MACHINE READABLE TRAVEL DOCUMENTS

(Logo)

TECHNICAL REPORT

DEVELOPMENT
OF A
LOGICAL DATA STRUCTURE - LDS
For
OPTIONAL CAPACITY EXPANSION TECHNOLOGIES

Revision –1.7
Published by authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Revision History

Revision	Date	Description
1.0	Apr 2003	Initial release
1.5	Jan 05, 2004	Errata, update to reflect • Data security methodology • Optical and sequential mapping relegated to informative • Contact IC mapping relegated to informative • Removal of fingerprint image • Update of CBEFF template structure • Update of references • Editorial corrections
1.5AA	March 19, 2004	All comments received to date, post NTWG meetings Den Haag
1.6	March 25, 2004	Combined version of 1.5A (US) and 1.5a2 (NL/D), Results Fredericksburg
1.7	May 18, 2004	Incorporates the errata corrections from TAG 15

FOREWORD

The International Civil Aviation Organization published the first edition of Doc 9303 in 1980. Titled *A Passport with Machine Reading Capability*, this document contained specifications and guidance material solely for machine readable passports and was the basis for ISO Standard 7501 (1985).

During the 1990s, Doc 9303 was expanded to cover a family of machine readable travel documents and is now issued in separate parts. Part 1, *Machine Readable Passports*, contains the basic specifications of the 1980 edition, integrated with ISO Standard 7501 (1985) and updated in the light of technological developments and experience by the ICAO consultative body now known as the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD). The technical specifications sections of the previous editions of Part 1, Part 2 (*Machine Readable Visas*), and Part 3 (*Size 1 and Size 2 Machine Readable Official Travel Documents*) have been endorsed by the International Organization for Standardization as ISO/IEC Standards 7501-1, 7501-2, and 7501-3, respectively. Part 4 (*Machine Readable Crew Member Certificate*) was not submitted for ISO endorsement since its specifications are technically a subset of Part 3.

As developmental work on Parts 2, 3 and 4 proceeded, the design concepts evolved, and it was believed that some of the new concepts incorporated in the more recently completed parts could also be applied to those issued earlier; for example, the flexibility of layout in the visual inspection zone that has been permitted in the specifications for visas and official travel documents could well be extended to the specifications for passports. Moreover, there are many features that are common to every document in the family, and the contents of the various parts have many similarities. Therefore, the fourth edition of Doc 9303, Part 1, is the result of a comprehensive review of the four parts, with the objective of harmonizing them to the maximum extent.

In addition to expanded and enhanced specifications and guidance material on matters such as naming conventions, transliteration of national characters in the machine readable zone and the calculation of check digits, a number of new concepts have been introduced to reflect the most recent work of the TAG/MRTD in the light of technological progress. With the introduction of a specification for placement of a bar code on the data page, States now have the option of expanding the machine readable passport's storage capacity for machine readable data, which may be used in machine-assisted identity confirmation and machine-assisted verification of document security. Further, the specifications for a "passport card", previously presented as a Size-3 document, have been replaced with a provision for issuing the passport as a wallet-size card in accordance with the specifications for the Size-1 machine readable official travel document as set forth in Doc 9303, Part 3.

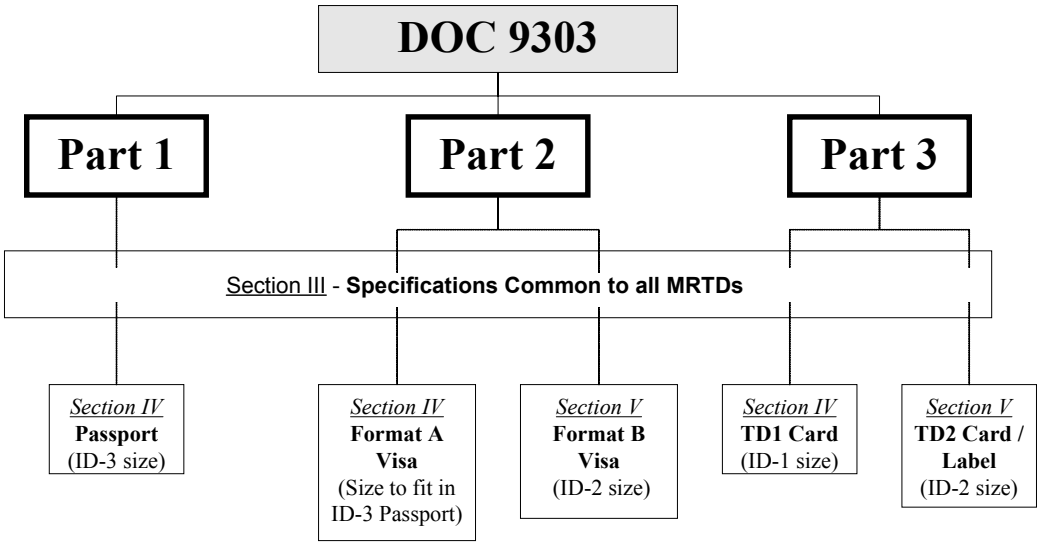
A concept that is highlighted in the fourth edition is that of "global interoperability". In this context, the term is understood as the capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs.

I. INTRODUCTION

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

In 1984, ICAO established what is now known as the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), comprised of government officials who specialize in the issuance of passports and other travel documents, in order to update and enhance the specifications which had been prepared by the Panel. Subsequently, this group's terms of reference were expanded to include, first, the development of specifications for a machine readable visa and, later, specifications for machine readable cards that may be used as official travel documents. Doc 9303 is now published in separate parts, one for each type of document.

In 1997 the TAG/MRTD commenced a comprehensive revision of Doc 9303, Parts 1, 2 and 3. In this revision process the structure and organization of the three parts have been harmonized in order to ease implementation by issuing States and Organizations. Each part of Doc 9303 contain a section which outlines the specifications which are common to all types of machine readable travel documents, followed by one or more sections detailing the specifications unique to the type of travel document addressed in the particular part. This familial relationship among the three parts of Doc 9303 is demonstrated in the following diagram.



During the revision of Doc 9303 TAG/MRTD determined that a State or organization might wish to expand the machine readable data capacity of the MRTD beyond that defined for global interchange (optical character reading of the MRZ), for such purposes as providing machine readable access to breeder document information (e.g. birth certificate details), stored personal identity confirmation and/or document authenticity verification details. Since *co-existence* of an optional machine readable data storage technology with the *mandatory OCR technology* is critical to ensure global interoperability of the MRTD, specifications where developed governing the location of the capacity expansion technologies (i.e. magnetic stripe, IC(s) with contacts, contactless IC(s), optical memory and bar code(s)) on a MRTD. These specifications have been included in the new editions of each Part of Doc 9303.

To ensure global interoperability for machine reading of stored details, TAG/MRTD initiated the development of a standardized organization of data ("Logical Data Structure" or 'LDS' as referred to herein) for the recording of details in a capacity expansion technology. As part of this work, unique 'mappings' – *ways of storing the Logical Data Structure* - were developed to ensure optimal recording for each capacity expansion technology, as well as compliance with published International Standards specific to that technology.

Given the lengthy time required to develop the LDS and the various technology specific mappings; the importance ICAO places on proactively supporting the needs of Member States and their solution providers by sharing information on planned developments in advance of publication of specifications in Doc 9303; and the need to establish a sense of order, which is important for achieving and maintaining global interoperability during this period of development, ICAO has decided to publish a Technical Report in advance of publication of formal specifications for the LDS in future Editions of Doc 9303 as follows:

- Technical Report: Development of a Logical Data Structure (LDS) For Optional Capacity Expansion Technologies

GENERAL CONSIDERATIONS

ICAO's leadership role

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

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

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

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

Under this mandate, ICAO develops and maintains international standards in Annex 9 to the Convention *(Facilitation)* for implementation by Contracting States. In the development of such standards, it is a fundamental precept that if public authorities are to offer facilitation benefits to the vast majority of air travelers, those authorities must have a satisfactory level of confidence in the reliability of travel documents and in the effectiveness of inspection procedures. The production of standardized specifications for travel documents is aimed at building that confidence.

For these reasons, the Council of ICAO has affirmed that work on specifications for travel documents is an appropriate part of the work programme for the Organization. Nevertheless, ICAO is prepared to cooperate with any other international organization that might wish to promote the use of MRTDs. In addition to the International Organization for Standardization (ISO), consultants to the TAG/MRTD include the International Air Transport Association (IATA), the Airports Council International (ACI), and the International Criminal Police Organization (INTERPOL).

Relative costs and benefits of machine readable travel documents

Experience with the issuance of machine readable passports, in conformity with the specifications set forth in Doc9303, Part 1, indicates that the cost of producing MRTDs may be no greater than that of producing conventional documents. As traffic volumes grow and more States focus on how they can rationalize their clearance processes with the employment of computerized databases and electronic data interchange, the MRTD plays a pivotal part in modern, enhanced compliance systems. Equipment to read the documents and access the databases may entail a substantial investment, but this can be expected to be returned by the improvements in security, clearance speed and accuracy of verification that such systems provide. Use of MRTDs in automated clearance systems may also make it possible for States to eliminate both the requirement for paper documents, such as passenger manifests and embarkation/disembarkation cards, and the administrative costs associated with the related manual procedures.

Operations

The machine readable travel document, with its OCR medium, is designed for both visual and mechanical reading. This feature is essential, since the conversion of travel documents to machine readable format can only be made gradually as current travel documents expire and are renewed or reissued, and the introduction of machine readability at border-crossing points is only being introduced gradually according to traffic volumes. As additional machine reading technologies are introduced on an optional basis in various travel documents, the OCR will be retained as the basic technology, considered mandatory to ensure international interoperability.

It has been discovered that the benefits of adopting the machine readable formats for passports and other travel documents extend beyond the obvious advantages for States that have the machine readers and databases for use in automated clearance systems. Many developing countries have elected to invest resources in the introduction of machine readable travel documents because the physical characteristics and data security features of the documents themselves offer strong defense against alteration, forgery or counterfeit. Moreover, adoption of the standardized format for the visual zone of an MRTD facilitates inspection by airline and government officials, with the result that clearance of low-risk traffic is expedited, problem cases are more readily identified, and enforcement is improved.

Endorsement of Doc 9303 by ISO

The technical specifications sections of Doc 9303, Part 1 (third edition), Part 2 (second edition) and Part 3 (first edition) have received the endorsement of the International Organization for Standardization as ISO Standards 7501-1, 7501-2, and 7501-3, respectively. Such endorsement is made possible by means of a liaison mechanism through which designers and manufacturers of travel documents and readers provide technical and engineering advice to the TAG/MRTD under the auspices of ISO, thus coordinating the development of Doc 9303 with the relevant ISO standards. Through this working relationship, the ICAO specifications have achieved the status of worldwide standards by means of a simplified procedure within ISO.

The liaison mechanism with ISO has been successfully applied not only to the endorsement of new specifications for travel documents as ISO standards but also to the approval of amendments to the specifications. Subsequent revisions to Doc 9303, Parts 1, 2 and 3, will therefore be processed for ISO endorsement in the same manner as previously.

II. DEVELOPMENT OF A LOGICAL DATA STRUCTURE FOR OPTIONAL CAPACITY EXPANSION TECNOLOGIES

Scope

1. *Technical Report: Development of a Logical Data Structure (LDS) For Optional Capacity Expansion Technologies* defines the current state of development of specifications[1] for the standardized organization of data ('Logical Data Structure - LDS') recorded to a capacity expansion technology of a MRTD at the discretion of an issuing State or organization.

Normative references

2. Certain provisions of the following International Standards, referenced in this text, constitute provisions of this Technical Report. Where differences exist between the emerging specifications[1] contained in this Technical Report and the referenced Standards, to accommodate specific construction requirements for machine readable travel documents including machine readable passports, the specifications[1] contained herein shall prevail. Note, individual mapping annexes list additional normative references specific to the technologies associated with that mapping methodology.

ISO 1073-IIII: 1976	Alphanumeric character sets for optical character recognition - Part 2: Character set OCR-B - Shapes and dimensions of the printed image
ISO 1831: 1980	printing specifications for optical character recognition
ISO 3166-1: 1997	Codes for representation of names of countries and their subdivisions – Part 1: Country codes
ISO 3166-2: 1998	Codes for representation of names of countries and their subdivisions – Part 2: Country subdivision code
ISO 3166-3: 1999	Codes for representation of names of countries and their subdivisions – Part 3: Code for formerly used names of countries
ISO/IEC 7810: 1995	Identification cards - Physical characteristics
ISO/IEC 7816-1: 1998	Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics
ISO/IEC 7816-2: 1998	Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of the contacts
ISO/IEC 7816-3: 1997	Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic interface and transmission protocols
ISO/IEC 7816-4: 1995	Identification cards - Integrated circuit(s) cards with contacts - Part 4: Organization, security and commands for interchange
2nd FDIS ISO/IEC 7816-4:2003	Part4 – Organization, security and commands for interchange

[1] *Specifications* as envisaged based on work completed to date.

ISO/IEC 7816-5: 2003 Identification cards - Integrated circuit(s) cards with contacts - Part 5: Registration of application providers

ISO/IEC 7816-6: 2003 Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements for interchange (Defect report included)

ISO/IEC 7816-7: 1998 Identification cards - Integrated circuit(s) cards with contacts - Part 7: Commands for Structured Card Query Language (SCQL)

ISO/IEC 7816-8: 2003 Identification cards - Integrated circuit(s) cards with contacts - Part 8: Commands for security operations

ISO/IEC 7816-9: 1999 Identification cards - Integrated circuit(s) cards with contacts - Part 9: Commands for card and file management

ISO/IEC 7816-10: 1999 Identification cards - Integrated circuit(s) cards with contacts - Part 10: Electrical interface for synchronous cards

ISO/IEC 7816-11: 2003 Identification cards – Integrated circuit(s) cards with contacts – Part 11: Personal verification through biometric methods

ISO/IEC 7816-15: 2003 Identification cards – Integrated circuit(s) cards with contacts – Part 15: Cryptographic information application

ISO/IEC 8601:2000 Data elements and interchange formats – Information interchange – Representation of dates and times

ISO/IEC 8824-2:1998 ITU-T Recommendation X.681 (1997), Information technology – Abstract Syntax Notation One (ASN.1): Information object specification

ISO/IEC 8824-3:1998 ITU-T Recommendation X.682 (1997), Information technology – ISO/IEC 8824-1:1998

ISO/IEC 8824-4:1998 ITU-T Recommendation X.683 (1997), Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications

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

ISO/IEC 8825-2:2003 Information technology -ASN.1 encoding rules: Specification of Packed Encoding Rules (PER),

ISO/IEC 8825-3:2003 Information technology - ASN.1 encoding rules: Specification of Encoding Control Notation

ISO/IEC 8825-4:2003 Information technology -ASN.1 encoding rules: XML Encoding Rules (XER)

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

ISO/IEC 14443-1 Identification cards - Contactless integrated circuit(s) cards - Proximity cards – Part 1: Physical Characteristics

ISO/IEC 14443-2 Identification cards - Contactless integrated circuit(s) cards - Proximity cards – Part 2: Radio frequency power and signal interface

ISO/IEC 14443-3 Identification cards - Contactless integrated circuit(s) cards - Proximity cards – Part 3: Initialization and anti-collision

ISO/IEC 14443-4 Identification cards - Contactless integrated circuit(s) cards - Proximity cards – Part 4: Transmission protocol

NISTIR 6529 CBEFF (Common Biometric Exchange File Format)

ISO/IEC 8601: 1988 Data elements and interchange formats - Information interchange - Representation of dates and times

ISO/IEC 8825-1:1988 Information technology – Open Systems Interconnections – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)

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

Definitions

3. For the purpose of this Technical Report, the following definitions shall apply.

- ASN.1: Abstract Syntax Notation One

- *CBEFF:* Common Biometric Exchange File Format, NISTIR 6529-A, a common file format that facilitates exchange and interoperability of biometric data. This document is currently being promoted by ISO/IEC JTC1/SC37 as a draft international standard.

- *Machine readable travel document (MRTD):* Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read.

- *Machine readable passport (MRP):* Passport conforming to the specifications contained herein, formulated to improve facilitation and enhance security. Contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. Presentation of optional data is permitted in accordance with the specifications defined herein. Normally constructed as an ID-3 size book containing pages with information on the holder and the issuing State or Organization and pages for visas and other endorsements. Machine readable information is contained in two lines of OCR-B text, each with 44 characters. May also be a free-standing card of ID-1 size with three lines of machine readable OCR-B text, each with 30 characters.

- *MRP Data Page:* Fixed dimensional page within the MRP containing a standardized presentation of visual and machine readable data. When constructed to form an end leaf of the MRP, the presentation of details is restricted to the front of the MRP Data Page, with the back securely bonded to the cover stock of the MRP.

- *Machine readable visa (MRV):* A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to

improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport.

- *Full size (Format-A) machine readable visa (MRV-A):* An MRV conforming with the dimensional specifications contained in Doc 9303, Part 2, for use by States who wish to ensure they have sufficient space available to accommodate their data requirements (including the use of two 44-character machine readable lines of data) and who do not need to maintain a clear area on the passport visa page adjacent to the visa.

- *Small size (Format-B) machine readable visa (MRV-B):* An MRV conforming with the dimensional specifications (ID-2 size) contained in Doc 9303, Part 2, and enabling States to maintain a clear area on the passport visa page adjacent to the visa to allow, for example, a seal to be placed on the visa and the passport page on which it is affixed. Consistent with its smaller size, the MRV-B contains two 36-character machine readable lines of data.

- *Machine readable official travel document:* An official document issued by a State or Organization which may, at the discretion of States, be accepted in lieu of a passport or visa for international travel, and suitable for machine reading.

- *Size 1 machine readable official travel document (TD1):* A card with nominal dimensions guided by those specified for the ID-1 type card (ISO 7810) (excluding thickness).

- *Size 2 machine readable official travel document (TD2):* A card or label conforming to the dimensions defined for the ID-2 type card (ISO 7810) (excluding thickness).

- *Machine readable zone (MRZ):* Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods.

- *Effective reading zone (ERZ):* Fixed dimensional area, common to all MRTDs, in which the mandatory machine readable data can be read by document readers.

- *Visual inspection zone (VIZ):* Those portions of the MRTD (data page in the case of MRP), i.e. front and back (where applicable), not defined as the MRZ.

- *Issuing State:* The Country issuing the MRTD.

- *Receiving State:* The Country to which the MRTD holder is applying for entry.

- *Issuing Organization:* Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer).

- *Authorized Receiving Organization:* Organization authorized to process an official travel document (e.g. an air carrier) and as such, allowed to record details in the optional capacity expansion technology.

- *Zone:* An area containing a logical grouping of data elements on the MRTD. Seven (7) zones are defined for MRTDs.

- *Field:* Specified space for an individual data element within a zone.

- *Caption:* Printed field name used to identify a field. Several captions are mandatory on the MRTD.

- *Portrait:* A visual representation of the facial image of the holder of the document.

- *Logical Data Structure (LDS):* The collection of groupings of Data Elements stored in the optional capacity expansion technology.

- *Data Group:* A series of related Data Elements grouped together within the Logical Data Structure.

- *Issuer Data Block:* A series of Data Groups that are written to the optional capacity expansion technology by the issuing State or organization.

- *Receiver Data Block:* A series of Data Groups that are written to the optional capacity expansion technology by a receiving State or authorized receiving organization.

- *Authenticity:* The ability to confirm that the Logical Data Structure and its components were created by the issuing State or organization.

- *Integrity:* The ability to confirm that the Logical Data Structure and its components have not been altered from that created by the issuing State or organization.

Development of a Logical Data Structure for Optional Capacity Expansion Technologies

4. Details on the LDS [Version 1.7] as developed to date are in the six sections as follow:

   Section III – Background;
   Section IV – Requirements;
   Section V – Organization of Mandatory and Optional Data Elements;
   Section VI – Security Principles;
   Section VII – Mapping Principles Common to All Optional Capacity Expansion Technologies;
   Section VIII - Mapping Annexes

III. BACKGROUND

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

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

Mapping the LDS to contactless integrated circuits is delineated in Section VIII, Annex A (Normative). Mapping of the LDS of Optical Stripes is delineated in Section VIII, Annex B (Normative) for those countries that wish to use the technology under bilateral and multilateral agreements between nations. Two-dimensional barcodes (Annex C) is retained as an informative annex in case member states wish to utilize this technology for applications that are not internationally interoperable.

The LDS continues to evolve, as more is confirmed about the capacity expansion needs of ICAO Member States and other organizations that will use the LDS. The evolution of data security requirements, in particular, may impact the LDS as more is known about the needs for data integrity and privacy.

IV. REQUIREMENTS

1. ICAO has determined that the predefined, standardized Logical Data Structure - LDS must meet a number of *mandatory* requirements:

- Ensure efficient and optimum facilitation of the rightful holder;
- Ensure protection of details recorded in the optional capacity expansion technology;
- Allow global interchange of capacity expanded data based on the use of a single LDS common to all MRTDs;
- Address the diverse optional capacity expansion needs of issuing States and organizations;
- Provide expansion capacity as user needs and available technology evolve;
- Support a variety of data protection options;
- Support the updating of details by a issuing State or organization, if it so chooses;
- Support the addition of details by a receiving State or approved receiving organization while maintaining the authenticity[2] and integrity[3] of data created by the issuing state or organization; and
- Utilize existing International Standards to the maximum extent possible **in** particular the emerging international standards for globally interoperable biometrics.

[2] *Authenticity* - ability to confirm the LDS and its components were created by the issuing State or organization.

[3] *Integrity* – ability to confirm the LDS and its components have not been altered from that created by the issuing State or organization.

V. ORGANIZATION OF MANDATORY AND OPTIONAL DATA ELEMENTS

Scope

1. This Section defines the pinnacle level of data organization defined for the Logical Data Structure – LDS; that being, the identification of all mandatory and optional data elements and any prescriptive ordering and/or grouping of data elements that must be followed to achieve global interoperability for reading of details (Data Elements) recorded in a capacity expansion technology optionally included on a MRTD. Details on the writing (mapping) of the LDS common to all the different types of optional capacity expansion technologies are presented in Section VII, while comprehensive details specific to a technology are included in the normative Mapping Annexes contained in Section VIII.

Mandatory and Optional Data Elements

2. A series of mandatory and optional **Data Elements** has been defined for the LDS to meet the global requirements of processing persons presenting MRTDs as illustrated in Figure V-1.

Ordering and Grouping of Data Elements

3. A logical order[4] supported by ordered groupings of related Data Elements has been established for the series of mandatory and optional Data Elements as illustrated in Figure V-1.

4. The ordered groupings of Data Elements are further grouped depending on whether they have been recorded by (1) an issuing State or organization or (2) a receiving State or approved receiving organization. *Note: The ability for a receiving State or approved receiving organization to add data to the LDS is not supported in LDS [Version 1.7].*

5. The only Data Elements that must be present (mandatory) if a LDS is recorded to an optional capacity expansion technology are those that define the contents of the Machine Readable Zone (MRZ) of the MRTD (Data Group 1).

6. While the *use* of biometrics is optional for issuing authorities, *IF* a choice is made to incorporate biometrics, Data Group 2, the encoded face, is therefore Mandatory. All other Data Elements defined for recording by an issuing State or organization are *optional*.

7. Groupings of Data Elements added by receiving States or approved receiving organizations may or may not be present in a LDS. More than one recording of grouped Data Elements added by receiving States or approved receiving organizations can be present in the LDS. Note*: The ability for a receiving State or approved receiving organization to add data to the LDS is not supported in LDS [Version 1.7.].*

8. 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.

---

[4] The logical order for Data Elements defined in Section V has been standardized to meet the global requirements established for enhanced facilitation and improved security when processing persons presenting MRTDs. The actual order of recording of the grouped Data Elements is defined by specifications established to ensure efficient performance of each capacity expansion technology. These specifications are defined in the individual normative Mapping Annexes contained in Section VIII.

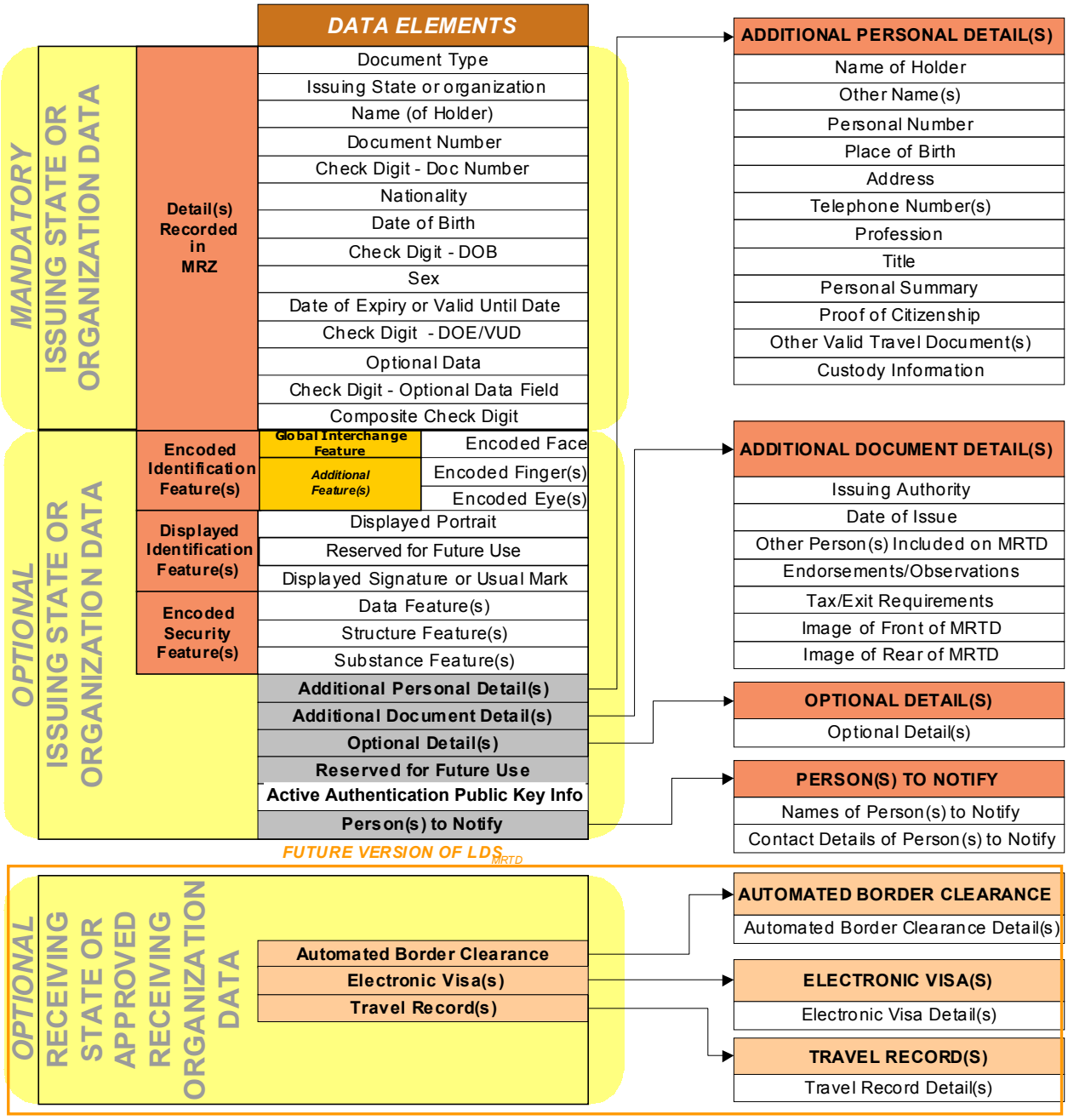


FIGURE V-1. MANDATORY AND OPTIONAL DATA ELEMENTS DEFINED FOR LDS [Version 1.7]

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

10. Each Data Group is assigned a reference number. Figure V-2 identifies the reference number assigned to each Data Group**]**. *For Example,* "DG2" identifies Data Group # 2, Encoded Identification Feature(s) for the face of the rightful holder of the MRTD (*i.e.* facial biometric details). *Note: Receiving State Data Groups (Data Groups 17-19) are not supported in LDS [Version 1.7]*.

Data Groups Coded to Allow Confirmation of Authenticity and Integrity of Data

11. To allow confirmation of the authenticity and integrity of recorded details, authenticity/Integrity object is included. Each Data Group will be represented in this Authenticity/Integrity object, which is recorded within a separate elementary file (EF.SOD). (Refer to Technical Report "PKI for Machine Readable Travel Documents offering ICC read only access" for details) Using the CBEFF structure utilized for Encoded Identification Feature Data Groups 2-4 and optional "Additional Biometric Security" features defined in the Technical Report "PKI for Machine Readable Travel Documents offering ICC read only access", identity confirmation details (e.g. biometric templates) may also be individually protected at the discretion of the issuing State or organization.

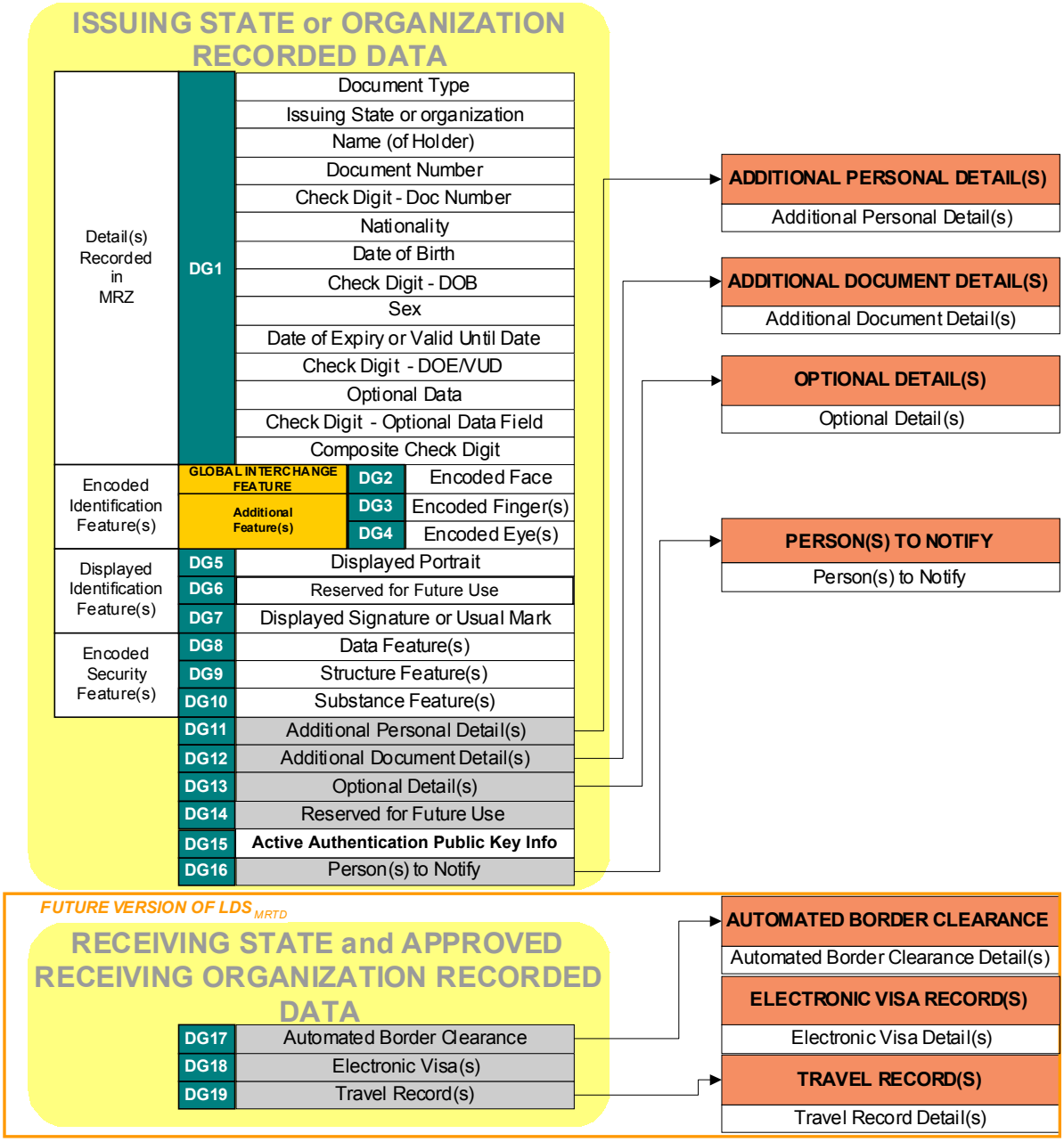


FIGURE V-2. DATA GROUP REFERENCE NUMBERS ASSIGNED TO LDS [Version 1.7]

DATA GROUPS RECORDED BY THE ISSUING STATE OR ORGANIZATION

12. The following Table defines the mandatory and optional Data Groups that combine to form that portion of the LDS [Version 1.7] recorded by the Issuing State or Organization.

DATA GROUP	MANDATORY (M) / OPTIONAL (O)	DATA ITEM	
Detail(s) Recorded in MRZ of the MRTD			
1	M	Machine Readable Zone (MRZ) Data *[See 13.1]*	
Machine Assisted Identity Confirmation Detail(s) – Encoded Identification Feature(s)			
2	M	**GLOBAL INTERCHANGE FEATURE**	Encoded Face *[See 13.2]*
3	O	Additional Feature	Encoded Finger(s) *[See 13.2]*
4	O	Additional Feature	Encoded Iris(s) *[See 13.2]*
Machine Assisted Identity Confirmation Detail(s) – Displayed Identification Feature(s)			
5	O	Displayed Portrait *[See 13.3]*	
6	O	Reserved for future use	
7	O	Displayed Signature or Usual Mark *[See 13.3]*	
Machine Assisted Security Feature Verification – Encoded Security Feature(s)			
8	O	Data Feature(s) *[See 13.4]*	
9	O	Structure Feature(s) *[See 13.4]*	
10	O	Substance Feature(s) *[See 13.4]*	
Additional Personal Detail(s)			
11	O	Additional Personal Data Elements *[See 13.5]*	
Additional Document Detail(s)			
12	O	Additional Document Data Elements *[See 13.6]*	
Optional Detail(s)			
13	O	Discretionary Data Element(s) defined by issuing State or organization *[See 13.7]*	
Reserved for Future Use			
14	O	Reserved for future use	
15	O	Active Authentication Public Key Info	
Person(s) to Notify			
16	O	Person(s) to Notify Data Element(s) *[See 13.9]*	

DATA ELEMENTS FORMING DATA GROUPS 1 THROUGH 16

13. Data Groups 1 (DG1) through 16 (DG16) individually consist of a number of mandatory and optional Data Elements. The order of Data Elements within the Data Group is standardized.

14. The following Tables define the mandatory and optional Data Elements that combine to form the structure of Data Groups 1 (DG1) through 16 (DG16).

14.1 *Detail(s) Recorded in MRZ of the MRTD.* Data Elements assigned to Data Group 1 (DG1) are as follows. The Data Elements of 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 specified in ICAO Doc 9303.

Data Group	Data Element	Fixed/ Variable	Mandatory / Optional	Data Item
DG1			**M**	**MRZ (Summary of details as recorded on MRTD, Refer to ICAO Doc 9303)**
	01	F	M	Document Type
	02	F	M	Issuing State or organization
	03	F	M	Name (*of Holder*)
	04	F	M	Document Number (*9 most significant characters*) *[see 13.1.1]*
	05	F	M	Check digit - Document Number or filler character (<) indicating Document Number exceeds 9 characters. *[see 14.1.1]*
	06	F	M	Nationality
	07	F	M	Date of Birth
	08	F	M	Check digit - Date of Birth
	09	F	M	Sex
	10	F	M	Date of Expiry *(For MRP, TD-1 and TD-2)*
		F	M	Valid Until Date *(For MRV-A and MRV-B)*
	11	F	M	Check digit - Date of Expiry or Valid Until Date
	12	F	M	Optional Data and/or *in the case of a TD-1* Least Significant Characters of Document Number + Document Number Check digit + filler character (<) *[when Document Number > 9 characters] [see 14.1.1 and 14.1.2]*
	13	F	M	Check digit – Optional Data Field
	14	F	M	Composite Check Digit

14.1.1 *If Document Number on a TD-1 has more than 9 characters.* The nine (9) principal (most significant) characters shall be recorded in Data Element 04. Data Element 05 shall be coded with the filler character (<). The remaining characters of the document number shall be recorded at the beginning of Data Element 12 (Optional Data) followed by the Document Number Check digit and a filler character (<).

14.1.2 *Data Element 12 on a TD-1 contains least significant characters for Document Number exceeding 9 characters.* The remaining characters of the document number shall be recorded at the beginning of Data Element 12 followed by the Document Number Check digit and a filler character (<). Optional Data, if present, shall be located in the remaining character positions of Data Element 12.

[5] The order of Data Elements within a Data Group is standardized in a logical sense. The final ordering can be effected by the mapping requirements of the individual capacity expansion technologies, as set out in Section VII.

14.1.3 Refer to ICAO Document 9303 for details regarding calculation of *check digits*

14.2 *Machine Assisted Identity Confirmation Detail(s) – Encoded Identification Feature(s)*. Data Elements assigned to Data Groups 2 (DG2) through 4 (DG4) are as follows,

Data Group	Data Element	Mandatory / Optional	Data Item
DG2		**M**	**GLOBAL INTERCHANGE IDENTIFICATION FEATURE – FACE** *[see 14.2.1]*
	01	M *(If encoded face feature recorded)*	Number of Face Biometric Encodings Recorded
	02[6]	M *(If encoded face feature recorded)*	Header *[see A.13.3]*
	03[6]	M *(If encoded face feature recorded)*	Face Biometric Data Encoding(s) *[see A.13.3]*
ADDITIONAL IDENTIFICATION FEATURE(s) *[see 13.2.2]*			
DG3		**O**	**ADDITIONAL IDENTIFICATION FEATURE – FINGER(S)** *[see 14.2.2]*
	01	M *(If encoded finger(s) feature recorded)*	Number of Finger(s) Biometric Encodings Recorded
	02[6]	M *(If encoded finger(s) feature recorded)*	Header *[see A.13.3]*
	03[6]	M *(If encoded finger(s) feature recorded)*	Finger Biometric Data Encoding(s) *[see A.13.3]*
DG4		**O**	**ADDITIONAL IDENTIFICATION FEATURE – IRIS(S)** *[see 14.2.2]*
	01	M *(If encoded eye(s) feature recorded)*	Number of Iris(s) Biometric Encodings Recorded
	02[6]	M *(If encoded eye(s) feature recorded)*	Header *[see A.13.3]*
	03[6]	M *(If encoded eye(s) feature recorded)*	Iris Biometric Data Encoding(s) *[see A.13.3]*

14.2.1 Data Group 2 (DG2) when present represents the globally interoperable biometric for machine assisted identity confirmation with machine readable travel documents, which shall be face recognition. If there is more than one recording, the most recent internationally interoperable encoding shall be the first entry. The primary purpose of using chip technology is to have the ability to capture biometrics in travel documents. While the *use* of biometrics is optional for issuing authorities, *IF* a choice is made to incorporate biometrics, this Data Group is therefore characterized as Mandatory.

14.2.2 ICAO recognizes that Member States may elect to use fingerprint and/or iris recognition as additional biometric technologies in support of machine assisted identity confirmation, which shall be encoded as Data Group 3 (DG3) and Data Group 4 (DG4) respectively.

[6] Data Element will repeat within the Data Group when more than one recording of the biometric feature is present; *i.e.* as defined through Data Element 01. Refer to technology mapping annexes for specific implementations.

14.3 *Machine Assisted Identity Confirmation Detail(s) – Displayed Identification Feature(s).* Data Elements Assigned to Data Groups 5 (DG5) through 7 (DG7) are as follows,

Data Group	Data Element	Mandatory / Optional	Data Item
DG5		**O**	**DISPLAYED PORTRAIT**
	01	M *(If displayed portrait recorded)*	Number of Displayed Portraits Recorded
	02[7]	M *(If displayed portrait recorded)*	Displayed Portrait Representation(s) *[see 14.3.1]*
DG6		**O**	**Reserved for Future Use**
DG7		**O**	**DISPLAYED SIGNATURE OR USUAL MARK**
	01	M *(If displayed signature or usual mark recorded)*	Number of Displayed Signature or Usual Marks
	02[7]	M *(If displayed signature or usual mark recorded)*	Displayed Signature or Usual Mark Representation *[see 14.3.1]*

14.3.1 Data Element 02 of Data Groups 5 (DG5) and 7 (DG7) shall be encoded as defined in ISO 10918-1 using the JFIF option, or ISO 15444 (JPEG2000).

14.4 *Machine Assisted Security Feature Verification – Encoded Detail(s).* Data Elements combining to form Data Groups 8 (DG8) through 10 (DG10) are as follows,

Data Group	Data Element	Mandatory /Optional	Data Item
DG8		**O**	**DATA FEATURE(S)**
	01	M *(If this Encoded feature is used)*	Number of Data Feature(s)
	02[8]	M *(If this Encoded feature is used)*	Header *(to be defined)*
	03[8]	M *(If this Encoded feature is used)*	Data Feature(s) Data
DG9		**O**	**STRUCTURE FEATURE(S)**
	01	M *(If this Encoded feature is used)*	Number of Structure Feature(s)
	02[8]	M *(If this Encoded feature is used)*	Header *(to be defined)*

[7] Data Element will repeat within the Data Group when more than one recording of the displayed feature is present; *i.e.* as defined through Data Element 01.
[8] Data Element will repeat within the Data Group when more than one recording of the encoded security feature is present; *i.e.* as defined through Data Element 01.

Data Group	Data Element	Mandatory /Optional	Data Item
	03[8]	M *(If this Encoded feature is used)*	Structure Feature(s) Data
DG10		**O**	**SUBSTANCE FEATURE(S)**
	01	M *(If this Encoded feature is used)*	Number of Substance Feature(s) Recorded
	02[8]	M *(If this Encoded feature is used)*	Header *(to be defined)*
	03[8]	M *(If this Encoded feature is used)*	Substance Feature(s) Data

14.5 *Additional Personal Detail(s).* Data Elements combining to form Data Group 11 (DG11) are as follows,

Data Group	Data Element	Mandatory /Optional	Date Item
DG11		**O**	**ADDITIONAL PERSONAL DETAIL(S)**
	01	O	Name of Holder (Primary and Secondary Identifiers, in full)
	02	O	Other Name(s)
	03	O	Personal Number
	04	O	Place of Birth
	05	O	Date of Birth (in full)
	06	O	Address
	07	O	Telephone Number(s)
	08	O	Profession
	09	O	Title
	10	O	Personal Summary
	11	O	Proof of Citizenship *[see 14.5.1]*
	12	M* * *If DE 13 recorded.*	Number of Other Valid Travel Documents
	13	O	Other Travel Document Numbers
	14	O	Custody Information

14.5.1 Data Element 11 shall be encoded as defined in *ISO 10918-1*, or ISO 15444 (JPEG2000).

14.6 *Additional Document Detail(s).* Data Elements combining to form Data Group 12 (DG12) are as follows,

Data Group	Data Element	Mandatory /Optional	Data Item

Data Group	Data Element	Mandatory /Optional	Data Item
DG12			**ADDITIONAL DOCUMENT DETAILS**
	01	O	Issuing Authority *(for the MRTD)*
	02	O	Date of Issue *(of MRTD)*
	03	M* ** If Other Person(s) Included on MRTD*	Number of Other Person(s) on MRTD *(MRV only)*
	04	O	Other Person(s) Included on MRTD *(MRV only)*
	05	O	Endorsements / Observations *(related to MRTD)*
	06	O	Tax / Exit Requirements
	07	O	Image of Front of MRTD *[see 14.6.1]*
	08	O	Image of Rear MRTD *[see 14.6.1]*
	09	O	Time MRTD Personalized
	10	O	Machine Used to Personalize MRTD

14.6.1 Data Elements 07 and 08 shall be encoded as defined in *ISO 10918-1*, or ISO 15444 (JPEG2000).

14.7 *Optional Detail(s)*. Data Elements combining to form Data Group 13 (DG13) are as follows,

Data Group	Data Element	Mandatory /Optional	Data Item
DG13		**O**	**OPTIONAL DETAIL(S)**
	01	M *(If Data Group13 Recorded)*	Details as Determined by the issuing State or organization

14.8 *Data Group 14: Unassigned Data Group*. Reserved for future use.

Data Group	Data Element	Mandatory /Optional	Data Item
DG14		**O**	**Reserved for future use**

14.9 Data Group 15 (DG15): Active Authentication Public Key Information. This Data Group contains the optional Active Authentication Public Key (refer to Technical Report "PKI for Machine Readable Travel Documents offering ICC read only access")

Data Group	Data Element	Mandatory /Optional	Data Item
DG15		**O**	**Active Authentication Public Key Info**

14.10 *Person(s) to Notify*. Data Elements combining to form Data Group 16 (DG16) are as follows,

Data Group	Data Element	Mandatory /Optional	Data Item
DG16		**O**	**PERSON(S) TO NOTIFY**
	01	M *(If Data Group16 Recorded)*	Number of Persons Identified

Data Group	Data Element	Mandatory /Optional	Data Item
	02	M *(If Data Group16 Recorded)*	Date details Recorded
	03	M *(If Data Group16 Recorded)*	Name of Person to Notify
	04	M *(If Data Group16 Recorded)*	Telephone Number of Person to Notify
	05	O	Address of Person to Notify

DATA GROUPS RECORDED BY A RECEIVING STATE OR APPROVED RECEIVING ORGANIZATION

15. The following Table defines the optional Data Groups that combine to form that portion of the LDS available for recording data by the Receiving State or approved receiving organization. *Note: A Receiving State or approved receiving organization is not allowed to record data under LDS [Version 1.7]. Therefore, Data Groups 17 through 19 are not valid, nor are they supported in LDS [Version 1.7].*

DATA GROUP	MANDATORY (M) / OPTIONAL (O)	DATA ITEM
Automated Border Clearance Detail(s)		
DG17	O	Automated Border Clearance
Electronic Visas		
DG18	O	Electronic Visa(s)
Travel Record Detail(s)		
DG19	O	Travel Record(s)

FORMAT OF DATA ELEMENTS

16. *Data Element Directory*.

This section describes the Data Elements that may be present in each Data Group.

16.1 Issuing State or approved issuing organization Data Elements

Data Groups 1 (DG1) through 16 (DG16): Data Elements and their format within each Data Group area as follows,

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

Data Element	Optional or Mandatory	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
DATA GROUP 1: Data Recorded in MRZ						
01	M	Document Type	2	F	A,N,S	Document Type (as per ICAO Doc. 9303 MRZ)
02	M	Issuing State or organization	3	F	A,S	Issuing State or organization (as per ICAO Doc. 9303 MRZ)
03	M	Name of Holder				
	M	*Primary and Secondary Identifiers*	30, 31 or 39[9]	F	A,S,	Single and Double Filler characters (<) inserted as per ICAO Doc. 9303 MRZ. .
04	M	Document Number	9	F	A,N,S	Document Number (as per MRZ) Note: Consistent with specifications defined in Part 3 of ICAO Doc 9303 for the TD-1, if the Document Number exceeds 9 characters in length a filler character (<) shall be inserted in the Document Check Digit position (DE 05) and the remaining characters making up the Document Number shall be recorded at the beginning of DE 12 followed by the Document Number Check digit and a filler character (<).
05	M	Check digit - *Document Number*	1	F	N,S	Check digit for Data Element 04 (as per ICAO Doc. 9303 MRZ).
06	M	Nationality	3	F	A,S	Alpha-3 Code (as per MRZ).
07	M	Date of Birth	6	F	N,	Format = YYMMDD as per ICAO Doc. 9303 MRZ. Full DOB may be stored in DG11 in CCYYMMDD format to avoid the ambiguity in the year's encoding.
08	M	Check digit - *Date of Birth*	1	F	N	Check digit for Data Element 07 (as per ICAO Doc. 9303 MRZ).
09	M	Sex	1	F	A,S	As per MRZ in ICAO Doc 9303
10	M if MRP, TD-1, TD-2	Date of Expiry	6	F	N	Format = YYMMDD as per MRZ.
	M if MRV-A, MRV-B	Valid Until Date	6	F	N	Format = YYMMDD as per MRZ.

[9] Length depends upon document type. Refer to ICAO DOC 9303

Data Element	Optional or Mandatory	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
11	M	Check digit - *Date of expiry or Valid Until Date*	1	F	N	Check digit for Data Element 10 (as per ICAO Doc. 9303 MRZ).
12	M *if Optional Data in MRZ*	Optional Data				
	M if Optional Data in MRZ	*Optional Data*	7, 14 or 26[9]	F	A,N,S	As per MRZ. Note: If the Document Number in the MRZ exceeds 9 characters in length (TD-1 only), the remaining characters of the Document Number shall be presented at the beginning of Data Element 12 followed by the Document Number Check digit, a filler character (<) and any optional data to be recorded.
13	M	Check digit – *Optional Data Field*	1	F	N	Check digit for Data element 12 (as per ICAO Doc. 9303 MRZ).
14	M	Check digit - *Composite Check digit*	1	F	N	As per ICAO Doc. 9303 MRZ.
DATA GROUP 2: Encoded Identification Features – FACE						
01	M *if Encoded Face Feature included*	Number of Face Biometric Encodings Recorded	1	F	N	1 to 9 identifying number of unique encodings of data on the Face.
02	M *if Encoded Face Feature included*	Header		F		See *Normative Supporting Appendix A Section 13..3* for details on encoding. Data Element may recur as defined by DE 01.
03	M *if Encoded Face Feature included*	Face Biometric Data Encoding(s)	99999 Max	Var	A,N,S, B	See *Normative Supporting Appendix A Section 13.3* for details on encoding. Data Element may recur as defined by DE 01.
DATA GROUP 3: Encoded Identification Features – FINGER(s)						
01	M *if Encoded Finger(s) Feature included*	Number of Finger Biometric Encodings Recorded	1	F	N	1 to 9 identifying number of unique encodings of data on the Finger(s).
02	M *if Encoded Finger(s) Feature included*	Header		F		See *Normative Supporting Appendix A Section 13.3* for details on encoding. Data Element may recur as defined by DE 01.
03	M *if Encoded Finger(s) Feature included*	Finger Biometric Data Encoding(s)	99999 Max	Var	A,N,S, B	See *Normative Supporting Appendix B to Section XIII* for details on encoding. Data Element may recur as defined by DE 01.
DATA GROUP 4: Encoded Identification Features – IRIS(s)						
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		F		See *Normative Supporting Appendix B to Section XIII* for details on encoding. Data Element may recur as defined by

Data Element	Optional or Mandatory	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
						DE 01.
03	M *if Encoded Eye(s) Feature included*	Eye Biometric Data Encoding(s)	99999 Max	Var	A,N,S, B	See *Normative Supporting Appendix B to Section XIII* for details on encoding. Data Element may recur as defined by DE 01.
DATA GROUP 5: Displayed Identification Feature(s) – PORTRAIT						
01	M *if Displayed Portrait included*	Number of entries: Displayed Portrait	1	F	N	1 to 9 identifying number of unique recordings of Displayed Portrait.
02	M *if Displayed Portrait included*	Displayed Portrait Data		F		Data Element may recur as defined by DE 01.
	M *if Displayed Portrait included*	*Number of bytes in representation of Displayed Portrait*	5	F	N	00001 to 99999, identifying number of bytes in representation of Displayed Portrait immediately following.
	M *if Displayed Portrait included*	*Representation of Displayed Portrait*	99999 Max	Var	A,N,S, B	Formatted as per ISO 10918-1 or ISO 15444.
DATA GROUP 6: Reserved for future use						
DATA GROUP 7: Displayed Identification Features – SIGNATURE or USUAL MARK						
01	M *if Displayed Signature or Usual Mark included*	Number of entries: Displayed Signature or Usual Mark	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 included*	Displayed Signature or Usual Mark Data		V		Data Element may recur as defined by DE 01.
	M *if Displayed Signature or Usual Mark included*	*Representation of Displayed Signature or Usual Mark*	99999 Max	Var	A,N,S, B	Formatted as per ISO 10918-1 or ISO 15444.
DATA GROUP 8: Encoded Security Features – DATA FEATURE(s)						
01	M *if encoded Data Feature included*	Number of Data Features	1	F	N	1 to 9, identifying number of unique encodings of Data Feature(s) (embraces DE 02 through DE 04).
02	M *if encoded Data Feature included*	Header Information	1	TBD		Header details to be defined.
03	M *if encoded Data Feature included*	Data Feature Data		Var		
	M *if encoded Data Feature included*	*Encoded Data Feature*	999 Max	Var	B	Format defined at the discretion of issuing State or organization.
DATA GROUP9: Encoded Security Features – STRUCTURE FEATURE(s)						
	M	Number of Structure				1 to 9, identifying number of unique

Data Element	Optional or Mandatory	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	*if encoded Structure Feature included*	Features	1	F	N	encodings of Structure Feature(s) (embraces DE 02 through DE 04).
02	M *if encoded Structure Feature included*	Header information	TBD	TBD	N	Header details to be defined
03	M *if encoded Structure Feature included*	Structure Feature Data		Var		
	M if encoded Structure Feature included	*Encoded Structure Feature*	999 Max	Var	B	Format defined at the discretion of issuing State or organization.
DATA GROUP10: Encoded Security Features – SUBSTANCE FEATURE(s)						
01	M *if encoded Substance Feature included*	Number of Substance Features	1	F	N	1 to 9, identifying number of unique encodings of Substance Feature(s) (embraces DE 02 through DE 04).
02	M *if encoded Substance Feature included*	Header information	TBD	TBD	N	Details to be defined
03	M *if encoded Substance Feature included*	Substance Feature Data		Var		
	M if encoded Substance Feature included	*Encoded Substance Feature*	999 Max	Var	B	Format defined at the discretion of issuing State or organization.
DATA GROUP 11: Additional Personal Detail(s)						
See Data Element Directory - Additional Personal Detail(s) [see 16.1.1]						
DATA GROUP 12: Additional Document Detail(s)						
See Data Element Directory - Additional Document Detail(s) [see 16.1.2]						
DATA GROUP 13: Optional Detail(s)						
See Data Element Directory - Optional Detail(s) [see 16.1.3]						
DATA GROUP 14: Reserved for Future Use						
Reserved						
DATA GROUP 15: Active Authentication Public Key Info						
Active Authentication Public Key Info as specified in Technical Report "PKI for Machine Readable Travel Documents offering ICC read only access"						
DATA GROUP 16: Person(s) to Notify						
See Data Element Directory – Details on Person(s) to Notify [see 16.1.4]						

16.1.1 *Data Group 11 (DG11)*: Data Elements and their format within **DG11 – Additional Personal Detail(s)** are as follows,

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

DATA GROUP 11: Additional Personal Detail(s)						
Data Element	**Optional or Mandatory**	**Name of Data Element**	**Number of Bytes**	**Fixed or Variable**	**Type of Coding**	**Coding Requirements**
01	O	Name of Holder (in full)				
	M if DE 01 included	*Primary and Secondary Identifiers*	99 Max	Var	A,S	Filler characters (<) inserted as per MRZ. No fillers inserted at end of line. Truncation not permitted.
02	O	Other Name(s)				
		Primary and Secondary Identifiers	99 Max	Var	A,S	Filler characters (<) inserted as per MRZ. No fillers inserted at end of line. Truncation not permitted.
03	O	Personal Number				
		Personal Number	99 Max	Var	A,N,S	Free-Form Text.
04	O	Place of Birth				
		Place of Birth	99 Max	Var	A,N,S	Free-Form Text
05	O	Address				
		Address	99 Max	Var	A,N,S	Free-Form Text
06	O	Full Date of Birth				
		Date of Birth	8	F	N	CCYYMMDD
07	O	Telephone				
	M if DE 06 included	*Telephone*	99 Max	Var	N,S	Free-Form Text
08	O	Profession				
	M if DE 07 included	*Profession*	99 Max	Var	A,N,S	Free-Form Text
09	O	Title				
	M if DE 08 included	*Title*	99 Max	Var	A,N,S	Free-Form Text
10	O	Personal Summary				
	M if DE 09 included	*Personal Summary*	99 Max	Var	A,N,S	Free-Form Text
11	O	Proof of Citizenship		Var		
	M if DE 10 included	*Citizenship Detail*	9999999 Max	Var	B	Image of Citizenship Document formatted as per ISO 10918-1.
12	O	Other Valid Travel Document(s)		Var		
	M if DE 12 included	*Travel Document Number*	99 Max		A,N,S	Free-Form Text, separated by <
13	O	Custody Information		Var		
	M	*Custody Information*	999	Var	A,N,S	Free-Form Text

	if DE 13 included		Max			

16.1.2 *Data Group 12 (DG12)*: Data Elements and their format within **DG12 – Additional Document Detail(s)** are as follows,

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

DATA GROUP 12: Additional Document Detail(s)						
Data Element	**Optional or Mandatory**	**Name of Data Element**	**Number of Bytes**	**Fixed or Variable**	**Type of Coding**	**Coding Requirements**
01	O	Issuing Authority				
		Issuing Authority	99 Max	Var	A,N,S	Free-Form Text
02	O	Date of Issue	8	F	N	Date of Issue of Document; i.e. YYYYMMDD
03	O	Other Person(s) Included				** Only valid with MRV **
		Other Person Detail(s)	99 Max	Var	A,N,S	Free-Form Text
04	O	Endorsement(s) / Observation(s)				
		Endorsement(s) / Observation(s)	99 Max	Var	A,N,S	Free-Form Text
05	O	Tax / Exit Requirements				
		Tax / Exit Requirements	99 Max	Var	A,N,S	Free-Form Text
06	O	Image of Front of MRTD				
		Image of MRTD (front)	9999999 Max	Var	B	Formatted as per ISO 10918-1.
07	O	Image of Rear of MRTD				
		Image of MRTD (rear)	9999999 Max	Var	B	Formatted as per ISO 10918-1.
08	O	Personalization time				
		Time document was personalized		F	F 14N	ccyymmddhhmmss
09	O	Personalization serial number				
		Serial number of personalization device		V	V 99ANS	Free format

16.1.3 *Data Group 13 (DG13)*: Data Elements and their format within **DG13 – Optional Detail(s)** are as follows,

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

DATA GROUP 13: Optional Detail(s)						
Data Element	**Optional or Mandatory**	**Name of Data Element**	**Number of Bytes**	**Fixed or Variable**	**Type of Coding**	**Coding Requirements**
TBD	O	Optional Details		Var		At the Discretion of Issuing State or organization

16.1.4 *Data Group 16 (DG16)*: Data Elements and their format within **DG16 – Person(s) to Notify** are as follows,

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

DATA GROUP 16: Person(s) to Notify						
Data Element	**Optional or Mandatory**	**Name of Data Element**	**Number of Bytes**	**Fixed or Variable**	**Type of Coding**	**Coding Requirements**
01	M *if DG 15 included*	Number of Persons Identified	2	F	N	Identifies number of persons included in the Data Group.
02	M *if DG 15 included*	Date Details Recorded	8	F	N	Date notification date recorded; Format = CCYYMMDD
03	M *if DG 15 included*	Name of Person to Notify *Primary and Secondary Identifiers*		Var	A,S	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	A,N,S	Free-Form Text

VI. Security Principles

Note, for further discussion of the security principles used to protect the recorded Logical Data Structure (LDS) and ensure that the receiving State or approved receiving organization can confirm the authenticity and integrity of data read from the optional capacity expansion technology refer to Technical Report "PKI for Machine Readable Travel Documents offering ICC read only access".

VII. MAPPING PRINCIPLES COMMON TO ALL OPTIONAL CAPACITY EXPANSION TECHNOLOGIES

Scope

1. This Section defines the mapping principles common to all optional capacity expansion technologies that must be followed when recording the Logical Data Structure – LDS. Details on those mapping principles that are unique to an optional capacity expansion technology are included in the normative Mapping Annexes contained in Section VIII.

Ordering of LDS

1.1 Three types of sequencing (data arrangement) schemes are available for mapping the LDS to a capacity expansion technology. Only the Random Order Scheme is permitted for international interoperability. It is described in Annex A (Normative) and Annex B (Normative). The Sequential Scheme is described in an informative annex in case issuing States wish to use the scheme for internal, non-internationally interoperable applications.

1.2 *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. Random Order Recording can only be used with accommodating technologies such as Contactless IC(s) and Optical Memory. Variable length data elements are encoded as *Length|Value* and lengths are specified in ASN.1 notation. This scheme is valid for recording to Contactless IC(s). This scheme may also be used by contact IC(s); however, this technology is not supported for international interoperability. (Random Ordering Scheme for Optical Memory differs and is described below.)

1.3 *Sequential Ordering Scheme*: The Sequential Ordering Scheme requires that Data Groups and Data Elements be recorded following the logical order defined in Section V. Those Data Groups and Data Elements that are not required, determined at the discretion of the State or organization recording the data, are omitted, with no space left as a placeholder. Variable length data elements are encoded as *Length|Value* and lengths are specified in ASN.1 notation. This scheme is valid for recording to *2-D Bar Codes*. This scheme is not internationally interoperable, but may be used for intracountry applications.

1.4 *Optical Memory Scheme:* Optical Cards utilize a Random Ordering Scheme specifically designed to take advantage of optical stripe capabilities. Variable length data elements are encoded as *Length|Value* and lengths are specified in decimal notation.

Header and Data Group Presence Information

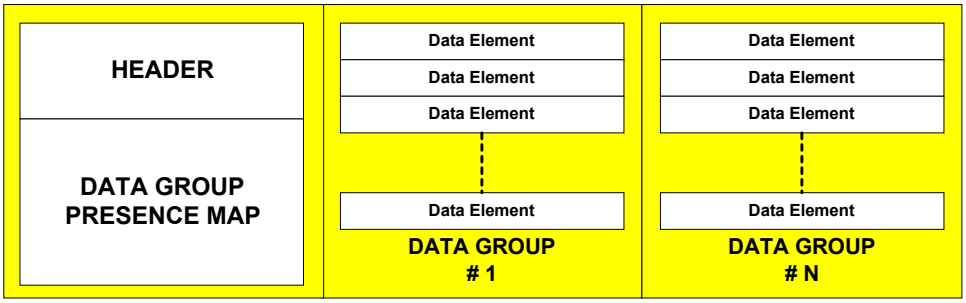


FIGURE VII-1. MANDATORY HEADER AND DATA GROUP PRESENCE INFORMATION

A *mandatory* Header and Data Group Presence Map are included with each implementation method, In the case of mapping to contactless chips, this information is stored in EF.COM. Please refer to Annex A.

1.1 *Header.* The Header contains the following information, which enables a receiving State or approved receiving organization locate and decode the various Data Groups and Data Elements contained within the block of data recorded by the issuing State or organization.

APPLICATION IDENTIFIER (AID)
LDS VERSION NUMBER
UNICODE VERSION NUMBER

1.1.1 *LDS Version Number.* The LDS Version Number defines the format version of the LDS[10]. The exact format to be used for storing this value will be defined in the technology mapping annexes. Standardized format for an LDS Version Number is "aabb", where,

"aa" = number (01 –99) identifying the Version of the LDS (i.e., Significant additions to the LDS)

"bb" = number (01-99) identifying the Update of the LDS

1.1.2 *Unicode Version Number*[11]. The Unicode Version Number identifies the coding method used when recording alpha, numeric and special characters, including national characters. The standardized format for a Unicode Version Number is “aabbcc”, where, The exact format to be used for storing this value will be defined in the technology mapping annexes.

“aa” = number identifying the **Major version** of the Unicode Standard (i.e. Significant additions to the standard, published as a book);

[10] Future upgrades to the standardized organization of the 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.

[11] *Unicode* is based on ISO/IEC 10646. Details on *Unicode* can be found on the Internet at www.unicode.org.

"bb" = number identifying the **Minor version** of the Unicode Standard (i.e. Character additions or more significant normative changes, published as a Technical Report); and

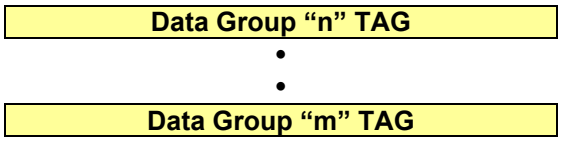
"cc" = number identifying the **Update version** of the Unicode Standard (i.e. Any other changes to normative or important informative portions of the Standard that could change program behavior. These changes are reflected in new Unicode Character Database files and an update page).

Note: For historical reasons, the numbering within each of the fields (i.e. a, b, c) is not necessarily consecutive.

1.2 *Data Group Presence Map*. The Data Group Presence Map (DGPM) contains information, which enables a receiving State or approved receiving organization determine which Data Groups are present in the block of data recorded by the issuing State or organization.

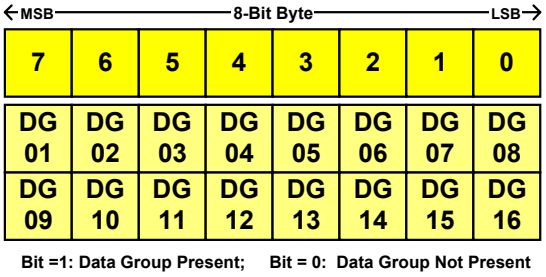
1.2.1 DGPMs can take two (2) forms as follows,

1.2.1.1 *Form 1 DGPM*. Form 1 DGPM is used with integrated circuit implementations. It consists of a list of "TAGs", consistent with the convention for identifying Data Elements recorded in IC(s) with contacts and contactless IC(s) in which each TAG identifies if a specific Data Group is recorded in the block of data recorded by the issuing State or organization. This DGPM is implemented as a tag list, Tag = '5C', within EF.COM. Refer to Annex A



Presence of TAG = Data Group Present
Absence of TAG = Data Group Not Present

1.2.1.2 *Form 2 DGPM*. Form 2 DGPM is used with 2-D barcode implementations[12]. It consists of a series of bytes in which each bit identifies the presence or non-presence of a specific Data Group in the block of data recorded by the issuing State or organization.



Note: the number of the bytes allocated for the DGPM is defined in each of the normative Mapping Annexes contained in Section VIII.

2. A similar 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 Map**s are located at the start of those specific Data Groups that allow optional expansion as illustrated in Figure VII-2.

Data Groups requiring the use of a Data Element Presence Map are specified in each of the normative Mapping Annexes contained in Section VII.

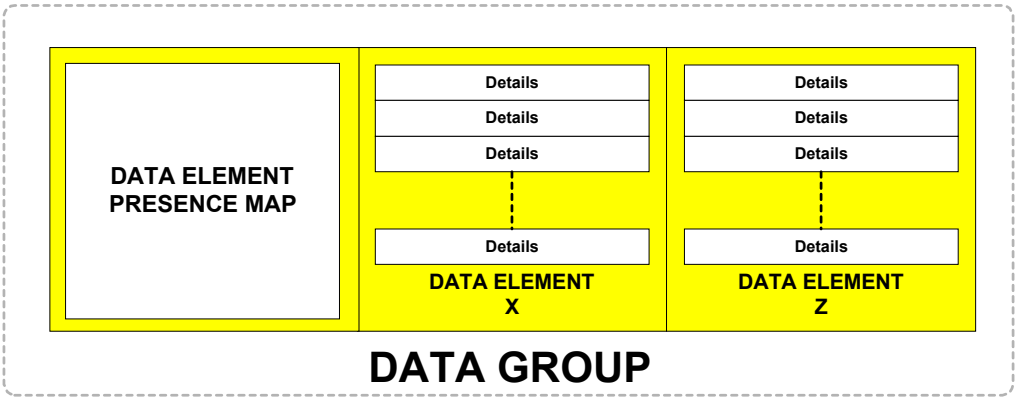


FIGURE VII-2. DATA ELEMENT PRESENCE MAP

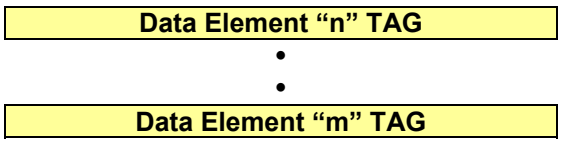
2.1 *Data Element Presence Map*. A Data Element Presence Map (DEPM) contains information to

[12]2-D barcode implementations of the LDS are not internationally interoperable. This form of the DGPM is retained for those issuers who may wish to use a 2-D barcode implementation for domestic reasons.

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

DEPMs can take two (2) forms as follows,

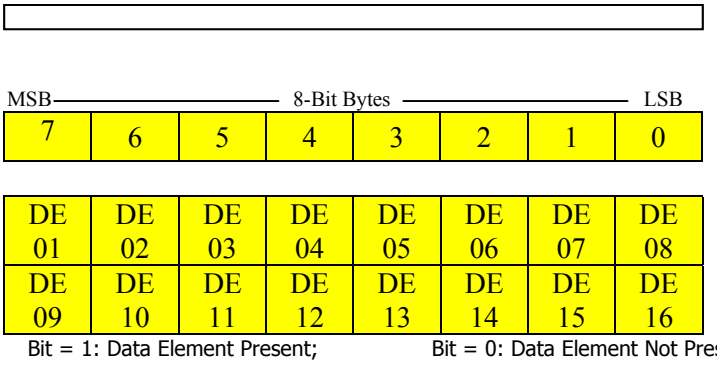
2.1.1 *Form 1 DEPM*. Form 1 DEPM consists of a list of "TAGs", consistent with the convention for identifying Data Elements recorded in IC(s) with contacts and contactless IC(s) in which each TAG identifies if a specific Data Element is recorded in the Data Group. This form of DEPM is encoded as a Tag list within the relevant Data Group.



Presence of TAG = Data Element Present
Absence of TAG = Data Element Not Present

Note: the number of the bytes allocated for the DEPM is defined in each of the normative Mapping Annexes contained in Section VIII.

2.1.2 *Form 2 DEPM*. Form 2 DEPM is used with barcode implementations.[11] It consists of a series of bytes in which each bit identifies the presence or non-presence of a specific Data Element within the Data Group; and



Note: the number of the bytes allocated for the DEPM is defined in each of the normative Mapping Annexes contained in Section VIII.

VIII. MAPPING ANNEXES

Scope

1. This Section defines the principles that shall be followed when mapping the Logical Data Structure – LDS [Version 1.7] to any of the optional capacity expansion technologies specified for use with MRTDS.

2. Principles are presented in normative Mapping Annexes specific to each technology as follows,

ANNEX A: Normative - Mapping of LDS [Version 1.7] Using Random Access File Representation to *Integrated Circuits (IC(s))*

ANNEX B: Normative Under Bilateral and Multilateral Agreements - Mapping of LDS [Version 1.7] Using Random Access File Representation to *Optional Optical Memory*; and

ANNEX C: Informative - Mapping of LDS [Version 1.7] Using Sequential File Representation to *Optional 2-D Bar Codes*;

ANNEX A (NORMATIVE) to Section VIII

MAPPING OF LDS [VERSION 1.7] USING RANDOM ACCESS REPRESENTATION TO CONTACTLESS INTEGRATED CIRCUITS (IC(S))

A.1 Scope - Annex A defines the current specifications[13] governing mapping of the Logical Data Structure – LDS [Version 1.7] using a *random access representation* to integrated circuits (IC(s)) on an MRTD to allow expansion of the machine readable data capacity at the discretion of the issuing State or organization.

Note: The specifications presented in Annex A apply only to a LDS supporting "off-card" biometric authentication, i.e., where the MRTD provides the LDS to machine-assisted identity confirmation that requires the MRTD to act only as the carrier of data.

A.2 Normative references - Please refer to Section II.2

A.3 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 MRTD authentication, rightful holder authentication, and expedite processing at document/person points.
- The data structure must support
  - 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 and on chip asymmetrical encryption. Details of such active authentication are contained in the Technical Report "PKI for Machine Readable Travel Documents offering ICC read only access".
- Support rapid access of selected Data Elements to facilitate rapid document holder processing
  - Immediate access to necessary data elements
  - Direct access to data templates, biometric data in particular

[13] *Specifications* as envisaged based on work completed to date.

A.3.1 To provide interoperability Annex A defines:

- Initializations, anticollisions and transmission protocol
- Command set;
- The use of commands including security references
- The file structure for the ICAO MRTD LDS application; and
- The Data Element mappings to the files.
- Character set[14]

A.4 Security Requirements - Data integrity and authenticity are needed for trusted international interchange. For detailed specifications refer to Technical Report "PKI for Machine Readable Travel Documents offering ICC read only access".

A.5 Compatibility with Existing International Standards - Compatibility with existing standards is critical to facilitate implementation and insure interoperability. Therefore, this specification will maximize compatibility with the standards mentioned in II.2 ,

A.6 Definitions - Please refer to Section II.2

A.7 Physical Characteristics - The physical characteristics of the document shall adhere to the physical characteristics specified by ICAO Doc. 9303.

A.8 Location and Dimensions of Coupling Areas –

A.8.1 The size of the coupling area shall be in accordance with ISO/IEC 14443.
A.8.2 The location of the coupling area shall be in accordance with ISO/IEC 14443 for TD-1 size documents and left to the issuer's discretion for TD-3 documents.

A.9 Electronic signals: The radio frequency power and signal interface are defined in ISO/IEC14443.

A.10 Transmission Protocols and Answer to Request

A.10.1 **Transmission protocols -** The MRTD will support half-duplex transmission protocol defined in ISO/IEC14443-4. The MRTD may support either Type A or Type B transmission protocols

[14] UTF-8 encoding is used. Most of the data elements used in the LDS are Basic Latin (ASCII) characters or binary. A small number of data elements such as "Name in National Characters," "Place of Birth" etc cannot always be encoded with the Basic Latin code set. Therefore, characters will be encoded using the Unicode Standard: UTF-8. It is a variable length encoding that preserves ASCII transparency. UTF-8 is fully compliant with Unicode Standard and ISO/IEC 10646. UTF-8 uses one byte to encode standard ASCII characters (code values 0…127). Many non-ideographic scripts are represented with two bytes. The remaining characters are represented with three or four bytes. Using UTF-8 allows for easy incorporation of non-ASCII characters without the overhead of two, three or four byte representation for all characters.

.

A.10.2 **Request for Command –** The IC shall respond to Request for Command - Type A (REQA) or Request for Command – Type B (REQB) with Answer to Request – Type A (ATRA) or Answer to Request – Type B (ATAB) as appropriate with the settings defined in Normative Appendix 3 to Annex A

A.10.3 **Application Selection –** IC cards shall support at least one Machine Readable Travel Document (MRTD) applications, as follows:

- One application shall consist of data recorded by the issuing State or organization [Data Groups 1-16] and Security Data (EF.SOD) that is needed to validate the integrity of data created by the issuer and stored in DF1. The Security Data (EF.SOD) consists of the hashes of the Data Groups in use, Refer to Technical Report "PKI for Machine Readable Travel Documents offering ICC read only access" for detailed information.

- The second application, **not supported in Version 1.7**, will consist of data added by receiving States or approved receiving organizations. [Data Groups 17-19].

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 this normative Annex.

The MRTD applications shall be selected by use of the Application Identification (AID) as a reserved DF name. The AID shall consist of the Registered Application Identifier (RID) assigned by ISO according to ISO/IEC 7816-5 and a Proprietary Application Identifier Extension (PIX) as specified within this document.

```
The RID is 'A0 00 00 02 47'.
     The issuer stored data application shall use PIX = '1001'
     .
```

A.10.4 **Security**

Data Groups 1 – 15 inclusive shall be write protected. A hash for each Data Group in use shall be stored in the Security Data (EF.SOD). The Security Data shall also contain a digital signature of the hashes in use. Refer to Technical Report "PKI for Machine Readable Travel Documents offering ICC read only access".

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

Data Group 16 shall be write-protected. Only the issuing State or organization shall have write access to the Data Elements in this Data Group.

Data Groups 17, 18 and 19 - To be defined in Version 2 of the LDS.

A.11 File Structure - Information on an IC card is stored in a file system defined in ISO/IEC 7816-4. The card file system is organized hierarchically into dedicated files (DF's) and elementary files (EF's). Dedicated files (DF's) contain elementary files or other dedicated files. An optional[15] master file (MF) may be the root of the file system.

[15] The need for a master file is determined by the choice of operating systems

DF1 (Mandatory) as defined by this specification contains issuer data elements. This DF has the name 'A0 00 00 02 47 10 01' for the application (the registered RID and PIX) and is selected by this name. If the card has an MF, it can be placed anywhere in the DF tree attached to the MF of the card.

Within each application there may be a number of "Data Groups." The issuing State or organization application may have up to 16 Data Groups. Data Group 1 [DG1], the Machine Readable Zone (MRZ), is mandatory. While the *use* of biometrics is optional for issuing authorities, *IF* a choice is made to incorporate biometrics, Data Group 2, the encoded face, is therefore also Mandatory. All other Data Groups are optional. The receiving State or approved receiving organization application may have three Data Groups (DG17-19). These three Data Groups are optional. All Data Groups are in the form of data templates and have individual ASN.1 Tags.

A.11.1 **DF1**

DF1 has one file (name EF.COM) that contains the common information for the application. The short file identifier as the file identifier for this file is 30 ('1E'). This file will contain the LDS version information, Unicode version information and a list of the Data Groups that are present for the application. Each Data Group shall be stored in one transparent EF addressable by short file ID as shown in table A1. 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. The name of the EF containing the security data is EF.SOD. See Figure A-1 for a graphical representation of the file structure.

ISSUING STATE OR ORGANIZATION APPLICATION				
Data Group	EF Name	Short EF 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'
Security Data	$EF.SO_D$	'1D'	'01 1D'	'77'

Table A1

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.

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 7816-6. Each data object has an identification Tag that is specified in hexadecimal coding (for example, '5A'). The tags defined in this Annex 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). The definitions contain the specific reference to the Data Element number defined in section 13. 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 MRTD application. As examples,

Tag 5A is defined as Document Number rather than Primary Account Number and has the format F9N rather than V19N.

Tag 5F20, Cardholder name, has been redefined as "Name of holder" with length of up to 39 characters, encoded per ICAO 9303 format.

Tag 65 is defined as the Displayed Portrait rather than Cardholder Related Data.

As needed additional Tags have been defined within the 5F01 through 5F7F range.

A.12 Command Set - The minimum set of commands to be supported by the MRTD are as follows:

- SELECT FILE
- READ BINARY

The command parameters that are mandatory and optional are specified in Appendix 2 to this Annex. Appendix 2 also describes the command option for accessing files with length greater than 32,767 bytes.

All commands, formats, and their return codes are defined in ISO/IEC 7816-4. Please refer to normative Appendix 2 to this Annex for examples of use of these commands.

It is recognized that additional commands will be needed to load and update data securely, establish the correct security environment, and implement the optional security provisions identified in the Technical Report "PKI for Machine Readable Travel Documents offering ICC read only access". Such commands are outside the scope of this interoperability specification, but may include

- GET _CHALLENGE
- EXTERNAL_AUTHENTICATE
- PSO_MSE
- PSO_CDS
- VERIFY_CERTIFICATE.

A.13 Issuer Data Application

Issuer data application**, AID = 'A0 00 00 02 47 10 01' -** The issuer application consists of two mandatory Data Groups and fourteen optional Data Groups. The information common to the Data Groups

is stored in the application template ‘60’. This template is stored in the mandatory file EF.COM.

A.13.1 EF.COM – common data elements (short file ID = 30 (‘1E’))

Application Template Tag ’60’ – application level information

Note: this template currently only contains revision levels and the tag list ‘5C.’ The template structure has been defined to support future developments, such as dynamic signatures and Biometric Information Templates BITs). The data elements that may occur in this template are:

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’	X	Tag list. List of all Data Groups present.

The following example indicates that 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 RED, the Lengths printed in blue, and the Values are printed in black. 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.13.2 EF.DG1 Machine Readable Zone Information Tag = '61' Mandatory

- This EF contains the mandatory Machine Readable Zone (MRZ) information for the document in template '61.' The template contains one data object, the MRZ in data object '5F1F.' The MRZ data object is a composite data element, identical to the OCR-B MRZ information printed on the document.

Tag	L	Value
'5F1F'	F	The MRZ data object as a composite data element. (Mandatory) (The data element contains all 13 primitive fields from Document Type through Composite – check digit.)

The MRZ data element is structured as follows: Note, tags are not used within this composite data element. They are included for reference only. They can be used once the data object has been parsed into individual data elements.

Field	Content	Mandatory /Optional	Format	Example	Tag (Information only)
1	Document type	M	F 2A,S	P<	5F03
2	Issuing State or Organization	M	F 3A,S	ATA	5F28
3	Name of holder[16]	M	F nn[17] ANS	Smith<<John<T	5F20
4	Document number	M	F 9A,N,S[18]	123456789	5A
5	Check digit –document number	M	F 1N,S	1 or <	5F04
6	Nationality	M	F 3A,S	HMD	5F2C
7	Date of birth	M	F 6N,S	740622 (yymmdd)	5F82
8	Check digit – Date of birth	M	F 1N	2	5F05
9	Sex	M	F 1A,S	F, M, or <	5F35
10	Date of Expiry or valid Until Date	M	F 6N	101231 (yymmdd)	59
11	Check digit – Date of Expiry	M	F 1N	3	5F06
12	Optional data	M	F nn[19]ANS	0121	53
13	Check digit – Optional data (ID-3 documents only)	M	F 1N	5	5F02
14	Check digit – Composite	M	F 1N	4	5F07

[16] Refer to ICAO 9303 for truncation rules for names longer than 39 characters
[17] For ID-1 documents nn= 30, for ID-2 documents nn+ 31, for ID-3 documents nn = 39
[18] If the document number length exceed 9 characters, a '<' character is placed in the following check digit field (Field 5) and the remaining document number digits are placed in the optional data field, immediately followed by the document number check digit. In the above example the total document number length is 12 (value = 123456789012) with check digit = 1.
[19] For ID-1 documents nn = 26, for ID-2 documents nn= 7, for passports (ID-3) nn = 14

An example of the DG1 using this information is shown below. The length of the MRZ data element is 88 bytes (‘58’).

’61’ ’5B’ ’5F1F’ ’58’
P<ATASMITH<<JOHN<T<<<<<<<<<<<<<<<<<<<<<<<<<123456789<HMD7406222M10123
130121<<<<<<<<<<54

Another example,

’61’ ’5B’ ’5F1F’ ’58’
P<NLDMEULENDIJK<<LOES<ALBERTINE<<<<<<<<<<<<XA00277324NLD7110195F06100
10123456782<<<<<08

A.13.3 EF.DG2 - EF.DG4 (one EF for each DG) Biometric Templates Tags = ‘’75’’63’’76’

DG2 – DG4 use the nested off-card option of ISO/IEC 7816-11, Table C-10, for having 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.

Each nested template has the following structure.

Notes,

The nested option of ISO/IEC 7816-11, Table C-10 is always to be used, even for encodings of a single biometric template. The latter case is indicated by numbering with n=1.

The default OID of CBEFF is used Data element ‘06’ 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 the ISO SC37 internationally interoperable biometric data block. Please refer to the Technical Report for Biometric Implementation.

The biometric data block may be encrypted for privacy using secure messaging templates as *defined in Annex D of 7816-11. Such implementations are beyond the scope of this specification.*

Tag	**L**	**Value**				
‘7F61’	**X**	**Biometric Information Group Template**				
		Tag	**L**	**Value**		
		‘02’	1	Integer - Number of instances of this type of biometric		
		7F60	X	1st Biometric Information Template		
			Tag	**L**		
			‘A1’	X	Biometric Header Template (BHT)	
				Tag	**L**	**Value**
				‘80’	‘02’	ICAO header version ’01 00’ (Optional) – Version of the CBEFF patron header format
				‘81’	‘01’	Biometric type (Optional)
				‘82’	’01’	Biometric feature (Optional for DG2,

						mandatory for DG3, DG4.)
				‘83’	’07’	Creation date and time (Optional)
				‘84’	‘08’	Validity period (from through) (Optional)
				‘86’	‘02’	Creator of the biometric reference data (PID) (Optional)
				‘87’	‘02’	Format owner (Mandatory)
				‘88’	‘02’	Format type (Mandatory)
			‘5F2E’ or ‘7F2E’	x	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).	
		Tag	**L**			
		7F60	X	2nd Biometric Information Template		
			Tag	**L**		
			‘A2’	X	Biometric Header Template (BHT)	
				Tag	**L**	**Value**
				‘80’	‘02’	ICAO header version ’01 00’ (Optional) – Version of the CBEFF patron header format
				‘81’	‘01’	Biometric type (Optional)
				‘82’	’01’	Biometric feature (Optional for DG2, mandatory for DG3, DG4.)
				‘83’	’07’	Creation date and time (Optional)
				‘84’	‘08’	Validity period (from through) (Optional)
				‘86’	‘02’	Creator of the biometric reference data (PID) (Optional)
				‘87’	‘02’	Format owner (Mandatory)
				‘88’	‘02’	Format type (Mandatory)
			‘5F2E’ or ‘7F2E’	x	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).	

Each single biometric information template has the following structure. The given biometric header template tags and their given values are the minimum each implementation must support.
Example,

One signed, facial biometric with the biometric data block length of 12642 bytes (‘3162’ bytes), encoded using a device with a PID of ’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 is being used.

The total length of the template is 12704 bytes. The template is stored starting at the beginning of EF.DG2 (SFID 02).

‘75’ ’82319C’
‘7F61’ ’823197’
‘02’ ’01’ ‘01’
‘7F60’ ‘82318F’
‘A1’ ‘26’
‘80’ ‘02’ ’0100’
‘81’ ’01’ ’02’
‘83’ ’07’ ’20020315133000’

‘84’ ’08’ ’2002040120070331’
‘86’ ’02’ ’0001’
‘87’ ’02’ ’000A’
‘88’ ’02’ ’0004’
‘5F2E’ ’823162’ ’… 12642 bytes of biometric data …’

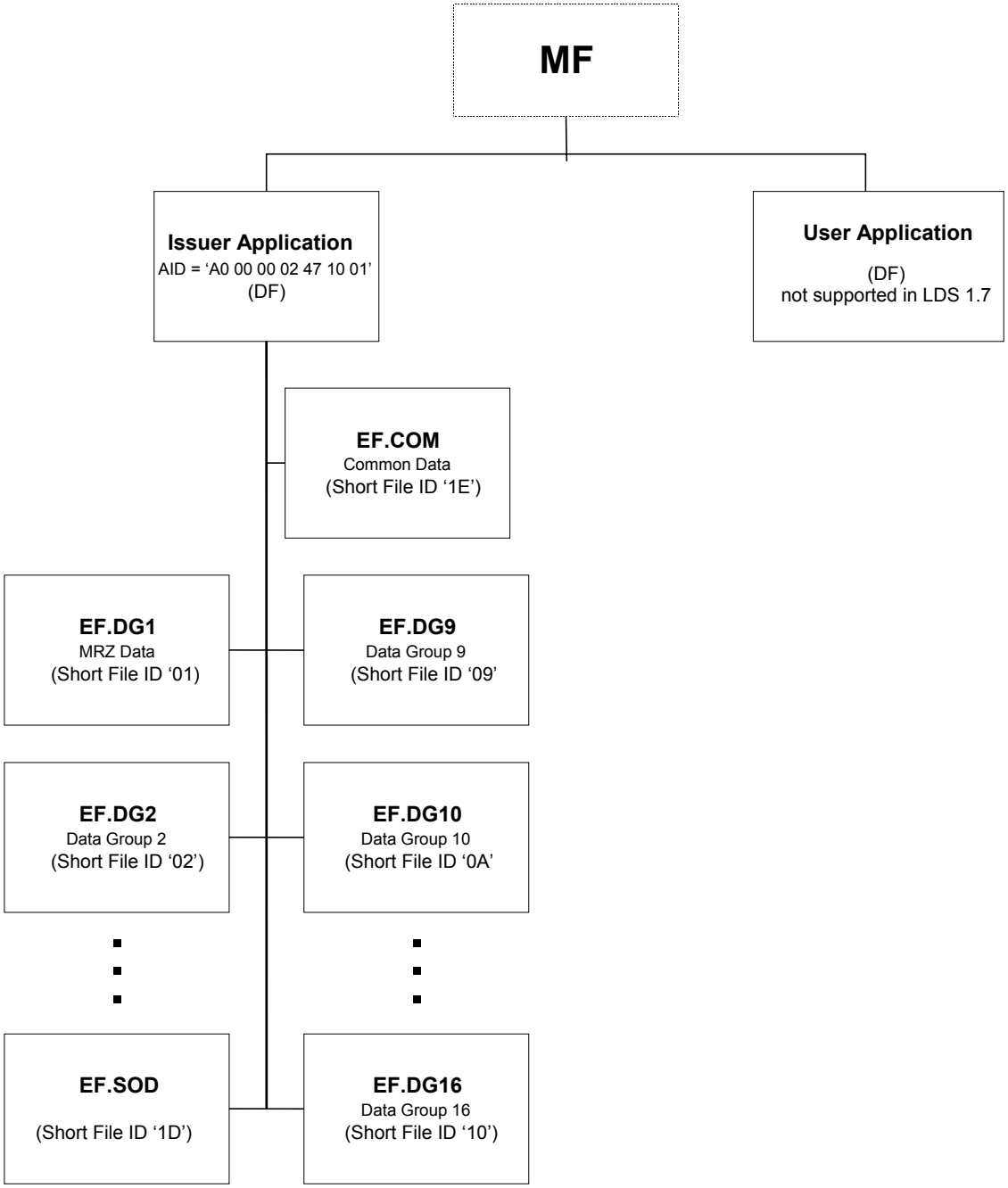

MF
Issuer Application
AID = 'A0 00 00 02 47 10 01'
(DF)
User Application
(DF)
not supported in LDS 1.7
EF.COM
Common Data
(Short File ID '1E')
EF.DG1
MRZ Data
(Short File ID '01)
EF.DG9
Data Group 9
(Short File ID '09'
EF.DG2
Data Group 2
(Short File ID '02')
EF.DG10
Data Group 10
(Short File ID '0A'
EF.SOD
(Short File ID '1D')
EF.DG16
Data Group 16
(Short File ID '10')

Figure A.1

A.13.3 EF.DG5 - EF.DG7 (one EF for each DG) Displayed Image Template

Tag = ’65’ Displayed Portraits Tag = ‘67’ Displayed Signature or Usual Mark

Tag	L	Value
‘02’	1	Integer – Number of instances of this type of displayed image (Mandatory in first template. Not used in succeeding templates.)
‘5F40’ or ‘5F43’	X	Displayed portrait Displayed signature or mark

Example, image template with the displayed image data length of 2000 bytes. The length of the template is 2008 bytes (‘07D8’).

‘65’ ’8207D8’
’02’ ’01’ 1
’5F40’ ’8207D0’ ‘….2000 bytes of image data …’

The following Format Owners are recognized for the specified type of displayed image.

Displayed Image	Format Owner
Displayed Facial Image	ISO 10918, JFIF option
Displayed Finger	ANSI/NIST-ITL 1-2000
Displayed Signature/ usual mark	ISO 10918, JFIF option

A.13.4 EF.DG8-EF.DG10 Machine Assisted Security Features, Tags ’68’’69’’6A’

These three data groups remain to be defined. Until then, they are available for temporary proprietary usage. These data elements could use a structure similar to that for biometric templates.

Tag	L	Value
‘02’	1	Integer - Number of instances of this type of template (Mandatory in first template. Not used in succeeding templates.)
	x	Header Template. Details to be defined.

A.13.5 EF. DG11 Additional Personal Details, Tag = 6B

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. Note, this template may contain non-Latin characters.

Tag	L	Value
‘5C’	X	Tag list with list of data elements in the template.
‘5F0E’	X	Full name of document holder in national characters. Encoded per ICAO 9303 rules
’A0’	‘01’	Content specific constructed data object of names
‘02’	01	Number of other names
‘5F0F’	X	Other name formatted per ICAO 9303. The data object repeats as many times as specified in the ’02’ element.
‘5F10’	X	Personal number
‘5F2B’	08	Full date of birth yyyymmdd
‘5F11’	X	Place of Birth. Fields separated by ‘<’
‘5F42’	X	Permanent Address. Fields separated by ‘<’
‘5F12’	X	Telephone
‘5F13’	X	Profession
‘5F14’	X	Title
‘5F15’	X	Personal summary
‘5F16’	X	Proof of citizenship. Compressed image per ISO/IEC 10918
‘5F17’	X	Other valid TD numbers. Separated by ‘<’
‘5F18’	X	Custody information

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’ 1-612-555-1212
’5F13’ ’0C’ TRAVEL<AGENT
’

A.13.6 EF.DG12 Additional Document Details, Tag = 6C

This data group is used for additional information about the document. All data elements within this group are optional.

Tag	L	Value
‘5C’	X	Tag list with list of data elements in the template.
‘5F19’	X	Issuing Authority
‘5F26’	X	Date of Issue. yyyymmdd
‘A0’	‘01’	Context specific constructed data object of other people
‘02’	‘01’	Number of other people

‘5F1A’	X	Name of other person formatted per ICAO 9303 rules
‘5F1B’	X	Endorsements, Observations
‘5F1C’	X	Tax / Exit Requirements
‘5F1D’	X	Image of front of document. Image per ISO/IEC 10918
‘5F1E’	X	Image of rear of document. Image per ISO/IEC 10918
‘5F85’	X	Date and time of document personalization yyyymmddhhmmss
‘5F86’	X	Serial number of personalization system

The following example contains the Issuing Authority (United States of America), the Data of Issue (May 31, 2002), one other person included on the document (Brenda P Smith). The length of the template is 64 bytes (‘40’).

’6C’ ’40’
‘5C’ ‘06’ ’5F19’ ’5F26’ ’5F1A’
‘5F19’ ’18’ UNITED STATES OF AMERICA
’5F26’ ’08’ 20020531
’5F1A’ ’0F’ SMITH<<BRENDA<P

A.13.7 EF.DG13 Optional Details

This Data Group is reserved for national specific data. Its format is country defined.

A.13.8 EF.DG15 Active Authentication Public Key Info, Tag = ‘6F’

This Data Group contains the Active Authentication Public Key Information, conforming RFC3280.

Tag	L	Value
‘6F’	X	Refer to Technical Report “PKI for Machine Readable Travel Documents offering ICC read only access”

A.13.9 EF.DG16 Person(s) to Notify, Tag ‘70’

This data group lists emergency notification information. It is encoded as a series of templates using the tag ‘Ax’ designation. The data is not signed, allowing for updating by the document holder.

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

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

A.13.10 EF.SOD LDS Security Data, Tag = ‘77’

This EF contains a signed data structure conforming to RFC3369 (ref. PKCS#7).

Tag	L	Value
‘77’	X	Refer to Technical Report “PKI for Machine Readable Travel Documents offering ICC read only access”

A.15 Receiving state application

Not supported by LDS Version 1.7.

A.16 Tags used

Revise this list once final agreement reached. If correct and complete, delete this sentence.

13.1 Normative tags used in the LDS

Tag	Definition	Where Used
02	Integer	Biometric and display templates
5C	Tag list	EF.COM and Numerous other
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
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
5F52	Telephone	Telephone number of Person to Notify
5F53	Address	Address of Person to Notify
5F85	Date and time document personalized	Additional document details
5F86	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	
70	Person to Notify	
75	Template for Facial biometric data group	
76	Template for Iris (eye) biometric template	
77	EF.SOD (EF for security data)	
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 Additional document details
Ax or Bx	Repeating template, where x defines occurrence	Biometric header,

13.2 Tags useful for intermediate processing (informative)

Tag	Definition	Where Used
53	Optional Data	Part of MRZ
59	Date of expiry or valid Until Date	Part of MRZ

5A	Document Number	Part of MRZ
5F02	Check digit – Optional data (ID-3 only)	Part of MRZ
5F03	Document Type	Part of MRZ
5F04	Check digit – Doc Number	Part of MRZ
5F05	Check digit - DOB	Part of MRZ
5F06	Check digit – Expiry date	Part of MRZ
5F07	Check digit – Composite	Part of MRZ
5F20	Name of document holder	Part of MRZ
5F28	Issuing State or Organization	Part of MRZ
5F2B	Date of birth	Part of MRZ
5F2C	Nationality	Part of MRZ
5F35	Sex	Part of MRZ
5F82	Date of birth (6 digit)	Part of MRZ

13.3 Tags reserved for future use (normative)

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	

Appendix 1 to Annex A (Normative)

This appendix defines the minimum requirements for interoperability of proximity[20] (ISO/IEC 14443) contactless IC based MRTDs.

- ISO/IEC 14443 Parts 1-4 and ISO/IEC 10373-6 compliant also considering amendments to both standard series.
- Type A or Type B signal interface[21]
- Support for a file structure as defined by ISO/IEC 7816-4 for variable length records
- Support for one or more applications and appropriate commands as defined by ISO/IEC 7816-4, 5.
- For more detailed information please refer to the Biometrics Deployment Technical Report.

[20] The use of vicinity cards, ISO/IEC 15693, may be considered in the future
[21] Note this implies that readers (Proximity Coupling Devices) must be capable of reading Type A and B.

Appendix 2 to Annex A (Normative)

This Appendix defines the commands and command parameters that may be used by the interface device. The required commands and the required and optional command parameters are described with their use in a typical processing sequence. Other commands and command parameters are outside the scope of this specification.

The Appendix describes the typical processing sequence for the selection of the DF1 application and the retrieval of data from an elementary file. The same retrieval (read) process is used for all elementary files in the DF. The validity of the data groups from DF1 may then be verified by calculating the hash value for a data group and comparing it to the hash valued retrieved from the Security Data EF.SO_D.

The typical sequence of actions will be as follows:

- Document enters operating field of Proximity Coupling Device (PCD)

- IC responds to Request for Command-Type A (REQA) or Request for Command-Type B (REQB) with Answer to Request-Type A (ATQA) or Answer to Request-Type B (ATQB) as appropriate.

- The PCD shall detect and resolve any collision that may occur if multiple documents are within the operating field.
  - ICAO AFI = *See "Biometric Deployment Technical Report"*

- Compliance with 7816 commands shall be indicated by
  - Type A: SAK (Select Acknowledge) bit 6 = 1, bit 3 = 0
  - Type B: ProtocolProtocol Type = "0001"

  The ICAO MRTD Issuing State Application shall be selected.

- The elementary files are then selected and read as required. The same selection and read process is used for all EFs. The commands formats are described at the end of the Appendix.

  - An EF may be selected by use of a SELECT command. The data is read from the EF by a series of basic READ BINARY commands with each command specifying a subsequent data area to be read. This command is mandatory.

  - Optionally, the EF may be selected by specifying the SFID of the EF in the first READ BINARY command (initial data area). The remaining data is then read by the series of basic READ BINARY commands with each command specifying a subsequent data area to be read. Note: support of this selection method is optional.

- First, the common data file EF.COM (Short File ID = '1E') containing Application Identifier, Version levels and tag list in template '60' is read.

- The tag list in EF.COM lists the Data Groups (Elementary Files) that are present in DF1. The interface device determines which of the Data Groups (EFs) are to be read and used. Each EF is then accessed to obtain the Data Group from the EF.

- The Machine Readable Zone (MRZ) is normally the first EF read.
- Other EF's are read to obtain the corresponding Data Groups as needed.
- $EF.SO_D$ is then read to confirm the integrity of the Data Groups read from DF1. Note, optionally, $EF.SO_D$ could be read first.

DETAILS ON ISO 14443 TYPE A
INITIALIZATION AND ANTICOLLISION ACCOURDING TO ISO 14443 TYPE A

REQA AND WUPA

The PICC is expected to be in the IDLE state after it is powered. It listens for commands and shall recognize REQA and WUPA commands. Both commands are transmitted within a short frame (7 bits).

Command	b7	b6	b5	b4	b3	b2	b1
REQA = '26'	0	1	0	0	1	1	0
WUPA = '52'	1	0	1	0	0	1	0

A compatible PICC must respond to these commands, all other values are prohibited in this context.

ATQA

After a REQA Command is transmitted by the PCD, all PICCs in the IDLE state shall respond synchronously with ATAQ.
After a WUPA Command is transmitted by the PCD, all PICCs in the IDLE or HALT state shall respond synchronously with ATQA.
The ATQA Response consists of two byte. According to ISO 14443-3 the MSB contains only RFU and proprietary bits, so this byte must be ignored by any compliant software.

The bits 7 and 8 of the LSB specify the PICC UID size according to the following table

b8	b7	Meaning
0	0	UID size : single
0	1	UID size : double
1	0	UID size : triple
1	1	RFU

A compliant PICC must return one of the three valid UID sizes.
The bits 1 – 5 of the LSB indicate bitframe anticollision. One and only one of these bits must be set. Bit 6 is RFU and must not be evaluated by any software.

ANTICOLLISION AND SELECT

According to the UID size determined by the ATQA Response, a select command must be sent for each cascade level. If a collision occurs a anticollision loop shall be performed.
For the select command only the values of '93' (cascade level 1), '95' (cascade level 2) and '97' (cascade level 3) are allowed.
After the anticollision loop is done, a single PICC is selected and returns SAK Response. The

SAK consists of a single byte where only two bits are significant. Bit 3 indicates that the UID is not yet completely transmitted, that means that another select/anticollision loop must be performed on the next cascade level.
If Bit 3 is not set, Bit 6 specifies whether the PICC is ISO 14443-4 compliant. All PICCs used to store LDS data are required to support 14443-4, so this Bit must be set.

REQUEST FOR ANSWER TO SELECT (RATS)

After the anticollision and select loop is performed, a RATS must be sent to the PICC. The RATS consists of a fix start byte 'E0' and a parameter byte which specifies the maximum frame size of the PCD and a CID. The CID is specified in the least significant half byte; it is used to identify the PICC while it is active.
The most significant half byte (FDSI) contains the maximum frame size (FSD) according to the following conversion schema.

FDSI	'0'	'1'	'2'	'3'	'4'	'5'	'6'	'7'	'8'	'9' – 'F'
FSD	16	24	32	40	48	64	96	128	256	RFU (>256)

For transfer of LDS data, a compliant reader must support a frame size of 256 bytes; therefore the most significant half byte of the parameter byte must be '8'.

ANSWER TO SELECT

The answer to select specifies information about the PICC capabilities. It contains up to three interface bytes. The first interface byte TA (1) contains the bit rate capability of the PICC. The second byte TB (1) conveys information to define the frame waiting time and the start-up frame guard time. The third interface byte TC (1) specifies protocol parameter. The least significant byte must be 1 if the PICC supports NAD. The second byte must be 1 if the PICC supports CID.
All other bits are RFU and must be ignored by any compliant software.
After the interface bytes the historical bytes follow. They contain general information about the PICC and should not be evaluated by compliant software.

DETAILS ON ISO 7816
COMMAND FORMATS AND PARAMETER OPTIONS

Application Selection
Applications have to be selected ether by their file identifier or their application name. After the selection of an application, the file within this application can be accessed.
Hint: Application names have to be unique. Therefore selection of an application using the application name can be done from wherever needed.

Selection of Master File

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

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.

CLA	INS	P1	P2	Lc	Data	Le

‘00’	‘A4’	‘04’	‘0C’	Var.	AID	-

EF Selection using the SELECT command

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

CLA	**INS**	**P1**	**P2**	**Lc**	**Data**	**Le**
‘00’	‘A4’	‘02’	‘0C’	‘02’	FileID	-

Reading Data from the EF

There are mainly two ways to read data. First by selecting the file and then read the data (recommended) or by reading the data directly using the SFI.

Reading Data of a selected file (transparent file)

CLA	**INS**	**P1**	**P2**	**Lc**	**Data**	**Le**
‘00’	‘B0’	Offset MSB	Offset LSB	-	-	MaxRet

Definition of P1 and P2:

	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**
Offset MSB	0	X	X	X	X	X	X	X
Offset LSB	X	X	X	X	X	X	X	X

Reading Data using SFI (transparent file)

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

Definition of P1 and P2:

	b7	b6	b5	b4	b3	b2	b1	b0
SFI	1	0	0	X	X	X	X	X
Offset LSB	X	X	X	X	X	X	X	X

Examples for ISO 7816 usage with LDS

Reading MRZ-Data using File Selection

The following sequence has to be used to read the data of data group 1 (mrz).

CLA	INS	P1	P2	Lc	Data	Le	Remark
'00'	'A4'	'04'	'0C'	'07'	'0A 00 00 02 47 10 01'	-	Select Issuer Application
'00'	'A4'	'02'	'0C'	'02'	'01 01'	.	Select DG1
'00'	'B0'	'00'	'00'	-	-	'00'	Read max 256 bytes

Reading Data-Group 2

The following sequence has to be used to read the data of data group 2 (Encoded Face). The length of the template is given as 12,543 bytes. The total data area is 12,547 bytes (adding one for the template tag and three bytes for the length field). This requires 49 blocks of 256 bytes each plus a final block of 3 bytes.

The next portion of the template is read by incrementing the offset by 256 bytes ('01 00'). The total amount of data to read is determined from the length of the template. It is recommended that the last READ BINARY command be issued for only the residual amount of data. The final offset is '31 00'.

CLA	INS	P1	P2	Lc	Data	Le	Remark
'00'	'A4'	'04'	'0C'	'07'	'0A 00 00 02 47 10 01'	-	Select Issuer Application
'00'	'A4'	'02'	'0C'	'02'	'01 02'	.	Select DG2
'00'	'B0'	'00'	'00'	-	-	'00'	Read first 256 bytes
'00'	'B0'	'01'	'00'	-	-	'00'	Read next 256 bytes
'00'	'B0'	'02'	'00'	-	-	'00'	Read next 256 bytes
'00'	'B0'	'03'	'00'	-	-	'00'	:

When reading more than one data group consecutively, the Issuer Application has to be selected only once (before reading the first file).

Reading MRZ-Data using global SFI

CLA	INS	P1	P2	Lc	Data	Le	Remark
'00'	'B0'	'81'	'00'	-	-	'00'	Direct Read of 256 bytes

Reading Data-Group 2 using global SFI

The first bytes of the file can be read using the Read Binary Command in combination with the SFI. The following bytes have to be read using the "standard" Read Binary Command.

CLA	INS	P1	P2	Lc	Data	Le	Remark
'00'	'B0'	'82'	'00'	-	-	'00'	Direct Read of 256 bytes
'00'	'B0'	'01'	'00'	-	-	'00'	Read next 256 bytes
'00'	'B0'	'02'	'00'	-	-	'00'	Read next 256 bytes
'00'	'B0'	'03'	'00'	-	-	'00'	:

EFs larger than 32,767 bytes

The maximum size of an EF is normally 32,767 bytes, but some 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.

CLA	INS	P1	P2	Lc	Data	Le	Remark
'00'	'B1'	'00'	'00'	Var.	*Offset TLV encoded*	'00'	Reading files greater than 32.767 bytes

Example for encoded Offset in Data-field:
Offset: 'FF FF' is encoded as '54 02 ff ff'

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

APPENDIX 3 TO NORMATIVE ANNEX A

ASN.1 LENGTH ENCODING RULES

Range	# 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 MS byte	LS byte
MS = most significant byte; LS = least significant byte				

Note: Quotation marks (') are used to visually separate hexadecimal characters. They are not encoded in the LDS.

Based on the above defined rules,

Example 1: a Length of thirty nine (39) would be encoded as '27' in hexadecimal representation.

Example 2: a Length of one hundred ninety nine (199) would be encoded as '81C7' in hexadecimal representation.

Example 3: a Length of one thousand (1000) would be encoded as '8203E8' in hexadecimal representation.

Appendix 4 to Normative Annex A
Biometric Sub-feature Encoding

b8	b7	b6	b5	b4	b3	b2	b1	Biometric Feature
0	0	0	0	0	0	0	0	No information given
		0						Indication of mask
1								Right e.g., right iris
	1							Left
			0	0	0	0	1	Right Thumb
			0	0	0	1	0	Right Index
			0	0	0	1	1	Right Middle
			0	0	1	0	0	Right Ring
			0	0	1	0	1	Right Little
			0	0	1	1	0	Left Thumb
			0	0	1	1	1	Left Index
			0	1	0	0	0	Left Middle
			0	1	0	0	1	Left Ring
			0	1	0	1	0	Left Little

ANNEX B (NORMATIVE) to Section VIII

MAPPING OF LDS [Version 1.7]

TO OPTIONAL
OPTICAL MEMORY

B.1 Scope - Annex B defines the current state of development of specifications[22] governing mapping of the Logical Data Structure – LDS [Version 1.7] using *random access* to optical memory on TD-1 size cards to allow expansion of the machine readable data capacity at the discretion of the issuing State or organization.

B.2 Normative references - The following International Standards contain provisions which, through reference herein, constitute provisions of Annex B to Section VIII of this Technical Report. Where differences exist between the specifications contained in this Technical Report and the referenced Standards to accommodate the use of bar code(s), the specifications contained herein shall prevail.

ISO/IEC 11693:2000 Identification cards - Optical memory cards - General characteristics.

ISO/IEC 11694-1:2000 Identification cards - Optical memory cards - Linear recording method - Part 1: Physical characteristics.

ISO/IEC 11694-2:2000 Identification cards - Optical memory cards - Linear recording method - Part 2: Dimensions and location of the accessible optical area.

ISO/IEC 11694-3:2001 Identification cards - Optical memory cards - Linear recording method - Part 3: Optical properties and characteristics.

ISO/IEC 11694-4:2001 Identification cards - Optical memory cards - Linear recording method - Part4: Logical data structures.

NISTIR 6529-A Common Biometric Exchange File Format (CBEFF)

B.3 Definitions – The following definitions shall apply,

Application: Since the optical memory on a TD-1 contains digital storage, this data is accessed by a computer application that reads the data and makes use of the information it contains. Applications change just like data formats, and so application versions as well as data format versions must be a consideration.

Data item: A well defined data element or set of data. A data item requires no other data in order to be useful. It is read in its entirety from one or more sectors. A data item may contain sub-elements, but should contain no optional sub-elements that cannot fit into the sector with the required sub-elements.

Sector: The smallest area on a random access media that can be accessed. A fraction of a sector cannot be written to or read from. The entire sector must be read or written to.

Data sector: A sector that contains all or part of a TLV data stream.

[22] *Specifications* as envisaged based on work completed to date. Specifications will only be considered final when they have been published in Doc 9303.

Directory: A structure used to keep track of the presence and/or location of data on a random access media.

Directory sector: A sector on a random access media that contains directory information.

MRTD Tag: A unique unsigned 16-bit number used to identify a data item stored on the document. A single set of tags applies to any and all data stored on any random access optical memory resident on a TD-1 that conforms to the specifications defined herein.

Tag, Length, Value (TLV) data stream: A storage structure that involves placing data in serial fashion on a storage medium and keeping track of it through a tag, which identifies the meaning of the data, followed by the length of the data in bytes, followed by the value, which is the data itself. The last byte of the 'value' part is then optionally followed by another TLV structure. The stream is terminated by a tag of zero. Although such a data stream is a serial entity, a random access technology can contain any number of such streams, and parts of a TLV stream can be read independently if desired.

Track: A data area on an optical memory resident on a TD-1 that can contain one or more sectors

Unique stamp: A unique 12-byte value that is created based on the time of writing and the unique serial number of the optical memory card writer. This is used to identify two separate sectors as containing parts of the same logical data stream.

Note: All numbers are in decimal unless otherwise specified.
Note: All multi-byte numbers are stored little-Endian format (least significant byte first) unless otherwise specified.

B.4 General Structure – While access to serial devices is relatively simple, random access storage has associated with it the idea of 'geography'. The issuer of the document can and must define where on the document a given item of data is to be written. In the case of optical memory cards, this is defined by track and sector numbers and by the choice of sector format for a given track.

For serial storage technologies, all of the data must be read if any is read. For random access technologies, a part of the data set can be read without having to read other parts. To take advantage of this capability, a directory structure is required on the media. This structure allows the reader to read a desired subset of the data by telling the reader which data items (specified by a unique MRTD tag) are present on the media, and where to find each.

This standard does not define the exact location of any piece of data on the media. It defines only a starting point for the directory of the media. The starting point tells the reader where the directory for the media starts. The location of the remainder of the directory and of the data itself is contained in the directory itself. The reading application can make use of the standard and the directory to find the rest of the directory and the data no matter where the writing application has chosen to write it.

So the starting point and the directory structure allow the reader to determine the presence and location of any desired data item on the media. This leaves only the definition of the data item itself to be resolved. This is done through tags and the tag document

B.5 The TLV Structure and TAG - An MRTD tag is a unique number that is used to identify a type of data item. The standard will define some of the tags and their associated data items. Other tags will be issued and defined as needed by the document issuer. The tags will be kept unique and their meaning published by the tag issuing body. Groups of numerically adjacent tags will be issued to a document issuer by the tag issuing body as required for the document being issued. It is the responsibility of the document issuer to return to the tag issuing body a description of the data item associated with each tag it intends to use when issuing its document. Each tag or set of tags will be described by a 'tag document' which will completely describe the use and format of the data to be

associated with the tag. These new tags and definitions will then be added to the standard so that other document issuers or receiving organizations can use them. A tag that is issued to a given document issuer that is not then described to the tag issuing body is considered 'issued and proprietary" and documents created using such tags still fall within the standard. A standard reading system will ignore the data associated with such tags. Tags that are not proprietary will be published by the tag issuing body as soon as they are accepted.

Each tag is a 16-bit unsigned number. This allows for 65535 tags, which will be adequate for all implementations. Within a TLV (tag, length, value) data stream, which contains one or more TLV items, the L or length part of the stream will be a 32-bit unsigned number, which allows a single piece of data to be up to 4 Gb in length. This is adequate because the highest capacity technology included in the standard has a maximum user data capacity of approximately 3 Mb.

What tags do:

- Tell the reader of the document (by lookup) the intended meaning of the associated data. This can be considered 'the type of data'.

- Tell the reader of the document (by lookup) the layout or format of the associated data

What tags do not do:

- Tell the reader the date or time that the data was obtained or recorded

- Tell the reader who recorded the data

- Tell the reader how many data items of this type exist on the document or indeed anything about any other piece of data of this type or any other type.

- Authenticate the source of the data

The functionality of this latter list is left to the data item itself. The data item will contain any information that is defined in the tag document for the associated tag, so the tag document can define the data item as having date and time stamps, who recorded the data, etc.

A tag may be associated with a single well defined piece of text, such as a person's name, but often will be associated with a standard fixed format data set. An example of such a set is a standard JPEG file. The data inside a JPEG file conforms to a standard, and many software applications and components know how to read and display such a file. The file itself contains information about the image contained in the file, such as width, height, etc. A tag may call out a standard JPEG file, or may call out a specific type of JPEG file. For example, the tag for a 'Document holder portrait' may call out a standard JPEG file that is of a specified minimum width and height that contains an image of the person's head and neck, and shows at least one ear. The data set associated with this tag is not limited to just holding a JPEG file: it may contain any other information which the card issuer wants to include with the image. For example, the date and time the picture was taken, the date and time the picture was written to the document, etc.

Another example of a standard data set that may be associated with a single tag is the machine readable zone (MRZ) data set that is currently printed as OCR characters on passports. Since the format of this set of fields is standardized, the tag document need only describe the standard that is used.

B.6 Guidelines for Assigning Data to Data Elements –

Because the standard allows different data elements to be placed within a single data item, or split up

into different data items, a card issuer must decide how to break up their data into items. Here are a few guidelines:

- If two data elements are useless without each other, they should be in the same data item
- If a data element is optional, it should be in its own data item
- If several data elements are always written and read together, they should be in the same data item
- If several data elements are small enough to fit in a single sector together, they should be in the same data item.

If a data element will be updated independently of other data elements, that element should not be in the same data item.

B.7 Biometric data –

It is expected that most MRTD's will contain at least one biometric identifier. In order to facilitate interoperability of MRTD's with other systems that make use of biometric data, the standard format for biometric data items in MRTD's will be the Common Biometric Exchange File Format (CBEFF) as defined in NISTIR 6529-A. CBEFF is not yet a standard, but is being promoted as a standard for the exchange of biometric data elements. A document issuer can issue documents that meet this standard (MRTD), but which do not meet CBEFF requirements - but such data elements will be considered as proprietary data items and the associated tag documents will be published by the MRTD tag issuing authority as "proprietary" with no details of the format included in the accepted tag document. In other words, any 'standard' biometric must meet the CBEFF requirements.

B.8 The Tag Document –

This standard requires the creation of a standard tag document that contains a unique tag or a unique consecutive set of tags and a description of the data that is associated with that tag or set of tags.

The tag document is a kind of a mini-standard that describes a single type of data. The document may itself completely describe the data in question or may refer to other standards or documents.

A tag document must contain the following minimum set of information:

1.) The tag or consecutive set of tags to be defined
2.) The title of the tag or tag set
3.) The name and contact information of the requesting organization
4.) The date the tag document was submitted to the tag issuing body
5.) The date the tag document was accepted by the tag issuing body (if accepted)
6.) The status of the tag document (submitted, accepted, etc.)
7.) Any standards that apply to the format of the data
8.) A complete description of the format and content of the data to be associated with the tag.
9.) If multiple tags are defined, a complete listing of the difference in meaning from one tag to another.

The description part can contain references to other documents, which together with the tag document completely define the associated data.

Here is an example of a tag document:

Tag(s):	2010 - 2019
Title:	Government of Potsylvania fingerprint biometric Version 1.7
Requested by:	Government of Potsylvania, Passport division

123 Main Street
Potsylvania

Administrator: Joe Smith (jsmith@potsylvania.gov)
Phone: 99 123-456-7890

Date submitted: 2001.10.03
Date accepted: 2001.12.04
Status: Accepted. In use.

Applicable Standards: NISTIR 6529-A Draft Version 2 (02/11/01)
Common Biometric Exchange File Format

Description:

This data item contains a CBEFF compliant file containing a fingerprint biometric template created by the FingerId corporation FP-101 fingerprint biometric identifier system version 4.5 or later compatible. The following required and optional CBEFF fields are included in this file:

Format owner:	C12B (hex)	Finger ID corporation
Format type:	0003 (hex)	FP-101 and compatibles
SBH Security Options	30 (hex)	Privacy and Integrity
Integrity	02 (hex)	Signed
Biometric Type	08 (hex)	Fingerprint
Biometric Feature	001fffhh (binary)	Finger as defined in CBEFF (f = finger, h = hand)
Format document:	CBEFF.C12B.0003	Document fully describing the BDB format

The SBH Security Options value will never change, but the reader of passports must be prepared for the Integrity option to switch from 0x02 (signed) to 0x01 (MAC'ed), which is planned for the future.

The BDB of this file contains the following fields:

Offset (bytes)	Length (bytes)	Example	Meaning
0	10	“2001.12.01”	Date the fingerprint template was created
10	8	“12345678”	ID number of biometric device
18	500	---	Standard Finger Id template version 4.5 or greater

The tag set applies as follows:

Tag	Finger
3010	Right hand thumb
3011	Left hand thumb
3012	Right hand index finger
3013	Left hand index finger
3014	Right hand middle finger
3015	Left hand middle finger
3016	Right hand ring finger
3017	Left hand ring finger
3018	Right hand little finger
3019	Left hand little finger

In addition to the particular finger being encoded into the tag to allow the reader to determine the finger from reading only the directory, the reader can determine the finger from the optional

'Biometric Feature' field of the CBEFF file.

The government of Potsylvania had a choice to encode the finger within the data item or to use different tags. It was decided to request one tag for each finger so that receiving states could determine more quickly from the directory which fingers were present on the media without having to read the data.

B.9 MRTD TAG Ranges Defined by the Standard –

Tag (decimal)	Data Group	Mandatory/ Optional	Data Item
0	-	-	Reserved for end of TLV stream. Finding a tag value of zero tells the reader to stop reading because the TLV stream has ended.
1000	1	M	Machine Readable Zone (MRZ) data
2000	2	O	Encoded Face
3000	3	O	Encoded Finger
4000	4	O	Encoded Eye
5000	5	O	Encoded Hand
6000	6	O	Displayed Portrait
7000	7	O	Displayed Single-Digit Fingerprint
8000	8	O	Displayed Signature or Usual Mark
9000	9	O	Data Features
10000	10	O	Structure Features
11000	11	O	Substance Features
12000	12	O	Additional Personal Data Elements
13000	13	O	Additional Document Data Elements
14000	14	O	Discretionary Data Elements
15000	15	O	Data Authentication Code
16000	16	O	Person(s) to Notify Data Elements

Each data group as defined by WD-002-2001-05-01 uses one tag in the preceding list. Each of these should have a corresponding tag document that contains the required data elements as specified in that document. Note that this table contains only 16 tags out of the possible 65535 tags. The rest will be defined as card issuers submit tag documents to the tag issuing body.

B.10 Mapping to TD-1 with Optical Memory

This section contains details of how the standard is mapped onto the optical memory card. This implementation allows for making the best use of the random access nature of the optical memory card.

This document uses references to ISO/IEC 11694 Part 4 Annex B. There is nothing in this document that prevents the standard from working with cards that conform to Annex A of ISO/IEC 11694 Part 4.

B.10.1 OMC Track Locations (Annex B of ISO/IEC 11694 Part 4):

Track	Meaning
0	Format Description Track (reserved by 11694 Part 4) describes card type
5	Application Description Track. This track will be written in the 1112

	byte sector format. The mandatory MRZ data set will be contained in a standard TLV stream in this sector at offset 320 (from 0) of the sector. The MRTD tag is 1000 and the length is 90 bytes. This data set is coded using the ASCII character set.
6	First directory track. This track will be written with the 1112 byte sector format on all issued documents.
7	Recommended second directory track
….	
2577	Maximum data/directory track

B.10.2 Sector Signature

Sector signatures have two purposes: to act as a signature so that a reader will be sure of only interpreting data that meets this standard, and to differentiate the different types of standard sectors on the card (i.e. data sectors vs. directory sectors).

Sector signatures defined by the standard:

Signature (hex)	Meaning
AB 4D 52 54 44 5F	Directory sector containing both tags and data addresses
AA 4C 43 46 53 5F	Data sector containing part of a TLV stream
BA EA	Alternative data sector containing multiple instances of the same type of data.

B.10.3 Layout of Directory Sectors

Directory sectors always start with the following header:

Offset (bytes)	Length (bytes)	Example	Meaning
0	6	AB 4D 52 54 44 5F (hex)	Sector signature for directory sector
2	3	7	Track address of next logical directory sector
5	1	4	Sector format of next logical directory sector

The rest of the directory sector contains multiple copies of the following structure:

Offset (bytes)	Length (bytes)	Example	Meaning
0	2	1000	Tag representing a data item on the media
2	3	200	Track address of track containing data associated with this tag
5	1	4	Sector format of track containing data associated with this tag
6	2	20	Number of tagged items in the described TLV stream

When an application that writes data to the document has written all its data, it knows which tracks it used and which track is the first available for subsequent applications to write. It points the next application to the first remaining free track by ending its list of the above structures with a final entry containing a tag of zero and containing the track address of the first free track on the media. All other fields of the structure will be set to zero. The reader application also uses this zero tag entry as a signal that no more valid tags exist in the current directory sector. Any unused part of a directory sector will be filled with zeroes.

If the number of tagged items in the described TLV stream is 1, then we already have the tag for the

data from the directory entry, and we will have the length in the data sector header (described below). In this case, the data portion of the sector will not contain the tag and length, but will contain only the single data item itself.

B.10.4 Layout Data Sectors

Most TLV stream data sectors will start out with the following header:

Offset (bytes)	Length (bytes)	Example	Meaning
0	6	AA 4C 43 46 53 5F (hex)	Sector signature for a sector containing a TLV data stream
6	2	0	Reserved for future use
8	4	3214	Length of this TLV data stream in bytes
12	4	0	Reserved for future use
16	12	-	Unique stamp for this TLV data stream
28	2	0	Offset of this sector within TLV data stream
30	2	4	Number of sectors in this TLV data stream
32	2	0	Reserved for future use
34	2	234	Byte offset of first tag within this sector

The first sector of a given TLV stream is specified in the directory. If the TLV stream consists of more than one sector, succeeding sectors of the stream will be written to and read from succeeding sectors on the same track. If the TLV stream is larger than one track, succeeding sectors of the stream will be written/read from succeeding physical tracks on the media.

For example, if a TLV stream is 3000 bytes in length and is written using a sector format with a length of 1112 bytes, the data portion of the stream will be 1112 – 36 bytes = 1076 bytes in length, so the stream will be written to 3000 / 1076 = 3 sectors (rounding up). Since the 1112 byte sector format is one sector per track, the stream will be written to and read from 3 consecutive physical tracks. If, for example, the track location for this stream in the directory was specified as track 20, then the stream will occupy tracks 20, 21, and 22 on the media. The remaining (3 * 1076) – 3000 = 228 bytes of track 22 will be written with zeroes and ignored by the application that reads the stream back.

Following the header, the data sector consists of either a partial or complete TLV stream. A TLV stream consists of one or more copies of the following structure:

Offset (bytes)	Length (bytes)	Example	Meaning
0	2	1005	Tag representing the data item to follow, e.g. First name (T field)
2	4	3	Length of the data item in bytes (L field)
6	Var	“Joe”	The data item itself has its length is the number in the L field (V field)

Any unused part of the sector will be filled with zeroes. The reader uses the first tag value of zero it encounters to signal the end of the TLV stream.

B10.4.1 Alternate Layout

Sometimes it is desired to store a lot of relatively small updates of data that has essentially the same meaning. For example, the MRV data corresponding to stamps or labels that are applied to a current passport. For such cases, the header above is inappropriate, so the following alternative header may

be used:

Offset (bytes)	Length (bytes)	Example	Meaning
0	2	BAEA (hex)	Signature for sector containing a single type of TLV entry
2	2	9031	Tag representing the data to follow
4	1	40	Length of data to follow
5	Var	"Entered Australia 2001.03.01"	Data associated with this tag

The above types of TLV entries are expected to occupy succeeding sectors in an area of the media that has its starting track and format specified by a single entry in the directory that is associated with the specified tag.

B.10.5 Track Addresses

The directory sector header contains a pointer to (address of) the next logical sector of the directory. This consists of the second and third fields in the header. This next logical sector contains the continuation of the directory.

The address of the next logical sector contains a track number and a sector format. This tells the reader how to read the track containing the next logical sector. The sector number is not included in the header because the directory will always be continued on the first sector of the indicated track. If there are multiple sectors on a track, all sectors except the last one on the track will contain the track number of the current track. The reader will look for the continuation of the directory in the following sectors on that track. The last sector on the track will contain the track number of another track where the directory continues.

At some point, the system which is initializing or updating the document will have written all of its directory sectors. At this point, the last sectors in the directory will contain a pointer to a blank track on the media where the next directory update will begin.

B.10.6 Unique Stamp

The 12 byte unique stamp referenced in the data sector header contains the following:

Offset (bytes)	Length (bytes)	Example	Meaning
0	3	123456h	Written with document writer serial number 123456
3	2	2002 = the year 2002	Year
5	1	3 = March	Month (1 = January)
6	1	31 = 31st day	Day (from 1 to 31)
7	1	14 = 2 pm	Hour (from 0 = midnight to 23 = 11 pm)
8	1	59	Minute (from 0 to 59)
9	1	59	Second (from 0 to 59)
10	2	999	Millisecond (from 0 to 999)

APPENDIX 1 TO INFORMATIVE ANNEX B

TAG DOCUMENTS

Tag(s): 1000
Title: Data contained in the Machine Readable Zone of a MRTD
Requested by: MRTD working group
[Contact Info required]

Date submitted: 2002.04.15
Date accepted: -
Status: Part of the initial standard. Will be accepted with it.

Description:

This data item consists of a set of fixed length fields. It is a copy of the data that is printed on the machine readable zone of a machine readable travel document. This is the minimum data set that is required on a machine readable travel document. As printed OCR text, this data is not digitally encoded – it exists as a set of characters which all belong to the ASCII character set. As such, this data written digitally will be encoded using the ASCII character set.

The set of text fields in this item is defined in the document: WD-002-2001-05-01

Tag(s): 9001
Title: Standard serial data format
Requested by: MRTD working group
[Contact Info required]

Date submitted: 2002.04.15
Date accepted: -
Status: Part of the initial standard. Will be accepted with it.

Description:

This data item contains the set of data defined as the standard serial implementation by the appropriate part of this standard. This allows the random access media to be used to store the exact same data stream used by serial-only technologies if desired.

Tag(s): 9002
Title: Default biometric identifier
Requested by: MRTD working group
[Contact Info required]

Date submitted: 2002.04.15
Date accepted: -

Status: Part of the initial standard. Will be accepted with it.

Description:

This data item contains the default CBEFF format biometric identifier for the cardholder. In addition to a tag issued to the card issuer that describes the exact content of the data item, the card issuer can include this tag on the document to reference the data item containing the primary biometric that was placed on the card at the time the card was issued. Note that because a tag is just a descriptor of data, two tags can reference the same data without having to write the data twice. Readers that do not recognize the card issuer's tag, but which have access to multiple biometric verification or identification devices - can use this tag to find the biometric data file. They can then use the CBEFF format to parse the file and determine if they can make use of the biometric template contained in the file.

ANNEX C (INFORMATIVE) to Section VIII

MAPPING OF LDS [Version 1.7]
USING SEQUENTIAL FILE REPRESENTATION
WITH OPTIONAL
2-D BAR CODE(S)

C.1 Scope – Annex A defines the current state specifications[23] governing mapping of the Logical Data Structure – LDS [Version 1.7] using a *sequential file representation*[24] to 2-D bar code(s) on an MRTD to allow expansion of the machine readable data capacity at the discretion of the issuing State or organization.

C.2 Normative references – The following International Standards contain provisions that, through reference herein, constitute provisions of Annex A to Section VIII of this Technical Report. Where differences exist between the specifications contained in this Technical Report and the referenced Standards to accommodate the use of bar code(s), the specifications contained herein shall prevail.

ISO/IEC 7501 (ICAO Doc 9303), Parts 1 through 3

–

CBEFF, Common Biometric Exchange File Format, NISTAR 6529-A

ISO/IEC 8824-1:1998 | ITU-T Recommendation X.680 (1997), *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 8824-2:1998 | ITU-T Recommendation X.681 (1997), *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*

ISO/IEC 8824-3:1998 | ITU-T Recommendation X.682 (1997), *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification*

ISO/IEC 8824-4:1998 | ITU-T Recommendation X.683 (1997), *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*

ISO/IEC 8825-1:1998 | ITU-T Recommendation X.690 (1997), *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 10918-1: Information Technology – Digital compression and coding of continuous-tone still images: Requirements and Guidelines

ISO/IEC 10918-1: Information Technology – Digital compression and coding of continuous-tone still images: Extensions

C.3 Sequential File Representation – The *sequential file representation* has been defined with the following considerations and assumptions:

- A single standardized sequential file representation must support use of 2-D barcode(s),

[23] *Specifications* as envisaged based on work completed to date. Specifications will only be considered final when they have been published in Doc 9303.

[24] Sequential file representations are often referred to as BLOB's (Binary Large Objects).

- A single standardized sequential file representation must accommodate an LDS containing limited data – i.e. typically less than 8K byes.

A.3.1 To minimize memory utilization a number of storage saving techniques are used.

As the entire LDS is read at one time, only one overall Authenticity/Integrity object (EF.SOD) is used. Data Presence Maps (DPM's) are used to indicate which of the optional Data Groups and Data Elements are present for a specific implementation. In the *sequential file representation* DPM's are simply strings of binary bits that, by their position, indicate if a specific Data Group is or is not present.

- A limited form of ASN.1 Tag-Length-Value (TLV) notation is used for each Data Group. The Data Group tags (T) are listed in Appendix C[25] to Normative Annex A. The length (L) of the Data Group immediately follows the Tag. Within a Data Group, the Data Elements are recorded sequentially (in order) as a value (V). The LDS defines the sequence of Data Elements and whether they are fixed length or variable length. Hence, position within the Data Group defines the identity of the Data Element and tags are not used to identify individual Data Elements.

- Some Data Groups permit one or more embedded templates, e.g., multiple occurrences of a specific type of biometric. In such cases, the tag Ax is used, where x = the occurrence count. The tag, Ax, designates the presence of the template within the Data Group. The length of this template immediately follows the tag. Template data elements follow and constitute the value of the template.

- A biometric data group may have an individual authenticity/integrity code. (The integrity options data element within the header defines whether one is or is not present.) If an authenticity/integrity code is being used, the data element immediately follows the biometric data.

- Variable length Data Elements are preceded by a length definition using ASN.1 encoding rules. Fixed length Data Elements do not use a length definition as their length is known.

A.3.2 To minimize memory utilization a number of storage saving techniques are used.
Within Data Group 1 (DG1 – details recorded in the MRZ of the MRTD), a length of "0" indicates that a variable length Data Element is not present.

.For example,

  - The fixed length Data Element "Date" with the value 'September 15, 1999' would be encoded as 19990915 if the format is CCYYMMDD or 990915 if the format is YYMMDD

  - The variable length Data Element "Name of holder" with the value 'John Q Document Holder' would be encoded as 16DOCUMENTHOLDER<<JOHN<Q.
    Note: 16_{16} (hexadecimal) = 22_{10} (base 10)

UTF-8 encoding is used. Most of the Data Elements used in the LDS are Basic Latin (ASCII) characters or binary. A small number of Data Elements such as "Name in National Characters," "Place of Birth" cannot always be encoded with the Basic Latin code set. Therefore, characters will be encoded using the Unicode Standard: UTF-8. It is a variable length encoding that preserves ASCII transparency. UTF-8 is fully compliant with Unicode

[25] ISO/IEC 7816-4 coexistent tag convention has been used.

Standard and ISO/IEC 10646. UTF-8 uses one byte to encode standard ASCII characters (code values 0 ….. 127). Many non-ideographic scripts are represented with two bytes. The remaining characters are represented with three or four bytes. Using UTF-8 allows for easy incorporation of non-ASCII characters without the overhead of two, three or four byte representation for all characters.

Note – use of Unicode means character counts do not always equal the number of storage bytes. As an example, the name François has 9 characters but requires 10 bytes storage because "ç" requires two bytes.

C.4 Security Requirements

Data integrity and authenticity are needed for trusted international interchange. A single, mandatory cryptographic checksum (enciphered hash) will be used within the LDS incorporating all implemented Data Groups except for Data Group 16 ["Person(s) to Notify]. In addition, the structure of Data Groups 2-4 allows for protection of biometric templates on an individual or group basis, if such protection is desired.
Write protection of the Data Elements is required. However, specific write protection schemes are outside the scope of this Technical Report. Details of such schemes are not needed for interchange as only the issuer may write to the capacity expansion technology.

C.5 Structure of Sequential File – Each implementation will be unique, reflecting the specific needs of an issuer. The overall structure, however, is the following:

[Header][DGPM][DG1][Optional DG2] …. [Optional DG13][DG15][Optional DG16]

Where,

Header	= Mandatory header information
DGPM	= Mandatory Data Group Presence Map
DG1	= Mandatory MRZ Data
Optional DG*n*	= Optional presence of Data Groups 2 through 14 inclusive
DG15	= Mandatory Authenticity/Integrity Code
DG16	= Optional presence of Person(s) to Notify – placed after the mandatory Authenticity/Integrity Code to permit updating of the Code without the need to re-compute and record the Authenticity/Integrity Code.

The structure above expands as follows.

[Header] = {AID}{LDS Version Level}{Unicode Version Level}{Total LDS length}. (*I.e.* less header and total length)},

where,

{AID} = ISO Application Identifier (registered identifier and pix)

[DGPM] = Two byte binary map that specified which data groups are present

[DG1 MRZ Data] = {Data Group tag}{Length}{Constructed MRZ data element} [26],

[Optional DGn] = {Data Group tag[27]}{Length}{Data Element Presence Map}[28]

[26] One Authenticity/Integrity Code will be included. It shall precede Data Group 16 (DG 16) in the LDS. Biometric templates may be individually signed if so indicated in the CBEFF header.

[27] Refer to Appendix B to Normative Annex A for a list of Data Element Tags

{Data Element$_1$}{Data Element$_2$}…{Data Element$_n$}[29]

C.6 Header Information – The Header data is used by the read/decode system to correctly interpret recorded LDS data. The Header is a single, 12-byte Data Element with the following format.

AIDVijUabcL

Where,

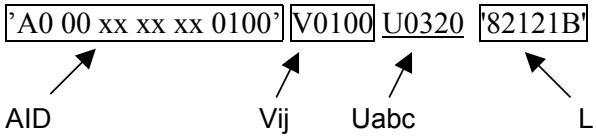
AID = Application Identifier in format 'A0 00 xx xx xx 0100'[30]
Vij = LDS Version Number, xxyy, where i defines the Major revision level (01-99) and j. defines the Minor revision level (01-99). Thus, Version 1.7 of the LDS would be expressed as V0100
Uabc = Unicode version level where a = the Major revision level (0-99), b = the Minor revision level (0-9) and c = the Update Version. The current version of Unicode is 03.2.0 (March 2002) or U0320.

L = Total length of LDS, exclusive of Header. Note: Length shall be encoded according to ASN.1 notation (*See Appendix A to Normative Annex A for details).*

Example: Assume a MRTD is encoded in LDS [Version 1.7] format using Unicode Level 3.2

Total length = 4635_{10} bytes (' 82121B' using ASN.1 notation as defined in Appendix A to this Normative Annex A)

Then the Header for the LDS would be encoded as



Note: Quotation marks ('and ') used above are not encoded within the LDS. They are shown to visually delineate hexadecimal characters.

C.7 Data Group Presence Map – A two (2) byte Data Group Presence Map (i.e. Form 1 DGPM as defined in Section VII of this Technical Report) will immediately follow the "Header".

As defined in Figure A-1 the DGPM indicates which of the 15 Data Groups defined for LDS [Version 1.7] are present for any specific encoding as determined at the discretion of the issuing State or organization. *Note:* the MRZ (Data Group 1) is mandatory and therefore, always present.

Figure A-1

	b7	*B6*	*b5*	*b4*	*b3*	*B2*	*b1*	*b0*	*Bit*
Data Group	1	2	3	4	5	6	7	8	*Byte 1 of DGPM*

---

[28] For Data Groups 12, 13, 15 only

[29] If the Data Element is variable length, the length, encoded in hexadecimal shall precede the value.

[30] The AID has the format 'AnnnnnnnnnPIX,' The 'Annnnnnnnn' characters are a registered identifier and identify the application(s) as an ICAO LDS. The PIX is an application specific suffix. The PIX is used to designate a specific application within the LDS, i.e., PIX = '0100'for the issuer data elements in a sequential representation.

Data Group	9	10	11	12	13	14	15	16-	*Byte 2 of DGPM*

For example, assuming the following Data Groups have been encoded in the LDS:

DG1 - MRZ
DG2 - Encoded face
DG5 - Displayed Portrait
DG11 - Additional Personal Detail(s)
DG15 - Authenticity/Integrity Code

The DGPM would be as follows:

Byte 1 = 11001000 (binary) or ‘C4’ (hex)

Byte 2 = 00100010 (binary) or ‘22’ (hex)

C.8 Data Element Presence Map(s) – A Data Element Presence Map (i.e. Form 1 DEPM as defined in Section VII of this Technical Report) will immediately follow the first data recorded in the following Data Groups if included in the LDS at the discretion of the issuing State or organization. The DEPM will be one or two bytes in length as noted.

DG11 – Additional Personal Detail(s);`Two bytes
DG12 – Additional Document Detail(s); Two bytes
DG16 – Person(s) to Notify; One byte

As defined in Figure A-2 the DEPM indicates which of the Data Elements, in this case sixteen (16) defined for the Data Group are have been encoded at the discretion of the issuing State or organization.

Figure A-2

	b7	*b6*	*B5*	*b4*	*B3*	*b2*	*b1*	*b0*	*Bit*
Data Element	1	2	3	4	5	6	7	8	*Byte 1 of DEPM*
Data Element	9	10	11	12	13	14	15	16	*Byte 2 of DEPM*

For example, assuming the following Data Elements have been encoded in the DG11 – additional Personal Detail(s) of the LDS:

DE1 - Name of Holder (Primary and Secondary Identifiers, in full)
DE3 - Personal Number
DE8 - Profession
DE9 - Title
DE15 - Data Group Authenticity/Integrity Code

The DEPM would be as follows:

Byte 1 = 10100001 (binary) or ‘A1’ (hex)

Byte 2 = 10000010 (binary) or ‘82’ (hex)

C.9 Structure for DG16 – Person(s) to Notify – The LDS allows for multiple recordings of one or more persons to notify. Since the Data Elements used for each recording are optional, a *one-byte* data presence map and length is needed for each individual recording included in the LDS. The resulting structure is as follows:

{Tag}{Overall length of Data Group 15}{Number of recordings included}{Length of first recording}{DEPM for first recording}{Data Elements for first recording}{Length of second recording}{DEPM for second recording}{Data Elements for second recording}{repeated structure for other recordings}

C.10 Structure for DG1 – MRZ Data – All machine readable OCR-B data contained within the MRZ is integrated sequentially and encoded as a single Data Element within the LDS. To minimize storage requirements the use of the filler characteristic (<) has been minimized. All fixed length data elements contained in the MRZ have known lengths and therefore their length is assumed and not defined separately within the integrated Data Element. Name and Optional Data are variable and are therefore preceded by their length.

For example, if the following MRZ data elements from an MRP are assumed:

Doc Type	= P<
Issuing State	= UTO
Name	= ERIKSSON<<ANNA<MARIA
Document #	= L898902C<
Document # Check Digit	= 3
Nationality	= UTO
Date of Birth	= 6 August 1969
Date of Birth Check Digit	= 1
Sex	= F
Date of Expiry	= 23 June 1994
Date of Expiry Check Digit	= 6
Optional Data	= ZE184226B
Optional Data Check Digit	= 1
Composite Check Digit	= 4

The integrated Data Element representation would be as follows:

'61"42'P<UTO'14'ERIKSSON<<ANNA<MARIAL898902C<3UTO
6908061F9406236'09'ZE184226B14

Where,

'61"42' are the Tag and length (in hexadecimal) of this group
The first underlined number (i.e. 14) defines the length of the name field (in hexadecimal); and
The second underlined number (i.e. 09) defines the length of the optional data field, in hexadecimal.

C.11 Example of Sequential Encoding of LDS

Assuming the MRZ from an MRP as defined in paragraph A.10 above, the following:

AID = A0 00 xx xx xx 0100

LDS Version:	1.0	
Unicode:	3.2	
MRZ re above		Data Group 1
Facial biometric	Tag = 75	Data Group 2
One entry		Data Element 1
With the following characteristics (header information)		Data Element 2

Authenticity/Integrity option = Digital signature = '2002'

ICAO patron template = Version 1.7 = '01 00'

Biometric type = face = '000002'

Biometric feature = Not applicable (no information) = '00'

Captured on 15 March 2002, at 2:45:00 PM, in
Mexico City, Mexico = 200203151445006

Valid from 1 April 2002 through 31 March 2007
= 2002040120070331

Captured using a device with a PID (Product Identifier) of '0001'
Template format owner'000A'

Format type '0004'

Data block length of 4568 bytes ('11D8')
= '82 11 D8' Data Element 3

Optional Integrity code Data Element 4
Digital signature
using algorithm type 1 (SHA-1 / ECDSA)
key reference 003

Displayed portrait – Using ISO 10918, length = 2132_{10} bytes

Data Group 6
Number of entries = 1 Data Element 1
Encoded portrait Data Element 2

Additional personal information - Data Group 12
Place of Birth: Nordberg, Germany - Data Element 4
Address: 23 Maple Rd, Pleasantville ZZ Z59065 Utopia Data Element 5
Phone Number:–99 800 555 1212 Data Element 6
One overall Authenticity/Integrity Code - Data Group 15

Person to Notify - Data Group 16
Number:01 Data Element 1
Date data recorded: January 15, 2001 - Data Element 2
Name: François de Peeve Data Element 3
Telephone: 99-800-555-1212 Data Element 4
Address: 23 Maple Rd, Pleasantville, ZZ, Z59065,
Utopia Data Element 5

Overall length of data = 5431_{10} bytes or 1537_{16}, encoded as '821537' per ASN.1 rules

Then the data stored within the IC would be (Note, Tag, Length, Value notation is not used within data groups.),

'A0 00 xx xx xx 0100' V0100U0320'821537"C413'

'61"42'P<UTO'14'ERIKSSON<<ANNA<MARIAL898902C<3UTO6908061F940623609ZE184226B14

'75"82122C7'1
'A1"821212'
'20"02"0100"000002"00'*2002030514450006200204012007033*1'0001"000A"0004'
‘8211D8’’ [4568 bytes of binary]
'B5"2C'3003[40 bytes of binary]

‘65’’8207D4’’1’’8207D0’’….2000 byte Portrait per ISO 10918…'

‘
6C’’54‘16’’00’
’11’Nünberg, Germany
’2E'23 Maple Rd, Pleasantville, ZZ, Z59065, Utopia
'0F'99 800 555 1212

‘
'B5"2C'3003[40 bytes binary]

‘70’’55’01‘’53’F0’
20010115 (Note, fixed length field, no length defined)
’15’François de Pélève
‘'0F’99 800 555 1212
‘
'30'23 Maple Rd, Pleasantville, ZZ, Z59065, Utopia

Where,

‘A0 00 xx xx xx ’0100’ =	AID and PIX extension
V0100	= Version level 1.0
U0320	= Unicode Version 3.2.0
’821537’	= Overall length of LDS ($1537_{16} = 5431_{10}$)
‘C413’	= Data Group Presence Map (1100 0100 0001 0011)
‘61’	= Tag for MRZ data element template (Data Group 1)
‘42’	= Length of MRZ (66_{10})
P<……6B14	= MRZ per pervious example
‘75’	= Tag for facial biometric template
'821217’	= Overall length of template(s)
1	= One template
‘A1’	= Start of first occurrence (in this case only occurrence)
‘821212’	= Length of this occurrence
‘2002’	= Integrity option – (MAC’ed)
‘0100’	= ICAO Patron template Version 1.7
‘00’	= Biometric feature, not applicable
‘2002031513300006’	= Captured 15 March 2002, at 1:30 PM, 00 sec (UTC + 6)
‘2002040120070331’ =	= Valid from 1 April 2002 through 31 March 2007
‘0001’	= Product identifier
‘000A’	= Format owner
‘0004’	= Format type
’8211D8’	= Length of biometric data block (4568 bytes)
‘B5’	= Tag for integrity code (for this template)
‘2C’	= Length of enciphered hash, algorithm identifier, and key identifier
3	= Algorithm reference 1 (SHA-1 / ECDSA)
003	= Key identifier 03
‘..40 bytes…’	= Digital signature
‘66’	= Tag for facial portrait (Data Group 6)
‘8207D4’	= Length of portrait data group
1	= Number of portraits
‘8207D0’	= Length of portrait
‘6C’	= Tag for Additional Personal Information (Data Group 12)
‘53’	= Overall length of Data Group 12 (84_{10} bytes)
‘1600’	= Data element presence map for Data Group 12
‘11’N…ny	= Length and value of Place of birth (Data element 4)

‘2E’…Utopia	= Length and value of address (Data element 5)
‘0F’99…..1212	= Length and value of phone number (data element 6)
‘B5”	= Tag for Authenticity/Integrity code (Data Group 15)
‘2C’	= Length
3	= Algorithm identifier
003	= Key ID
‘40 bytes binary’	= Digital signature
’70’	= Tag for Person(s) to Notify (Data Group 16)
‘61’	= Overall length of Data Group 16 (97_{10} bytes)
01	= Value of Number of entries (Data element 1) Note, fixed length, two character data element, no length designator used
‘5E’	= Length of first entry, including presence map
‘F0’	= Data element presence map for first instance of Data Group 16
20010115	= Value of Date Recorded (Data element 2)
‘15’Fran….ve	= Length and value of Name (Data element 3)
‘0F'99’ 1212	= Length and value of phone number (Data element 4)
‘2E’23…Utopia	= Length and value of address (Data element 5)

APPENDIX 1 TO NORMATIVE ANNEX C

TAG ASSIGNMENTS – *SEQUENTIAL FILE REPRESENTATION*

Appendix 3 to Normative Annex A defines the Data Group Tag assignments valid for LDS [Version 1.7].

Tags are only used to identify Data Groups in LDS [Version 1.7].

General Assumptions:

Tags are to be interpreted as a *Coexistent tag allocation scheme*.

Effort has been made to avoid use of existing tags in the 5Fxx range. However, a number of tags identified in ISO 7816-6 have been redefined, specifically in the 5F4x range.

DATA GROUP		TAG
Data Group Number	**ITEM**	
Issuing State Recorded Data		
DG1	Machine Readable Zone (MRZ)	**61**
DG2	Encoded Identification Feature(s) – Face	**75**
DG3	Encoded Identification Feature(s) - Finger(s)	**63**
DG4	Encoded Identification Feature(s) – Eye(s)	**76**
DG5	Displayed Identification Feature(s) – Portrait	**65**
DG6	*Reserved for Future Use*	
DG7	Displayed Identification Feature(s) – Signature of Usual Mark	**67**
DG8	Encoded Security Feature(s) – Data Feature(s)	**68**
DG9	Encoded Security Feature(s) – Structure Feature(s)	**69**
DG10	Encoded Security Feature(s) – Substance Feature(s)	**6A**
DG11	Additional Personal Detail(s)	**6B**
DG12	Additional Document Detail(s)	**6C**
DG13	Optional Detail(s)	**6D**
DG14	*Reserved for future use*	**6E**
DG15	Authenticity/Integrity Code (for sequential implementations)	**B5**
DG16	Person(s) to Notify	**70**
Receiving State Recorded Data		
DG17	Automated Border Clearance Details	**Not Used in LDS [Version 1.7]**
DG18	Electronic Visa(s)	**Not Used in LDS [Version 1.7]**
DG19	Travel Record(s)	**Not Used in LDS [Version 1.71]**

Abbreviations: A = Alpha, B = Binary, F = Fixed, M = Mandatory, N = Numeric, O = Optional, S = Special, V = Variable

ISSUING STATE or ORGANIZATION DATA GROUPS

Data Group	Data Element	Description	Tag	Optional or Mandatory	Format	Example
Header						
		Application identifier		M	Ax 00 xx xx xx yyyy	'A0 00 12 34 56 0100'
		ICAO LDS Version level		M	Vxxyy	V0100
		Unicode Version Level		M	Uxxyz	U0320
		Total length of LDS including presence map		M	ASN.1	'82 12 1B'
		Presence map		M	F 2B	'A4 12'

DG1		**Machine Readable Zone**	61	M		
	01	Document type		M	F 2AS	I<
	02	Issuing state or organization		M	F 3A	ATA
	03	Name of holder		M	F 39 ANS	SMITH<<JOHN<T
	04	Document Number (primary numbers)		M	F 9ANS	12345678<
	05	Check digit, document number		M	F 1N	1
	06	Nationality		M	F 3A	CND
	07	Date of Birth (truncated)		M	F 6N	740602 (yymmdd)
	08	Check Digit, DOB		M	F 1N	2
	09	Sex		M	F 1A	F, M or U
	10	Date of Expiry or Valid Until Date		M	F 6N	060531 (yymmdd)
	11	Check digit, date of expiry		M	F 1N	3
	12	Optional Data		O	Passports = F 14 NS ID-1 = F 26 ANS[31] ID-2 = F 7 ANS	123456
	13	Check digit, optional data (ID-3 only)		M if ID-3	F 1N	0
	14	Check digit, Composite		M	F 1N	4

Correct per updated CBEFF

DG2			**Facial Biometric Data**	75	M		
	01		Total length of facial data		M	ASN.1	'82 03 07'
	01		Number of templates (entries)		M	F 1N	2
	02		Biometric Header Template – ICAO patron format	Ax[32]	M	F 1B	'A1'
		01	Length of this entry		M	ASN.1	'82 03 05'
		02	Security Options		M	F 1B	'0000'= Plain biometric '2002' = with Integrity
		03	ICAO Header Version		M	F 2B	'01"00'
		04	Biometric type		M	F 3B	'000002'= Facial '000008'= Finger '000010'= Iris
		05	Biometric Feature		M	F 1B	Refer to Table x
		06	Capture (record) date		M	F 8B	Yyyy:mm;dd;hh;mm;ss[33]
		07	Validity period (From date, to date)		M	F 8B	Yyyy:mm:dd:yyyy:mm:dd[34]
		08	Biometric product identifier		M	F 4B	Refer to NISTIR 6529-A
		09	Format owner		M	F 2B	Refer to NISTIR 6529-A
		10	Format type		M	F 2B	Refer to NISTIR 6529-A
	03		Biometric data block		M	V	Binary data block (Includes length)

[31] For ID-1 documents the first 15 characters are printed in positions 16-20 of line 1 and the remaining 11 characters are printed in positions 19-29 of line 2.

[32] X denotes which template in data group, e.g., A2 = second template

[33] Colons are not encoded. Each character is expressed in 4 bit BCD (Binary Code Decimal). Example 15 December 2000, 5:35:30 AM would be encoded as 20001215053530

[34] From YYYY:MM::DD to YYYY:MM:DD, characters encoded in BCD

	04		Authenticity/Integrity Code	B5	M (if protected)	ASN.1	Length of integrity code
		01	Algorithm identifier		M (if signed)	F 1N	3
		02	Key reference		M (if signed)	F 3N	016
		03	Digital signature		M (if signed)	V	Binary data

DG3	**Finger Biometric Data**	**63**	**O**		**Same structure as DG2**

DG4	**Iris Biometric Data**	**76**	**O**		**Same structure as DG2**

DG5		**Displayed Portrait(s)**	**65**	**O**		
	01	Number of images		M	F 1N	1
	02	Digitized facial image(s)		M	V	Variable length template up to 99,999 bytes. Encoded ISO/IEC 10918

DG6		**Displayed Finger(s)**	**66**	**O**		
	01	Number of images		M	F 1N	1
	02	Digitized finger image(s)		M	V	Variable length template up to 99,999 bytes. Encoded per ANSI/NIST-ITL 1-2000

DG7		**Displayed Signature or Mark**	**67**	**O**		
	01	Number of images		M	F 1N	1
	02	Digitized Signature or Mark(s)		M	V	Variable length template up to 9999 bytes. Encoded per Encoded ISO/IEC 10918)

DG8	**Machine assisted Security Features - Encoded Data. Details to be defined**	**68**			

DG9	**Machine assisted Security Features - Structure. Details to be defined**	**69**			

DG10	**Machine assisted Security Features - Substance. . Details to be defined**	**6A**			

DG11			**Additional Personal Details Template**	**6B**	O		
			Presence map		M	F 1B	
	01		Full Name of Doc Holder in National Characters		O	99ANS	Free form
	02		Other names		O		
		01	Number of entries		M if 'Other names present'	F 2N	2
		02	Name entry		M if 'Other names present'	V 999ANS	'Free format
	03		Personal Number		O	V 99NAS	Free format
	04		Place of Birth		O	V 999 ANS	Free format
	05		Full DOB		O	F 8N	CCYYMMDD
	06		Address		O	V 999ANS	Free format
	07		Telephone Number		O	V 99ANS	Free format
	08		Profession		O	V 99ANS	Free format

	09	Title		O	V 99ANS	Free format
	10	Personal summary		O	V 999NS	Free format
	11	Proof of citizenship		O	V	Compressed image per ISO/IEC 10918
	12	Other valid ID numbers		O	V 99ANS	Free format
	13	Custody information		O	V 999ANS	Free format

DG12			**Additional Document Details Template**	**6C**	O		
			Presence map		M	F 1B	
	01		Issuing Authority		O	99ANS	Free form
	02		Date of issue		O	F 8N	CCYYMMDD
	03		Other people listed on document				
		01	Number of entries		M if 'Other people listed present'	F 2N	2
		02	Name entry		M if 'Other people listed present'	V 999ANS	'Free format
	04		Endorsements / Observations		O	V 999NAS	Free format
	05		Tax / Exit Requirements		O	V 999 ANS	Free format
	06		Image of front of document		O	V	Compressed image per ISO/IEC 10918
	07		Image of rear of document		O	V	Compressed image per ISO/IEC 10918
	08		Personalization time		O	F 14N	Ccyymmddhhmmss
	09		Personalization s/n		O	V 99ANS	Free format

DG13	**Optional Detail(s)**	**6D**	O		

DG14	**Reserved for future use**	**6E**	O		

DG15		**Authenticity/Integrity Code**	**B5**	M	ASN.1	
	01	Algorithm identifier		M	F 1N	2
	02	Key identifier		M	F 3N	013
	03	Authenticity/Integrity		M	40/128 B	

DG16			**Person to Notify**	**70**	O	ASN.1	
	01		Number of entries		M	F 1N	2
		01	Length of this entry		M	ASN.1	'82 03 05'
		02	Presence map for this entry		M	F 1B	
		03	Date data recorded		O	F 8N	Yyymmdd
		04	Name of person		O	V 999ANS	Free format
		05	Telephone		O	V 99ANS	Free format
		06	Address		O	V 999ANS	Free format