ICAO

Doc 9303

Machine Readable Travel Documents

Seventh Edition, 2015

Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

ICAO

Doc 9303

Machine Readable Travel Documents

Seventh Edition, 2015

Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

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

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

Doc 9303, *Machine Readable Travel Documents*
Part 10 — *Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)*
ISBN 978-92-9249-798-9

© ICAO 2015

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, without prior permission in writing from the International Civil Aviation Organization.

DOCUMENT CHANGE RECORD

Doc 9303, Part 10

DATE	NO.	SECTION/PAGES AFFECTED	
31/08/16	1	Page 4	2. Requirements of the Logical Data Structure — Correction to caption of Figure 1.
		Pages 5, 19 20, 22 to 27, 34, 59 and 60, and Tables 23, 26, 33 and 62	Multiple Changes introduced from: Resolved Wellington April-2016. Comment on Doc 9303-10, 7th Edition, and various minor editorial corrections
		Page 24	5.2.5 SignedData Type for SOD V1 — Table 14: changed “States may include the Document Signer Certificate (CDS) which can be used to verify the signature in the signerInfos field.” to “States SHALL include the Document Signer Certificate (CDS) which can be used to verify the signature in the signerInfos field.”
		Appendix A	Removed paragraph “A.6 EF.DG12 — Additional Document Details”
5/09/16	1	Appendix B	Incorporation of eMRTD sections of Application Profile in new Appendix B (The contactless IC in an eMRP (Informative))
		Appendix C	Incorporation of eMRTD Inspection Systems sections of Application Profile in new Appendix C (Inspection Systems (iInformative))

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of ICAO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

TABLE OF CONTENTS

Page

1. SCOPE 1

2. REQUIREMENTS OF THE LOGICAL DATA STRUCTURE 1

2.1 Security 2
2.2 Authenticity and Integrity of Data 2
2.3 Ordering of LDS 2

3. APPLICATION PROFILE FOR THE CONTACTLESS IC 5

3.1 Minimum Requirements for Interoperability 5
3.2 Electrical Characteristics 5
3.3 Physical Characteristics 5
3.4 Data Storage Capacity of the Contactless IC 5
3.5 Storage of Other Data 6
3.6 Minimum Data Items to be Stored in the LDS 6
3.7 Initialization, Anticollision, and Transmission Protocol according to ISO/IEC 14443 6
3.8 Command Set 7
3.9 Command Formats and Parameter Options 7

4. FILE STRUCTURE SPECIFICATIONS 11

4.1 Application Selection — DF 11
4.2 Data Groups 12
4.3 Data Elements Encoding Rules 13
4.4 Normative Tags used in LDS context 15
4.5 LDS Versioning 18

5. ELEMENTARY FILES 19

5.1 Header and Data Group Presence Information EF.COM (REQUIRED) 19
5.2 Document Security Object $EF.SO_D$ (REQUIRED) 20
5.3 EF.CardAccess (CONDITIONAL) 26
5.4 EF.CardSecurity (CONDITIONAL) 27

6. DATA ELEMENTS FORMING DATA GROUPS 1 THROUGH 16 28

6.1 Data Group 1 — Machine Readable Zone Information (REQUIRED) 29
6.2 Data Group 2 — Encoded Identification Features — Face (REQUIRED) 33
6.3 Data Group 3 — Additional Identification Feature — Finger(s) (OPTIONAL) 35
6.4 Data Group 4 — Additional Identification Feature — Iris(es) (OPTIONAL) 41
6.5 Data Group 5 — Displayed Portrait (OPTIONAL) 45
6.6 Data Group 6 — Reserved For Future Use 47
6.7 Data Group 7 — Displayed Signature or Usual Mark (OPTIONAL) 47
6.8 Data Group 8 — Data Feature(s) (OPTIONAL) 48
6.9 Data Group 9 — Structure Feature(s) (OPTIONAL) 49

Page

6.10 Data Group 10 — Substance Feature(s) (OPTIONAL) 50
6.11 Data Group 11 — Additional Personal Detail(s) (OPTIONAL) 51
6.12 Data Group 12 — Additional Document Detail(s) (OPTIONAL) 54
6.13 Data Group 13 — Optional Details(s) (OPTIONAL) 56
6.14 Data Group 14 — Security Options (CONDITIONAL) 56
6.15 Data Group 15 — Active Authentication Public Key Info (CONDITIONAL) 57
6.16 Data Group 16 — Person(s) to Notify (OPTIONAL) 58

7. REFERENCES (NORMATIVE) 59

APPENDIX A TO PART 10. Logical Data Structure Mapping Examples (Informative) ..... App A-1

APPENDIX B TO PART 10. The Contactless IC in an eMRP (Informative) ..... App B-1

APPENDIX C TO PART 10. Inspection Systems (Informative) ..... App C-1

1. SCOPE

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

This Part 10 of Doc 9303 defines the Logical Data Structure (LDS) for eMRTDs required for global interoperability and defines the specifications for the organization of data on the contactless IC. This requires the identification of all mandatory and optional Data Elements and a prescriptive ordering and/or grouping of Data Elements that MUST be followed to achieve global interoperability for electronic reading of the eMRTD.

Doc 9303-10 provides specifications to enable States and integrators to implement a contactless IC into an eMRTD travel document. This part defines all mandatory and optional data elements, file structures, and application profiles for the contactless IC.

Part 10 should be read in conjunction with:

- Part 1 — *Introduction*;
- Part 3 — *Specifications Common to all MRTDs*;
- Part 4 — *Specifications for Machine Readable Passports (MRP) and other TD3 size MRTDs*;
- Part 5 — *Specifications for TD1 Size Machine Readable Official Travel Documents (MROTDs)*;
- Part 6 — *Specifications for TD2 Size Machine Readable Official Travel Documents (MROTDs)*.

and the relevant contactless IC parts:

- Part 11 — *Security Mechanisms for MRTDs*;
- Part 12 — *Public Key Infrastructure for MRTDs*.

2. REQUIREMENTS OF THE LOGICAL DATA STRUCTURE

The contactless IC capacity expansion technology contained in an eMRTD selected by an issuing State or organization must allow data to be accessible by receiving States.

ICAO has determined that the predefined, standardized Logical Data Structure (LDS) shall meet a number of mandatory requirements:

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

2.1 Security

Data integrity and authenticity are needed for trusted global interoperability.

Data Groups 1 to 16 inclusive SHALL be write protected. A hash for each Data Group in use SHALL be stored in the Document Security Object ($EF.SO_D$).

Only the issuing State or organization shall have write access to these Data Groups. Therefore, there are no interchange requirements and the methods to achieve write protection are not part of this specification.

2.2 Authenticity and Integrity of Data

To allow confirmation of the authenticity and integrity of recorded details, an authenticity/integrity object is included. Each Data Group MUST be represented in this authenticity/integrity object, which is recorded within a separate elementary file ($EF.SO_D$). Using the Common Biometric Exchange File Format (CBEFF) structure utilized for Encoded Identification Feature Data Groups 2-4 and optional “additional biometric security” features defined in Doc 9303-12, identity confirmation details (e.g. biometric templates) MAY also be individually protected at the discretion of the issuing State or organization.

2.3 Ordering of LDS

The Random Ordering Scheme only SHALL be used for international interoperability.

2.3.1 Random Ordering Scheme

The Random Ordering Scheme allows Data Groups and Data Elements to be recorded following a random ordering which is consistent with the ability of the optional capacity expansion technology to allow direct retrieval of specific Data Elements even if they are recorded out of order. Variable length Data Elements are encoded as TLV data objects specified in ASN.1.

2.3.2 Random Access File Representation

The Random Access File Representation has been defined with the following considerations and assumptions.

- Support a wide variety of implementations. The LDS includes a wide variety of optional Data Elements. These Data Elements are included to facilitate eMRTD authentication, rightful holder authentication, and to expedite processing at document/person points.
- The data structure must support:
  - a limited or extensive set of Data Elements;
  - multiple occurrences of specific Data Elements;
  - continuing evolution of specific implementations.
- Support at least one application data set;
- Allow for other national specific applications;
- Support optional Active Authentication of the document using a stored asymmetrical key pair;
- Support rapid access of selected Data Elements to facilitate rapid document processing:
  - immediate access to necessary Data Elements;
  - direct access to data templates, and biometric data.

2.3.3 Grouping of Data Elements

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

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

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

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

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

Each Data Group is assigned a reference number. Figure 1 identifies the reference number assigned to each Data Group, for example, “DG2” identifies Data Group 2, Encoded Identification Feature(s) for the face of the holder of the eMRTD (i.e. facial biometric details).

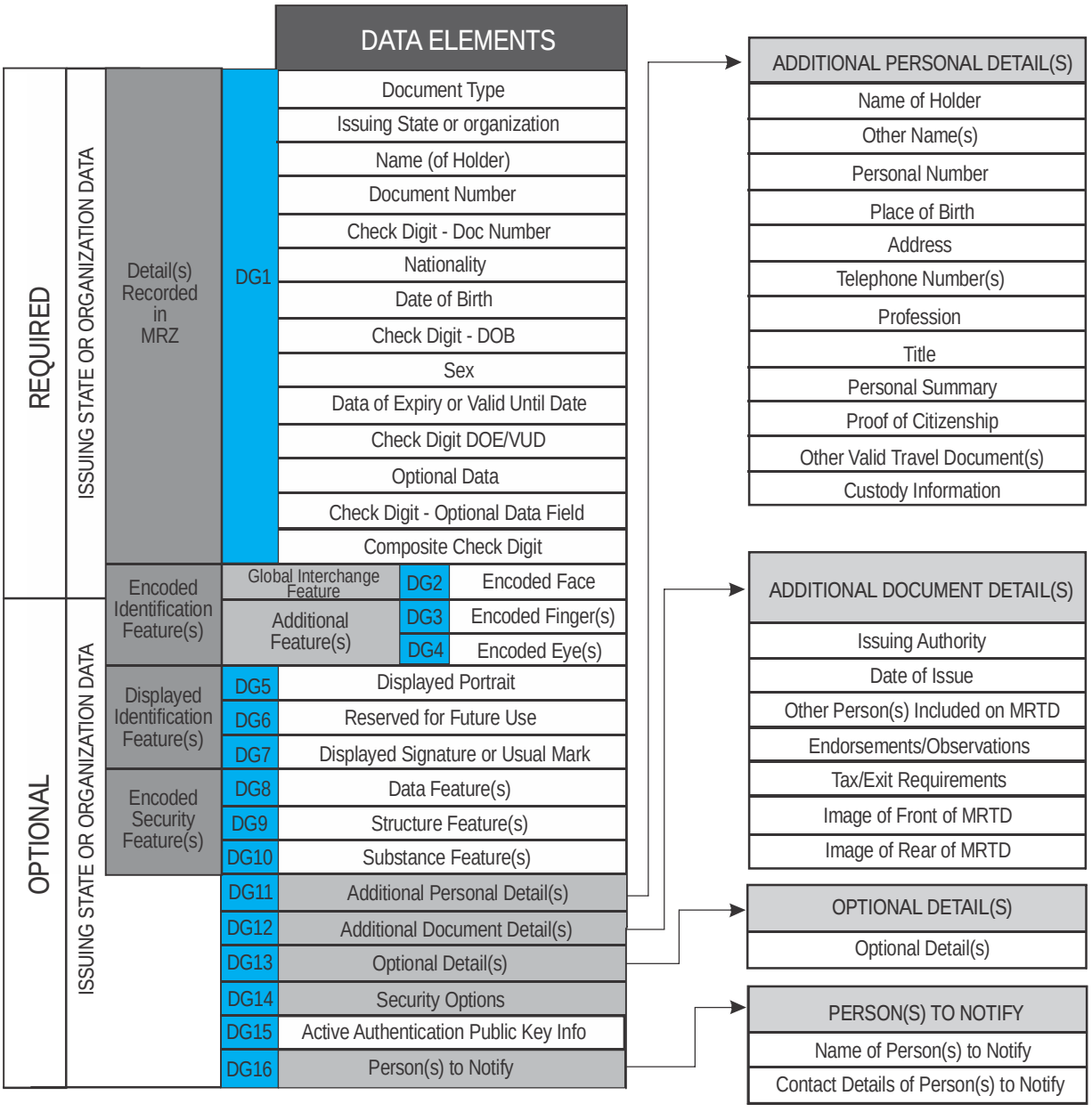

Figure 1. Data Group Reference Numbers Assigned to the LDS

3. APPLICATION PROFILE FOR THE CONTACTLESS IC

3.1 Minimum Requirements for Interoperability

The following SHALL be the minimum requirements for interoperability of proximity contactless IC-based eMRTDs:

- [ISO/IEC 14443-1], [ISO/IEC 14443-2], [ISO/IEC 14443-3], [ISO/IEC 14443-4] including all associated amendments, and corrigendums;
- [ISO/IEC 10373-6] test specification compliant including all associated amendments and corrigendums;
- Type A or Type B signal interface;
- Support for a file structure as defined by [ISO/IEC 7816-4] for variable length transparent files;
- Support for one or more applications and appropriate [ISO/IEC 7816-4] commands as specified in Doc 9303;
- Application Family Identifier (AFI) is 0xE1 (eMRTD). CRC_B of Application Identifier (AID: 0xA0000002471001) SHALL be 0xF35E.

3.2 Electrical Characteristics

The radio frequency power and signal interface SHALL be as defined in [ISO/IEC14443-2]. A minimum of 424 kilobits per second transmission speed is advised. Use of the EMD features specified in [ISO/IEC 14443-2] is OPTIONAL.

3.3 Physical Characteristics

It is recommended that the size of the coupling antenna area be in accordance with [ISO/IEC 14443-1] Class 1 (ID-1 antenna size) only.

3.4 Data Storage Capacity of the Contactless IC

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

In the event that a State's PKI infrastructure is not available to sign eMRTD data as part of personalization, and the issuance of the document(s) cannot be delayed, it is RECOMMENDED that the eMRTD contactless IC be left blank and be locked. The eMRTD SHOULD contain an appropriate endorsement on this. This is expected to be an exceptional circumstance.

3.5 Storage of Other Data

A State MAY use the storage capacity of the contactless IC in an eMRTD to expand the machine readable data capacity of the eMRTD beyond that defined for global interoperability. This can be for such purposes as providing machine readable access to identity document information (e.g. birth certificate details), stored personal identity confirmation (biometrics) and/or document authenticity verification details.

3.6 Minimum Data Items to be Stored in the LDS

The minimum mandatory items of data to be stored in the LDS on the contactless IC SHALL be a duplication of the machine readable zone data in Data Group 1 and the holder's facial image in Data Group 2. In addition, the IC in a compliant eMRTD SHALL contain the Document Security Object ($EF.SO_D$) that is required to validate the integrity of data created by the issuer. These data items are stored in a Dedicated File (DF) known as the eMRTD Application, and specified in the LDS. The Document Security Object ($EF.SO_D$) consists of the hashes of the Data Groups used.

3.7 Initialization, Anticollision and Transmission Protocol According to ISO/IEC 14443

3.7.1 Transmission Protocol

The eMRTD SHALL support half-duplex transmission protocol defined in [ISO/IEC14443-4]. The eMRTD SHALL support either Type A or Type B transmission protocols.

3.7.2 Request Command and Answer to Request

The contactless IC SHALL respond to Request Command Type A (REQA) or Request Command Type B (REQB) with Answer to Request Type A (ATQA) or Answer to Request Type B (ATQB), as appropriate.

3.7.3 Random vs Fixed Identifier for the Contactless IC

The eMRTD may serve as a "beacon" in which the contactless IC emits a Unique Identifier (UID) for Type A, and PUPI for Type B when initially activated. This might allow identification of the issuing authority. [ISO/IEC 14443] allows the choice of the option whether the eMRTD presents a fixed identifier, assigned uniquely for only that eMRTD, or a random number, which is different at each start of the communication dialogue. Some issuing States prefer to implement a unique number for security reasons or any other reason. Other issuers give greater preference to concerns about data privacy and the possibility to track persons due to fixed IC identifiers.

Choosing the one or the other option does not decrease interoperability since a reader terminal when compliant with ISO/IEC 14443 will understand both methods. The use of random IC identifiers is RECOMMENDED, but States MAY choose to apply unique UIDs for Type A or unique PUPIs for Type B.

3.8 Command Set

All commands, formats, and their return codes are defined in [ISO/IEC 7816-4]. The minimum set of commands to be supported by the eMRTD MUST be as follows:

SELECT;
READ BINARY.

It is recognized that additional commands will be required to establish the correct security environment and implement the optional security provisions identified in Doc 9303-11**.** Implementation of the mechanisms specified in Doc 9303-11 requires support of the following additional commands:

GET CHALLENGE;
EXTERNAL AUTHENTICATE;
INTERNAL AUTHENTICATE;
MANAGE SECURITY ENVIRONMENT;
GENERAL AUTHENTICATE.

Further details on command protocols can be found in Doc 9303-11.

3.8.1 SELECT

The eMRTD supports two structure selection methods that are file identifier and short EF identifier. Readers support at least one of the two methods. The file identifier and Short File Identifier is REQUIRED for the contactless IC operating system, but OPTIONAL for the reader.

3.8.2 READ BINARY

The support of the READ BINARY command with an odd INS byte by an eMRTD is CONDITIONAL. The eMRTD SHALL support this command variant if it supports data groups with 32 768 bytes or more.

3.9 Command Formats and Parameter Options

3.9.1 Application selection

Applications have to be selected either by their file identifier or their application name. After the selection of an application, the file within this application can be accessed.

Note.— Application names have to be unique. Therefore selection of an application using the application name can be done from wherever needed.

3.9.1.1 Selection of Master File

Table 1. Selection of MF

CLA	INS	P1	P2	Lc	Data	Le
00	A4	00	0C	Empty	Empty	Empty

Note.— It is RECOMMENDED that the SELECT MF command not be used.

3.9.1.2 Selection of application by application identifier

An application SHALL be selected by use of the DF Name. The parameters for the APDU command are shown below:

Table 2. SELECT Application command

CLA	INS	P1	P2	Lc	Data	Le
00	A4	04	0C	Var.	AID	–

The first [ISO/IEC7816-4] instruction is “select application”, with the code 0x00A4040C07A0000002471001. Every eMRTD application supports the select command.

3.9.2 EF selection using SELECT command

Files have to be selected by their file identifier. When files are selected by File Identifier, it has to be assured that the application the files are stored within has previously been selected.

Table 3. SELECT File command

CLA	INS	P1	P2	Lc	Data	Le
00	A4	02	0C	02	FileID	–

The eMRTD SHALL support the SELECT command with file identifier as specified in Table 3. The inspection system SHALL support at least one of the following methods:

- The SELECT command with file identifier as specified in Table 3;
- The READ BINARY command with even INS byte and SFI as specified in Table 5.

3.9.3 Reading data from EF (READ BINARY)

There are two methods to read data from the eMRTD: by selecting the file and then reading the data, or by reading the data directly using the Short File Identifier. Support for Short File Identifier is REQUIRED for the eMRTD. It is therefore RECOMMENDED that inspection systems use Short File Identifier.

3.9.3.1 Reading data of a selected file (transparent file)

Table 4. READ BINARY command

CLA	INS	P1	P2	Lc	Data	Le
00	B0	Offset MSB	Offset LSB	–	–	MaxRet

3.9.3.2 Reading data using Short File Identifier (transparent file)

Table 5. READ BINARY command with Short File Identifier

CLA	INS	P1	P2	Lc	Data	Le
00	B0	SFI	Offset LSB	–	–	MaxRet

3.9.4 Extended Lc/Le Support

Depending on the size of the cryptographic objects (e.g. public keys, signatures), APDUs with extended length fields MUST be used to send this data to the MRTD chip. For details on extended length, see [ISO/IEC 7816-4].

3.9.4.1 MRTD Chips

For MRTD chips, support of extended length is CONDITIONAL. If the cryptographic algorithms and key sizes selected by the issuing State require the use of extended length, the MRTD chips SHALL support extended length. If the MRTD chip supports extended length this MUST be indicated in the ATR/ATS or in EF.ATR/INFO as specified in [ISO/IEC 7816-4].

3.9.4.2 Terminals

For terminals, support of extended length is REQUIRED. A terminal SHOULD examine whether or not support for extended length is indicated in the MRTD chip's ATR/ATS or in EF.ATR/INFO before using this option. The terminal MUST NOT use extended length for APDUs other than the following commands unless the exact input and output buffer sizes of the MRTD chip are explicitly stated in the ATR/ATS or in EF.ATR/INFO.

- MSE:Set KAT;
- General Authenticate.

3.9.5 Command chaining

Command chaining MUST be used for the General Authenticate command to link the sequence of commands to the execution of the protocol. Command chaining MUST NOT be used for other purposes unless clearly indicated by the chip. For details on command chaining, see [ISO/IEC 7816-4].

3.9.6 EFs larger than 32 767 bytes

The maximum size of an EF is normally 32 767 bytes, but some contactless ICs support larger files. A different READ BINARY parameter option and command format is required to access the data area when the offset is greater than 32 767. This format of command should be used after the length of the template has been determined and the need to access the data in the extended data area has been determined. For example, if the data area contains multiple biometric data objects, it may not be necessary to read the entire data area. Once the offset for the data area is greater than 32 767, this command format shall be used. The offset is placed in the command field rather than in the parameters P1 and P2.

Table 6. Command format for EFs larger than 32 767 bytes

CLA	INS	P1	P2	Lc	Data	Le	Remark
00	B1	00	00	Var.	Offset TLV encoded	00	Reading files greater than 32 767 bytes

Both Length and Value fields of BER-TLV data object are variable length and can be encoded in different ways (see [ISO/IEC 7816-4]: "BER-TLV length fields").

For performance reasons, communication between the eMRTD and the terminal should be kept as short as possible. Therefore Length field and Value field in the BER-TLV data object SHOULD be as short as possible. This applies not only for Offset data objects in odd INS READ BINARY commands but also for all other BER-TLV data objects exchanged between the eMRTD and the terminal.

Examples for encoded Offset in Data-field:

- Offset: 0x0001 is encoded as Tag=0x54 Length=0x01 Value=0x01;
- Offset: 0xFFFF is encoded as Tag= 0x54 Length=0x02 Value=0xffff.

The subsequent READ BINARY commands shall specify the offset in the Data field. The final READ BINARY command should request the remaining data area.

The Le byte contains either 0x00 or number of bytes containing extended TL and V.

For some purposes, B1 and the traditional B0 READ Binary commands could not overlap. In other words, B0 only should be used to read the first 32 767 bytes and B1 from 32 K upward. For others there could be a small overlap of 256 bytes around the 32 767 threshold to allow a smoother transition between B0 and B1. For this latter group, B1 could be used right from the beginning of the file, i.e. with an offset starting from 0 to allow the same command to be used to read the full content. With respect to [ISO/IEC 7816-4], there are no constraints specified on the offset value when bit 1 of INS is set to 1 to allow a broader use.

The odd INS byte is not to be used by the inspection system if the size of an EF is 32 767 bytes or less.

4. FILE STRUCTURE SPECIFICATIONS

Information in an eMRTD is stored in a file system defined in [ISO/IEC 7816-4]. The file system is organized hierarchically into dedicated files (DFs) and elementary files (EFs). Dedicated files (DFs) contain elementary files or other dedicated files. An optional master file (MF) may be the root of the file system. See Figure 2 for a graphical representation of the file structure.

Note.— The need for a master file is determined by the choice of operating systems and optional access conditions.

4.1 Application Selection — DF

The eMRTDs SHALL support at least one application as follows:

- The application SHALL consist of data recorded by the Issuing State or organization, Data Groups 1 through to 16 together with the Document Security Object ($EF.SO_D$);
- The Document Security Object ($EF.SO_D$) consists of the hash values as defined in Doc 9303-11 and Doc 9303-12 for the Data Groups in use, and is needed to validate the integrity of data created by the issuer and stored in the eMRTD Application.

In addition, issuing States or organizations may wish to add other applications. The file structure SHALL accommodate such additional applications, but the specifics of such applications are outside the scope of Doc 9303.

The eMRTD application SHALL be selected by use of the Application Identification (AID) as a reserved DF name. The AID SHALL consist of the Registered Application Identifier assigned by ISO according to [ISO/IEC 7816-5] and a Proprietary Application Identifier Extension (PIX) as specified within this document:

- The Registered Application Identifier is 0xA000000247;
- The issuer stored data application SHALL use PIX = 0x1001;
- The full AID of the eMRTD application is ‘A0 00 00 02 47 10 01’.

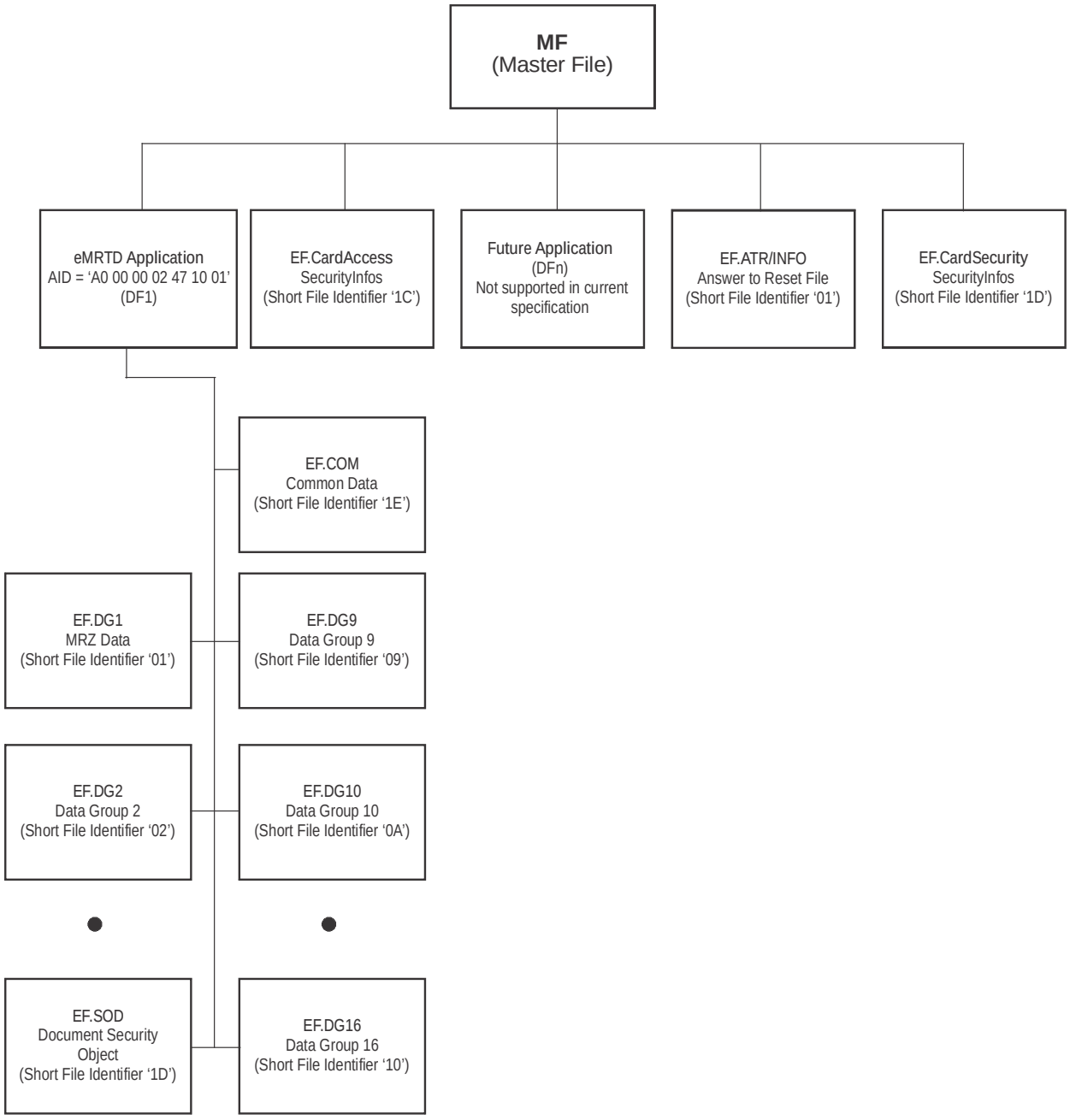

Figure 2. File Structure Summary

4.2 Data Groups

Within each application there may be a number of Data Groups sometimes referred to as Elementary Files (EFs). The issuing State or organization application may have up to 16 Data Groups. Data Group 1 (DG1), the machine readable zone (MRZ) and Data Group 2, the encoded face, are REQUIRED. All other Data Groups are OPTIONAL. All Data Groups are in the form of data templates and have individual ASN.1 Tags.

Each Data Group consists of a series of data objects within a template. Each Data Group SHALL be stored in a separate Elementary File (EF). Individual data objects from the Data Group can be retrieved directly after the relative position within the transparent file has been determined.

4.3 Data Elements Encoding Rules

The files contain the Data Elements as data objects within a template. The structure and coding of data objects are defined in [ISO/IEC 7816-4] and [ISO/IEC 7816-6]. Each data object has an identification Tag that is specified in hexadecimal coding (for example, 0x5A). The Tags defined in this section use the coexistent coding option. Each data object has a unique Tag, a length and a value. The data objects that may be present in a file are identified as mandatory (M) or optional (O). Whenever possible inter-industry Tags are used. Note that the specific definition and format of some Tags have been changed to make them relevant for the eMRTD application. As examples:

- Tag 0x5A is defined as Document Number rather than Primary Account Number and has the format F9N rather than V19N;
- Tag 0x5F20, Cardholder name, has been redefined as “Name of holder” with length of up to 39 characters, encoded per Doc 9303 format;
- Tag 0x65 is defined as the Displayed Portrait rather than Cardholder Related Data;
- As needed, additional Tags have been defined within the 0x5F01 through 0x5F7F range.

4.3.1 Data elements encoding normative note

There is a mismatch between the LDS (version 1.7 and 1.8) specifications and [ISO/IEC 8825-1] (BER/DER encoding rules) wherein [ISO/IEC 8825-1] States for Tags with a number ranging from zero to 30 (inclusive), the identifier octets shall comprise a single octet encoded as follows:

- bit 8 and bit 7 shall be encoded to represent the class of the Tag;
- bit 6 shall be a zero or a one;
- bits 5 to bit 1 shall encode the number of the Tag as a binary integer with bit 5 as the most significant bit.

This means that (for instance) the Tag for the version number of the LDS specification should be defined as Tag 0x41 = 0x01000001b:

- where 01 means application class (bits 8 and 7);
- where 0 means that it is a primitive (bit 6);
- where 00001 is the encoding of Tag number 1 (bits 5-1).

In Doc 9303 the Tag for the version number of the LDS specification is defined as Tag 0x5F01= 0x0101111100000001b:

- where 01 means application class;
- where 0 means that it is a primitive (not constructed);
- where 11111 means that the Tag number is encoded in the next bytes;

- where 0 means that it is the last byte encoding the Tag number;
- where 0000001 is the encoding of Tag number 1.

This counts for all TAGs from zero to 30 (inclusive):

- 0x5F01, 0x5F08, 0x5F09, 0x5F0A, 0x5F0B, 0x5F0C, 0x5F0E, 0x5F0F, 0x5F10, 0x5F11, 0x5F12, 0x5F13, 0x5F14, 0x5F15, 0x5F16, 0x5F17, 0x5F18, 0x5F19, 0x5F1A, 0x5F1B, 0x5F1C, 0x5F1D, 0x5F1E.

Implementers should be aware of this mismatch and follow the specifications as set out in Doc 9303. One should however note that:

- eMRTD implementations cannot be created using a generator based on ASN.1;
- ASN.1/BER parsers may return an error instead of correctly parsing EF.COM;
- The hash over EF.COM cannot be recreated by decoding the EF.COM structure and encoding it again afterwards.

4.3.2 Data Element Presence Map (DEPM)

A concept of presence maps is used with a number of Data Groups that contain a series of subordinate Data Elements which may be included at the discretion of the State or organization making the recording. These presence maps, called Data Element Presence Maps (DEPM) are located at the start of those specific Data Groups that allow optional expansion.

A DEPM contains information to enable a receiving State or approved receiving organization to determine which Data Elements are present in the Data Group.

The DEPM consists of a list of Tags consistent with the convention for identifying Data Elements recorded in eMRTDs in which each Tag identifies if a specific Data Element is recorded in the Data Group. This form of DEPM is encoded as a Tag list within the relevant Data Group.

4.3.3 Length encoding rules for ASN.1 BER TLV Data Object

The definite form of ANS.1 length encoding as defined in [ISO/IEC 8825-1] MUST be used.

Table 7. Length Encoding Rules

Range	number of bytes	1st byte	2nd byte	3rd byte
0 to 127	1	binary value	None	None
128 to 255	2	81	binary value	None
256 to 65 535	3	82	binary value MSB LSB	

4.4 Normative Tags Used in LDS Context

Table 8. Normative Tags Summary

Tag	Definition	Where Used
02	Integer	Biometric and display templates
5C	Tag list	EF.COM and numerous other files
5F01	LDS Version Number	EF.COM
5F08	Date of birth (truncated)	MRZ
5F09	Compressed image (ANSI/NIST-ITL 1-2000)	Displayed finger
5F0A	Security features — Encoded Data	Security features (details TBD)
5F0B	Security features — Structure	Security features (details TBD)
5F0C	Security features	Security features (details TBD)
5F0E	Full name, in national characters	Additional personal details
5F0F	Other names	Additional personal details
5F10	Personal number	Additional personal details
5F11	Place of birth	Additional personal details
5F12	Telephone	Additional personal details
5F13	Profession	Additional personal details
5F14	Title	Additional personal details
5F15	Personal summary	Additional personal details
5F16	Proof of citizenship (10918 image)	Additional personal details
5F17	Other valid TD Numbers	Additional personal details
5F18	Custody information	Additional personal details
5F19	Issuing Authority	Additional document details
5F1A	Other people on document	Additional document details
5F1B	Endorsements/Observations	Additional document details
5F1C	Tax/Exit requirements	Additional document details
5F1D	Image of document front	Additional document details

Tag	Definition	Where Used
5F1E	Image of document rear	Additional document details
5F1F	MRZ Data Elements	MRZ data objects
5F26	Date of issue	Additional document details
5F2B	Date of birth (8 digit)	Additional personal details
5F2E	Biometric data block	Biometric data
5F36	Unicode Version Level	EF.COM
5F40	Compressed image template	Displayed portrait
5F42	Address	Additional personal details
5F43	Compressed image template	Displayed signature or mark
5F50	Date data recorded	Person to notify
5F51	Name of person	Name of person to notify
5F52	Telephone	Telephone number of person to notify
5F53	Address	Address of person to notify
5F55	Date and time document personalized	Additional document details
5F56	Serial number of personalization system	Additional document details
60	Common Data Elements	EF.COM
61	Template for MRZ Data Group	
63	Template for finger biometric Data Group	
65	Template for digitized facial image	
67	Template for digitized signature or usual mark	
68	Template for machine assisted security — Encoded data	
69	Template for machine assisted security — Structure	
6A	Template for machine assisted security — Substance	
6B	Template for additional personal details	
6C	Template for additional document details	
6D	Optional details	
6E	Reserved for future use	

Tag	Definition	Where Used
70	Person to notify	
75	Template for facial biometric Data Group	
76	Template for iris (eye) biometric template	
77	$EF.SO_D$ (EF for Document Security Object)	
7F2E	Biometric data block (enciphered)	
7F60	Biometric information template	
7F61	Biometric information group template	
8x	Context specific Tags	CBEFF
90	Enciphered hash code	Authenticity/Integrity code
A0	Context specific constructed data objects	Additional personal details
Ax or Bx	Repeating template, where x defines occurrence	Biometric header

4.4.1 Tags For Intermediate Processing (Informative)

Table 9. Intermediate Tags

Tag	Definition	Where Used
53	Optional data	Part of MRZ
59	Date of expiry	Part of MRZ
5A	Document number	Part of MRZ
5F02	Check digit — Optional data (TD3 only)	Part of MRZ
5F03	Document type	Part of MRZ
5F04	Check digit — Doc number	Part of MRZ
5F05	Check digit — Date of birth	Part of MRZ
5F06	Check digit — Expiry date	Part of MRZ
5F07	Check digit — Composite	Part of MRZ
5B	Name of document holder	Part of MRZ
5F28	Issuing State or organization	Part of MRZ

Tag	Definition	Where Used
5F2B	Date of birth	Part of MRZ
5F2C	Nationality	Part of MRZ
5F35	Sex	Part of MRZ
5F57	Date of birth (6 digit)	Part of MRZ

4.4.1.1 Tags reserved for future use (normative)

Table 10. RFU Tags

Tag	Definition	Where Used
5F44	Country of entry/exit	Travel records
5F45	Date of entry/exit	Travel records
5F46	Port of entry/exit	Travel records
5F47	Entry/Exit indicator	Travel records
5F48	Length of stay	Travel records
5F49	Category (classification)	Travel records
5F4A	Inspector reference	Travel records
5F4B	Entry/Exit indicator	Travel records
71	Template for electronic visas	
72	Template for border crossing schemes	
73	Template for travel record Data Group	

4.5 LDS Versioning

Future upgrades to the organization of the eMRTD LDS have been anticipated and will be addressed through publication of amendments to the specifications by ICAO. A version number will be assigned to each upgrade to ensure that receiving States and approved receiving organizations will be able to accurately decode all versions of the LDS.

4.5.1 LDS Version 1.7

LDS Version 1.7 MUST implement Document Security Object EF.SO_D version V0 as found in section 5 of this document.

4.5.2 LDS Version 1.8

LDS Version 1.8 MUST implement Document Security Object $EF.SO_D$ version V1 as found in section 5 of this document.

5. ELEMENTARY FILES

5.1 Header and Data Group Presence Information EF.COM (REQUIRED)

EF.COM is located in the eMRTD application (Short File Identifier = 0x1E) and contains LDS version information, Unicode version information and a list of the Data Groups that are present for the application. The eMRTD application must have only one file EF.COM that contains the common information for the application.

The Data Elements that may occur in this template are as follows:

Table 11. EF.COM Normative Tags

Tag	**L**	**Value**		
60	Var	application level information		
		Tag	**L**	**Value**
		5F01	04	LDS Version number with format aabb, where aa defines the version of the LDS and bb defines the update level.
		5F36	06	Unicode Version number with format aabbcc, where aa defines the major version, bb defines the minor version and cc defines the release level.
		5C	Var	Tag list. List of all Data Groups present.

A Header and Data Group Presence Map SHALL be included. The header SHALL contain the following information which enables a receiving State or approved receiving organization to locate and decode the various Data Groups and Data Elements contained within the block of data recorded by the issuing State or organization.

Within the LDS version 1.7 the EF.COM file is not signed, resulting in potential for undetected manipulation of its contents. Therefore it is desirable that the LDS version number is part of the signed information and as such protected by Passive Authentication. It is RECOMMENDED that inspection systems that rely on the EF.COM be modified to use the SOD described in the LDS version 1.8 as soon as possible.

5.1.1 LDS version number

The LDS version number defines the format version of the LDS. The exact format to be used for storing this value will be defined in Section 6 of this document. Standardized format for an LDS Version Number is “aabb”, where:

- “aa” = number (01-99) identifying the major version of the LDS (i.e. significant additions to the LDS);
- “bb” = number (01-99) identifying the minor version of the LDS.

5.1.2 UNICODE version number

The Unicode version number identifies the coding method used when recording alpha, numeric and special characters, including national characters. The exact format to be used for storing this value will be defined in Section 6 of this document. The standardized format for a Unicode version number is “aabbcc”, where:

- “aa” = number identifying the major version of the Unicode specification (i.e. significant additions to the specification, published as a book);
- “bb” = number identifying the minor version of the Unicode specification (i.e. character additions or more significant normative changes, published as a technical report); and
- “cc” = number identifying the update version of the Unicode specification (i.e. any other changes to normative or important informative portions of the specification that could change programme behaviour. These changes are reflected in new Unicode character database files and an update page). For historical reasons, the numbering within each of the fields (i.e. a, b, c) is not necessarily consecutive.

The Universal Character Set (UCS) MUST comply with [ISO/IEC 10646].

5.2 Document Security Object EF.SO_D (REQUIRED)

In addition to the LDS Data Groups, the contactless IC also contains a Document Security Object stored in EF.SO_D. This object is digitally signed by the issuing State and contains hash values of the LDS contents.

Table 12. EF.SO_D Tags

Tag	L	Value
77	Var	Document Security Object

There are two versions of the Document Security Object EF.SO_D currently available. It is REQUIRED that either EF.SO_D V0 or EF.SO_D V1 be implemented. Only one EF.SO_D is allowed.

5.2.1 Document Security Object EF.SOD Version V0 LDS v1.7 (REQUIRED)

The Document Security Object V0 for the LDS v1.7 does not contain the LDS and Unicode version information:

```
LDSSecurityObject ::= SEQUENCE {
      version LDSSecurityObjectVersion,
      hashAlgorithm DigestAlgorithmIdentifier,
      dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
      DataGroupHash}
```

5.2.2 SignedData Type for SOD V0

The Document Security Object is implemented as a SignedData Type, as specified in [RFC 3369]. All security objects SHALL be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

Note 1.— m REQUIRED — the field SHALL be present.
Note 2.— x do not use — the field SHOULD NOT be populated.
Note 3.— o optional — the field MAY be present.
Note 4.— c choice — the field content is a choice from alternatives.

Table 13. Signed Data Type for SO_D V0

Value		Comments
SignedData		
Version	m	Value = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-mrtd-security-ldsSecurityObject
eContent	m	The encoded contents of an ldsSecurityObject.
Certificates	o	States may choose to include the Document Signer Certificate (C_{DS}) which can be used to verify the signature in the signerInfos field.
Crls	x	It is recommended that States do not use this field.
signerInfos	m	It is recommended that States provide only 1 signerInfo within this field.
SignerInfo	m	
Version	m	The value of this field is dictated by the sid field. See RFC3369 Doc 9303-12 for rules regarding this field.
Sid	m	
issuerandSerialNumber	c	It is recommended that States support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	Producing States may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by receiving States except to verify the signature value.

Value		Comments
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value and any associated parameters.
Signature	m	The result of the signature generation process.
unsignedAttrs	o	Producing States may wish to use this field, but it is not recommended and receiving States may choose to ignore them.

5.2.3 ASN.1 Profile LDS Document Security Object for SOD VO

```
LDSSecurityObjectV0 {joint-iso-itu-t (2) international(23) icao(136)
mrtd(1) security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Imports from RFC 3280 [PROFILE],
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
id-mod(0) id-pkix1-explicit(18) }

-- Constants

ub-DataGroups INTEGER ::= 16

-- Object Identifiers
id-icao  OBJECT IDENTIFIER::={joint-iso-itu-t(2) international(23)
icao(136)}
id-icao-mrtd  OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security   OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-mrtd-security-ldsSecurityObject   OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 1}

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {V0(0)}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
   DataGroupHash }

DataGroupHash ::= SEQUENCE {
   dataGroupNumber      DataGroupNumber,
   dataGroupHashValue   OCTET STRING }
DataGroupNumber ::= INTEGER {
```

```
      dataGroup1            (1),
      dataGroup2            (2),
      dataGroup3            (3),
      dataGroup4            (4),
      dataGroup5            (5),
      dataGroup6            (6),
      dataGroup7            (7),
      dataGroup8            (8),
      dataGroup9            (9),
      dataGroup10          (10),
      dataGroup11          (11),
      dataGroup12          (12),
      dataGroup13          (13),
      dataGroup14          (14),
      dataGroup15          (15),
      dataGroup16          (16)}
END
```

Note 1.— The field `dataGroupValue` contains the calculated hash over the complete contents of the Data Group EF, specified by `dataGroupNumber`.

Note 2.— `DigestAlgorithmIdentifiers` MUST omit "NULL" parameters, while the `SignatureAlgorithmIdentifier` (as defined in RFC 3447) MUST include `NULL` as the parameter if no parameters are present, even when using SHA2 Algorithms in accordance with RFC 5754. Implementations MUST accept `DigestAlgorithmIdentifiers` with both conditions, absent parameters or with `NULL` parameters.

5.2.4 Document Security Object EF.SOD V1 LDS v1.8 (REQUIRED)

The Document Security Object V1 for the LDS v1.8 has been extended with a signed attribute, containing the LDS and Unicode version information:

```
LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
   DataGroupHash,
   ldsVersionInfo LDSVersionInfo OPTIONAL
   -- If present, version MUST be V1 }

LDSVersionInfo ::= SEQUENCE {
ldsVersion PrintableString,
   unicodeVersion PrintableString }
```

Note.— `DigestAlgorithmIdentifiers` MUST omit "NULL" parameters, while the `SignatureAlgorithmIdentifier` (as defined in RFC 3447) MUST include `NULL` as the parameter if no parameters are present, even when using SHA2 Algorithms in accordance with RFC 5754. Implementations MUST accept `DigestAlgorithmIdentifiers` with both conditions, absent parameters or with `NULL` parameters.

5.2.5 SignedData Type for SOD V1

The Document Security Object is implemented as a SignedData Type, as specified in [RFC 3369], Cryptographic Message Syntax (CMS), August 2002. All security objects MUST be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

Note 1.— m REQUIRED — the field SHALL be present.
Note 2.— x do not use — the field SHOULD NOT be populated.
Note 3.— o optional — the field MAY be present.
Note 4. — c choice — the field content is a choice from alternatives.

Table 14. Signed Data Type for SO_D V1

Value		Comments
SignedData		
Version	m	Value = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-mrtd-security-ldsSecurityObject
eContent	m	The encoded contents of an ldsSecurityObject.
Certificates	m	States SHALL choose to include the Document Signer Certificate (C_{DS}) which can be used to verify the signature in the signerInfos field.
Crls	x	It is recommended that States do not use this field.
signerInfos	m	It is recommended that States provide only 1 signerInfo within this field.
SignerInfo	m	
Version	m	The value of this field is dictated by the sid field. See RFC3369 Doc 9303-12 for rules regarding this field.
Sid	m	
issuerandSerialNumber	c	It is recommended that States support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	Producing States may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by receiving States except to verify the signature value.

Value		Comments
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value and any associated parameters.
Signature	m	The result of the signature generation process.
unsignedAttrs	o	Producing States may wish to use this field, but it is not recommended and receiving States may choose to ignore them.

5.2.6 ASN.1 Profile LDS Document Security Object for SOD V1

```
LDSSecurityObjectV1 { joint-iso-itu-t(2) international(23) icao(136)
mrtd(1) security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Imports from RFC 3280 [PROFILE]
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
id-mod(0) id-pkix1-explicit(18) }

-- Constants

ub-DataGroups INTEGER ::= 16

-- Object Identifiers

id-icao OBJECT IDENTIFIER::={joint-iso-itu-t(2) international(23)
icao(136) }
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-mrtd-security-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 1}

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {V0(0), V1(1)
-- If LDSSecurityObjectVersion is V1, ldsVersionInfo MUST be present }

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
   DataGroupHash,
   ldsVersionInfo LDSVersionInfo OPTIONAL
   -- If present, version MUST be V1 }
```

```
DataGroupHash ::= SEQUENCE {
   dataGroupNumber DataGroupNumber,
   dataGroupHashValue OCTET STRING }

DataGroupNumber ::= INTEGER {
   dataGroup1            (1),
   dataGroup2            (2),
   dataGroup3            (3),
   dataGroup4            (4),
   dataGroup5            (5),
   dataGroup6            (6),
   dataGroup7            (7),
   dataGroup8            (8),
   dataGroup9            (9),
   dataGroup10          (10),
   dataGroup11          (11),
   dataGroup12          (12),
   dataGroup13          (13),
   dataGroup14          (14),
   dataGroup15          (15),
   dataGroup16          (16)}

LDSVersionInfo ::= SEQUENCE {
   ldsVersion PRINTABLE STRING
   unicodeVersion PRINTABLE STRING }
END
```

Note 1.— The field `dataGroupValue` contains the calculated hash over the complete contents of the Data Group EF, specified by `dataGroupNumber`.

Note 2.— `DigestAlgorithmIdentifiers` MUST omit "NULL" parameters, while the `SignatureAlgorithmIdentifier` (as defined in RFC 3447) MUST include NULL as the parameter if no parameters are present, even when using SHA2 Algorithms in accordance with RFC 5754. Implementations MUST accept `DigestAlgorithmIdentifiers` with both conditions, absent parameters or with NULL parameters.

5.3 EF.CardAccess (CONDITIONAL)

EF.CardAccess is a transparent elementary file contained in the master file and is conditionally required if the optional PACE access control as defined in Doc 9303-11 is invoked. A full description of `SecurityInfos protocols` for PACE can be found in Doc 9303-11.

5.3.1 Storage on the contactless IC

The file CardAccess contained in the master file is REQUIRED if PACE is supported by the MRTD chip and SHALL contain the following `SecurityInfos` that are required for PACE:

- `PACEInfo`;
- `PACEDomainParameterInfo`.

Table 15. EF.CardAccess storage on the IC

File Name	EF.CardAccess
File ID	0x011C
Short File ID	0x1C
Read Access	ALWAYS
Write Access	NEVER
Size	Variable
Content	DER encoded `SecurityInfos` . For specific protocols see Doc 9303-11.

5.4 EF.CardSecurity (CONDITIONAL)

EF.CardSecurity is a transparent elementary file contained in the master file and is conditionally REQUIRED if the optional PACE with Chip Authentication Mapping as defined in Doc 9303-11 is invoked. A full description of `SecurityInfos` for PACE with Chip Authentication Mapping can be found in Doc 9303-11.

5.4.1 Storage on the contactless IC

The file CardSecurity contained in the master file is REQUIRED if PACE with Chip Authentication Mapping is supported by the MRTD chip and SHALL contain the following `SecurityInfos`:

- ChipAuthenticationPublicKeyInfo as required for PACE-CAM;
- The `SecurityInfos` contained in CardAccess.

Table 16. EF.CardSecurity storage on the IC

File Name	EF.CardSecurity
File ID	0x011D
Short File ID	0x1D
Read Access	PACE
Write Access	NEVER
Size	Variable
Content	DER encoded `SignedData` encapsulated See Doc 9303-11.ID signed data

6. DATA ELEMENTS FORMING DATA GROUPS 1 THROUGH 16

Data Groups 1 (DG1) through 16 (DG16) individually consist of a number of mandatory, optional, and conditional Data Elements. The specified order of Data Elements within the Data Group SHALL be followed. Each Data Group SHALL be stored in one transparent EF. Addressing EFs SHALL be by Short File Identifier as shown in Table 16. The EFs SHALL have file names for these files that SHALL be according to the number n, EF.DGn, where n is the Data Group number.

Table 17. Mandatory and optional Data Elements that combine to form the structure of Data Groups 1 (DG1) through 16 (DG16)

Data Group	EF Name	Short File Identifier	FID	Tag
Common	EF.COM	1E	01 1E	60
DG1	EF.DG1	01	01 01	61
DG2	EF.DG2	02	01 02	75
DG3	EF.DG3	03	01 03	63
DG4	EF.DG4	04	01 04	76
DG5	EF.DG5	05	01 05	65
DG6	EF.DG6	06	01 06	66
DG7	EF.DG7	07	01 07	67
DG8	EF.DG8	08	01 08	68
DG9	EF.DG9	09	01 09	69
DG10	EF.DG10	0A	01 0A	6A
DG11	EF.DG11	0B	01 0B	6B
DG12	EF.DG12	0C	01 0C	6C
DG13	EF.DG13	0D	01 0D	6D
DG14	EF.DG14	0E	01 0E	6E
DG15	EF.DG15	0F	01 0F	6F
DG16	EF.DG16	10	01 10	70
Document Security Object	$EF.SO_D$	1D	01 1D	77
Common	EF.CARDACCESS	1C	01 1C	
Common	EF.ATR/INFO			
Common	EF.CardSecurity	1D	01 1D	

6.1 DATA GROUP 1 — Machine Readable Zone Information (REQUIRED)

The Data Elements of Data Group 1 (DG1) are intended to reflect the entire contents of the MRZ whether it contains actual data or filler characters. Details on the implementation of the MRZ are dependent on the type of eMRTD (TD1,TD2 or TD3 formats).

This Data Element contains the REQUIRED machine readable zone (MRZ) information for the document in template 0x61. The template contains one data object, the MRZ in data object 0x5F1F. The MRZ data object is a composite Data Element, identical to the OCR-B MRZ information printed on the document.

Table 18. Data Group 1 Tags

Tag	**L**	**Value**		
61	Var			
		Tag	**L**	**Value**
		5F1F	F	The MRZ data object as a composite Data Element. (REQUIRED) (The Data Element contains all mandatory fields from Document Type through to Composite check digit.)

6.1.1 DATA GROUP 1 – EF.DG1 Data Elements for TD1 Size eMRTD

This section describes the Data Elements that may be present in Data Group 1 (DG1). Storage, ordering and coding requirements of Data Group 1 are intended to be exactly the same as found in the printed MRZ and described in Doc 9303-3 and Doc 9303-5. Data Elements and their format within each Data Group area for TD1 shall be as in the following table:

Note.— A = Alpha character [A..Z], N = Numeric character [0..9], S = Special character ['<'], F = fixed-length field.

Table 19. Data Elements for TD1 format

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
01	M	Document code	2	F	A,S
02	M	Issuing State or organization	3	F	A,S
03	M	Document number (Nine most significant characters)	9	F	A,N,S
04	M	Check digit — Document number or filler character (<) indicating document number exceeds nine characters	1	F	N,S
05	M	Optional data and/or in the case of a Document Number exceeding 9 characters, least significant characters of document number plus document number check digit plus filler character	15	F	A,N,S
06	M	Date of birth	6	F	N,S
07	M	Check digit — Date of birth	1	F	N
08	M	Sex	1	F	A,S
09	M	Date of Expiry	6	F	N
10	M	Check digit — Date of expiry	1	F	N
11	M	Nationality	3	F	A,S
12	M	Optional data	11	F	A,N,S
13	M	Composite check digit	1	F	N
14	M	Name of holder	30	F	A,N,S

6.1.2 DATA GROUP 1 — EF.DG1 Data Elements for TD2 Size eMRTD

This section describes the Data Elements that may be present in Data Group 1 (DG1). Storage, ordering and coding requirements of Data Group 1 are intended to be exactly the same as found in the printed MRZ and described in Doc 9303-3 and Doc 9303-6. Data Elements and their format within each Data Group area for TD2 shall be as in the following table:

Note.— A = Alpha character [A..Z], N = Numeric character [0..9], S = Special character ['<'], F = fixed-length field.

Table 20. Data Elements for TD2 format

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
01	M	Document code	2	F	A,S
02	M	Issuing State or organization	3	F	A,S
03	M	Name of holder	31	F	A,N,S
04	M	Document number (Nine principal characters)	9	F	A,N,S
05	M	Check digit	1	F	N,S
06	M	Nationality	3	F	A,S
07	M	Date of birth	6	F	N,S
08	M	Check digit	1	F	N
09	M	Sex	1	F	A,S
10	M	Date of expiry	6	F	N
11	M	Check digit	1	F	N
12	M	Optional data plus filler character	7	F	A,N,S
13	M	Composite Check Digit - MRZ line 2	1	F	N

6.1.3 DATA GROUP 1 — EF.DG1 Data Elements for TD3 Size eMRTD

This section describes the Data Elements that may be present in Data Group 1 (DG1). Storage, ordering and coding requirements of Data Group 1 are intended to be exactly the same as found in the printed MRZ and described in Doc 9303-3 and Doc 9303-4. Data Elements and their format within each Data Group area for TD3 shall be as in the following table:

Note.— A = Alpha character [A..Z], N = Numeric character [0..9], S = Special character ['<'], F = fixed-length field.

Table 21. Data Elements for TD3 format

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
01	M	Document code	2	F	A,S
02	M	Issuing State or organization	3	F	A,S
03	M	Name of holder	39	F	A,S
04	M	Document number	9	F	A,N,S
05	M	Check digit — Document number	1	F	N,S
06	M	Nationality	3	F	A,S
07	M	Date of birth	6	F	N,S
08	M	Check digit — Date of birth	1	F	N
09	M	Sex	1	F	A,S
10	M	Date of expiry	6	F	N
11	M	Check digit — Date of expiry or valid until date	1	F	N
12	M	Optional data	14	F	A,N,S
13	M	Check digit	1	F	N
14	M	Composite check digit	1	F	N

6.2 DATA GROUP 2 — Encoded Identification Features — Face (REQUIRED)

Data Group 2 (DG2) represents the globally interoperable biometric for machine assisted identity confirmation with machine readable travel documents, which SHALL be an image of the face of the holder as an input to a face recognition system. If there is more than one recording, the most recent internationally interoperable encoding SHALL be the first entry.

Table 22. Data Group 2 Tags

Tag	L	Value
75	Var	See Biometric encoding of EF.DG2

6.2.1 Biometric encoding of EF.DG2

DG2 MUST use the Biometric Information Template (BIT) group template with nested BITs specified in [ISO/IEC 7816-11], which allows the possibility to store multiple biometric templates and is in harmony with the Common Biometric Exchange File Format (CBEFF). The biometric sub-header defines the type of biometric that is present and the specific biometric feature. The nested option of ISO/IEC [7816-11] is always to be used, even for encodings of a single biometric template. The latter case is indicated by numbering with n=1.

Each nested template has the following structure:

Table 23. Data Group 2 — Biometric Encoding Tags

Tag	L	Value				
7F61	Var	Biometric Information Group Template				
		Tag	**L**	**Value**		
		02	01	Integer — Number of instances of this type of biometric		
		7F60	Var	1st Biometric Information Template		
			Tag	**L**		
			A1	Var	Biometric Header Template (BHT)	
				Tag	**L**	**Value**
				80	02	ICAO header version 0101 (Optional) — Version of the CBEFF patron header format
				81	01-03	Biometric type (Optional)
				82	01	Biometric subtype Optional for DG2

Tag	L	Value				
				83	07	Creation date and time (Optional)
				85	08	Validity period (from through) (Optional)
				86	04	Creator of the biometric reference data (PID) (Optional)
				87	02	Format owner (REQUIRED)
				88	02	Format type (REQUIRED)
			5F2E or 7F2E	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).	

The default OID of CBEFF is used. The OID data object (Tag 0x06) just under Biometric Information Template (BIT, Tag 0x7F60) specified in [ISO/IEC 7816-11] is not included in this structure. Likewise the Tag allocation authority is not specified in the structure.

To facilitate interoperability, the first biometric recorded in each Data Group SHALL be encoded as per [ISO/IEC19794-5].

6.2.2 DATA GROUP 2 — EF.DG2 Data Elements

This section describes the Data Elements that may be present in Data Group 2 (DG2): Data Elements and their format within each Data Group area SHALL be as in the following tables:

Note.— A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 24. Data Elements for DG2

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M	Number of face biometric encodings recorded	1	F	N	1 to 9 identifying number of unique encodings of data on the face.
02	M	Header		Var	A,N	Data Element may recur as defined by DE 01.
03	M	Face biometric data encoding(s)		Var	A,N,S,B	Data Element may recur as defined by DE 01.

6.3 DATA GROUP 3 — Additional Identification Feature — Finger(s) (OPTIONAL)

ICAO recognizes that Member States may elect to use fingerprint recognition as additional biometric technologies in support of machine assisted identity confirmation, which SHALL be encoded as Data Group 3 (DG3).

Table 25. Data Group 3 Tags

Tag	L	Value
63	Var	See Biometric encoding of EF.DG3

6.3.1 Biometric Encoding of EF.DG3

DG3 MUST use the Biometric Information Template (BIT) group template with nested BITs specified in [ISO/IEC 7816-11], which allows the possibility to store multiple biometric templates and is in harmony with the Common Biometric Exchange File Format (CBEFF). The biometric sub-header defines the type of biometric that is present and the specific biometric feature. The nested option of [ISO/IEC 7816-11] MUST be used, even for encodings of a single biometric template. The latter case is indicated by numbering with n=1. The number of instances in DG3 can be '0...n'.

Each nested template has the following structure:

Table 26. Data Group 3 Nested Tags

Tag	L	Value				
7F61	Var	Biometric Information Group Template				
		Tag	**L**	**Value**		
		02	01	Integer — Number of instances of this type of biometric		
		7F60	Var	1st Biometric Information Template		
			Tag	**L**		
			A1	Var	Biometric Header Template (BHT)	
				Tag	**L**	**Value**
				80	02	ICAO header version ‘0101’ (Optional) — Version of the CBEFF patron header format
				81	01-03	Biometric type (Optional)
				82	01	Biometric subtype REQUIRED for DG3
				83	07	Creation date and time (Optional)
				85	08	Validity period (from through) (Optional)
				86	04	Creator of the biometric reference data (PID) (Optional)
				87	02	Format owner (REQUIRED)
				88	02	Format type (REQUIRED)
			5F2E or 7F2E	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).	
		Tag	**L**			
		7F60	X	2nd Biometric Information Template		
			Tag	**L**		
			A1	Var	Biometric Header Template (BHT)	
				Tag	**L**	**Value**
				80	02	ICAO header version ‘0101’ (Optional) — Version of the CBEFF patron header format
				81	01-03	Biometric type (Optional)

Tag	L	Value				
				82	01	Biometric subtype REQUIRED for DG3
				83	07	Creation date and time (Optional)
				85	08	Validity period (from through) (Optional)
				86	04	Creator of the biometric reference data (PID) (Optional)
				87	02	Format owner (REQUIRED)
				88	02	Format type (REQUIRED)
			5F2E or 7F2E	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).	

The default OID of CBEFF is used. The OID data object (Tag 0x06) just under Biometric Information Template (BIT, Tag 0x7F60) specified in [ISO/IEC 7816-11] is not included in this structure. Likewise the Tag allocation Authority is not specified in the structure.

To facilitate interoperability, the first biometric recorded in each Data Group SHALL be encoded as per [ISO/IEC19794-5].

6.3.2 DATA GROUP 3 — EF.DG3 Data Elements

This section describes the Data Elements that may be present in Data Group 3 (DG3). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note.— A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 27. Data Elements for DG3

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If encoded finger(s) feature recorded)	Number of finger(s) biometric encodings recorded	1	F	N	0 to n identifying number of unique encodings of data on the finger(s).
02	M (If encoded finger(s) feature recorded)	Header		Var	B	Data Element may recur as defined by DE 01.
03	M (If encoded finger(s) feature recorded)	Finger biometric data encoding(s)		Var	A,N,S, B	Data Element may recur as defined by DE 01.

6.3.2.1 Biometric sub-type encoding

The biometric header template Tags and their assigned values are the minimum each implementation shall support as shown in the following table. Each single biometric information template has the following structure:

Table 28. Encoding of sub-features scheme for the encoding of sub-features: CBEFF

b8	b7	b6	b5	b4	b3	b2	b1	Biometric Sub-type
0	0	0	0	0	0	0	0	No information given
						0	1	Right
						1	0	Left
			0	0	0			No meaning
			0	0	1			Thumb
			0	1	0			Pointer
			0	1	1			Middle
			1	0	0			Ring
			1	0	1			Little
X	X	X						Reserved for future use

6.3.2.2 Encoding of zero instance

States not issuing eMRTDs with fingerprints SHOULD NOT populate DG3. Data Group 3 of this structure has the drawback that it will result in a static DG3 hash in the SO_D for all eMRTDs where the biometric features are not present and populated at the time of eMRTD issuance, but the DG3 is declared. For interoperability purposes States supporting fingerprints in their eMRTDs MUST store an empty Biometric Information Group Template in cases where no fingerprints are available at the time of eMRTD issuance. The template counter denotes a value of 0x00 in this case.

It is RECOMMENDED to add Tag 0x53 with issuer defined content (e.g. a random number).

Table 29. Encoding zero instances

Tag	**L**	**Value**				
63	Var	LDS element				
		Tag	**L**	**Value**		
		7F 61	03	Biometric Information Group Template		
			02	01	00	Defines that there are no Biometric Information Templates stored in this Data Group.
		53	Var	Issuer defined content (e.g. a random number).		

6.3.2.3 Encoding of one instance

In cases where only one fingerprint is available, the single instance MUST be encoded in the following manner (example for DG3 – fingerprint):

Table 30. Encoding one instance

Tag	**L**	**Value**						
63	aa	LDS element where aa is the total length of the entire LDS data content						
		Tag	**L**	**Value**				
		7F 61	bb	Biometric Information Group Template, where bb is the total length of the entire Group Template content.				
			02	01	01	Defines the total number of fingerprints stored as Biometric Information Templates that follow.		
			7F 60	cc	First biometric information template where cc is the total length of the entire BIT			
				A1	dd	Biometric Header Template, where dd is the total length of the BHT		
					81	01	08	Biometric type “Fingerprint”
					82	01	0A	Biometric subtype “left pointer finger”
					87	02	01 01	Format Owner JTC 1 SC 37
					88	02	00 07	Format Type [ISO/IEC 19794-4]
					Note that the BHT may contain additional optional elements. Of course, this fingerprint can either be a left or right finger depending on the available image.			
				5F 2E	ee	Biometric Data Block where ee is total length of the encoded [ISO/IEC 19794-4] structure. The Biometric Data Block MUST contain exactly one fingerprint image.		

6.3.2.4 Encoding of more than one instance

To achieve interoperability each feature MUST be stored in an individual Biometric Information Template. The feature position MUST be specified within the CBEFF biometric subtype if this information is available. The following table contains a worked example for the CBEFF encoding of an interoperable DG 3 element with two fingerprint images.

Table 31. Encoding greater than one instance

Tag	**L**	**Value**						
63	aa	LDS element where *aa* is the total length of the entire LDS data content						
		Tag	**L**	**Value**				
		7F 61	bb	Biometric Information Group Template, where bb is the total length of the entire Group Template content.				
			02	01	02	Defines the total number of fingerprints stored as Biometric Information Templates that follow.		
			7F 60	cc	First biometric information template where cc is the total length of the entire BIT			
				A1	Dd	Biometric Header Template, where dd is the total length of the BHT		
					81	01	08	Biometric type “Fingerprint”
					82	01	0A	Biometric subtype “left pointer finger”
					87	02	01 01	Format Owner JTC 1 SC 37
					88	02	00 07	Format Type [ISO/IEC 19794-4]
					Note that the BHT may contain additional optional elements. It is also possible that the order of fingerprints (left/right) is different.			
				5F 2E	ee	Biometric Data Block where ee is total length of the encoded [ISO/IEC 19794-4] structure. The Biometric Data Block MUST contain exactly one fingerprint image.		
			7F 60	ff	Second biometric information template where ff is the total length of the entire BIT			
				A1	Gg	Biometric Header Template, where gg is the total length of the BHT		
					81	01	08	Biometric type “Fingerprint”

Tag	L	Value						
					82	01	09	Biometric subtype “right pointer finger”
					87	02	01 01	Format Owner JTC 1 SC 37
					88	02	00 07	Format Type [ISO/IEC 19794-4]
					Note that the BHT may contain additional optional elements. It is also possible that the order of fingerprints (left/right) is different.			
				5F 2E	Hh	Biometric Data Block where hh is total length of the encoded [ISO/IEC 19794-4] structure. The Biometric Data Block MUST contain exactly one fingerprint image.		

6.4 DATA GROUP 4 — Additional Identification Feature — Iris(es) (OPTIONAL)

ICAO recognizes that member States may elect to use iris recognition as additional biometric technologies in support of machine assisted identity confirmation, which SHALL be encoded as Data Group 4 (DG4).

Table 32. Data Group 4 Tags

Tag	L	Value
76	Var	See Biometric encoding of EF.DG4

6.4.1 Biometric encoding of EF.DG4

DG4 MUST use the Biometric Information Template (BIT) group template with nested BITs specified in [ISO/IEC 7816-11], which allows the possibility to store multiple biometric templates and is in harmony with the Common Biometric Exchange File Format (CBEFF). The biometric sub-header defines the type of biometric that is present and the specific biometric feature. The nested option of ISO/IEC [7816-11] MUST be used, even for encodings of a single biometric template. The latter case is indicated by numbering with n=1. The number of instances in DG4 can be ‘0...n’.

Each nested template has the following structure:

Table 33. Data Group 4 Nested Tags

Tag	**L**	**Value**				
7F61	Var	Biometric Information Group Template				
		Tag	**L**	**Value**		
		02	1	Integer — Number of instances of this type of biometric		
		7F60	Var	1st Biometric Information Template		
			Tag	**L**		
			A	Var	Biometric Header Template (BHT)	
				Tag	**L**	**Value**
				80	02	ICAO header version ‘0101’ (Optional) — Version of the CBEFF patron header format
				81	01-03	Biometric type (Optional)
				82	01	Biometric sub-type, REQUIRED for DG4
				83	07	Creation date and time (Optional)
				85	08	Validity period (from through) (Optional)
				86	04	Creator of the biometric reference data (PID) (Optional)
				87	02	Format owner (REQUIRED)
				88	02	Format type (REQUIRED)
			5F2E or 7F2E	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).	
		Tag	**L**			
		7F60	Var	2nd Biometric Information Template		
			Tag	**L**		
			A1	Var	Biometric Header Template (BHT)	
				Tag	**L**	**Value**
				80	02	ICAO header version ‘0101’ (Optional) — Version of the CBEFF patron header format
				81	01-03	Biometric type (Optional)
				82	01	Biometric subtype REQUIRED for DG4

Tag	L	Value				
				83	07	Creation date and time (Optional)
				85	08	Validity period (from through) (Optional)
				86	04	Creator of the biometric reference data (PID) (Optional)
				87	02	Format owner (REQUIRED)
				88	02	Format type (REQUIRED)
			5F2E or 7F2E	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).	

The default OID of CBEFF is used. The OID data object (Tag 0x06) just under Biometric Information Template (BIT, Tag 0x7F60) specified in [ISO/IEC 7816-11] is not included in this structure. Likewise the Tag allocation authority is not specified in the structure.

To facilitate interoperability, the first biometric recorded in each Data Group SHALL be encoded as per [ISO/IEC19794-5].

6.4.2 DATA GROUP 4 — EF.DG4 Data Elements

This section describes the Data Elements that may be present in Data Group (DG4*)*. Data Elements and their format within each Data Group area SHALL be as in the following table:

Note.— A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 34. Data Elements for DG4

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M, if encoded eye(s) feature included	Number of eye biometric encodings recorded	1	F	N	1 to 9 identifying number of unique encodings of data on the eye(s).
02	M, if encoded eye(s) feature included	Header		Var	B	Data Element may recur as defined by DE 01.
03	M, if encoded eye(s) feature included	Eye biometric data encoding(s)		Var	A,N,S,B	Data Element may recur as defined by DE 01.

6.4.2.1 Biometric sub-type encoding

The biometric header template Tags and their assigned values are the minimum each implementation SHALL support as shown in the following table. Each single biometric information template has the following structure:

Table 35. Encoding of sub-features scheme for the encoding of sub-features: CBEFF

b8	b7	b6	b5	b4	b3	b2	b1	Biometric Sub-type
0	0	0	0	0	0	0	0	No information given
						0	1	Right
						1	0	Left
			0	0	0			Reserved for future use
			0	0	1			Reserved for future use
			0	1	0			Reserved for future use
			0	1	1			Reserved for future use
			1	0	0			Reserved for future use
			1	0	1			Reserved for future use
X	X	X						Reserved for future use

6.4.2.2 Encoding of zero instance

States not issuing eMRTDs with irises SHOULD NOT populate DG4. Data Group 4 of this structure has the drawback that it will result in a static DG4 hash in the SO_D for all eMRTDs where the biometric features are not present and populated at the time of eMRTD issuance but the DG4 is declared. For interoperability purposes States supporting irises in their eMRTDs MUST store an empty Biometric Information Group Template in cases where no irises are available at the time of eMRTD issuance. The template counter denotes a value of 0x00 in this case.

It is RECOMMENDED to add Tag 0x53 with issuer defined content (e.g. a random number).

Table 36. Encoding zero instances

Tag	**L**	**Value**				
76	Var	LDS element				
		Tag	**L**	**Value**		
		7F 61	03	Biometric Information Group Template		
			02	01	00	Defines that there are no Biometric Information Templates stored in this Data Group.
		53	Var	Issuer defined content (e.g. a random number).		

6.4.2.3 Encoding of one instance

In cases where only one iris is available, the single instance MUST be encoded.

6.4.2.4 Encoding of more than one instance

To achieve interoperability each feature MUST be stored in an individual Biometric Information Template. The feature position MUST be specified within the CBEFF biometric subtype if this information is available.

6.5 DATA GROUP 5 — Displayed Portrait (OPTIONAL)

Data Elements assigned to Data Group 5 (DG5) SHALL be as follows:

Table 37. Data Group 5 Tags

Tag	**L**	**Value**		
65	Var			
		Tag	**L**	**Value**
		02	Var	Number of instances of this type of displayed image (REQUIRED in first template. Not used in succeeding templates.)
		5F40	Var	Displayed portrait

The following format owners are recognized for the specified type of displayed image.

Table 38. DG5 Formats

Displayed Image	Format Owner
Displayed Facial Image	[ISO/IEC 10918], JFIF option

6.5.1 DATA GROUP 5 — EF.DG5 Data Elements (Optional)

This section describes the Data Elements that may be present in Data Group 5 (DG5). Data Elements and their format within Data Group 5 SHALL be as in the following table:

Note.— A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 39. Data Elements for DG5

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If displayed portrait recorded)	Number of displayed portraits recorded	1	F	N	1 to 9 identifying number of unique recordings of displayed portrait.
02	M (If displayed portrait recorded)	Displayed portrait representation(s)		Var	A,N	Data Element may recur as defined by DE 01.
	M (If displayed portrait recorded)	Number of bytes in representation of displayed portrait	5	F	N	00001 to X9, identifying number of bytes in representation of displayed portrait immediately following.
	M (If displayed portrait recorded)	Representation of displayed portrait		Var	A,N,S,B	Formatted as per [ISO/IEC 10918-1] or [ISO/IEC 15444].

Note.— Data Element 02 SHALL be encoded as defined in [ISO/IEC 10918], using the JFIF option or [ISO/IEC 15444] using JPEG 2000 image coding system.

6.6 DATA GROUP 6 — Reserved for Future Use

Data Elements assigned to Data Group 6 (DG6) SHALL be as follows:

Table 40. Data Group 6 Tags

Tag	L	Value
66	Var	

6.6.1 DATA GROUP 6 — EF.DG6 Data Elements

The data elements for Data Group 6 (DG6) are reserved for future use.

6.7 DATA GROUP 7 — Displayed Signature or Usual Mark (OPTIONAL)

Data Elements assigned to Data Group 7 (DG7) SHALL be as follows:

Table 41. Data Group 7 Tags

Tag	L	Value		
67	Var			
		Tag	**L**	**Value**
		02	Var	Number of instances of this type of displayed image (REQUIRED in first template. Not used in succeeding templates.)
		5F43	Var	Displayed Signature

The following format owners are recognized for the specified type of displayed image:

Table 42. DG7 Formats

Displayed Image	Format Owner
Displayed Signature/usual mark	[ISO/IEC 10918], JFIF option

6.7.1 DATA GROUP 7 — EF.DG7 Data Elements (OPTIONAL)

This section describes the Data Elements that may be present in Data Group 7 (DG7). Data Elements and their format within each Data Group 7 SHALL be as in the following table:

Note.— A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 43. Data Elements for DG7

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If displayed signature or usual mark recorded)	Number of displayed signature or usual marks	1	F	N	1 to 9 identifying number of unique recordings of displayed signature or usual mark.
02	M (If displayed signature or usual mark recorded)	Displayed signature or usual mark representation		Var	A,N,S,B	Data Element may recur as defined by DE 01. Formatted as per [ISO/IEC 10918-1] or [ISO/IEC 15444].

Note.— Data Element 02 SHALL be encoded as defined in [ISO/IEC 10918], using the JFIF option, or [ISO/IEC 15444] using JPEG 2000 image coding system.

6.8 DATA GROUP 8 — Data Feature(s) (OPTIONAL)

This Data Group has yet to be defined. Until then, they are available for temporary proprietary usage. This Data Element could use a structure similar to that for biometric templates, machine assisted security feature verification and encoded detail(s). Data Elements combining to form Data Group 8 (DG8) SHALL be as follows:

Table 44. Data Group 8 Tags

Tag	L	Value		
68	Var	To Be Defined		
		Tag	**L**	**Value**
		02	1	Integer — Number of instances of this type of template (REQUIRED in first template. Not used in succeeding templates.)
			Var	Header Template. Details to be defined.

6.8.1 DATA GROUP 8 — EF.DG8 Data Elements

This section describes the Data Elements that may be present in Data Group 8 (DG8). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note.— A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 45. Data Elements for DG8

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If this encoded feature is used)	Number of data feature(s)	1	F	N	1 to 9, identifying number of unique encodings of data feature(s) (embraces DE 02 through DE 04).
02	M (If this encoded feature is used)	Header (to be defined)	1			Header details to be defined.
03	M (If this encoded feature is used)	Data feature(s) data	999 Max	Var	A,N,S,B	Format defined at the discretion of issuing State or organization.

6.9 DATA GROUP 9 — Structure Feature(s) (OPTIONAL)

This Data Group has yet to be defined. Until then, it is available for temporary proprietary use. These Data Elements could use a structure similar to that for biometric templates. Data Elements combining to form Data Group 9 (DG9) SHALL be as follows:

Table 46. Data Group 9 Tags

Tag	L	Value		
69	Var	To Be Defined		
		Tag	**L**	**Value**
		02	01	Integer — Number of instances of this type of template (REQUIRED in first template. Not used in succeeding templates.)
			X	Header Template. Details to be defined.

6.9.1 DATA GROUP 9 — EF.DG9 Data Elements

Data Group 9 (DG9) Data Elements and their format within each Data Group area SHALL be as in the following table:

Note.— A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 47. Data Elements for DG9

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If this encoded feature is used)	Number of structure feature(s)	1	F	N	1 to 9, identifying number of unique encodings of structure feature(s) (embraces DE 02 through DE 04).
02	M (If this encoded feature is used)	Header (to be defined)			N	Header details to be defined
03	M (If this encoded feature is used)	Structure feature(s) data		Var		

6.10 DATA GROUP 10 — Substance Feature(s) (OPTIONAL)

This Data Group has yet to be defined. Until then, it is available for temporary proprietary usage. These Data Elements could use a structure similar to that for biometric templates. Data Elements combining to form Data Group 10 (DG10) SHALL be as follows:

Table 48. Data Group 10 Tags

Tag	L	Value		
6A	Var			
		Tag	**L**	**Value**
		02	01	Integer — Number of instances of this type of template (REQUIRED in first template. Not used in succeeding templates.)
			Var	To Be Defined.

6.10.1 DATA GROUP 10 — EF.DG10 Data Elements

This section describes the Data Elements that may be present in Data Group 10 (DG10). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note.— A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 49. Data Elements for DG10

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If this encoded feature is used)	Number of substance feature(s) recorded	1	F	N	1 to 9, identifying number of unique encodings of substance feature(s) (embraces DE 02 through DE 04).
02	M (If this encoded feature is used)	Header (to be defined)	TBD	TBD	N	Details to be defined.
03	M (If this encoded feature is used)	Substance feature(s) data	999 Max	Var	A,N,S,B	Format defined at the discretion of issuing State or organization.

6.11 DATA GROUP 11 — Additional Personal Detail(s) (OPTIONAL)

This Data Group is used for additional details about the document holder. Since all of the Data Elements within this group are optional, a Tag list is used to define those present. Data Elements combining to form Data Group 11 (DG11) SHALL be as follows:

Note.— This template may contain non-Latin characters.

Table 50. Data Group 11 Tags

Tag	**L**	**Value**				
6B	Var					
		Tag	**L**	**Value**		
		5C	Var			Tag list with list of Data Elements in the template.
		5F0E	Var			Full name of document holder in national characters. Encoded per Doc 9303 rules.
		A0	Var			Content-specific class
				Tag	**L**	**Value**
				02	01	Number of other names
				5F0F	Var	Other name formatted per Doc 9303. The data object repeats as many times as indicated in number of other names (data object with Tag'02')
		Tag	**L**	**Value**		
		5F10	Var			Personal number
		5F2B	08			Full date of birth yyyymmdd
		5F11	Var			Place of birth. Fields separated by '<'
		5F42	Var			Permanent address. Fields separated by '<'
		5F12	Var			Telephone
		5F13	Var			Profession
		5F14	Var			Title
		5F15	Var			Personal summary
		5F16	Var			Proof of citizenship. Compressed image per [ISO/IEC 10918]
		5F17	Var			Other valid TD numbers. Separated by '<'
		5F18	Var			Custody information

6.11.1 DATA GROUP 11 — EF.DG11 Data Elements

This section describes the Data Elements that may be present in Data Group 11 (DG11). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note 1.— Data Element 11 SHALL be encoded as defined in [ISO/IEC 10918], using the JFIF option or [ISO/IEC 15444] using JPEG 2000 image coding system.

Note 2.— A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 51. Data Elements for DG11

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	O	Name of holder (in full)	99 Max	Var	B	Filler characters (<) inserted as per MRZ. No fillers inserted at end of line. Truncation not permitted.
02	O	Other name(s)	99 Max	Var	B	Filler characters (<) inserted as per MRZ. No fillers inserted at end of line. Truncation not permitted.
03	O	Personal number	99 Max	Var	A,N,S	Free-form text.
04	O	Full date of birth	8	F	B	CCYYMMDD
05	O	Place of birth	99 Max	Var	B	Free-form text.
06	O	Address	99 Max	Var	A,N,S,B	Free-form text.
07	O	Telephone	99 Max	Var	N,S	Free-form text.
08	O	Profession	99 Max	Var	B	Free-form text.
09	M, if DE 08 included	Title	99 Max	Var	B	Free-form text.
10	M, if DE 09 included	Personal summary	99 Max	Var	B	Free-form text.

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
11	M, if DE 10 included	Proof of citizenship		Var	A,N,S,B	Image of citizenship document formatted as per [ISO/IEC 10918-1]
12	O	Other valid travel document(s) Travel document number	99 Max	Var	A,N,S,B	Free-form text, separated by <.
13	O	Custody information	999 Max	Var	B	Free-form text.

Note.— In case the month (MM) or the day (DD) are unknown, the interoperable way to indicate this in DG11 is to set the respective characters to '00'. In case the century and the year (CCYY) are unknown, the interoperable way to indicate this in DG11 is to set the respective characters to '0000'. Issuer-assigned dates must always be used consistently.

6.12 DATA GROUP 12 — Additional Document Detail(s) (OPTIONAL)

This Data Group is used for additional information about the document. All Data Elements within this group are optional.

Table 52. Data Group 12 Tags

Tag	L	Value				
6C	Var					
		Tag	**L**	**Value**		
		5C	Var			Tag list with list of Data Elements in the template
		5F19	Var			Issuing Authority
		5F26	08			Date of issue. yyyymmdd
		A0	Var			Content-specific class
				Tag	**L**	**Value**
				02	01	Number of other persons
				5F1A	Var	Name of other person formatted per Doc 9303 rules. The data object repeats as many times as indicated in number of other names DE02 (data object with Tag'02').

		Tag	L	Value		
		5F1B	Var			Endorsements, observations
		5F1C	Var			Tax/Exit requirements
		5F1D	Var			Image of front of document. Image per ISO/IEC 10918
		5F1E	Var			Image of rear of document. Image per ISO/IEC 10918
		5F55	0E			Date and time of document personalization yyyymmddhhmmss
		5F56	Var			Serial number of personalization system

It is RECOMMENDED that Inspection Systems support both 8 bytes ASCII and BCD date/time encoding.

6.12.1 DATA GROUP 12 — EF.DG12 Data Elements

This section describes the Data Elements that may be present in Data Group 12 (DG12). Data Elements and their format within each Data Group SHALL be as in the following table:

Note 1.— A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Note 2.— Data Elements 07 and 08 SHALL be encoded as defined in [ISO/IEC 10918], using the JFIF option or [ISO/IEC 15444] using JPEG 2000 image coding system.

Table 53. Data Elements for DG12

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	O	Issuing Authority	99 Max	Var	B	Free-form text.
02	O	Date of issue	8	F	N	Date of issue of document; i.e. YYYYMMDD.
03	O	Other person(s) details	99 Max	Var	B	Free-form text
04	O	Endorsement(s)/ Observation(s)	99 Max	Var	B	Free-form text.
05	O	Tax/Exit requirements	99 Max	Var	B	Free-form text.
06	O	Image of front of MRTD		Var	A,N,S,B	Formatted as per [ISO/IEC 10918-1]

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
07	O	Image of rear of MRTD		Var	A,N,S,B	Formatted as per [ISO/IEC 10918-1]
08	O	Personalization Time	14	F	N	ccyymmddhhmmss
09	O	Personalization device serial number	99 max	Var	A,N,S	Free format.

6.13 DATA GROUP 13 — Optional Details(s) (OPTIONAL)

Data Elements combining to form Data Group 13 (DG13) are at the discretion of the issuing State or organization and SHALL be as follows:

Table 54. Data Group 13 Tags

Tag	L	Value
'6D'	Var	

6.14 DATA GROUP 14 — Security Options (CONDITIONAL)

Data Group 14 contains security options for additional security mechanisms. For details see Doc 9303-11. The file DG14 contained in the ePassport Application is REQUIRED if Chip Authentication Mapping or PACE-GM/-IM is supported by the eMRTD chip.

Table 55. Data Group 14 Tags

Tag	L	Value
6^E	Var	Refer to Doc 9303-10 Data Group 14 SecurityInfos

6.14.1 DATA GROUP 14 — EF.DG14 Data Elements

This section describes the Data Elements that may be present in Data Group 14 (DG14). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note.— A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 56. Data Elements for DG14

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
	O	SecurityInfos		Var	B	Refer to Doc 9303-10. Data Group 14 SecurityInfos as defined in 6.14.2

6.14.2 *DATA GROUP 14 SecurityInfos*

The following generic ASN.1 data structure SecurityInfos allows various implementations of security options for secondary biometrics. For interoperability reasons, it is RECOMMENDED that this data structure be provided by the eMRTD chip in DG14 to indicate supported security protocols. The data structure is specified as follows:

```
      SecurityInfos     ::=   SET of SecurityInfo

      SecurityInfo      ::=   SEQUENCE {
            protocol          OBJECT IDENTIFIER,
            requiredData      ANY DEFINED BY protocol,
            optionalData      ANY DEFINED BY protocol OPTIONAL
}
```

The elements contained in a SecurityInfo data structure have the following meaning:

- The object identifier protocol identifies the supported protocol;
- The open type requiredData contains protocol specific mandatory data;
- The open type optionalData contains protocol specific optional data.

6.15 DATA GROUP 15 — Active Authentication Public Key Info (CONDITIONAL)

This OPTIONAL Data Group contains the Active Authentication Public Key and is REQUIRED when implementing the optional Active Authentication chip authentication as described in Doc 9303-11.

Table 57. Data Group 15 Tags

Tag	L	Value
6F	Var	Refer to Doc 9303-11

6.15.1 *DATA GROUP 15 — EF.DG15 Data Elements*

This section describes the Data Elements that may be present in Data Group 15 (DG15). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note.— A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 58. Data Elements for DG15

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
	O	ActiveAuthentication PublicKeyInfo		Var	B	See Doc 9303-11

6.16 DATA GROUP 16 — Person(s) to Notify (OPTIONAL)

This Data Group lists emergency notification information. It is encoded as a series of templates using the Tag 'Ax' designation. DG16 (as all other Data Groups) should not be updated after issuance; DG16 is represented by a hash value in the SO_D and the SO_D is only signed once at issuance.

Table 59. Data Group 16 Tags

Tag	L	Value		
70	Var			
		Tag	**L**	**Value**
		02	01	Number of templates (occurs only in first template)
		Ax	Var	Start of template, where x (x=1,2,3…) increments for each occurrence
5F50	04			Date data recorded
5F51	Var			Name of person
5F52	Var			Telephone
5F53	Var			Address

6.16.1 DATA GROUP 16 — EF.DG16 Data Elements

This section describes the Data Elements that may be present in Data Group 16 (DG16). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note.— A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B= 8-bit Binary data (any other than A, N or S), F = fixed-length field, Var = variable-length field.

Table 60. Data Elements for DG16

Data Element	Optional or REQUIRED	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M, if DG 16 included	Number of persons identified	2	F	N	Identifies number of persons included in the Data Group.
02	M, if DG 16 included	Date details recorded	8	F	N	Date notification date recorded; Format = CCYYMMDD.
03	M, if DG 16 included	Name of person to notify Primary and secondary identifiers		Var	B	Filler characters (<) inserted as per MRZ. Truncation not permitted.
04	M, if DE 03 included	Telephone number of person to notify		Var	N,S	Telephone number in international form (country code and local number).
05	M	Address of person to notify		Var	B	Free-form text.

7. REFERENCES (NORMATIVE)

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*

ISO/IEC 14443-3 ISO/IEC 14443-3:2016, *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 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 7816-2 ISO/IEC 7816-2:2007, *Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimensions and location of the contacts*

ISO/IEC 7816-4 ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

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

ISO/IEC 7816-6	ISO/IEC 7816-6:2016, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange (Defect report included)*
ISO/IEC 7816-11	ISO/IEC 7816-11:2004, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*
ISO/IEC 8825-1	ISO/IEC 8825-1:2008, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*
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 10646	ISO/IEC 10646:2012*, Information technology — Universal Coded Character Set (UCS)*
RFC 3369	Cryptographic Message Syntax 2002
ISO/IEC 10918-1	ISO/IEC 10918-1:1994, *Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines*
ISO/IEC 15444	ISO/IEC 15444-n, *JPEG 2000 image coding system*
ISO/IEC 19785	ISO/IEC 19785-n, *Information technology — Common Biometric Exchange Formats Framework*

— — — — — — — —

Appendix A to Part 10

LOGICAL DATA STRUCTURE MAPPING EXAMPLES (INFORMATIVE)

The following informative text describes examples of mapping of the Logical Data Structure (LDS v1.7) using a random access representation to a contactless integrated circuit on an eMRTD.

A.1 EF.COM COMMON DATA ELEMENTS

The following example indicates an implementation of LDS Version 1.7 using Unicode Version 4.0.0 having Data Groups 1 (tag '61'), 2 (tag '75'), 4 (tag '76'), and 12 (tag '6C') present.

For this and all other examples, the Tags are printed in **bold**, the Lengths printed *italics*, and the Values are printed in roman. Hexadecimal Tags, lengths and values are in quote marks ('xx').

'60' *'16'*
'5F01' *'04'* '0107'
'5F36' *'06'* '040000'
'5C' *'04'* '6175766C'

The example would read in full hexadecimal representation as:

'60' *'16'*
'5F01' *'04'* '30313037'
'5F36' *'06'* '303430303030'
'5C' *'04'* '6175766C'

A hypothetic LDS Version 15.99 would be encoded as:

'60' *'16'*
'5F01' *'04'* '1599'
'5F36' *'06'* '040000'
'5C' *'04'* '6175766C'

or hexadecimal:

'60' *'16'*
'5F01' *'04'* '31353939'
'5F36' *'06'* '303430303030'
'5C' *'04'* '6175766C'

A.2 EF.DG1 MACHINE READABLE ZONE INFORMATION

A.2.1 TD1 Size eMRTD

An example of the DG1 using this information in a TD1 size eMRTD is shown below. The length of the MRZ data element is 90 bytes ('5A').

'61' *'5D'* **'5F1F'** *'5A'*

```
I<NLDXI85935F86999999990<<<<<<7208148F1108268NLD<<<<<<<<<<<4VAN<DER<STEEN<<MARI
ANNE<LOUISE
```

A.2.2 TD2 Size eMRTD

An example of the DG1 using this information in a TD2 size eMRTD is shown below. The length of the MRZ data element is 72 bytes ('48').

'61' *'4B'* **'5F1F'** *'48'*

```
I<ATASMITH<<JOHN<T<<<<<<<<<<<<<<<<<<<<<<<<<<123456789<HMD7406222M10123130121<<<54
```

A.3 EF.DG2 TO EF.DG4 BIOMETRIC TEMPLATES

DG2 to DG4 use the nested off-card option of [ISO/IEC 7816-11] to have the possibility to store multiple biometric templates of a kind which are in harmony with the Common Biometric Exchange File Format (CBEFF), [NISTR 6529a]. The biometric sub-header defines the type of biometric that is present and the specific biometric feature.

Example: One signed, facial biometric with the biometric data block length of 12 642 bytes ('3162' bytes), encoded using a device with a PID of '00 01 00 01', using format type '00 04' owned by template provider '00 0A' was captured on 15 March 2002 (no UTC offset) and is valid from 1 April 2002 through 31 March 2007. ICAO patron template Version 1.0 is being used.

The total length of the template is 12 704 bytes. The template is stored starting at the beginning of EF.DG2 (SFID 02).

'75' *'82319EC'*
- **'7F61'** *'823199'*
  - **'02'** *'01'* '01'
  - **'7F60'** *'823191'*
  - **'A1'** *'26'*
    - **'80'** *'02'* '0101'
    - **'81'** *'01'* '02'
    - **'83'** *'07'* '20020315133000'
    - **'85'** *'08'* '2002040120070331'
    - **'86'** *'04'* '00010001'
    - **'87'** *'02'* '000A'
    - **'88'** *'02'* '0004'
  - **'5F2E'** *'823162'* '… 12 642 bytes of biometric data …'

A.4 EF.DG5 TO EF.DG7 DISPLAYED IMAGE TEMPLATES

Note.— One EF for each DG.

Example: Image template with the displayed image data length of 2 000 bytes. The length of the template is 2 008 bytes (‘07D8’).

‘65’ *‘8207D8’*
‘02’ *‘01’* 1
‘5F40’ *‘8207D0’* ‘….2 000 bytes of image data …’

A.5 EF.DG11 ADDITIONAL PERSONAL DETAILS

The following example shows the following personal details: Full name (John J. Smith), Place of birth (Anytown, MN), Permanent address (123 Maple Rd, Anytown, MN), Telephone number 1-612-555-1212 and Profession (Travel Agent). The length of the template is 99 bytes (*‘63’*).

‘6B’ *‘63’*
‘5C’ *‘0A’* **‘5F0E’ ‘5F11’ ‘5F42’ ‘5F12’ ‘5F13’**
‘5F0E’ *‘0D’* SMITH<<JOHN<J
‘5F11’ *‘0A’* ANYTOWN<MN
‘5F42’ *‘17’* 123 MAPLE RD<ANYTOWN<MN
‘5F12’ *‘0E’* 16125551212
‘5F13’ *‘0C’* TRAVEL<AGENT

A.6 EF.DG16 PERSON(S) TO NOTIFY

Example with two entries: Charles R. Smith of Anytown, MN and Mary J. Brown of Ocean Breeze, CA. The length of the template is 162 bytes (‘A2’).

‘70’ *‘81A2’*

‘02’ *‘01’* 2
‘A1’ ‘4C’
‘5F50’ *‘08’* 20020101
‘5F51’ *‘10’* SMITH<<CHARLES<R
‘5F52’ *‘0B’* 19525551212
‘5F53’ *‘1D’* 123 MAPLE RD<ANYTOWN<MN<55100
‘A2’ ‘4F’
‘5F50’ *‘08’* 20020315
‘5F51’ *‘0D’* BROWN<<MARY<J
‘5F52’ *‘0B’* 14155551212
‘5F53’ *‘23’* 49 REDWOOD LN<OCEAN BREEZE<CA<94000

— — — — — — — —

Appendix B to Part 10

THE CONTACLESS IC IN AN eMRP (INFORMATIVE)

B.1 The Antenna Size and Class of an eMRTD

The antenna size is at the discretion of the issuing State. With the exception of the antenna size, the eMRTD SHALL fulfil all tests specified in [ISO/IEC 18745-2] applying the Class 1 specifications.

Note.— [ISO/IEC 14443-2] has elaborated the Class 1 requirements for maximum interoperability. In [ISO/IEC 14443-2] and [ISO/IEC 10373-6], a contactless object claiming no class is always tested against Class 1.

It is RECOMMENDED for eMRTDs to be also compliant with Class 1 specifications, including with its antenna size specification, see B.8 below, since eMRTDs not compliant with Class 1 specifications may result in interoperability issues.

For **TD3** size eMRTDs (i.e. ID-3), the eMRTD SHALL contain an antenna together with an integrated circuit (IC) which are together compliant with Class 1 as defined in [ISO/IEC 14443-1] and [ISO/IEC 14443-2] with the exception of the antenna size. There is no mandatory position of the IC, which MAY be placed in an arbitrary position. The location of the contactless antenna is at the discretion of the issuing State as long as it is in one of the following locations:

Data page —	IC and antenna within the structure of a data page forming an internal page;
Centre of booklet —	Placing the IC and its antenna between the centre pages of the book;
Cover —	Placement within the structure or construction of the cover;
Separate sewn-in page —	Incorporating the IC and its antenna into a separate page, which MAY be in the form of an ID3 size plastic card, sewn into the book during its manufacture; or
Back cover —	Placement within the structure or construction of the back cover.

Note.— There had previously been no mandatory position of the antenna in the past editions of Doc 9303.

B.2 Booting and polling

An eMRTD brought to an alternate magnetic field of 1.5 A/m as measured in [ISO/IEC 18745-2] is strongly RECOMMENDED to be able to respond to any REQ/WUP appropriate to its Type after an unmodulated alternate magnetic field of 5 ms.

Note.— For the eMRTD associated Inspection System, it is required that 10 ms of unmodulated carrier shall be provided for legacy reasons. However, it may be desirable for eMRTDs to also communicate with other contactless Inspection Systems and mobile devices, e.g. NFC smartphones use 5 ms.

B.3 Anticollision and Type

The eMRTD MAY either declare compliance with Type A or with Type B as defined in [ISO/IEC 14443-2]. It SHALL not change its Type unless it has been reset by the eMRTD associated Inspection System.

B.4 Mandatory Bit rates

The eMRTD SHALL provide at least the following bit rates, as defined in [ISO/IEC 14443-2], mandatorily: 106 kbit/s and 424 kbit/s in both directions between the eMRTD and the eMRTD associated Inspection System.

B.5 Electromagnetic disturbance (EMD)

The support of EMD is not mandatory.

Note.— The EMD feature enhances the robustness of the contactless communication between the eMRTD and the eMRTD associated Inspection System against eMRTD generated electromagnetic disturbance. The eMRTD dynamic current consumption during execution of a command may cause an arbitrary load modulation effect (which may not be purely resistive) on the magnetic field. In some cases, the eMRTD associated Inspection System may misinterpret EMD as data sent by the eMRTD, and this may negatively impact proper reception of the eMRTD response.

B.6 (Optional) Bit rates

The bit rate of 212 kbit/s, and all bit rates from 848 kbit/s up to 6.78 Mbit/s for both directions, and from 10.17 Mbit/s to 27.12 Mbit/s from the eMRTD associated Inspection System to the eMRTD, as defined in [ISO/IEC 14443-2], are optional. The applicant of this Application Profile SHALL declare its supported bit rates in the applicant declaration table for appropriate testing.

Note 1.— The Support of Exchange of Additional Parameters is mandatory for bit rates higher than 848 kbit/s.

Note 2.— Backwards compatibility is fully provided since the eMRTD associated Inspection System solely selects the bit rate it supports.

B.7 (Optional) Support of Exchange of Additional Parameters

The eMRTD MAY support the exchange of additional parameters as defined in [ISO/IEC 14443-4] in order to negotiate bit rates higher than 106 kbit/s. It MAY also use the same additional parameters to negotiate frames with error correction as specified in[ISO/IEC 14443-4].

B.8 Antenna Size and Class

It is RECOMMENDED to follow the rules for the antenna position as defined in [ISO/IEC 14443-1] and [ISO/IEC 14443-2] for Class 1.

B.9 Shielding

It is RECOMMENDED to not shield any page of the eMRTD.

B.10 (Recommended) Unique Identifier (UID) and Pseudo-unique PICC identifier (PUPI)

The eMRTD MAY provide a random or fixed UID/PUPI as defined in [ISO/IEC 14443-3].

It is RECOMMENDED to use a random UID/PUPI to enhance the eMRTD holder's privacy and to reduce the possibility of tracking.

Note.— A random UID/PUPI has been RECOMMENDED in all editions of Doc 9303.

B.11 (Recommended) Node address (NAD)

It is RECOMMENDED to support NAD.

Note.— NAD may be used for multiple contactless cards and eMRTDs in one field, or multiple hosts within one Inspection System.

B.12 (Recommended) Card identifier (CID)

The eMRTD SHOULD support CID.

B.13 (Recommended) Resonance Frequency Range

Although there is no requirement on the resonance frequency, some applicants of this Application Profile MAY limit their resonance frequency by default to a certain range to increase interoperability. In such case, this range SHOULD be provided to the test house together with all other features in the applicant declaration table which is found in [ISO/IEC 18745-2].

B.14 (Recommended) Frame Sizes

The eMRTD MAY support frame sizes of up to 4 kbyte according to [ISO/IEC 14443]. However, it is RECOMMENDED to support frame sizes of at least 1 kbyte. If supporting frame sizes higher than 1 kbyte, the use of frames with error correction as defined in [ISO/IEC 14443-4] is RECOMMENDED.

Note.— A higher frame size substantially decreases the total processing time of an eMRTD application.

B.15 (Recommended) Frame Waiting Time Integer (FWI) and S-block Request for Waiting Time Extension [S(WTX)]

It is strongly RECOMMENDED for the eMRTD to set an FWI value of less or equal to 11 in order to enhance performance. It is strongly RECOMMENDED to use S(WTX) commands to extend the Frame Waiting Time for each particular command that requires additional time by using S(WTX) commands of an WTXM no greater than 10.

In case multiple S(WTX) requests are sent by the eMRTD, the total processing time for the current I-Block is RECOMMENDED to not exceed 5s.

Note.— Lower FWI values as RECOMMENDED herein decrease the loss of time in transmission errors substantially, whereas S(WTX) are the ideal means of providing more time when needed.

— — — — — — — —

Appendix C to Part 10

INSPECTION SYSTEMS (INFORMATIVE)

C.1 Operating Volume and Test Positions

An eMRTD associated Inspection System SHALL have an operating volume in accordance with one of the defined Inspection System types in [ISO/IEC 18745-2]. The operating volume is the volume in which all requirements of this technical report are fulfilled.

Note.— The test positions for each Inspection System Type are further specified in [ISO/IEC 18745-2] with respect to the (device) 0 mm surface of the eMRTD associated Inspection System.

C.2 Particular Waveform and RF Requirements

The waveforms of the alternate magnetic field used to communicate SHALL be fully compliant with [ISO/IEC 14443-2]. In general, there are no exceptions or divergences from the basic standard, except for the field strength.

For eMRTD associated Inspection Systems of Type 1, 2 and 3, the field strength is strongly RECOMMENDED to be at least 2 A/m at all positions for Class 1. For eMRTD associated Inspection Systems of Type M, the field strength SHALL be at least 1.5 A/m at all positions for Class 1.

Note.— It may be desirable for eMRTDs to also communicate with other contactless Inspection Systems and mobile devices, e.g. NFC smartphones use 1.5 A/m.

C.3 Polling Sequences and eMRTD Detection Time

The polling sequence of the eMRTD associated Inspection System SHALL provide 10 ms of unmodulated carrier before any REQA/WUPA or REQB/WUPB.

For fast detection and processing, the eMRTD Inspection System:

- SHALL poll for Type A and Type B with an equal occurrence of requests for both Types;
- for Inspection System Types 1, 2 and 3, one RF reset SHOULD occur in between any REQ/WUP of the same type;
- SHALL guarantee at least one polling command for both Type A and Type B within 150 ms for an eMRTD present in the minimum mandatory operating volume according [ISO/IEC !8745- 2] at any position.

The eMRTD Inspection System MAY poll for contactless products of any other modulation type on the carrier of 13.56 MHz as long as all the requirements above are fulfilled.

Note.— The unmodulated carrier of 10 ms is required to detect all eMRTDs in the field and is based on former specifications.

C.4 Mandatory Bit rates

The eMRTD associated Inspection System SHALL provide the following bit rates, as defined in [ISO/IEC 14443-2] mandatorily: 106 kbit/s and 424 kbit/s in both directions from the eMRTD to the eMRTD associated Inspection System and vice versa.

C.5 Frame Sizes

The eMRTD associated Inspection System

- of Types 1, 2, and 3 are strongly RECOMMENDED to support all defined frame sizes of up to 256 byte,
- of Type M has no mandatory requirement on frame sizes.

Note.— All sizes in between the minimum and maximum are not tested explicitly in [ISO/IEC 18745-2:2016].

C.6 The Contactless Interface of Mobile Inspection Systems of Type M

If a mobile device is used to read eMRTDs of any size, it is of Type M. In that case, the centre position of the Inspection System is defined as the position on the surface of the Inspection System with the highest field strength when measured for Class 1. eMRTD associated Inspection Systems of Type M SHALL provide sufficient guidance for the user to place the eMRTD correctly on the device.

C.7 Electromagnetic disturbance (EMD)

The support of EMD is not mandatory.

Note.— The EMD feature enhances the robustness of the contactless communication between the eMRTD and the eMRTD associated Inspection System against eMRTD generated electromagnetic disturbance. The eMRTD dynamic current consumption during execution of a command may cause an arbitrary load modulation effect (which may not be purely resistive) on the magnetic field. In some cases, the eMRTD associated Inspection System may misinterpret EMD as data sent by the eMRTD and this may negatively impact proper reception of the eMRTD response.

C.8 Supported Antenna Classes

The eMRTD associated Inspection System of Type 1 and Type 2 SHALL at least support Class 1 eMRTDs in the operating volume.

In order to have a migration period, Class 2 and Class 3 are not mandatory on all positions as mandated by the basic standard. Since non-eMRTD projects may use Class 2 and Class 3, as a minimum the eMRTD Inspection System of Type 1 and Type 2 SHALL support in addition Class 2 and Class 3 in the sole particular position defined in the Figure C-1.

The eMRTD associated Inspection System of Type 3 SHALL support Class 1, Class 2 and Class 3 on its sole central position.

The eMRTD associated Inspection System of Type M SHALL support Class1, Class 2 and Class 3 antennas on its central position.

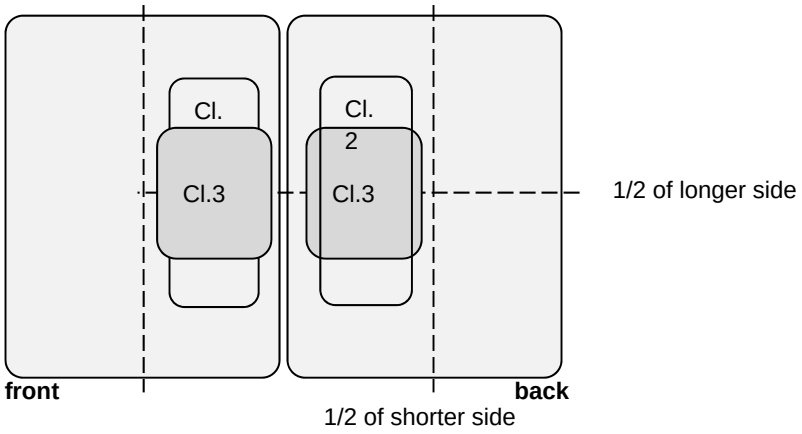

Figure C-1. Mandatory positions in each ID-3 surface in which a Class 2 and Class 3 antenna SHALL be read by an eMRTD associated Inspection System of Type 1 and 2.

C.9 (Optional) Frame Sizes and Error Correction

The eMRTD associated Inspection System MAY optionally support all frame sizes of up to 4 kbyte as defined in [ISO/IEC 14443-3]. It is RECOMMENDED to use frames with error correction as defined in [ISO/IEC 14443-3] for all supported frame sizes higher than 1 kbyte.

Note.— For eMRTD associated Inspection Systems of Type M, frame sizes higher than the 256 byte are currently not envisaged.

C.10 (Optional) Support of Additional Classes

eMRTD associated Inspection Systems of all Types MAY in addition support Class 4, Class 5 and Class 6 to be interoperable, for example, with mobile devices providing less coupling to the eMRTD associated Inspection System antenna coil.

C.11 (Optional) Bit rates

The bit rate of 212 kbit/s, and all bit rates from 848 kbit/s up to 6.78 Mbit/s for both directions and from 10.17 Mbit/s to 27.12 Mbit/s from eMRTD associated Inspection System to eMRTD as defined in [ISO/IEC 14443-2], are optional.

*Note 1.— The Support of Exchange of Additional Parameters is mandatory to use bit rates higher than 848 kbit/*s.

Note 2.— Backwards compatibility is fully provided in the feature of Additional Parameters.

C.12 (Recommended) Operating Temperature

It is RECOMMENDED that the eMRTD associated Inspection System works with temperatures of -10° to 50° Celsius.

C.13 (Recommended) Support of Multiple eMRTDs and other cards or objects or Multiple Hosts

It is highly RECOMMENDED to design the eMRTD associated Inspection System to handle more than one eMRTD, or one eMRTD and any other card or object compliant with [ISO/IEC 14443].

One of the following rules or a combination MAY be applied, among others:

- Apply full anticollision algorithms defined in [ISO/IEC 14443-3];
- Check for support of [ISO/IEC 14443-4] and dismiss all non-supporting cards;
- Check for an eMRTD application;
- Use CID and NAD.

Note.— NAD may be also used for mobile devices with multiple hosts.

C.14 (Recommended) Frame Sizes

The eMRTD associated Inspection System MAY support frame sizes of up to 4 kbyte according to [ISO/IEC 14443-3]. However, it is RECOMMENDED to support frame sizes of at least 1 kbyte. If supporting frame sizes of 1 kbyte or higher, the use of frames with error correction as defined in [ISO/IEC 14443-4] is RECOMMENDED.

It is RECOMMENDED to perform any splitting of payload from the application layer into a minimum number of frames with an effective length of the maximum supported frame size with the exception of the last frame.

C.15 (Recommended) Error Recovery

Subsequent to a transmission error or an unresponsive eMRTD, it is strongly RECOMMENDED for the eMRTD associated Inspection System to send a second R(NAK) according to the Inspection System rule 4 of [ISO/IEC 14443-4].

C.16 (Recommended) Error Detecting and Recovery Mechanism

When using the optional bit rates as well as optional frame sizes of higher than 256 byte, in case of a higher than usual number of transmission errors, it is RECOMMENDED to reduce the bit rate and effective frame size.

— END —

ISBN 978-92-9249-798-9