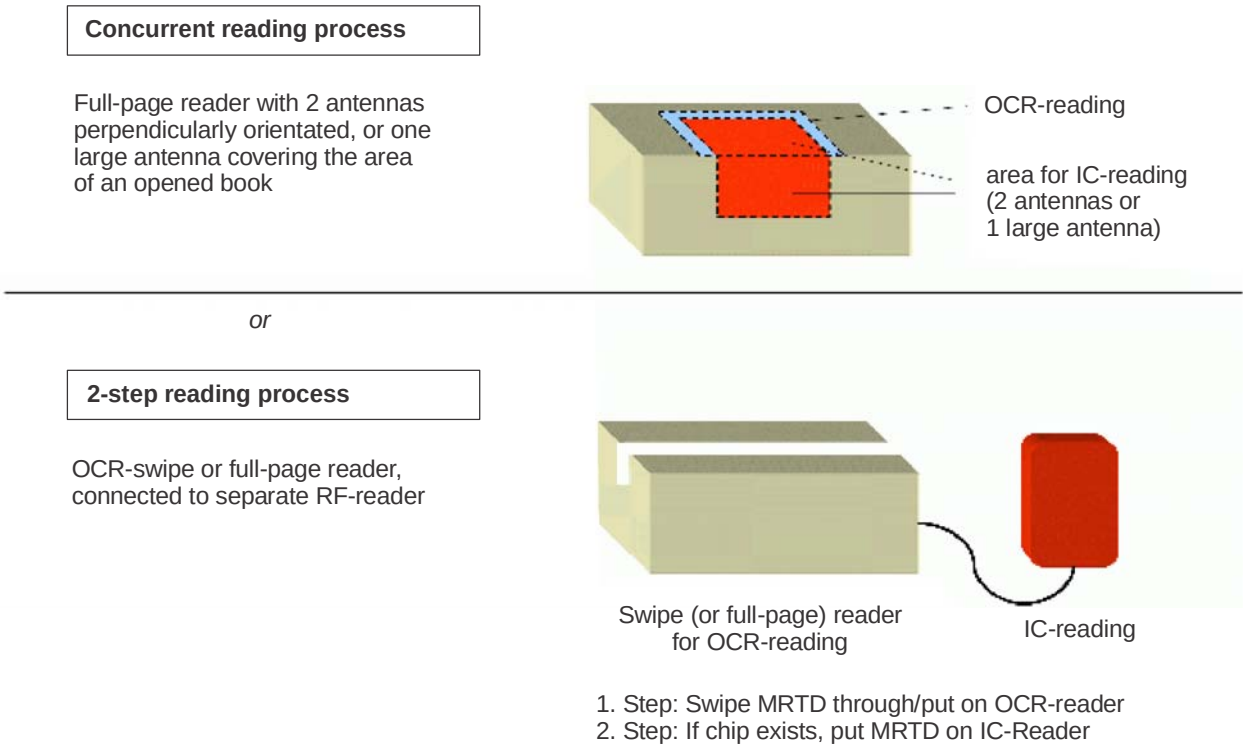


Figure 6. Reading geometries

A.4 READING PROCESSES

Figure 7 shows the processes involved in the reading of an eMRTD prior to and including the biometric verification of the holder.

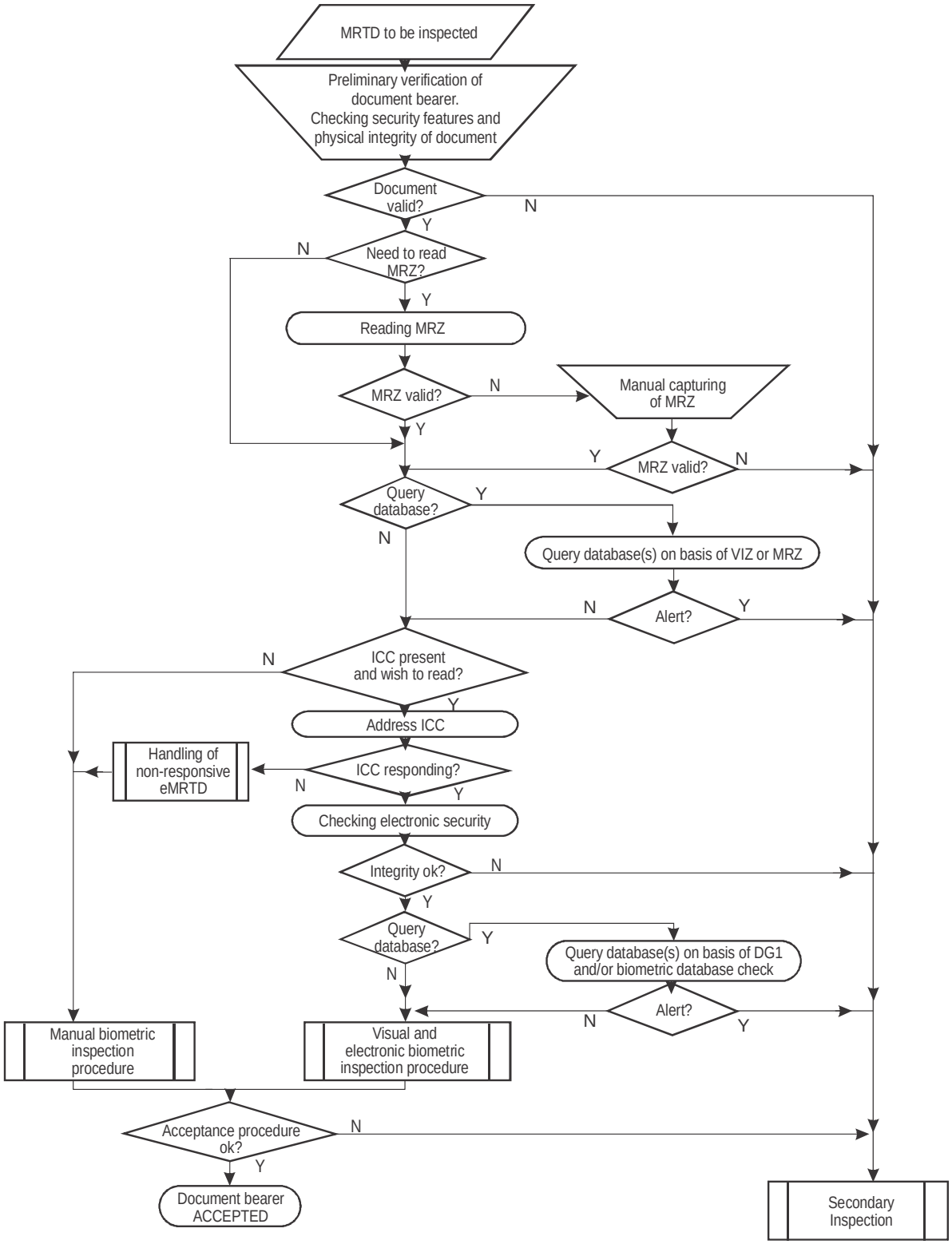


Figure 7. eMRTD reading process

— END —

ISBN 978-92-9249-797-2