ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 2021

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

Eighth Edition, 2021

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

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 978-92-9265-381-1 (print version)
ISBN 978-92-9275-331-3 (electronic version)

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
1	20/3/24	ICAO

CORRIGENDA		
No.	Date	Entered by

TABLE OF CONTENTS

1. SCOPE

Part 9 of Doc 9303 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 or organizations wishing to issue an electronic Machine Readable Travel Document (eMRTD) capable of being used by any suitably equipped receiving State or organization 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 or organization. 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.

Part 9 shall be read in conjunction with:

- Part 1 — *Introduction*;
- Part 10 — *Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)*;
- Part 11 — *Security Mechanisms for MRTDs*;
- Part 12 — *Public Key Infrastructure for MRTDs*.

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 or organization; 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. One 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, Part 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:

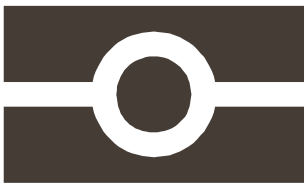

Figure 1. Chip Inside symbol

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 sufficient to hold the mandatory data elements in accordance with the Logical Data Structure (Doc 9303-10), 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 or organization may also print the symbol on the inside page or cover of the passport book that contains the contactless IC and, at its 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.

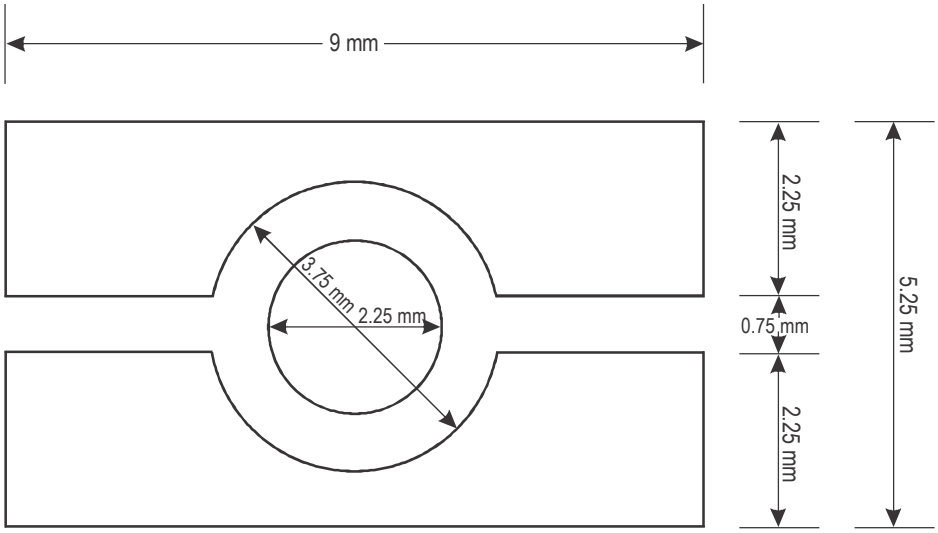

Figure 2. Dimensions of the symbol

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 or organization 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 or organization to select a biometric system that suits its requirements, the data have to be stored in a form from which its 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 or organizations 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 – REQUIRED;
- fingerprint recognition – OPTIONAL;
- iris recognition – OPTIONAL.

ISO/IEC 39794 succeeded ISO/IEC 19794:2005 as international standard for encoding biometrics. The following transition time table has been defined:

- Inspection systems MUST be able to handle ISO/IEC 39794 data by 01-01-2026 after a six-year preparation period starting 01-01-2020;
- between 2026 and 2030, issuing States and organizations can use the data formats specified in ISO/IEC 19794-X:2005 or in ISO/IEC 39794-X during a four-year transition period. During this transition period, interoperability and conformity testing will be essential;
- from 01-01-2030 on, issuing States and organizations MUST use ISO/IEC 39794-X for encoding biometric data.

Doc 9303, Part 10, Amendment 1, provides guidance on the transition from ISO/IEC 19794:2005 to ISO/IEC 39794.

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.

For the purposes of this part, the terms and definitions of the biometrics vocabulary given in ISO/IEC 2382-37:2017 apply.

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 issuing States or organizations;
- *Technical Reliability* — the need to provide guidelines and parameters to ensure issuing States or organizations deploy technologies that have been proven to provide a high level of confidence from an identity confirmation viewpoint; and that States or organizations reading data encoded by other issuing States or organizations 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 or organizations 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 the holder 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 or organization).

When end users collect the eMRTD (or present themselves for any step in the issuance process after the initial application is made and the biometric data are captured) their 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, the traveller's identity can be verified against the image created at the time the traveller's 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. An issuing State or organization 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 the traveller's 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 the traveller's 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 the person's eMRTD with the database recording the data that were put in that eMRTD at the time it was issued.

Four-way check — A fourth confirmatory check, albeit not an electronic one, is visually matching the results of the three-way check with the digitized photograph on the data page of the traveller's eMRTD.

Besides the enrolment and border security applications of biometrics as manifested in one-to-one and one-to-many matching, States and organizations should also have regard to, and set their own criteria in regard to:

- accuracy of the biometric matching functions of the system. Issuing States or organizations 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 or organization.) Given an ICAO-standardized biometric image, receiving States or organizations 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 or organization.

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 or organization is the person at a receiving State or organization purporting to be that same holder.

The only method of relating the person irrevocably to the person's travel document is to have a physiological characteristic, i.e. a biometric, of that person associated with that person's travel document in a tamper-proof manner.

4.1 Primary Biometric: Facial Image

Encoding of reference face images

The face portrait printed on the ICAO-compliant MRTD is an essential element of that document and one of the most important information carriers binding the document to the holder. A standardized face portrait produced at a high quality helps issuing agencies to screen identity and border agencies to inspect the travel document manually or via automated processing. Requirements to capture and encoding of face images are specified in ISO/IEC 39794-5, Annex D.1.

4.2 Optional Additional Biometrics

Issuing States or organizations 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 or organizations 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 or organization 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 or organization.

When an issuing State or organization elects to store fingerprint image(s) on the contactless IC, the optimal image size SHOULD be adequate for 1:1 verification.

Requirements to capture and encoding of finger images are specified in ISO/IEC 39794-4.

Storage of an optional iris biometric

Where an issuing State or organization 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 or organization.

When an issuing State or organization elects to store iris image(s) on the contactless IC, the optimal image size SHOULD be adequate for 1:1 verification.

Requirements to capture and encoding of iris images are specified in ISO/IEC 39794-6.

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/IEC 14443 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) typically is 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 or organization but SHALL be large enough to store the mandatory stored facial image, 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

An issuing State or organization 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 or organizations 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 or organization 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 issuing States or organizations 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 or organization 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 LDS1 data will not be written to the contactless IC after personalization. Therefore the personalization process SHALL lock the contactless IC as a final step. Once the contactless IC has been locked (after personalization and before issuance) further data can only be written to the contactless IC after successful execution of an authentication mechanism (TA), as specified in Doc 9303-10 and Doc 9303-11. 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 or organizations) 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 or organizations 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 States or organizations, and the PKI is customized for ICAO purposes.

The PKI specifications are described in detail in Doc 9303-12.

6. TEST METHODOLOGIES FOR eMRTDS

ICAO, in cooperation with ISO, has developed test methodologies for qualifying eMRTDs with respect to their conformance to the specifications set out in Doc 9303, Parts 9, 10, 11 and 12. These test methodologies are specified in ICAO Technical Reports, being maintained under the coordination of ISO/IEC JTC 1/SC 17/WG 3.

Issuing States and organizations are RECOMMENDED to qualify their eMRTDs, inspection systems and PKI solutions according to the test specifications listed hereunder:

ISO/IEC 18745-2	Specific tests on the contactless interface for eMRTDs
ICAO TR RF & PROTOCOL P3	LDS and Protocol testing
ICAO TR RF & PROTOCOL P4	Tests for inspection systems
ICAO TR RF & PROTOCOL P5	Tests for PKI objects

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
ICAO TR RF & PROTOCOL P4	RF Protocol and Application Test Standard for eMRTD — Part 4: Conformity Test for Inspection Systems
ICAO TR RF & PROTOCOL P5	RF Protocol and Application Test Standard for eMRTD — Part 5: Tests for PKI objects
ISO/IEC 2382-37	Information Technology – Vocabulary – Part 37: Biometrics
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
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 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
ISO/IEC 39794-4	ISO/IEC 39794-4, Information technology — Extensible biometric data interchange formats — Part 4: Finger image data
ISO/IEC 39794-5	ISO/IEC 39794-5, Information technology — Extensible biometric data interchange formats — Part 5: Face image data
ISO/IEC 39794-6	ISO/IEC 39794-6, Information technology — Extensible biometric data interchange formats — Part 6: Iris image data

— — — — — — — —

Appendix A to Part 9

PROCESS FOR READING eMRTDS (INFORMATIVE)

A.1 PRECAUTIONS IN eMRTD MANUFACTURE

Issuing States or organizations 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 or organization read both the OCR data and the data stored on the IC. Where an issuing State or organization 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 or organizations shall therefore install reading equipment capable of handling MRPs of both geometries, preferably capable of reading both OCR and the IC. Figure A-1 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.

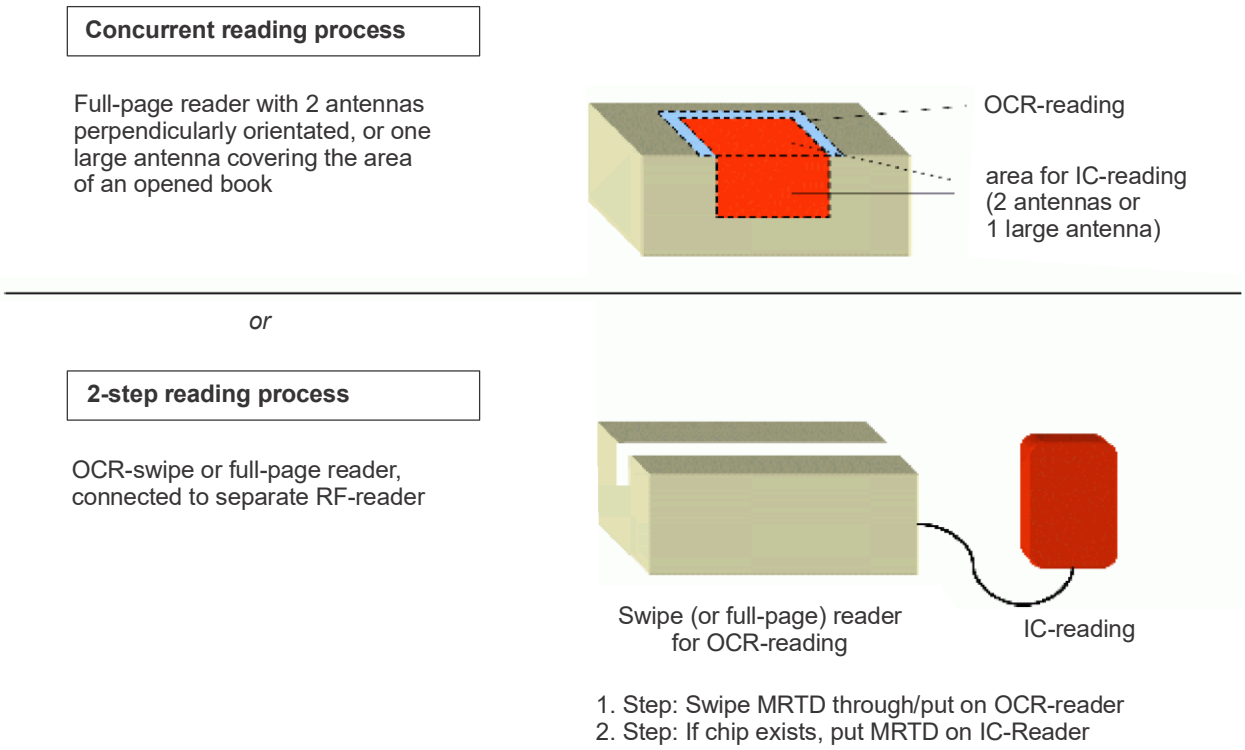

Figure A-1. Reading geometries

A.4 READING PROCESSES

Figure A-2 shows the processes involved in the reading of an eMRTD prior to and including the biometric verification of the holder.

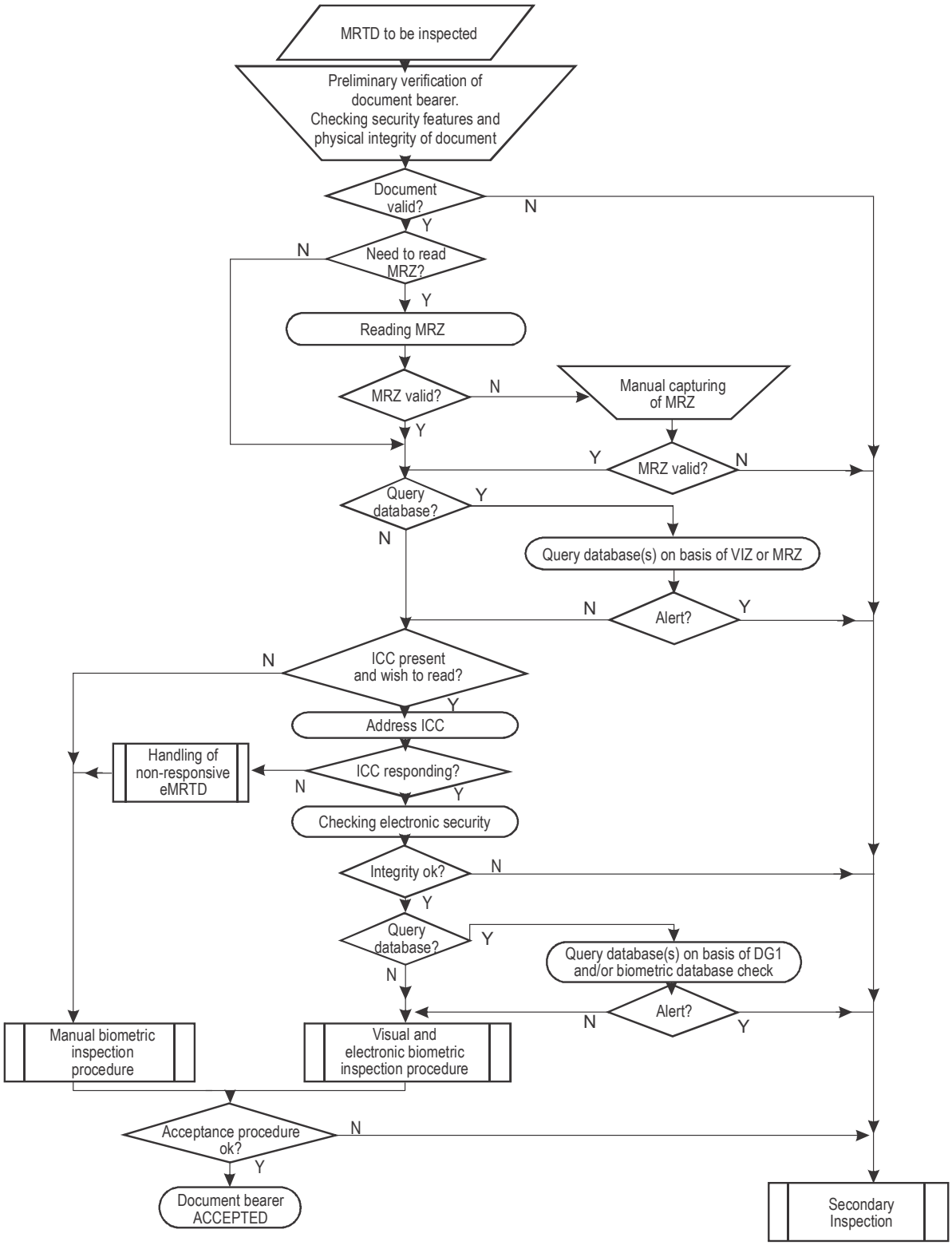

Figure A-2. eMRTD reading process

— END —

ISBN 978-92-9275-331-3