

Doc 9303



Machine Readable Travel Documents

Part 3 Machine Readable Official Travel Documents Volume 2 Specifications for Electronically Enabled MRtds with Biometric Identification Capability

Approved by the Secretary General
and published under his authority

Third Edition — 2008

International Civil Aviation Organization

AVA Documents
Document Sharing Hub

.....

Doc 9303



Machine Readable Travel Documents

Part 3 **Machine Readable Official Travel Documents** **Volume 2** **Specifications for Electronically Enabled MRtds** **with Biometric Identification Capability**

Approved by the Secretary General
and published under his authority

Third Edition — 2008

International Civil Aviation Organization



Documents
Document Sharing Hub

AMENDMENTS

Amendments are announced in the supplements to the *Catalogue of ICAO Publications*; 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

[illegible][illegible]

(iii)

Downloaded from https://www.icao.int/publications/9303 PART 3 V2 2008

TABLE OF CONTENTS

	<i>Page</i>
Acronyms and Definitions	(ix)
I. Introduction.....	I-1
1. Introduction to Volume 2	I-1
2. Definitions and terms	I-3
3. Supplement	I-3
4. Key words	I-4
5. References	I-5
II. The deployment of biometric identification and the electronic storage of data in machine readable official travel documents	I-1
1. Scope	II-1
2. eMRtd	II-1
3. Chip inside symbol	II-1
4. Biometric identification	II-3
5. Key considerations	II-3
6. Key processes with respect to biometrics	II-4
7. Applications for a biometrics solution	II-5
8. Constraints on biometrics solutions	II-6
9. ICAO vision on biometrics	II-6
10. The selection of biometrics applicable to eMRTDs	II-6
11. Optional additional biometrics	II-7
12. Image storage, compression and cropping	II-8
13. Storage of the biometric and other data in a logical format in a contactless IC	II-10
14. Manufacture of eMRtds and the reading of data	II-12
15. Process for reading eMRtds	II-12
16. Protection of the data stored in the contactless IC	II-12
III. A logical data structure for contactless integrated circuit data storage technology	III-1
1. Scope	III-1
2. References	III-1
3. Terminology, Terms and Definitions	III-1
4. The need for a Logical Data Structure	III-1
5. Requirements of the Logical Data Structure	III-1
6. Mandatory and optional Data Elements	III-2
7. Ordering and grouping of Data Elements	III-2
8. Data Groups coded to allow confirmation of authenticity and integrity of data	III-4
9. Data Groups recorded by the issuing State or organization	III-6
10. Data Elements forming Data Groups 1 through 16	III-7
11. Data Groups recorded by a receiving State or approved receiving organization	III-14
12. Format of Data Elements	III-14
13. Security principles	III-23
14. Mapping principles for contactless IC data expansion technology	III-23
15. Heading and Data Group presence information	III-24

Appendix 1 (Normative) to Section III. Mapping of LDS using random access representation to contactless integrated circuits (IC(s))	III-27
A1.1 Scope.....	III-27
A1.2 Random access file representation	III-27
A1.3 Security requirements	III-28
A1.4 Compatibility with existing international standards	III-28
A1.5 Physical characteristics	III-28
A1.6 Location and dimensions of coupling areas.....	III-28
A1.7 Electronic signals.....	III-28
A1.8 Transmission protocols and answer to request	III-28
A1.9 File structure	III-29
A1.10 Command set	III-31
A1.11 Issuer data application.....	III-31
A1.12 Receiving State application	III-42
A1.13 Tags used	III-42
A1.14 Minimum requirements for interoperability.....	III-46
A1.15 Commands and command parameters that may be used by the interface device	III-46
A1.16 Details on ISO/IEC 14443 Type A initialization and anticollision according to ISO/IEC 14443 Type A	III-47
A1.17 Details on ISO/IEC 7816: Command formats and parameter options	III-49
A1.18 EF selection using the SELECT command.....	III-49
A1.19 Reading data from the EF.....	III-49
A1.20 Examples for ISO/IEC 7816 usage with LDS	III-50
A1.21 EFs larger than 32 767 bytes.....	III-51
A1.22 ASN.1 BER length encoding rules.....	III-52
A1.23 Biometric sub-feature encoding	III-52
IV. PKI for machine readable travel documents offering ICC read only access.....	IV-1
1. Scope	IV-1
2. Assumptions.....	IV-1
3. Terminology	IV-2
4. Reference documentation	IV-3
5. General outline.....	IV-3
6. Securing electronic data in MRtds (Summary).....	IV-8
7. Specifications	IV-10
8. Algorithms	IV-14
9. Key Management	IV-16
10. Certificate and CRL distribution	IV-19
Appendix 1 (Normative) to Section IV. Certificate Profile.....	IV-22
A1.1 Certificate body.....	IV-22
A1.2 Extensions	IV-23
A1.3 SignatureAlgorithm	IV-24
A1.4 SignatureValue	IV-24
A1.5 SubjectPublicKeyInfo.....	IV-25
A1.6 Certificate and naming conventions.....	IV-25
Appendix 2 (Normative) to Section IV. CRL Profile.....	IV-26

Appendix 3 (Normative) to Section IV. Document Security Object	IV-28
A3.1 Signed data type	IV-28
A3.2 ASN.1 Profile LDS security object	IV-29
Appendix 4 (Normative) to Section IV. Active Authentication Public Key Info	IV-31
A4.1 Active Authentication public key info	IV-31
A4.2 Active Authentication mechanism	IV-31
Appendix 5 (Normative) to Section IV. Basic Access Control and Secure Messaging	IV-33
A5.1 Key derivation mechanism	IV-33
A5.2 Authentication and key establishment	IV-34
A5.3 Secure messaging	IV-34
A5.4 DES modes of operation	IV-38
Appendix 6 (Informative) to Section IV. Worked Examples	IV-41
A6.1 Command sequences	IV-41
A6.2 Lifetimes	IV-51
Appendix 7 (Informative) to Section IV. PKI and Security Threats	IV-53
A7.1 Key management	IV-53
A7.2 Cloning threats	IV-54
A7.3 Privacy threats	IV-54
A7.4 Cryptographic threats	IV-55
Appendix 8 (Informative) to Section IV. C_{csc}a Distribution Mechanism	IV-57



ACRONYMS AND DEFINITIONS

The following acronyms and terms are used in this volume of Doc 9303, Part 3. The lists are additional to those in Volume 1.

Acronym	Full form
AID	Application Identifier
APDU	Application Protocol Data Unit
CA	Certification authority
CID	Card Identifier
CRL	Certificate Revocation List
DES	Data encryption standard
DO	Data object
DSA	Digital signature algorithm
EAL	Evaluation assurance level
EEPROM	Electrically erasable programmable read only memory. A non-volatile memory technology where data can be electrically erased and rewritten.
eMRTD	An MRTD (passport, visa or card) that has a contactless IC imbedded 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 ICAO Doc 9303.
eMRtd	A Machine Readable Official Travel Document that has a contactless IC imbedded in it and the capability of being used for biometric identification of the MRtd holder in accordance with the standards specified in this volume of ICAO Doc 9303, Part 3.
FRR	False rejection rate
IC	Integrated circuit
ICC	Integrated circuit card
IFD	Interface device
JPEG	A Standard for the data compression of images, used particularly in the storage of facial images.
JPEG 2000	An updated version of the JPEG standard
LDS	Logical data structure
MAC	Message authentication code
MRTD	Machine Readable Travel Document conforming to ICAO Doc 9303, Part 1, 2 or 3
MRZ	Machine Readable Zone
NAD	Node Address
NIST	National Institute of Standards and Technology

Acronym	Full form
NTWG	New Technologies Working Group
OCR	Optical character recognition
PCD	Proximity coupling device
PICC	Proximity Integrated Circuit Card
PID	Creator of Biometric Reference Data
PKD	Public key directory
PKI	Public key infrastructure
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.
SHA	Secure Hash Algorithm
SM	Secure Messaging
TAG	Technical Advisory Group
UID	Unique IDentifier
WSQ	Wavelet Scalar Quantization
X.509v3	ITU-T digital 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.

Term	Definition
Algorithm	A specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result.
Application Identifier (AID)	Data element that is used to uniquely identify an application in a card. It consists of a relative identifier (RID) and a proprietary identifier extension (PIX).
Application Protocol Date Unit (APDU)	Standard communication messaging protocol between a card acceptance device and a smart card.
Asymmetric	Different keys needed on each end of a communication link.
Asymmetric algorithm	This type of cryptographic operation uses one key for encryption of plain text and another key for decryption of associated cipher text. These two keys are related to each other and are called a Key Pair.
Asymmetric keys	A separate but integrated user key pair comprised of one public key and one private key. Each key is one-way, meaning that a key used to encrypt information cannot be used to decrypt the same information.
Authentication	A process that validates the claimed identity of a participant in an electronic transaction.

Term	Definition
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	Unique raw data representing a unique biometric characteristic of an enrollee as captured by a biometric system.
Biometric system	An automated system capable of: 1. capturing a biometric sample from the holder of an MRTD; 2. extracting biometric data from the biometric sample; 3. comparing that specific biometric data with that contained in one or more references; 4. deciding how well two sources of data match; 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.
Bit	A binary digit. The smallest possible unit of information in a digital code.
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.
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.
Capture	The method of taking a biometric sample from the holder.
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.
Cipher	Secret writing based on a key, or set of predetermined rules or symbols.
Contactless Integrated Circuit	An electronic microchip coupled to an aerial (antenna) which allows data to be communicated between the chip and an encoding/reading device without the need for a direct electrical connection.
Cryptography	Science of transforming information into an enciphered, unintelligible form using an algorithm and a key.

Term	Definition
Data Encryption Standard (DES)	A method of data encryption using a specific algorithm.
Data storage	A means of storing data on a document such as an MRTD. Volume 2 of ICAO Doc 9303, Part 1 and 3 specifies that the data storage on an eMRTD will be on a Contactless Integrated Circuit.
Database	Storage of biometric templates and related end user information in an electronic format.
Decryption	The act of restoring an encrypted file to its original state through the use of a key.
Digital Signature Algorithm (DSA)	Asymmetric algorithm published by the NIST as a federal information processing standard (FIPS) in 1991 and revised in 1993. This algorithm only provides digital signature function.
Digital Signature Scheme (DSS)	A standard for digital signing, including the DSA, approved by the NIST, defined in NIST FIPS PUB 186, published May 1994 by the US Department of Commerce.
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 signer	A body which issues a biometric document and certifies that the data stored on the document is genuine in a way which will enable detection of fraudulent alteration.
Eavesdropping	The unauthorized interception of data communication.
End user	A person who interacts with a biometric system to enrol or have his identity checked.
Enrollee	A person applying for an eMRTD.
Enrollment	The process of collecting biometric samples from an enrollee and the subsequent preparation and storage of biometric reference templates representing that person's identity.
Evaluation Assurance Level (EAL)	An assurance requirement as defined by Common Criteria, an international standard in effect since 1999. The increasing assurance levels define increasing assurance requirements in computer systems.
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 from an end user to enrol in the system.
Failure to enrol	The failure of a biometric system to enrol a potential end user.
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.

Term	Definition
False Match Rate	Alternative to “False Acceptance Rate”. Used to avoid confusion in applications that reject the claimant if his biometric data match that of an enrollee.
False Non-Match Rate	Alternative to “False Rejection Rate”. Used to avoid confusion in applications that reject the claimant if his biometric data match that 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.
Full frontal (facial) image	A portrait of a holder of the MRTD produced in accordance with the specifications established in ICAO Doc 9303, Part 3, Volume 1, Section IV.
Gallery	The database of biometric templates of persons previously enrolled, which may be searched to find a Probe.
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.
Hash	A mathematical formula that converts a message of any length into a unique fixed-length string of digits (typically 160 bits) 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.
Holder	A person possessing an eMRTD, submitting a biometric sample for verification or identification whilst claiming a legitimate or false identity. A person who interacts with a biometric system to enrol or have his identity checked.
IC module	The sub-assembly embedded into the ICC comprising the IC, the IC carrier and contacts. Integrated circuits serial number: A number common to all IC in a lot, corresponding to a particular place in the mask (used in the manufacturing process).
Identification/Identify	The 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. Contrast with “Verification”.
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 a birth certificate and citizenship certificate.
Image	A representation of a biometric as typically captured via video, camera or scanning device.

Term	Definition
Impostor	A person who submits a biometric sample in either an intentional or inadvertent attempt to pass for someone else.
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 examining an eMRTD presented to it by a traveller (the eMRTD holder) and verifying its authenticity.
Inspection system	A system used for inspecting (e)MRTDs by any public or private entity having the need to validate the (e)MRTD, and using this document for identity verification, e.g. border control authorities, airlines and other transport operators, financial institutions.
Integrated circuit(s) card (IC card, ICC)	A card into which been inserted one or more ICs.
Interface	A standardized technical definition of the connection between two components.
Interface device	Any terminal, communication device or machine to which the IC card is electrically connected during operation.
Key	See Public Key Cryptography.
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.
Live capture	The process of capturing a biometric sample by an interaction between an eMRTD holder and a biometric system.
Logical Data Structure (LDS)	Describes how data are to be written to and formatted in the contactless IC from eMRTD.
Machine Readable Travel Document (MRTD)	Travel document conforming to ICAO Doc 9303, Part 1, 2 or 3.
Master key	Root of the derivation chain for keys.
Match/Matching	The process of comparing a biometric sample against a previously stored template and scoring the level of similarity.
Matching ¹	The process of comparing a biometric sample against a previously stored template (i.e. biometric reference template) and scoring the level of similarity. An accept or reject decision is then based upon whether this score exceeds the given threshold.

1. This definition is only applicable in a biometric system context.

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.
Multiple biometric	The use of more than one biometric.
Nonce	In security engineering, a nonce is a “number used once”. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in “replay attacks”. For instance, nonces are used in HTTP digest access authentication to calculate an MD5 digest of the password. The nonces are different each time the 401 authentication challenge response code is presented, thus making the replay attack virtually impossible (Source: wikipedia.org).
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.
Padding	Appending extra bits to either side of a data string up to a predefined length.
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.
PI data	Information related to a cardholder and used by a PI system.
PI retry count	The number of consecutive unsuccessful PI data inputs by the cardholder.
PI system	A technique used to confirm the identity of a cardholder.
Private Key	A cryptographic key known only to the user, employed in public key cryptography in decrypting or signing information.
Public key	The public component of an integrated asymmetric key pair, used in encrypting or verifying information.

Term	Definition
Public key certificate	The public key information of an entity signed by the certification authority and thereby rendered unforgeable.
Public key cryptography	A form of asymmetric encryption where all parties possess a pair of keys, one private and one public, for use in encryption and digital signing of data.
Public Key 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 secret and one is public. If encipherment is done using the public key, decipherment requires application of the corresponding secret key and vice versa.
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.
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 distance.
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 (of a person)	Obtaining sufficient proof of the identity of the intended card holder by traditional means, possibly including attributes (e.g. as required for a specific eService). Registration is to a defined level of proof of identity.
Registration Authority	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.
Response	A message returned by the slave to the master after the processing of a command received by the slave.
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 developed by the NIST and published as a federal information processing standard in 1993.
Secured message	A message that is protected against illegal alteration or origination.
SHA	See secure hash algorithm.
SHA-1	1994 revision to SHA which is considered more secure.

Term	Definition
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.
System	A specific IT installation, with a particular purpose and operational environment.
System integration	The process by which cardholder-facing, internal and partner-facing systems and applications are integrated with each other.
System security policy	The set of law, rules and practices that regulate how sensitive information and other resources are managed, protected and distributed within a specific system.
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.
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.
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. (See paragraph 12 of Section II in this volume.)
Validation	The process of demonstrating that the system under consideration meets in all respects the specification of that system.
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”.
Wavelet Scalar Quantization	A means of compressing data used particularly in relation to the storage of fingerprint images.



SECTION I

INTRODUCTION

1. INTRODUCTION TO VOLUME 2

1.1 The third edition of Doc 9303, Part 3 is composed of two volumes. Volume 1 defines the specification for a basic machine readable official travel document (MRtd), the machine readable data being presented in the form of optical character recognition (OCR). All States issuing machine readable official travel documents (MRtds) shall produce these in accordance with the specifications given in Volume 1.

1.2 The amount of data that can be stored in the OCR format of a Machine Readable Travel Document (MRTD) is limited. States require the storage in the document of more data relating both to the document holder and to the validity of the document. The principal reason for the need for more data is to permit the biometric identification of the document holder, this to strengthen defence against illegal immigration and terrorism. States have begun to offer greater facilitation at immigration if a person's travel documents contain biometric identification conforming to ICAO's specifications on the matter.

1.3 Volume 1 of the third edition of Doc 9303, Part 3, updates the specifications for machine readable official travel documents as published in the second edition (2002). These updates have arisen primarily as a result of the decision to enable global interoperability through standardization based on a specific combination of a single high-capacity data storage technology and a system of biometric identification. This has meant some changes in Volume 1, particularly in a tighter specification for the portrait of the holder so that, even if a State is not initially utilizing the new technologies, a database will be established that will be of value when the State does upgrade. Also a number of biometric and data storage technologies were described in the second edition which do not conform to the new globally interoperable standard. A State is, of course, free to continue to use these technologies for its own or agreed bilateral purposes but they will not be globally interoperable. The specifications for the new globally interoperable system contained in this Volume 2 are only for use by States wishing to issue an MRtd that is electronically and biometrically enabled. Such States need to observe the specifications in *both* volumes to conform to the standards laid down in Doc 9303, Part 3.

1.4 The specifications contained herein were drawn up following a detailed study over several years, begun in 1998, by the New Technologies Working Group (NTWG) of ICAO's Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD). The study examined different biometric identification systems concentrating on their relevance to the facilitation for a traveller in applying for and obtaining a biometrically enabled MRTD and in using that document for travel between States. The privacy laws applied by States around the world and the requirement for the biometric to be acceptable to the MRTD holder strongly favoured the use of the holder's face as the globally interoperable biometric, as the face, in the form of a photograph, is universally accepted as a means of identification in a travel document. Facial recognition requires the recording of the relationships of a number of dimensions between features of the face, e.g. the distance between the eyes. This is followed by comparing the relationships between data on the person to whom the MRTD was issued, recorded at the time of issue, and the person presenting himself¹ to travel or to enter a State. The relationships may be mathematically reduced to a "template" requiring a relatively small amount of data storage capacity. Unfortunately the templates used by the various competing manufacturers of

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

facial recognition systems are not compatible. To allow States the freedom to choose the facial recognition system they prefer, the NTWG decided that a relatively high resolution portrait of the person to whom the MRTD was issued should be stored. Though facial recognition is the primary globally interoperable biometric, the NTWG recognized that some States would wish to use more than one biometric. Many States have extensive fingerprint databases which they might wish to refer to in order to verify the identity of a traveller. As a second alternative, iris recognition is gaining acceptance as a reliable method of identification. Though technically commendable, fingerprint and iris recognition involve a rather more invasive and time-consuming collection of the biometric data both at original enrollment for an MRTD and at a port of entry. The NTWG therefore decided that it would recommend that fingerprint and iris recognition data should be optional secondary means of biometric identification. Again the storage of images is specified to enable a State to choose the supplier of its fingerprint or iris recognition system, as templates are not compatible between manufacturers.

1.5 The freedom to choose the facial recognition system and, optionally, systems for fingerprint and iris comes at the expense of the data storage capacity required. Several data storage technologies that had been considered in the past were eliminated by the high data capacity required. Though there were still several options, the NTWG decided that, to establish a globally interoperable system, Doc 9303 must specify a single data storage technology. After careful examination, the NTWG decided to select a contactless integrated circuit (IC), conforming to ISO/IEC 14443. This technology involves communication between the IC module (the IC attached to an antenna) contained within the MRTD and a reader situated within a distance of 10 cm (3.9 in). The technology offers the following advantages:

- The technology has been proven in other fields.
- There are a significant number of manufacturers of suitable ICs of various data capacities, and integrators who can construct the IC module.
- The use of ISO/IEC 14443 technology does not demand accuracy of positioning of the MRTD on the reader, but the close read distance means there is little risk of unauthorized reading of the data stored on the IC, provided suitable electromagnetic screening is used in the reader and associated communications.

1.6 The data storage capacity of the IC is specified to be a minimum of 32 kB (kilobytes), which is large enough to store the mandatory facial image and, also mandatory, a duplication of the MRZ data. However, the optional storage of more than one facial image and/or fingerprint/iris images requires considerably larger data capacity.

1.7 ISO/IEC 14443 specifies two alternative types of contactless IC: A and B. The specifications in this volume allow either type to be used, necessitating the use of a reader at the port of entry capable of operating with an IC of either type.

1.8 For the system to be globally interoperable, it is important that the data is stored in a standard format. The NTWG therefore developed a Logical Data Structure (LDS) which specifies the way in which a wide range of data may be stored in standardized groups. In preparing the LDS, the NTWG tried to ensure that a State could store not only biometric data but also any data it wished relating to the holder or to the validity of the MRTD, consistent only with the data storage capacity of the IC selected. Optional provision is therefore made for the storage of one or more facial recognition templates in addition to more than one facial image and images and templates of the holder's fingerprints and/or iris. The storage of data, such as the holder's name in a language using other than Latin characters, is permitted as is the use of diacritical marks. However, the only mandatory data to be stored on the IC are a duplication of the MRZ data in Data Group 1 *and* one facial image in Data Group 2 together with a digital signature to ensure that the data are as written by the issuing State at the time of issue of the document.

1.9 It is intended that, in the future, there will be provision for States, other than the issuing State, to write data to the IC such as electronic visa information. This is not yet, however, permitted.

1.10 The security of the data on the IC is of paramount importance. A receiving State must be confident that the data it reads from the IC have not been altered in any way since they were encoded by the State that issued the MRTD. In addition, some of the data may need to be secured against unauthorized access, either because the data could be used fraudulently or because the privacy laws of many States prohibit unauthorized access to some forms of personal data. Accordingly, a special task force, established by the NTWG, has developed appropriate levels of security and privacy to be met through the use of digital signatures.

1.11 In 2003 the TAG/MRTD formally presented to ICAO a four-part recommendation. The facial image as a high resolution portrait image stored on a contactless IC, conforming to ISO/IEC 14443, types A or B, should be the global biometric standard. Fingerprint and iris, both stored as images, are also supported as secondary biometrics. The biometrics, a duplication of the MRZ data, and a wide range of other data options should be stored in the IC in accordance with the Logical Data Structure and the requirements for security and privacy. This recommendation was accepted and endorsed as the ICAO blueprint.

1.12 This volume formalizes that decision, providing detailed specifications set out in the sections that follow. Section II, *Biometric Deployment*, defines the method of capture and use of the biometric data, and the requirements of the contactless IC used to store the data. Section III, *The Logical Data Structure*, defines how the data are to be stored on the IC, and Section IV, *The Public/Private Key Infrastructure*, defines the system and procedures to be used for securing the data on the IC and ensuring that access to the data is appropriately restricted.

1.13 ICAO acknowledges the assistance provided by ISO in the development of this highly specialized standard. Volume 2 has been submitted to ISO for that organization's endorsement as an International Standard.

1.14 It is recognized that the specifications contained herein require a high level of technical expertise on the part of those employees of States, and their contractors, who may be involved in the work of creating the eMRtd and the systems for capturing, encoding and reading the stored data and in its use in biometric verification and identification. Therefore, the TAG/MRTD has established a network of various experts employed by States that have already implemented such systems. These experts may be approached for advice, through ICAO's Aviation Security and Facilitation Policy Section at sfp@icao.int.

2. DEFINITIONS AND TERMS

A glossary of terms and their definitions is given at the beginning of this volume. Additional terms and definitions applicable to all MRTDs may be found in Volume 1.

3. SUPPLEMENT

ICAO will issue from time-to-time a "Supplement to Doc 9303", to this standard Doc 9303. The supplement will contain information intended to clarify, amplify or elaborate on issues with respect to travel document standards and will correct errors encountered during 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-line 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/mrtd>.

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

4. KEY WORDS

Key words are used to signify the requirements in Volume 2.

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” used in capitalized form in this volume 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).

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

Security considerations. These terms are frequently used to specify behaviour with security implications. The effects on security of not implementing a MUST or SHOULD, or doing something the specification says MUST NOT or SHOULD NOT be done, may be very subtle. Document authors should take the time to elaborate the

security implications of not following recommendations or requirements as most implementors will not have had the benefit of the experience and discussion that produced the specification.

In case OPTIONAL features are implemented, they MUST be implemented as described in this volume.

5. REFERENCES

Certain provisions of the following international Standards, referenced in this text, constitute provisions of this volume. Where differences exist between the emerging specifications contained in this volume and the referenced Standards, to accommodate specific construction requirements for machine readable travel documents, the specifications contained herein SHALL prevail.

FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB) 180-2, Secure Hash Standard (SHS), August 2002.

FIPS 186-2, Federal Information Processing Standards Publication (FIPS PUB) 186-2 (+ Change Notice), Digital Signature Standard (DSS), 27 January 2000. (Supersedes FIPS PUB 186-1 dated 15 December 1998.)

Doc 9303, Machine Readable Travel Documents, Part 1, Machine Readable Passports (6th Edition, 2006).

ISO 3166-1: 2006, Codes for the representation of names of countries and their subdivisions — Part 1: Country codes.

ISO 3166-2: 2007, Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code.

ISO/IEC 7816-4: 2005, Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange.

ISO/IEC 7816-5: 2004, Identification cards — Integrated circuit cards — Part 5: Registration of application providers.

ISO/IEC 7816-6: 2004, Identification cards — Integrated circuit cards— Part 6: Interindustry data elements for interchange (Defect report included).

ISO/IEC 7816-11: 2004, Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods.

ISO/IEC 8825-1:2003, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

ISO/IEC 9796-2: 2002, Information Technology — Security Techniques — Digital Signature Schemes giving message recovery — Part 2: Integer factorization based mechanisms.

ISO/IEC 9797-1:1999, Information technology —Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher.

ISO/IEC 10373-6:2001, Identification cards —Test methods — Part 6: Proximity cards.

ISO/IEC 10373-6:2001/Amd1:2007, Test methods for proximity cards (Amendment 1: Protocol test methods for proximity cards).

ISO/IEC 10373-6:2001/Amd2:2003, Test methods for proximity cards (Amendment 2: Improved RF test methods).

ISO/IEC 10373-6:2001/Amd4:2006, Test methods for proximity cards (Amendment 4: Additional test methods for PCD RF interface and PICC alternating field exposure).

ISO/IEC 10373-6:2001/Amd5, Test methods for proximity cards (Amendment 5: Bit rates of fc/64/, fc/32 and fc/16).

ISO/IEC 10646:2003, Information technology — Universal Multiple-Octet Coded Character Set (UCS).

ISO/IEC 10918, Information technology — Digital compression and coding of continuous-tone still images.

ISO 11568-2:2005, Banking — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle.

ISO/IEC 11770-2:1996, Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques.

ISO/IEC 14443-1:2000, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1: Physical Characteristics.

ISO/IEC 14443-2:2001, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio Frequency Power and Signal Interface.

ISO/IEC 14443-2:2001/AM1:2005, Proximity cards: Radio Frequency Power and Signal Interface (Amendment 1: Bit Rates of fc/64, fc/32 and fc/16).

ISO/IEC 14443-3:2001, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and Anticollision.

ISO/IEC 14443-3:2001/AM1:2005, Proximity cards: Initialization and Anticollision (Amendment 1: Bit Rates of fc/64, fc/32 and fc/16).

ISO/IEC 14443-4:2001, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol.

ISO/IEC15444, Information technology — JPEG 2000 Image coding system.

ISO/IEC 15946: 2002, Information technology — Security techniques — Cryptographic techniques based on elliptic curves.

ISO/IEC 19794-4:2005, Information technology — Biometric data interchange formats — Part 4: Finger image data.

ISO/IEC 19794-5:2005, Information technology — Biometric data interchange formats — Part 5: Facial image data.

ISO/IEC 19794-6:2005, Information technology — Biometric data interchange formats — Part 6: Iris image data.

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

RFC 3279, W. Polk, R. Housley, L. Bassham, “Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, April 2002.

RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, April 2002.

RFC 3369, R. Housley, Cryptographic Message Syntax (CMS), August 2002.

RFC 3447, J. Jonsson, B. Kaliski, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1”, February 2003.

Unicode 4.0.0, The Unicode Consortium. The Unicode Standard, Version 4.0.0, defined by: *The Unicode Standard, Version 4.0* (Boston, MA, Addison-Wesley, 2003. ISBN 0-321-18578-1) (Consistent with ISO/IEC 10646-1, but containing additional characters).

ANSI X9.62:2005, “Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)”, 7 January 1999.

Copyright International Civil Aviation Organization
Provided by IHS under license with ICAO
No reproduction or networking permitted without license from IHS

Downloaded from https://www.icao.int/publications/9303PART3V22008/

SECTION II

THE DEPLOYMENT OF BIOMETRIC IDENTIFICATION AND THE ELECTRONIC STORAGE OF DATA IN MACHINE READABLE OFFICIAL TRAVEL DOCUMENTS

1. SCOPE

Section II defines the specifications, additional to those for the basic td1 and td2 set forth in Volume 1 of Doc 9303, Part 3, to be used by States wishing to issue an electronically enabled machine readable official 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 MRtd 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 on a high-capacity contactless integrated circuit (IC), the IC also being encoded with a duplicate of the MRZ data. The specifications also permit the storage of a range of optional data at the discretion of the issuing State. Since the use of the contactless integrated circuit is independent of the size of the document, all specifications apply to both the td1 and td2 in their electronically enabled form. Differences between td1 and td2 format eMRtds relate to the MRZ, with consequences for the storage of the MRZ in the contactless IC. These differences are indicated in the specifications in this volume.

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 MRtd and eMRtd are used to refer only to the corresponding official travel documents. The terms td1 and td2 refer to the two sizes of MRtd. All MRtds referred to in this volume are electronically enabled.

2.1 *Conformance to Doc 9303, Part 3, Volume 1 specifications.* An electronically enabled MRtd (eMRtd) SHALL conform in all respects to the specifications provided in Volume 1 of Doc 9303, Part 3 as well as to those set forth in this volume.

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.

3. CHIP INSIDE SYMBOL

3.1 *Visual indication that an MRTD is an eMRtd:* All eMRtds SHALL carry the following symbol (Figure II-1):

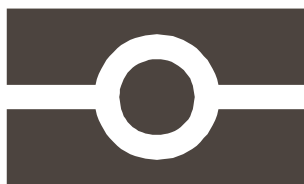


Figure II-1.

An electronic file of the symbol is available from the ICAO web site. The symbol SHALL only appear on an MRtd 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 (Section III of this volume) with, as a minimum, the MRZ data in Data Group 1 and a facial image as specified in this Section in Data Group 2, with all entered data secured with a digital signature as specified in Section IV of this volume. Unless an MRtd conforms to these minimum requirements, it SHALL NOT be described as an eMRtd nor display the eMRtd symbol. The symbol SHALL appear on the front of the eMRtd preferably in Zone 1. The image, as shown above, is a positive, i.e. the black part of the image shall be printed or otherwise imaged. It is RECOMMENDED that the symbol appear eye-visible and be easily recognizable.

3.2 Figure II-2 shows the RECOMMENDED dimensions of the symbol as it is to appear on an electronically enabled td2. The following are the corresponding dimensions in inches: 9.0 mm (0.35 in), 5.25 mm (0.21 in), 3.75 mm (0.15 in), 2.25 mm (0.09 in), 0.75 mm (0.03 in).

3.3 A smaller size of 4.2 × 7.2 mm (0.17 × 0.28 in), scaled in proportion, is RECOMMENDED for use on an electronically enabled td1.

3.4 The symbol MAY be scaled in proportion for use in, for example, background designs.

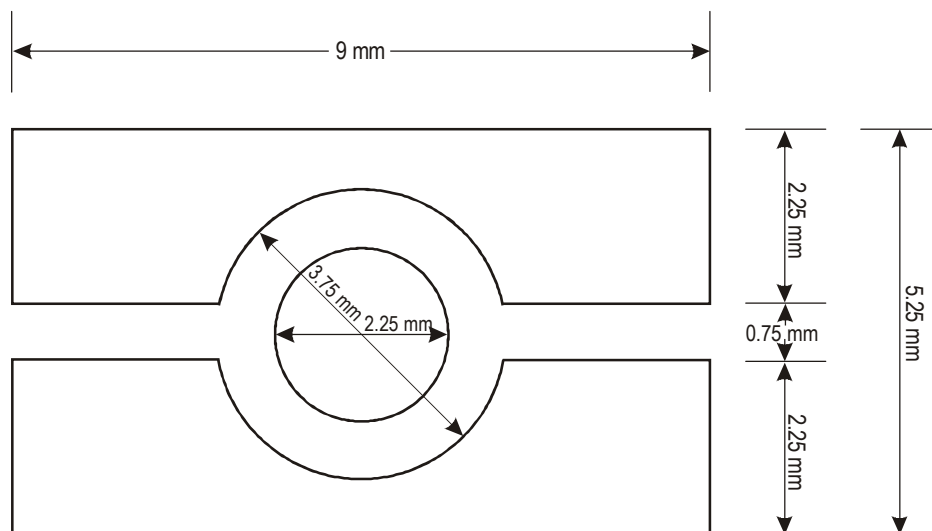


Figure II-2.

4. BIOMETRIC IDENTIFICATION

4.1 “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.

4.2 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.

4.3 Doc 9303 considers only three types of biometric identification systems. These are the physiological ones of:

- facial recognition (mandatory)
- fingerprint recognition (optional)
- iris recognition (optional)

An international standard, ISO/IEC 19794 composed of several parts, provides specifications for these types of biometric identification. Issuing States SHALL conform to these specifications.

4.4 *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.

4.5 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.

5. KEY CONSIDERATIONS

In specifying biometric applications for MRtds, 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 maximum 10-year life of a travel document, and that future updates will be backward compatible.

6. KEY PROCESSES WITH RESPECT TO BIOMETRICS

6.1 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.

6.2 These processes involve:

- The *enrollment* process is the *capture* of a raw biometric sample. It is used for each new person (potential MRtd 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.

7. APPLICATIONS FOR A BIOMETRICS SOLUTION

7.1 The key application of a biometrics solution is the identity verification of relating an MRtd holder to the MRtd he is carrying.

7.2 There are several typical applications for biometrics during the enrollment process of applying for an MRtd.

7.2.1 The end user's biometric data generated by the enrollment 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 MRtd under a different identity, having a criminal record, holding an MRtd from another State).

7.2.2 When the end user collects the MRtd (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.

7.2.3 The identities of the staff undertaking the enrollment 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.

7.3 There are also several typical applications for biometrics at the border.

7.3.1 Each time a traveller (i.e. MRtd 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.

7.3.2 *Two-way check* — The traveller's current captured biometric image data, and the biometric template from his travel document (or from a central database), can be matched to confirm that the travel document has not been altered.

7.3.3 *Three-way check* — The traveller's current biometric image data, the image from his travel document, and the image stored in a central database can be matched (by constructing biometric templates of each) to confirm that the travel document has not been altered. This technique matches the person and his MRtd with the database recording the data that were put in that MRtd at the time it was issued.

7.3.4 *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 MRtd.

7.4 Besides the enrollment 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 one or more facial, fingerprint or iris biometrics on the MRtd 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.

8. CONSTRAINTS ON BIOMETRICS SOLUTIONS

8.1 It is recognized that implementation of most biometrics technologies are subject to further development. Given the rapidity of technological change, any specifications (including those herein) must allow for, and recognize there will be, changes resulting from technology improvements.

8.2 The biometrics information stored on travel documents shall comply with any national data protection laws or privacy laws of the issuing State.

9. 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 the maximum ten-year validity as specified in Doc 9303;
- having no proprietary element thus ensuring that any States investing in biometrics are protected against changing infrastructure or changing suppliers.

10. THE SELECTION OF BIOMETRICS APPLICABLE TO eMRTDs

10.1 It has long been recognized that name and reputation are not sufficient traits to guarantee that the holder assigned a travel document (MRTD) by the issuing State is the person at a receiving State purporting to be that same holder.

10.2 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.

10.3 After a five-year investigation into the operational needs for a biometric identifier which combines suitability for use in the MRTD 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.

10.4 In reaching this conclusion, ICAO observed that for the majority of States the following advantages applied to facial images:

10.4.1 Facial photographs do not disclose information that the person does not routinely disclose to the general public.

10.4.2 The photograph (facial image) is already socially and culturally accepted internationally.

10.4.3 The facial image is already collected and verified routinely as part of the MRTD application form process in order to produce an MRTD to Doc 9303 standards.

10.4.4 The public is already aware of the capture of a facial image and its use for identity verification purposes.

10.4.5 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.

10.4.6 Facial image capture does not require new and costly enrollment procedures to be introduced.

10.4.7 Capture of a facial image can be deployed relatively immediately, and the opportunity to capture facial images retrospectively is also available.

10.4.8 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.

10.4.9 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.

10.4.10 For watch lists, a photograph of the face is generally the only biometric available for comparison.

10.4.11 Human verification of the biometric against the photograph/person is relatively simple and a familiar process for border control authorities.

10.5 *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 MRtd holder with the facial image read from the data storage technology in their MRtd.

11. OPTIONAL ADDITIONAL BIOMETRICS

11.1 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.

11.2 *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.

11.3 *Storage of an optional iris biometric.* Iris biometrics are complicated by the dearth of proven vendors. A de facto standard for iris biometrics has therefore emerged based on the methodology of the one recognized vendor. Other vendors may in future provide iris technology, but it is likely they will need the image of the iris as their starting point, rather than the template created by the current vendor. 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.

12. IMAGE STORAGE, COMPRESSION AND CROPPING

12.1 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.

12.2 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.

12.3 *Facial image data size.* An ICAO-standard 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.

12.4 Studies undertaken using standard photograph images but with different vendor algorithms and JPEG and/or JPEG2000 compression showed the *minimum* practical image size for an ICAO-standard MRTD photo image to be approximately 12 kB of data. The studies showed higher compression beyond this size results in significantly less reliable facial recognition results. Twelve kilobytes cannot always be achieved as some images compress more than others at the same compression ratio — depending on factors such as clothes, colouring and hair style. In practice, facial image average compressed sizes in the 15 kB – 20 kB range should be the optimum for use in eMRtds.

12.4.1 *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 MRtd, is diminished significantly.

For example, in Figure II-3 the image to the left provides a greater challenge in recognition than that on the right.



Figure II-3.

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 MRtd;
- cropped from chin to crown and edge-to-edge as a minimum, as shown in Figure II-4.



Figure II-4.

12.4.2 To assist in the facial recognition process, the facial image SHALL be stored either as a full frontal image or as a token image in accordance with the specifications established in ISO/IEC 19794-5, Information technology — Biometric data interchange formats — Part 5: Facial image data. A token image is a facial image in which the image is rotated if necessary to ensure that an imaginary horizontal line drawn between the centres of the eyes is parallel to the top edge of the picture and the size adjusted. It is RECOMMENDED that the centres of the eyes be approximately 90 pixels apart as in Figure II-5.

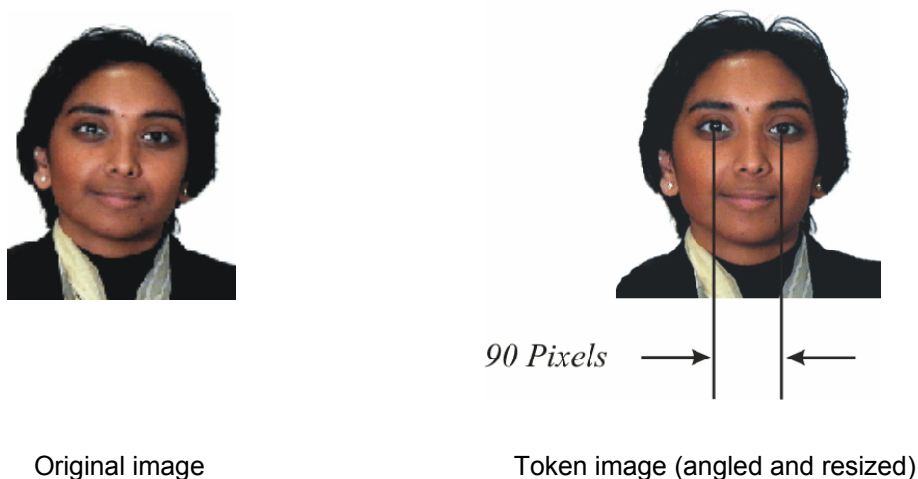


Figure II-5.

The Logical Data Structure (see Section III) can accommodate the storage of the eye coordinates.

12.4.3 *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.

12.5 *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).

12.6 *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.

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

13.1 It is REQUIRED that digital images be used and that these be electronically stored in the travel document.

13.2 These images are to be standardized.

13.3 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.

13.3.1 *Data storage capacity of the contactless IC.* The data storage capacity of the contactless IC is at the discretion of the issuing State but SHALL be a minimum of 32 kB. This minimum capacity is necessary to store the mandatory stored facial image (typically 15 — 20 kB), the duplicate MRZ data and the necessary elements for securing the data. The storage of additional facial, fingerprint and/or iris images may require a significant increase in data storage capacity. There is no maximum contactless IC data capacity specified.

13.4 *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 MRtd 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.

13.5 *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. The LDS is specified in detail in Section III of this volume.

13.6 *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 Section IV 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 MRtds 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 Section IV permit the issuing State to protect the stored data from unauthorized access by the use of Access Control.

13.7 The present specifications state that the writing of data to the IC SHALL take place only at the time of issue of the MRtd.

13.8 *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 incompatible to the total framework.

13.8.1 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.

13.8.2 The PKI specifications are described in detail in Section IV of this volume.

13.9 *PKI and LDS.* The sections on the LDS and the PKI specify how data integrity and data privacy are to be achieved in the context of biometrics deployment in MRtds.

13.10 *Contactless IC and encoding.* The contactless ICs used in MRtds 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.

13.11 *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 Section III). The Security Object (EF.SOD) consists of the hashes of the Data Groups in use. Refer to Section IV for detailed information.

13.12 *Structure of the stored data.* The Logical Data Structure specified in Section III describes in detail the mandatory and optional information to be included within specific biometric data blocks within the LDS.

14. MANUFACTURE OF eMRtds AND THE READING OF DATA

14.1 *Manufacture of eMRtds.* The manufacturing techniques normally used for the manufacture of plastic cards containing contactless ICs are appropriate for the production of eMRtds. However, to achieve the typical 5-to 10-year life of an MRtd requires the careful selection of the materials used in its construction.

14.2 *Reading both the OCR and the data on the contactless IC.* It is RECOMMENDED that a receiving State read both the OCR data printed on the MRtd and the data stored on the contactless IC. Where a State has locked the contactless IC against unauthorized reading, the reading of the OCR is required in order to access the data on the contactless IC. For reasons of facilitation, it is desirable that only one reader be used for both operations, the reader being equipped to read both, ideally in a single operation. Because most reading operations will be carried out in locations that are required to read both MRPs and MRtds, States should seek to acquire readers capable of reading both types of documents.

15. PROCESS FOR READING eMRtds

Figure II-6 shows the processes involved in the reading of an eMRtd prior to and including the biometric verification of the holder.

16. PROTECTION OF THE DATA STORED IN THE CONTACTLESS IC

The data stored on the contactless IC needs to be protected against alteration. This means that the data **MUST** be protected and authenticated by digital signature. Optionally, data can be encrypted. These concepts are explained in detail in Sections III, *LDS* and IV, *PKI*.



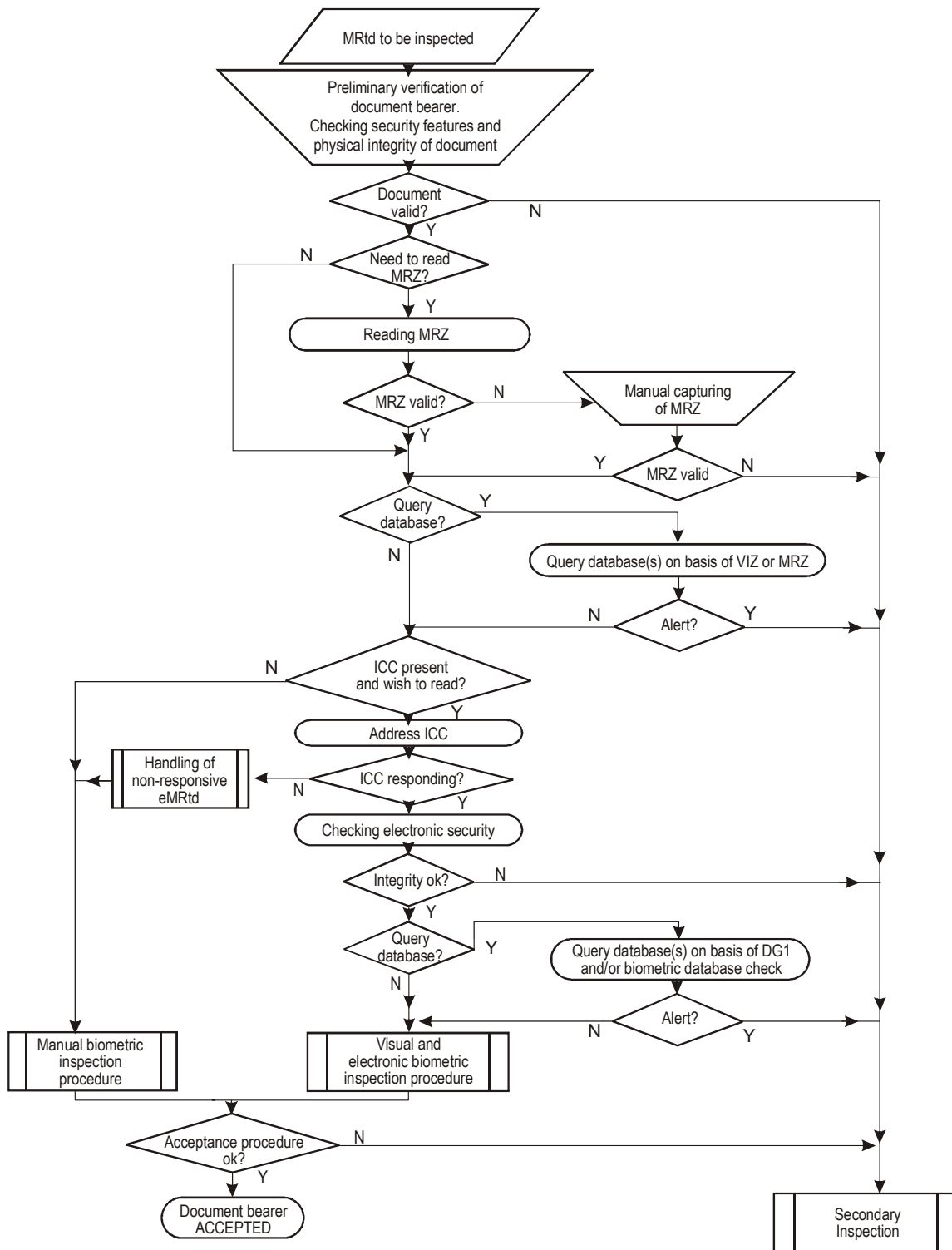


Figure II-6.

11/11/2015 11:16:34 AM

SECTION III

A LOGICAL DATA STRUCTURE FOR CONTACTLESS INTEGRATED CIRCUIT DATA STORAGE TECHNOLOGY

1. SCOPE

This Section defines a Logical Data Structure (LDS) for eMRtds required for global interoperability. The contactless integrated circuit capacity expansion technology contained in an MRtd selected by an issuing State or organization must allow data to be accessible by receiving States. This section 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 **MUST** be followed to achieve global interoperability for reading of details (Data Elements) recorded in the capacity expansion technology optionally included on an MRtd (eMRtd).

2. REFERENCES

Certain provisions of the International Standards referenced in this text constitute provisions of this volume. This reference documentation is listed in Section I, Paragraph 5.

3. TERMINOLOGY, TERMS AND DEFINITIONS

A glossary of terms, definitions and abbreviations appears at the beginning of this volume.

4. THE NEED FOR A LOGICAL DATA STRUCTURE

4.1 A standardized Logical Data Structure (LDS) is required to enable global interoperability for machine reading of recorded details stored in an optional capacity expansion technology that has been added to an MRTD at the discretion of an issuing State or organization.

4.2 In developing the LDS, ICAO initially established as a preeminent requirement the need for a single LDS for all MRTDs using any of the optional capacity expansion technologies under consideration. As deliberations progressed it became apparent that the contactless integrated circuit was the only technology that could satisfy all of ICAO's needs.

5. REQUIREMENTS OF THE LOGICAL DATA STRUCTURE

ICAO has determined that the predefined, standardized LDS must meet a number of **MANDATORY** requirements:

- ensure efficient and optimum facilitation of the rightful holder;
- ensure protection of details recorded in the optional capacity expansion technology;
- allow global interchange of capacity expanded data based on the use of a single LDS common to all MRTDs;
- address the diverse optional capacity expansion needs of issuing States and organizations;
- provide expansion capacity as user needs and available technology evolve;
- support a variety of data protection options;
- utilize existing international standards to the maximum extent possible in particular the emerging international standards for globally interoperable biometrics.

6. MANDATORY AND OPTIONAL DATA ELEMENTS

A series of MANDATORY and OPTIONAL Data Elements has been defined for the LDS to meet the global requirements of processing persons presenting MRtds as illustrated in Figure III-1.

7. ORDERING AND GROUPING OF DATA ELEMENTS

7.1 A logical order¹ supported by ordered groupings of related Data Elements has been established for the series of mandatory and optional Data Elements as illustrated in Figure III-1.

7.2 The ordered groupings of Data Elements are further grouped depending on whether they have been recorded by: 1) an issuing State or organization; or 2) a receiving State or approved receiving organization.

Note.—The ability for a receiving State or approved receiving organization to add data to the LDS is not supported in the LDS defined in this edition of Doc 9303, Part 3.

7.3 Four groups of Data Elements MUST be included if an LDS is recorded to the optional capacity expansion technology (contactless IC):

- those that define the contents of the machine readable zone (MRZ) of the eMRtd (Data Group 1);
- an encoded image of the face of the eMRtd holder as defined in Volume 1 and Section II of Volume 2 of Doc 9303, Part 3;

1. The logical order for Data Elements has been standardized to meet the global requirements established for enhanced facilitation and improved security when processing persons presenting MRtds. The actual order of recording of the grouped Data Elements is defined by specifications established to ensure efficient performance of the contactless integrated circuit expansion technology. These specifications are defined in Appendix 1.

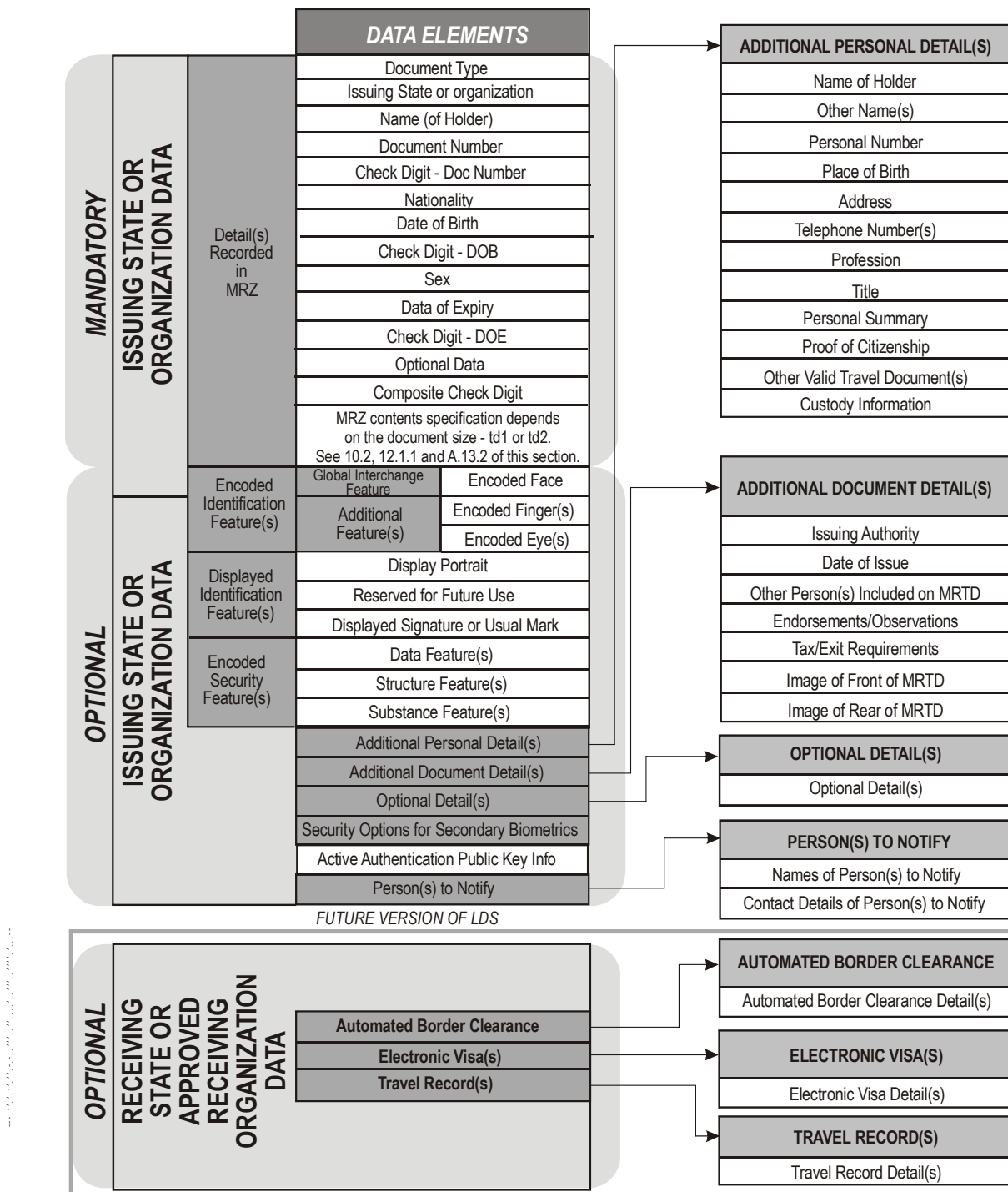


Figure III-1. Mandatory and optional Data Elements defined for LDS

- EF.COM, containing version information and tag list;
- EF.SOD, containing data integrity and authenticity information.

7.4 All other Data Elements defined for recording by an *issuing State or organization* are OPTIONAL.

7.5 Groupings of Data Elements added by *receiving States or approved receiving organizations* may or may not be present in an LDS. More than one recording of grouped Data Elements added by receiving States or approved receiving organizations can be present in the LDS.

Note.— The ability for a receiving State or approved receiving organization to add data to the LDS is not supported in this edition of Doc 9303, Part 3.

7.6 The LDS is considered to be a single cohesive entity containing the number of groupings of Data Elements recorded in the optional capacity expansion technology at the time of machine reading.

Note.—The LDS has been designed with sufficient flexibility that it can be applied to all types of MRTD. Within the figures and tables which follow, some data items are only applicable to machine readable visas and to machine readable passports or require a different presentation in relation to these documents. These items should be ignored in relation to the eMRtds.

7.7 Within the LDS, logical groupings of related Data Elements have been established. These logical groupings are referred to as Data Groups.

7.8 Each Data Group is assigned a reference number. Figure III-2 identifies the reference number assigned to each Data Group, for example, “DG2” identifies Data Group # 2, Encoded Identification Feature(s) for the face of the rightful holder of the MRtd (i.e. facial biometric details).

8. DATA GROUPS CODED TO ALLOW CONFIRMATION OF AUTHENTICITY AND INTEGRITY OF DATA

To allow confirmation of the authenticity and integrity of recorded details, an authenticity/integrity object is included. Each Data Group MUST be represented in this authenticity/integrity object, which is recorded within a separate elementary file (EF.SOD). (Refer to Section IV, *PKI*, for details.) Using the CBEFF structure utilized for Encoded Identification Feature Data Groups 2-4 and optional “additional biometric security” features defined in Section IV, *PKI*, identity confirmation details (e.g. biometric templates) MAY also be individually protected at the discretion of the issuing State or organization.

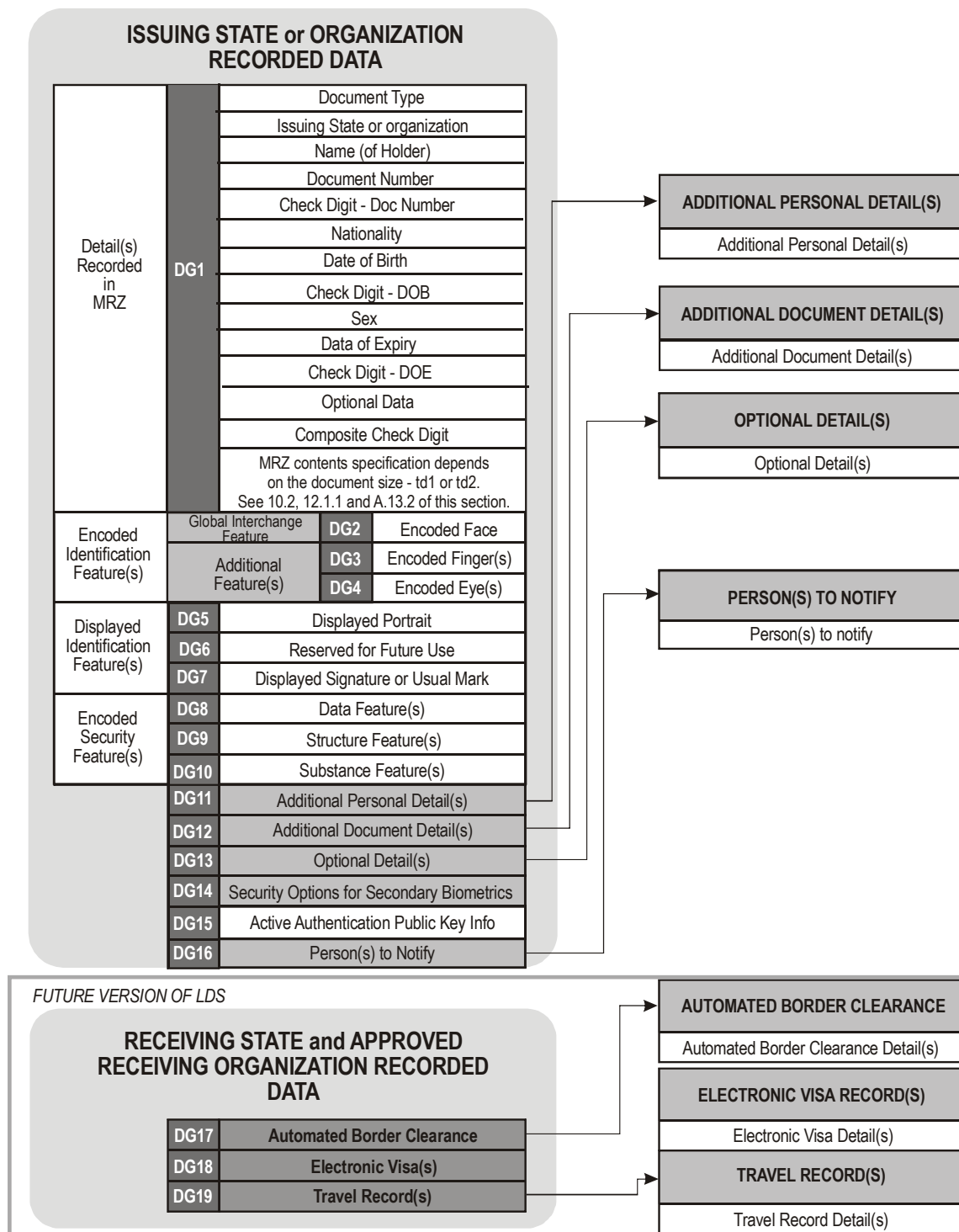


Figure III-2. Data group reference numbers assigned to LDS

Note to Figure III-2.—The option for a receiving State to add data on border clearance, electronic visas and travel records (Data Groups 17 to 19) is not yet permitted but is included as an indication of future development.