Doc 9303

Machine Readable Travel Documents

Part 1
Machine Readable Passports

Volume 2
Specifications for Electronically Enabled Passports with Biometric Identification Capability

Approved by the Secretary General
and published under his authority

Sixth Edition — 2006

International Civil Aviation Organization

AMENDMENTS

The issue of amendments is announced regularly in the *ICAO Journal* and in the supplements to the *Catalogue of ICAO Publications and Audio-visual Training Aids*, which holders of this publication should consult. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by

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

TABLE OF CONTENTS

SECTION I

INTRODUCTION

The specifications in this volume of Doc 9303, Part 1 are the culmination of several years' work, beginning in 1998, to do a systematic study of biometrics and their potential to enhance identity confirmation with passports and other travel documents, and subsequently to develop technical specifications for the incorporation of biometric identification in MRTDs. Most of this work was carried out by the New Technologies Working Group (NTWG) of the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD).

The first step was to identify the "right biometric" for use in or with travel documents, and to do this the approach was to first identify the *requirements* that are unique to travel document issuance and inspection and then to measure the compatibility of each biometric with these requirements. Briefly, the requirements identified were: compatibility with travel document issuance and renewal; compatibility with machine-assisted identity verification requirements in the issuance and inspection processes; redundancy; global public perception of the biometric and its capture procedure; storage requirements; and performance. When evaluated against all of these factors the *face* received the highest compatibility rating while the *finger* and the *iris* were tied in second place. Hence the face was recommended as the primary biometric, mandatory for global interoperability in passport inspection systems, while the finger and iris were recommended as secondary biometrics to be used at the discretion of the passport-issuing State.

The next step was to identify an appropriate medium for electronic data storage on the document. The medium chosen would have to offer enough data storage space for facial *images* and possibly other biometrics, as the concept of using templates had been abandoned due to the fact that templates and their readers are not internationally standardized. The technology had to be non-proprietary, available in the public domain worldwide, in the interests of global interoperability, and it had to be usable in book-style documents made of paper and cloth. Ease of use, without a requirement to position or fit the document into a reading device, was also a factor. The technology that met all of these requirements was the contactless integrated circuit (IC), and after further study it was decided that of the two ISO-standard options, the "proximity" type (ISO/IEC 14443) should be specified.

Next, a standardized "logical data structure" for programming the chip was specified to ensure that chips programmed in any country could be read in any other country. Finally, because data written to a chip can be written over, a public key infrastructure (PKI) scheme was required, in order to give the reader of the chip confidence that the data had been placed there by the authorized issuer and that it had not been altered in any way. Thus an expert group within the NTWG developed specifications for a specialized PKI for application to travel document issuance and inspection.

In 2003 the TAG/MRTD formally presented to ICAO a four-part recommendation. The facial image as a high resolution portrait stored on a contactless IC, conforming to ISO/IEC 14443, should be the global biometric standard. Fingerprint and iris, both stored as images, are also supported as secondary biometrics. The biometrics, a duplication of the MRZ data, and a wide range of other data options should be stored in the IC in accordance with the Logical Data Structure and secured against unauthorized alteration using a specially tailored PKI. This recommendation was accepted and endorsed as the ICAO blueprint.

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

SECTION II

THE DEPLOYMENT OF BIOMETRIC IDENTIFICATION AND THE ELECTRONIC STORAGE OF DATA IN MACHINE READABLE PASSPORTS

1. Scope

1.1 Section II defines the specifications, supplementary to those for the basic MRP set forth in Volume 1 of Doc 9303, Part 1, to be used by States that decide to issue an electronically enabled machine readable passport (ePassport) capable of being used by any suitably equipped receiving State to read from the document a greatly increased amount of data relating to the MRP itself and its holder. This includes mandatory globally interoperable biometric data that can be used as an input to facial recognition systems, and, optionally, to fingerprint or iris recognition systems. The specifications require the globally interoperable biometric data to be stored in the form of high-resolution images on a high-capacity contactless integrated circuit (IC), the IC also being encoded with a duplicate of the MRZ data. The specifications also permit the storage of a range of optional data at the discretion of the issuing State.

Note on Supplement.—

ICAO will issue from time-to-time a "Supplement to Doc 9303, Part 1", to this standard Doc 9303. The supplement will contain information intended to clarify, amplify or elaborate on issues with respect to travel document standards as well as to correct errors encountered during implementation experiences. It is intended that the information contained in the supplement will augment the existing guidance in Doc 9303 as well as in technical reports issued by ICAO. The supplement will be issued on a continuing and consistent basis.

The specifications of Doc 9303 should always be read in conjunction with the additional information set out in the latest release of the supplement which will be available on the ICAO web site at http://www.icao.int/mrtd.

2. ePassport

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

2.2 *Validity period for an ePassport.* The validity period of an ePassport is at the discretion of the issuing State; however, in consideration of the limited durability of documents and the changing appearance of the passport holder over time, a validity period of not more than ten years is recommended. States may wish to consider a shorter period to enable the progressive upgrading of the ePassport as the technology evolves.

2.3 Doc 9303, Part 1, Volume 2 focuses on biometrics in relation to machine readable passports, and for simplicity uses the term "*ePassports*" to denote such biometrically-enabled and globally-interoperable passports. Any MRP that does not comply with the specifications given in this volume may not be called an ePassport and shall not display the ePassport logo.

3. Visual indication that an MRP is an ePassport

3.1 All ePassports shall carry the following symbol (Figure II-1):

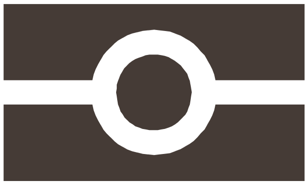


Figure II-1

An electronic file of the symbol is available from the ICAO web site. The symbol may only appear on an MRP that contains a contactless microchip, with a data storage capacity of at least 32kB, that is encoded in accordance with the Logical Data Structure (Section III of this volume) with, as a minimum, the MRZ data in Data Group 1 and a facial image as specified in this Section in Data Group 2, with all entered data secured with a digital signature as specified in Section IV of this volume. Unless a passport conforms to these minimum requirements, it shall not be described as an ePassport nor display the ePassport symbol. The symbol shall appear on the front cover of the ePassport either near the top or the bottom of the cover. The image, as shown above, is a positive, i.e. the black part of the image shall be printed or otherwise imaged. The symbol shall be included in the foil blocking or other image on the front cover. It is recommended that the symbol also be printed on the data page in a suitable colour and in a location which does not interfere with the reading of other data. The issuing State may also print the symbol on the inside page or cover of the ePassport that contains the contactless IC and, at the State's discretion, elsewhere in the ePassport.

3.2 Figure II-2 shows the recommended dimensions of the symbol as it is to appear on an ePassport book cover or data page.

The following are the corresponding dimensions in inches: 9.0 mm (0.35 in), 5.25 mm (0.21 in), 3.75 mm (0.15 in), 2.25 mm (0.09 in), 0.75 mm (0.03 in).

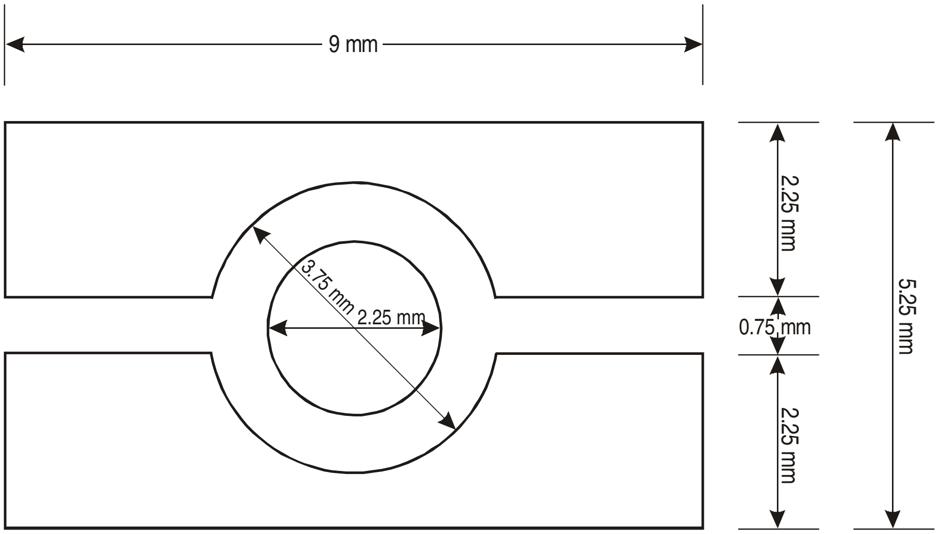


Figure II-2

3.3 A smaller size of 4.2 × 7.2 mm (0.17 × 0.28 in), scaled in proportion, is recommended for use on ePassports in the form of an ID1 size card.

3.4 The symbol may be scaled in proportion for use in, for example, background designs of ePassport pages or directional signs.

3.5 *Warning regarding care in handling an ePassport*. It is suggested that a warning urging the holder of an ePassport to take care of the document be placed in an obvious location on the book. A suggested wording is:

"This passport contains sensitive electronics. For best performance please do not bend, perforate or expose to extreme temperatures or excess moisture".

In addition, the issuing State may mark the part of the page containing the IC and the corresponding parts of some adjacent pages with the caveat:

"Do not stamp here".

4. Biometric identification

4.1 "Biometric identification" is a generic term used to describe automated means of recognizing a living person through the measurement of distinguishing physiological or behavioural traits.

4.2 A "biometric template" is a machine-encoded representation of the trait created by a computer software algorithm and enables comparisons (matches) to be performed to score the degree of confidence that separately recorded traits identify (or do not identify) the same person. Typically, a biometric template is of relatively small data size; however, each manufacturer of a biometric system uses a unique template format, and templates are not interchangeable between systems.

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

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

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

4.4 *Biometrics terms.* The following terms are used with biometric identification:

- "*verify*" means to perform a *one-to-one* match between proffered biometric data obtained from the MRP holder now and a biometric template created when the holder enrolled in the system;

- "*identify*" means to perform a *one-to-many* search between proffered biometric data and a collection of templates representing all of the subjects who have enrolled in the system.

4.5 Biometrics can be used in the identification function to improve the quality of the background checking performed as part of the passport, visa or other travel document application process. In the verification function, they can be used to establish a positive match between the travel document and the person who presents it.

5. Key considerations

5.1 In specifying biometric appreciations in MRPs, key considerations are:

- *Global Interoperability* — the crucial need to specify a system for biometrics deployment that is universally interoperable;

- *Uniformity* — the need to minimize via specific standard setting, to the extent practical, the different solution variations that may potentially be deployed by member States;

- *Technical reliability* — the need to provide guidelines and parameters to ensure member States deploy technologies that have been proven to provide a high level of confidence from an identity confirmation viewpoint; and that States reading data encoded by other States can be sure that the data supplied to them is of sufficient quality and integrity to enable accurate verification in their own systems;

- *Practicality* — the need to ensure that specifications can be operationalized and implemented by States without their having to introduce a plethora of disparate systems and equipment to ensure they meet all possible variations and interpretations of the standards;

- *Durability* — the requirement that the systems introduced will last the maximum 10-year life of a travel document, and that future updates will be backward compatible.

6. Definitions and term*s*

6.1 Terms related to biometrics are defined as follows:

Biometric. A measurable, physical characteristic or personal behavioural trait used to recognize the identity, or verify the claimed identity, of an enrollee.

Biometric data. The information extracted from the biometric sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data).

Biometric sample. Raw data captured as a discrete unambiguous, unique and linguistically neutral value representing a biometric characteristic of an enrollee as captured by a biometric system (for example, biometric samples can include the image of a fingerprint as well as its derivative for authentication purposes).

Biometric system. An automated system capable of:

1. capturing a biometric sample from an end user for an MRP;
2. extracting biometric data from that biometric sample;
3. comparing that specific biometric data value(s) with that contained in one or more reference templates;
4. deciding how well the data match, i.e. executing a rule-based matching process specific to the requirements of the unambiguous identification and person authentication of the enrollee with respect to the transaction involved; and
5. indicating whether or not an identification or verification of identity has been achieved.

Capture. The method of taking a biometric sample from the end user.

Certificating authority. A body that issues a biometric document and certifies that the data stored on the document are genuine in a way which will enable detection of fraudulent alteration.

Comparison. The process of comparing a biometric sample with a previously stored reference template or templates. See also *"One-to-many"* and *"One-to-one"*.

Contactless integrated circuit. An electronic microchip coupled to an aerial (antenna) which allows data to be communicated between the chip and an encoding/reading device without the need for a direct electrical connection.

Database. Any storage of biometric templates and related end user information.

Data storage (Storage). A means of storing data on a document such as an MRP. Doc 9303, Part 1, Volume 2 specifies that the data storage on an ePassport will be on a contactless integrated circuit.

End User. A person who interacts with a biometric system to enroll or have his[1] identity checked.

Enrollment. The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.

Enrollee. A human being, i.e. natural person, assigned an MRTD by an issuing State or organization.

ePassport. A Machine Readable Passport (MRP) containing a contactless integrated circuit (IC) chip within which is stored data from the MRP data page, a biometric measure of the passport holder and a security object to protect the data with Public Key Infrastructure (PKI) cryptographic technology, and which conforms to the specifications of Doc 9303, Part 1.

Extraction. The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.

Failure to acquire. The failure of a biometric system to obtain the necessary biometric to enroll a person.

Failure to enroll. The failure of a biometric system to enroll a person.

False acceptance. When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity.

False acceptance rate/FAR. The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The false acceptance rate may be estimated as *FAR = NFA / NIIA or FAR = NFA / NIVA* where *FAR* is the false acceptance rate, *NFA* is the number of false acceptances, *NIIA* is the number of impostor identification attempts, and *NIVA* is the number of impostor verification attempts.

False match rate. Alternative to "false acceptance rate"; used to avoid confusion in applications that reject the claimant if his biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of "false acceptance" and "false rejection".

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

False non-match rate. Alternative to “false rejection rate”; used to avoid confusion in applications that reject the claimant if his biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of “false acceptance” and “false rejection”.

False rejection. When a biometric system fails to identify an enrollee or fails to verify the legitimate claimed identity of an enrollee.

False rejection rate/FRR. The probability that a biometric system will fail to identify an enrollee or verify the legitimate claimed identity of an enrollee. The false rejection rate may be estimated as follows: *FRR = NFR / NEIA or FRR = NFR / NEVA* where *FRR* is the false rejection rate, *NFR* is the number of false rejections, *NEIA* is the number of enrollee identification attempts, and *NEVA* is the number of enrollee verification attempts. This estimate assumes that the enrollee identification/verification attempts are representative of those for the whole population of enrollees. The false rejection rate normally excludes “failure to acquire” errors.

Full frontal (facial) image. A portrait of the holder of the MRP produced in accordance with the specifications established in Doc 9303, Part 1, Volume 1, Section IV, 7.

Gallery. The database of biometric templates of persons previously enrolled, which may be searched to find a probe.

Global interoperability. The capability of inspection systems (either manual or automated) in different States throughout the world to obtain and exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye readable and machine readable data in all ePassports.

Holder. A person possessing an ePassport, submitting a biometric sample for verification or identification whilst claiming a legitimate or false identity. A person who interacts with a biometric system to enroll or have his identity checked.

Identifier. A unique data string used as a key in the biometric system to name a person’s identity and its associated attributes. An example of an identifier would be a passport number.

Identity. The collective set of distinct personal and physical features, data and qualities that enable a person to be definitively identified from others. In a biometric system, identity is typically established when the person is registered in the system through the use of so-called “breeder documents” such as birth certificate and citizenship certificate.

Identification/Identify. The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the ePassport holder whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with “*Verification*”.

Image. A representation of a biometric as typically captured via a video, camera or scanning device. For biometric purposes this is stored in digital form.

Impostor. A person who submits a biometric sample in either an intentional or inadvertent attempt to pass for another person.

Inspection. The act of a State examining an ePassport presented to it by a traveller (the ePassport holder) and verifying its authenticity.

Issuing State. The country writing the biometric to enable a receiving State (which could also be itself) to verify it.

JPEG and JPEG 2000. Standards for the data compression of images, used particularly in the storage of facial images.

LDS. The Logical Data Structure describing how biometric data is to be written to and formatted in ePassports.

Live capture. The process of capturing a biometric sample by an interaction between an ePassport holder and a biometric system.

Match/Matching. The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. A decision to accept or reject is then based upon whether this score exceeds the given threshold.

MRTD. Machine Readable Travel Document, e.g. passport, visa or official document of identity accepted for travel purposes.

Multiple biometric. The use of more than one biometric.

One-to-a-few. A hybrid of one-to-many identification and one-to-one verification. Typically the one-to-a-few process involves comparing a submitted biometric sample against a small number of biometric reference templates on file. It is commonly referred to when matching against a “watch list” of persons who warrant detailed identity investigation or are known criminals, terrorists, etc.

One-to-many. Synonym for *“Identification”*.

One-to-one. Synonym for *“Verification”*.

Operating system. A programme which manages the various application programmes used by a computer.

PKI. The Public Key Infrastructure methodology of enabling detection as to whether data in an ePassport has been tampered with.

Probe. The biometric template of the enrollee whose identity is sought to be established.

Random access. A means of storing data whereby specific items of data can be retrieved without the need to sequence through all the stored data.

Read range. The maximum practical distance between the contactless IC with its antenna and the reading device.

Receiving State. The country reading the biometric and wanting to verify it.

Registration. The process of making a person’s identity known to a biometric system, associating a unique identifier with that identity, and collecting and recording the person’s relevant attributes into the system.

Score. A number on a scale from low to high, measuring the success that a biometric probe record (the person being searched for) matches a particular gallery record (a person previously enrolled).

Template/Reference template. Data which represent the biometric measurement of an enrollee used by a biometric system for comparison against subsequently submitted biometric samples.

Template size. The amount of computer memory taken up by the biometric data.

Threshold. A “benchmark” score above which the match between the stored biometric and the person is considered acceptable or below which it is considered unacceptable.

Token image. A portrait of the holder of the MRP, typically a full frontal image, which has been adjusted in size to ensure a fixed distance between the eyes. It may also have been slightly rotated to ensure that an imaginary horizontal line drawn between the centres of the eyes is parallel to the top edge of the portrait rectangle if this has not been achieved when the original portrait was taken or captured. (See Section II, 13 in this volume of Doc 9303, Part 1.)

Validation. The process of demonstrating that the system under consideration meets in all respects the specification of that system.

Verification/Verify. The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee’s template. Contrast with *“Identification”*.

WSQ (Wavelet Scalar Quantization). A means of compressing data used particularly in relation to the storage of fingerprint images.

7. Key processes with respect to biometrics

7.1 The major components of a biometric system are:

Capture — acquisition of a raw biometric sample
Extract — conversion of the raw biometric sample data to an intermediate form
Create template — conversion of the intermediate data into a template for storage
Compare — comparison with the information in a stored reference template.

7.2 These processes involve:

- The enrollment process is the capture of a raw biometric sample. It is used for each new person (potential MRP holder) taking biometric samples to establish a new template. This capture process is the automatic acquisition of the biometric via a capture device such as a fingerprint scanner, photograph scanner, live-capture digital image camera, or live-capture iris zooming camera. Each capture device will need certain criteria and procedures defined for the capture process — for example, standard pose facing the camera straight-on for a facial recognition capture; whether fingerprints are captured flat or rolled; eyes fully open for iris capture.

- The template creation process preserves the distinct and repeatable biometric features from the captured biometric sample and is generally done with a proprietary software algorithm to extract a template from the captured image, which defines that image in a way that it can subsequently be compared with another captured image and a comparative score determined. Inherent in this algorithm is quality control, wherein through some mechanism, the sample is rated for quality. Quality standards need to be as high as possible since all future checks are dependent on the quality of the originally captured image. If the quality is not acceptable, the capture process should be repeated.

- The identification process takes new samples and compares them to saved templates of enrolled end users to determine whether the end user has enrolled in the system before, and if so, whether in the same identity.

- The verification process takes new samples of an ePassport holder and compares them to previously saved templates of that holder, to determine whether the holder is presenting in the same identity.

8. Applications for a biometrics solution

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

8.2 There are several typical applications for biometrics during the enrollment process of applying for an MRP.

8.2.1 The end user's biometric data generated by the enrollment process can be used in a search of one or more biometric databases (identification) to determine whether the end user is known to any of the corresponding systems (for example, holding a passport under a different identity, having a criminal record, holding a passport from another State).

8.2.2 When the end user collects the passport or visa (or presents himself for any step in the issuance process after the initial application is made and the biometric data is captured) his biometric data can be taken again and verified against the initially captured biometric data.

8.2.3 The identities of the staff undertaking the enrollment can be verified to confirm they have the authority to perform their assigned tasks. This may include biometric authentication to initiate digital signature of audit logs of various steps in the issuance process, allowing biometrics to link the staff members to those actions for which they are responsible.

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

8.3.1 Each time a traveller (i.e. MRP holder) enters or exits a State, his identity can be verified against the image created at the time his travel document was issued. This will ensure that the holder of a document is the legitimate person to whom it was issued and will enhance the effectiveness of any advance passenger information (API) system. Ideally, the biometric template or templates should be stored on the travel document along with the image, so that a traveller's identity can be verified in locations where access to the central database is unavailable or for jurisdictions where permanent centralized storage of biometric data is unacceptable.

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

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

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

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

— Accuracy of the biometric matching functions of the system. Issuing States must encode one or more facial, fingerprint or iris biometrics on the MRP as per LDS specifications. (It may also be stored on a database accessible to the receiving State). Given an ICAO-standardized biometric image, receiving States must select their own biometric verification software and determine their own biometric scoring thresholds for identity verification acceptance rates — and referral of impostors.

— Throughput (e.g. travellers per minute) of either the biometric system or the border-crossing system as a whole.

— Suitability of a particular biometric technology (face or finger or eye) to the border-crossing application.

9. Constraints on biometrics solutions

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

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

10. ICAO vision on biometrics

10.1 The ICAO vision for the application of biometrics technology encompasses:

— specification of a primary interoperable form of biometrics technology for use at border control (verification, watch lists) as well as by carriers and document issuers and specification of agreed supplementary biometric technologies;

— specification of the biometrics technologies for use by document issuers (identification, verification and watch lists);

— capability of data retrieval for maximum ten-year validity as specified in Doc 9303;

— having no proprietary element to ensure that any States investing in biometrics are protected against changing infrastructure or changing suppliers.

11. The selection of biometrics applicable to ePassports

11.1 It has long been recognized that names and honour are not sufficient to guarantee that the holder of an identity document (MRP) assigned to that person by the issuing State is guaranteed to be the person purporting at a receiving State to be the same person to whom that document was issued.

11.2 The only method of relating the person irrevocably to his travel document is to have a physiological characteristic of that person associated with the travel document in a tamper-proof manner. This physiological characteristic is a biometric.

11.3 After a five-year investigation into the operational needs for a biometric identifier which combines suitability for use in the MRP issuance procedure and in the various processes in cross-border travel consistent with the privacy laws of various States, ICAO has specified that facial recognition shall become the globally interoperable biometric technology. A State may also optionally elect to use fingerprint and/or iris recognition in support of facial recognition.

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

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

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

11.4.3 The facial image is already collected and verified routinely as part of the MRP application form process in order to produce a passport to Doc 9303 standards.

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

11.4.5 The capture of a facial image is non-intrusive. The end user does not have to touch or interact with a physical device for a substantial timeframe to be enrolled.

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

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

11.4.8 Many States have a legacy database of facial images captured as part of the digitized production of passport photographs which can be encoded into facial templates and verified against for identity comparison purposes.

11.4.9 In appropriate circumstances, as decided by the issuing State, a facial image can be captured from an endorsed photograph, not requiring the person to be physically present.

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

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

11.5 *Storage of the facial biometric*. Facial recognition vendors all use proprietary algorithms to generate their biometric templates. These algorithms are kept secret by the vendors as their intellectual property and cannot be reverse-engineered to create a recognizable facial image. Therefore facial recognition templates are not interoperable between vendors — the only way to achieve interoperability with facial images is for the “original” captured photograph to be passed to the receiving State. The receiving State then uses its own vendor algorithm (which may or may not be the same vendor/version as the issuing State used) to compare a facial image captured in real time of the MRP holder with the facial image read from the data storage technology in their MRP.

12. Optional additional biometrics

12.1 States optionally can provide additional data input to their (and other States) identity verification processes by including multiple biometrics in their travel documents, i.e. a combination of face and/or fingerprint and/or iris. This is especially relevant where States may have existing fingerprint or iris databases in place against which they can verify the biometrics proffered to them, for example, as part of an ID card system.

12.2 *Storage of an optional fingerprint biometric*. There are three classes of fingerprint biometric technology: finger image-based systems, finger minutiae-based systems, and finger pattern-based systems. Whilst standards have been developed within these classes to make most systems interoperable amongst their class, they are not interoperable between classes. Three standards for fingerprint interoperability are therefore emerging: storage of the image data, storage of the minutiae data and storage of the pattern data. Where an issuing State elects to provide fingerprint data in its ePassport, the storage of the fingerprint image is mandatory to permit global interoperability between the classes. The storage of an associated template is optional at the discretion of the issuing State.

12.3 *Storage of an optional iris biometric*. Iris biometrics are complicated by the dearth of proven vendors. A de facto standard for iris biometrics has therefore emerged based on the methodology of the one recognized vendor. Other vendors may in future provide iris technology, but it is likely they will need the image of the iris as their starting point, rather than the template created by the current vendor. Where an issuing State elects to provide iris data in its ePassport, the storage of the iris image is mandatory to permit global interoperability. The storage of an associated template is optional at the discretion of the issuing State.

13. Image storage, compression and cropping

13.1 In the LDS structure, the variable size data item that has the most impact on LDS size is the displayed image. The next question becomes "to what level can the image be compressed by the issuing State without degrading the results of biometric comparison by the receiving State?"

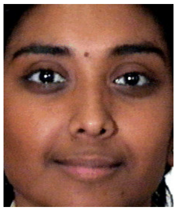
13.2 Biometric systems reduce the raw acquired image (face/fingerprint/iris) to a feature space that is used for matching — it follows that as long as compression does not compromise this feature space, it can be undertaken to reduce the storage requirements of the images retained.

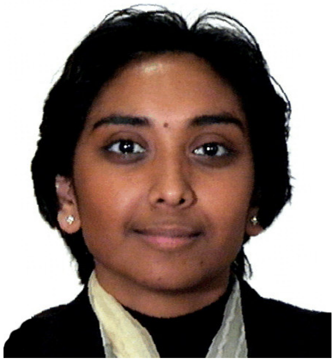
13.3 *Facial image data size*. An ICAO-standard size portrait colour-scanned at 300 dpi results in a facial image with approximately 90 pixels between the eyes and a size of approximately 643 K (kilobytes). This can be reduced to 112 K (kilobytes) with very minimal compression.

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

13.4.1 *Cropping*: Whilst images can be cropped to save storage and show just the eye/nose/mouth features, the ability for a human to easily verify that image as being of the same person who is in front of them, or appearing in the photograph in the data page of the passport, is diminished significantly.

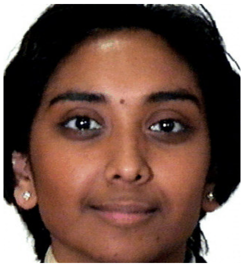
For example, the image to the left provides a greater challenge in recognition than that on the right.





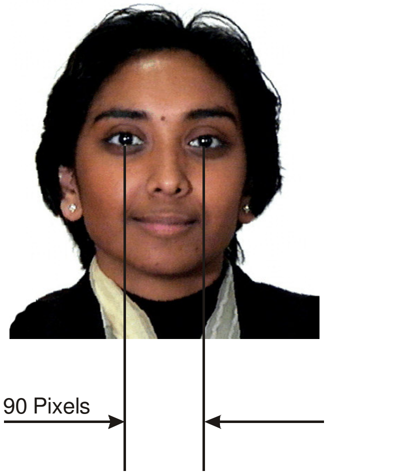
It is therefore recommended that images stored in the LDS are to be either:

- not cropped, i.e. identical to the portrait printed on the data page;
- cropped from chin to crown and edge-to-edge as a minimum, as shown below.



13.4.2 To assist in the facial recognition process, the facial image shall be stored either as a full frontal image or as a token image in accordance with the specifications established in ISO/IEC 19794-5. A token image is a facial image in which the image is rotated if necessary to ensure that an imaginary horizontal line drawn between the centres of the eyes is parallel to the top edge of the picture and the size adjusted. ICAO recommends that the centres of the eyes be approximately 90 pixels apart as in the following illustration.

Original image



Token image (angled and resized)

The Logical Data Structure (see Section III) can accommodate the storage of the eye coordinates. (For details on recording the facial image within the LDS see 10.3.1 of Section III in this volume.)

13.4.3 *Facial ornaments.* The issuing State shall decide to what extent it permits facial ornaments to appear in stored (and displayed) portraits. In general, if such ornaments are permanently worn, they should appear in the stored image.

13.5 *Optional fingerprint image size*. When a State elects to store fingerprint image(s) on the IC, the optimal image size is specified at approximately 10 K of data per finger (e.g. when compressed with the typical WSQ compression technique).

13.6 *Optional iris image size*. When a State elects to store iris image(s) on the IC, the optimal image size is approximately 30 K of data per eye.

14. Storage of the biometric and other data in a logical format in a contactless IC

14.1 These specifications also require that digital images be used, and that these be "on-board," i.e. electronically stored in the travel document.

14.2 These images are to be standardized.

14.3 A high-capacity contactless IC is the electronic storage medium specified by ICAO as the capacity expansion technology for use with ePassports in the deployment of biometrics.

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

14.4 *Storage of other data*. A State may wish to use the storage capacity of the IC in an ePassport to expand the machine readable data capacity of the MRP beyond that defined for global interchange. This can be for such purposes as providing machine readable access to breeder document information (e.g. birth certificate details), stored personal identity confirmation (biometrics) and/or document authenticity verification details.

14.5 *Logical Data Structure.* To ensure global interoperability for machine reading of stored details, a "Logical Data Structure" or "LDS" defines the format for the recording of details in the contactless IC. The LDS is specified in detail in Section III of this volume.

14.6 *Security and privacy of the stored data*. Both the issuing and any receiving States need to be satisfied that the data stored on the IC has not been altered since it was recorded at the time of issue of the document. In addition, the privacy laws or practice of the issuing State may require that the data cannot be accessed except by an authorized person or organization. Accordingly ICAO has developed specifications in Section IV regarding the application and usage of modern encryption techniques, particularly interoperable public key infrastructure (PKI) schemes, to be used by States with their machine readable travel documents as made in accordance with the specifications set out in Doc 9303. The intent is primarily to augment security through automated means of authentication of MRPs and their legitimate holders internationally. In addition, ways and means are recommended to implement international ePassport authentication and to provide a path to the use of ePassports to facilitate biometric or e-commerce applications. The specifications in Section IV permit the issuing State to protect the stored data from unauthorized access by the use of access control. Two access control methods are specified, basic access control and extended access control.

14.7 The present specifications permit the writing of data to the IC only at the time of issue of the MRP.

14.8 *PKI*. The aim of the PKI scheme, as described, is mainly to enable ePassport inspecting authorities (receiving States) to verify the authenticity and integrity of the data stored in the ePassport. The specifications do not try to prescribe a full implementation of a complicated PKI structure, but rather are intended to provide a way of implementation in which States are able to make choices in several areas (such as active or passive authentication, anti-skimming and access control, automated border crossing, etc.), thus having the possibility to phase in implementation of additional features without being incompliant to the total framework.

14.8.1 Certificates are used for security purposes, along with a methodology for public key (certificate) circulation to member States, and the infrastructure is customized for ICAO purposes.

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

14.9 *PKI and LDS*. The sections on the LDS and the PKI specify how data integrity and data privacy is to be achieved in the context of biometrics deployment in MRPs.

14.10 *Contactless IC and encoding.* The contactless ICs used in MRPs are to conform to ISO/IEC14443 Type A or Type B. The on-board Operating System shall conform to ISO/IEC Standard 7816-4. The LDS is to be encoded according to the Random Access method. The read range (achieved by a combination of the ePassport and the reader) should be up to 10 cm as noted in ISO/IEC 14443.

14.11 *Minimum data items to be stored in the LDS.* The minimum mandatory items of data to be stored in the LDS on the contactless IC shall be a duplication of the machine readable zone data in Data Group 1 and the holder's facial image in Data Group 2. In addition, the IC in a compliant ePassport shall contain the Security Data (EF.SOD) that is needed to validate the integrity of data created by the issuer — this is stored in Dedicated File No 1 as specified in the LDS (See Section III). The Security Data (EF.SOD) consists of the hashes of the Data Groups in use. Refer to Section IV for detailed information.

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

15. Placement of the contactless IC in the MRP

15.1 *Location of the contactless IC and its associated antenna in the MRP*. The location of the contactless IC with its associated antenna in the MRP is at the discretion of the issuing State. States should be aware of the importance of the need for the contactless IC to be protected against physical tampering and casual damage including flexing and bending.

15.2 *Optional locations for the contactless IC and its antenna*. The following locations have been identified:

Data page — placing the IC and antenna within the structure of a data page forming an internal page of the book.

Centre of booklet — placing the IC and its antenna between the centre pages of the book.

Cover — placement within the structure or construction of the cover.

Separate sewn-in page — incorporating the IC and its antenna into a separate page, which may be in the form of an ID3 size plastic card, sewn into the book during its manufacture.

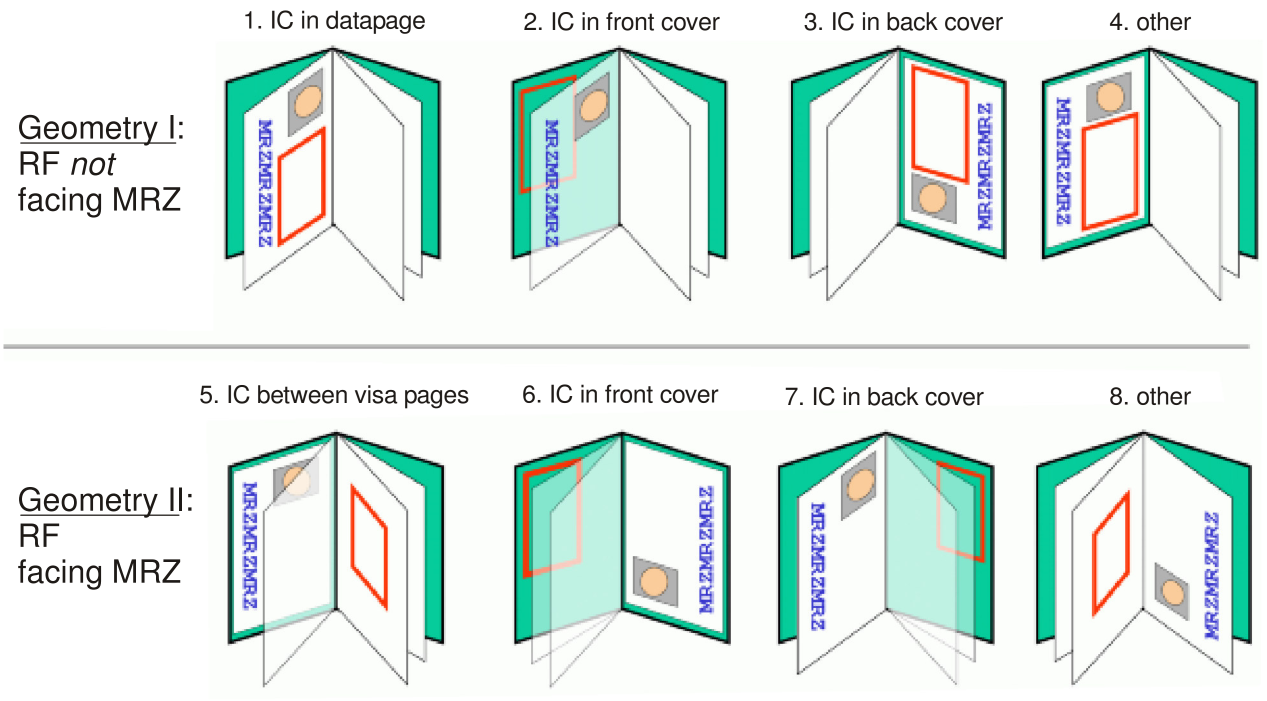


Figure II-3

Figure II-3 illustrates the above options.

Note.— In these illustrations the IC and its antenna are shown as an outlined rectangle. The data page is shown with MRZMRZMRZ representing the MRZ and with a circle inside a rectangle indicating the portrait.

15.3 *Precautions in ePassport manufacture*. States need to ensure the booklet manufacturing process and the personalization process do not introduce unexpected damage to the IC or to its antenna. For example, excessive heat in lamination or image perforation in the area of the IC or its antenna may damage the IC assembly. Similarly, when the IC is in the front cover, foil blocking on the outside of the cover, after it is assembled, can also damage the IC or the connections to its antenna.

15.4 *Reading both the OCR and the data on the IC*. It is strongly recommended that a receiving State read both the OCR data and the data stored on the IC. Where a State has locked the IC against eavesdropping, the reading of the OCR is required in order to access the IC data. It is desirable that only one reader be used for both operations, the reader being equipped to read both. If the MRP is opened at the data page and placed on a whole page reader, some MRPs will have the IC situated behind the face of the data page, while others will have the IC in the part of the book that is not in the whole page reader.

15.5 *Reader construction*. States shall therefore install reading equipment capable of handling MRPs of both geometries, preferably capable of reading both OCR and the IC. Figure II-4 shows possible reader configurations, each capable of reading the OCR and the IC. The book is half opened and two antennae ensure that the IC is read irrespective of whether it faces the MRZ or not. Also shown is a less satisfactory configuration in which the ePassport is placed on an OCR reader or swiped through an OCR reader to read the MRZ and then on a reader for the IC data. This arrangement will be less convenient for immigration staff.

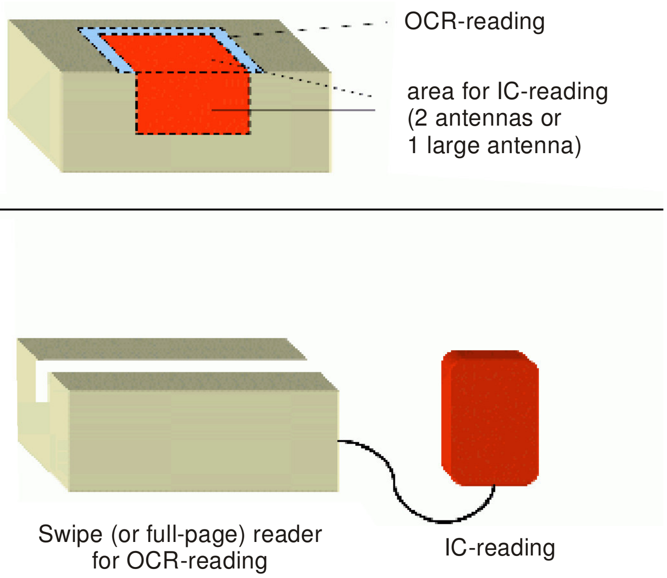
Concurrent reading process

Full-page reader with 2 antennas perpendicularly orientated, or one large antenna covering the area of an opened book

or

2-step reading process

OCR-swipe or full-page reader, connected to separate RF-reader


OCR-reading
area for IC-reading (2 antennas or 1 large antenna)
Swipe (or full-page) reader for OCR-reading
IC-reading

1. Step: Swipe MRTD through/put on OCR-reader
2. Step: If chip exists, put MRTD on IC-Reader

Figure II-4

15.6 *Reading geometries*. Reader manufacturers therefore need to consider how to design machine reading solutions that account for the various orientational possibilities and (ideally) are capable of reading the MRZ and the contactless IC simultaneously.

16. Process for reading ePassports

16.1 Figure II-5 shows the processes involved in the reading of an ePassport prior to and including the biometric verification of the holder.

17. Protection of the data stored in the contactless IC

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

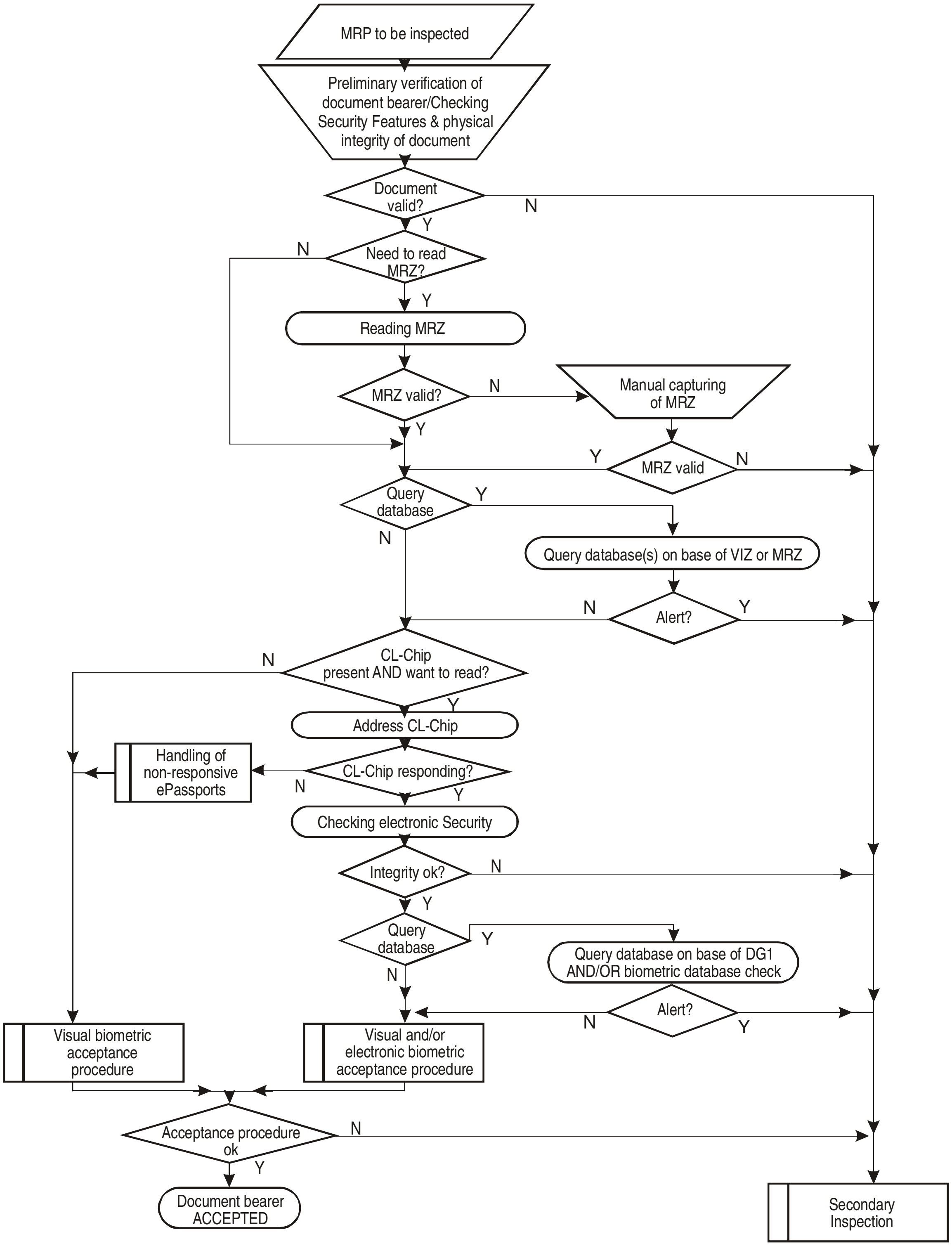

MRP to be inspected
Preliminary verification of document bearer/Checking Security Features & physical integrity of document
Document valid?
N
Y
Need to read MRZ?
N
Y
Reading MRZ
MRZ valid?
N
Manual capturing of MRZ
Y
Y
MRZ valid
N
Query database
Y
N
Query database(s) on base of VIZ or MRZ
N
Alert?
Y
CL-Chip present AND want to read?
N
Y
Address CL-Chip
Handling of non-responsive ePassports
CL-Chip responding?
N
Y
Checking electronic Security
Integrity ok?
N
Y
Query database
Y
N
Query database on base of DG1 AND/OR biometric database check
Alert?
N
Y
Visual biometric acceptance procedure
Visual and/or electronic biometric acceptance procedure
Acceptance procedure ok
N
Y
Document bearer ACCEPTED
Secondary Inspection

Figure II-5

SECTION III

A LOGICAL DATA STRUCTURE FOR CONTACTLESS INTEGRATED CIRCUIT DATA STORAGE TECHNOLOGY

1. Scope

1.1 This Section defines a Logical Data Structure (LDS) for ePassports required for global interoperability. It defines the specifications for the standardized organization of data recorded to a contactless integrated circuit capacity expansion technology of an MRP when selected by an issuing State or organization so that the data is accessible by receiving States. This requires the identification of all mandatory and optional Data Elements and a prescriptive ordering and/or grouping of Data Elements that must be followed to achieve global interoperability for reading of details (Data Elements) recorded in the capacity expansion technology optionally included on an MRP (ePassport).

2. Normative references

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

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 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: 2005	Identification cards — Integrated circuit(s) cards with contacts — Part 4: Organization, security and commands for interchange
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 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 10373-6:2001	Test methods for proximity cards
ISO/IEC 10373-6:2001/FDAM1	Test methods for proximity cards (Amendment 1: Protocol test methods for proximity cards)
ISO/IEC 10373-6:2001/AM2:2003	Test methods for proximity cards (Amendment 2: Improved RF test methods)

ISO/IEC 10373-6:2001/FDAM4	Test methods for proximity cards (Amendment 4: Additional test methods for PCD RF interface and PICC alternating field exposure)
ISO/IEC 10373-6:2001/FDAM5	Test methods for proximity cards (Amendment 5: Bit rates of fc/64, fc/32 and fc/16)
ISO/IEC 10918	Information technology — Digital compression and coding of continuous-tone still images
ISO/IEC 14443-1:2000	Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1: Physical Characteristics
ISO/IEC 14443-2:2001	Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio Frequency Power and Signal Interface
ISO/IEC 14443-2:2001/AM1:2005	Proximity cards: Radio Frequency Power and Signal Interface (Amendment 2: Bit Rates of fc/64, fc/32 and fc/16).
ISO/IEC 14443-3	Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and Anticollision
ISO/IEC 14443-3:2001/AM1:2005	Proximity cards: Initialization and Anticollision (Amendment 1: Bit Rates of fc/64, fc/32 and fc/16).
ISO/IEC 14443-4	Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol
ISO/IEC15444	JPEG 2000
ISO/IEC 19785-1	Information Technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification
ISO/IEC 19794-4	Information technology — Biometric data interchange formats — Part 4: Finger image data
ISO/IEC 19794-5	Information technology — Biometric data interchange formats — Part 5: Facial image data
ISO/IEC 19794-6	Information technology — Biometric data interchange formats — Part 6: Iris image data
ISO/IEC 9797-1:1999	Information technology —Security techniques — Message authentication Codes (MACs) — Part 1: Mechanisms using a block cipher
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)

3. Definitions

For the purpose of this section, the following additional definitions shall apply.

(*Note.— Definitions relating to the basic machine readable passport, visa and official travel document are found in Section II of Volume 1 of Doc 9303, Part 1.)*

ASN.1. Abstract Syntax Notation One

CBEFF. Common Biometric Exchange Format Framework, 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.

Authorized Receiving Organization. Organization authorized to process an official travel document (e.g. an aircraft operator) and, as such, potentially allowed in the future to record details in the optional capacity expansion technology.

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.

4. The need for a Logical Data Structure

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

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

Note.—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.

5. Requirements of the Logical Data Structure

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

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

6. Mandatory and optional Data Elements

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

7. Ordering and grouping of Data Elements

7.1 A logical 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 III-1.

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

Note.—The ability for a receiving State or approved receiving organization to add data to the LDS is not supported in the LDS defined in this edition of Doc 9303, Part 1.

[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.

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

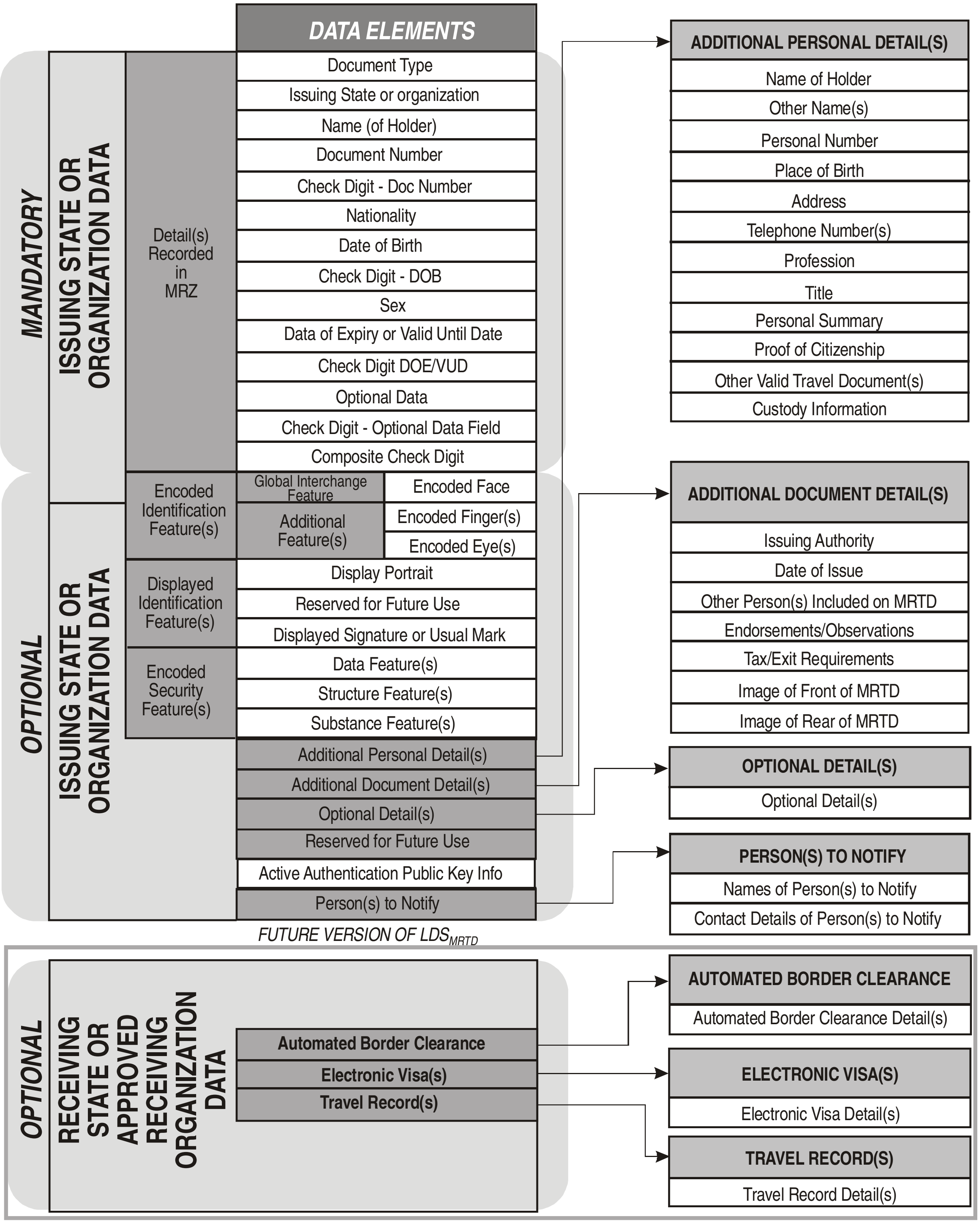

DATA ELEMENTS
MANDATORY
ISSUING STATE OR ORGANIZATION DATA
Detail(s) Recorded in MRZ
Document Type
Issuing State or organization
Name (of Holder)
Document Number
Check Digit - Doc Number
Nationality
Date of Birth
Check Digit - DOB
Sex
Data of Expiry or Valid Until Date
Check Digit DOE/VUD
Optional Data
Check Digit - Optional Data Field
Composite Check Digit
OPTIONAL
ISSUING STATE OR ORGANIZATION DATA
Encoded Identification Feature(s)
Global Interchange Feature
Encoded Face
Additional Feature(s)
Encoded Finger(s)
Encoded Eye(s)
Displayed Identification Feature(s)
Display Portrait
Reserved for Future Use
Displayed Signature or Usual Mark
Encoded Security Feature(s)
Data Feature(s)
Structure Feature(s)
Substance Feature(s)
Additional Personal Detail(s)
Additional Document Detail(s)
Optional Detail(s)
Reserved for Future Use
Active Authentication Public Key Info
Person(s) to Notify
FUTURE VERSION OF LDS$_{MRTD}$
ADDITIONAL PERSONAL DETAIL(S)
Name of Holder
Other Name(s)
Personal Number
Place of Birth
Address
Telephone Number(s)
Profession
Title
Personal Summary
Proof of Citizenship
Other Valid Travel Document(s)
Custody Information
ADDITIONAL DOCUMENT DETAIL(S)
Issuing Authority
Date of Issue
Other Person(s) Included on MRTD
Endorsements/Observations
Tax/Exit Requirements
Image of Front of MRTD
Image of Rear of MRTD
OPTIONAL DETAIL(S)
Optional Detail(s)
PERSON(S) TO NOTIFY
Names of Person(s) to Notify
Contact Details of Person(s) to Notify
OPTIONAL
RECEIVING STATE OR APPROVED RECEIVING ORGANIZATION DATA
Automated Border Clearance
Electronic Visa(s)
Travel Record(s)
AUTOMATED BORDER CLEARANCE
Automated Border Clearance Detail(s)
ELECTRONIC VISA(S)
Electronic Visa Detail(s)
TRAVEL RECORD(S)
Travel Record Detail(s)

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

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

- those that define the contents of the machine readable zone (MRZ) of the ePassport (Data Group 1);
- an encoded image of the face of the ePassport holder as defined in Volume 1 and Section II of Volume 2 of Doc 9303, Part 1;
- EF.COM, containing version information and tag list;
- EF.SOD, containing data integrity, authenticity information.

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

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

Note.— The ability for a receiving State or approved receiving organization to add data to the LDS is not supported in this edition of Doc 9303, Part 1.

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

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

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

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

Note.—Receiving State Data Groups (Data Groups 17-19) are not supported in this edition of Doc 9303, Part 1.

8. Data Groups coded to allow confirmation of authenticity and integrity of data

8.1 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 Section IV *PKI* for details.) Using the CBEFF structure utilized for Encoded Identification Feature Data Groups 2-4 and optional “additional biometric security” features defined in Section IV, *PKI*, identity confirmation details (e.g. biometric templates) may also be individually protected at the discretion of the issuing State or organization.

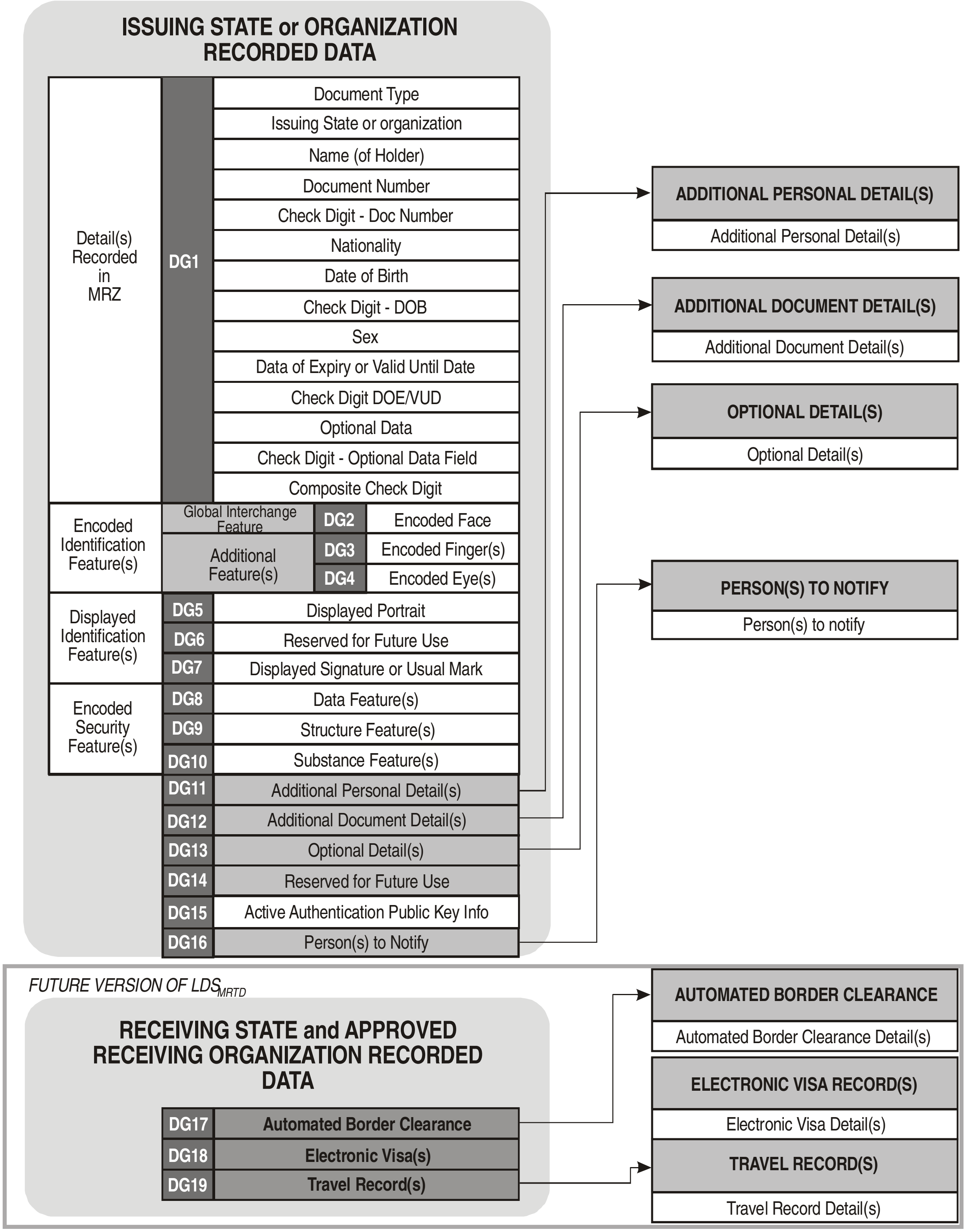

ISSUING STATE or ORGANIZATION RECORDED DATA
Detail(s) Recorded in MRZ
DG1
Document Type
Issuing State or organization
Name (of Holder)
Document Number
Check Digit - Doc Number
Nationality
Date of Birth
Check Digit - DOB
Sex
Data of Expiry or Valid Until Date
Check Digit DOE/VUD
Optional Data
Check Digit - Optional Data Field
Composite Check Digit
Encoded Identification Feature(s)
Global Interchange Feature
DG2
Encoded Face
Additional Feature(s)
DG3
Encoded Finger(s)
DG4
Encoded Eye(s)
Displayed Identification Feature(s)
DG5
Displayed Portrait
DG6
Reserved for Future Use
DG7
Displayed Signature or Usual Mark
Encoded Security Feature(s)
DG8
Data Feature(s)
DG9
Structure Feature(s)
DG10
Substance Feature(s)
DG11
Additional Personal Detail(s)
DG12
Additional Document Detail(s)
DG13
Optional Detail(s)
DG14
Reserved for Future Use
DG15
Active Authentication Public Key Info
DG16
Person(s) to Notify
ADDITIONAL PERSONAL DETAIL(S)
Additional Personal Detail(s)
ADDITIONAL DOCUMENT DETAIL(S)
Additional Document Detail(s)
OPTIONAL DETAIL(S)
Optional Detail(s)
PERSON(S) TO NOTIFY
Person(s) to notify
FUTURE VERSION OF LDS$_{MRTD}$
RECEIVING STATE and APPROVED RECEIVING ORGANIZATION RECORDED DATA
DG17
Automated Border Clearance
DG18
Electronic Visa(s)
DG19
Travel Record(s)
AUTOMATED BORDER CLEARANCE
Automated Border Clearance Detail(s)
ELECTRONIC VISA RECORD(S)
Electronic Visa Detail(s)
TRAVEL RECORD(S)
Travel Record Detail(s)

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

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

9. Data Groups recorded by the issuing State or organization

The following table defines the mandatory and optional Data Groups that combine to form that portion of the LDS 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	
Machine assisted identity confirmation detail(s) — Encoded identification feature(s)			
2	M	**GLOBAL INTERCHANGE FEATURE**	Encoded face
3	O	Additional feature	Encoded finger(s)
4	O	Additional feature	Encoded iris(es)
Machine assisted identity confirmation detail(s) — Displayed identification feature(s)			
5	O	Displayed portrait *[See 10.3]*	
6	O	Reserved for future use	
7	O	Displayed signature or usual mark	
Machine assisted security feature verification — Encoded security feature(s)			
8	O	Data feature(s)	
9	O	Structure feature(s)	
10	O	Substance feature(s)*]*	
Additional personal detail(s)			
11	O	Additional personal Data Elements	
Additional document detail(s)			
12	O	Additional document Data Elements	
Optional detail(s)			
13	O	Discretionary Data Element(s) defined by issuing State or organization	
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)	

10. Data Elements forming Data Groups 1 through 16

10.1 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.

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

10.2.1 *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 Doc 9303, Part 1, Volume 1.

Data Group	Data Element	Fixed/ Variable	Mandatory/ Optional	Data Item
DG1			**M**	**MRZ (Summary of details as recorded on MRTD. Refer to 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 (*Nine most significant characters*)
	05	F	M	Check digit — Document number or filler character (<) indicating document number exceeds nine characters. *[see 10.2.2]*
	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)*
	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 plus document number check digit plus filler character
	13	F	M	Check digit — Optional data field
	14	F	M	Composite check digit

10.2.2 Refer to Doc 9303, Part 1, Volume 1 for details regarding calculation of check digits.

10.3 *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 10.3.1]*
	01	M	Number of face biometric encodings recorded
	02[5]	M	Header *[see A.13.3]*
	03[6]	M	Face biometric data encoding(s) *[see A.13.3]*
ADDITIONAL IDENTIFICATION FEATURE(s) *[see 10.3.2]*			
DG3		**O**	**ADDITIONAL IDENTIFICATION FEATURE — FINGER(S)** *[see 10.3.2]*
	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(ES)** *[see 10.3.2]*
	01	M *(If encoded eye(s) feature recorded)*	Number of iris(es) 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]*

[5] 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 Appendix 1 for specific implementation.

[6] Data Element will repeat within the Data Group when more than one recording of the displayed signature or usual mark/encoded security feature is present; *i.e.* as defined through Data Element 01.

10.3.1 Data Group 2 (DG2) represents the globally interoperable biometric for machine assisted identity confirmation with machine readable travel documents, which shall be an image of the face of the holder as an input to a face recognition system. If there is more than one recording, the most recent internationally interoperable encoding shall be the first entry. The primary purpose of using chip technology is to have the ability to capture biometrics in travel documents. The face biometric data interchange image recorded in DG2 shall be derived from the passport photo used to create the displayed portrait printed on the data page of the ePassport and shall be encoded either according to full frontal or token frontal image type formats set out in the latest version of ISO/IEC 19794-5. DG2 shall contain either a full frontal or token frontal face biometric data interchange format image or both as determined at the discretion of the issuing State. Where a full frontal image is included, the eye positions MAY also be included along with a full frontal image using an optional feature point data block set out in ISO/IEC 19794-5. Issuing States wishing to record the displayed portrait, i.e. when the face biometric data interchange format image is substantially different from the displayed portrait image, shall record the image in DG5.

10.3.2 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.

10.4 *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 10.4.1]*
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[6]	M *(If displayed signature or usual mark recorded)*	Displayed signature or usual mark representation *[see 10.4.1]*

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

10.5 *Machine assisted security feature verification — Encoded detail(s).* Data Elements combining to form Data Groups 8 (DG8) through 10 (DG10) are as follows.

[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.

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[6]	M *(If this encoded feature is used)*	Header *(to be defined)*
	03	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	M *(If this encoded feature is used)*	Header *(to be defined)*
	03	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	M *(If this encoded feature is used)*	Header *(to be defined)*
	03	M *(If this encoded feature is used)*	Substance feature(s) data

10.6 *Additional personal detail(s).* Data Elements combining to form Data Group 11 (DG11) are as follows:

Data Group	Data Element	Mandatory/ Optional	Data 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

Data Group	**Data Element**	**Mandatory/ Optional**	**Data Item**
	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 10.6.1]*
	12	M* ** If DE 13 recorded.*	Number of other valid travel documents
	13	O	Other travel document numbers
	14	O	Custody information

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

10.7 *Additional document detail(s).* Data Elements combining to form Data Group 12 (DG12) are as follows.

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 10.7.1]*
	08	O	Image of rear MRTD *[see 10.7.1]*
	09	O	Time MRTD personalized
	10	O	Machine used to personalize MRTD

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

10.8 *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

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

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

10.10 Data Group 15 (DG15): Active Authentication Public Key Information. This Data Group contains the optional Active Authentication Public Key (refer to Section IV PKI).

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

10.11 *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
	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

11. Data Groups recorded by a receiving State or approved receiving organization

11.1 The following table defines the optional Data Groups that combine to form that portion of the LDS which may in the future be 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 this edition of Doc 9303, Part 1. Therefore, Data Groups 17 through 19 are not valid, nor are they supported in LDS at the present time. Their inclusion here indicates planned future development.

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)

12. Format of Data Elements

12.1 *Data Element Directory*

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

12.1.1 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,S	Document type (as per Doc 9303 MRZ)
02	M	Issuing State or organization	3	F	A,S	Issuing State or organization (as per Doc 9303 MRZ)
03	M	Name of holder				
	M	*Primary and secondary identifiers*	39	F	A,S	Single and double filler characters (<) inserted as per Doc 9303 MRZ.

Data Element	Optional or Mandatory	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
04	M	Document number	9	F	A,N,S	Document number (as per MRZ) Note: Consistent with specifications defined in Part 3 of Doc 9303 for the TD-1, if the document number exceeds nine 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 Doc 9303 MRZ).
06	M	Nationality	3	F	A,S	Alpha-3 code (as per MRZ).
07	M	Date of birth	6	F	N,S	Format = YYMMDD as per 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 Doc 9303 MRZ).
09	M	Sex	1	F	A,S	As per MRZ in 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.
11	M	Check digit — *Date of expiry or valid until date*	1	F	N	Check digit for Data Element 10 (as per Doc 9303 MRZ).
12	M *if optional data in MRZ*	Optional data				
	M if optional data in MRZ	*Optional data*	14	F	A,N,S	As per MRZ.
13	M	Check digit — *Optional data field*	1	F	N	Check digit for Data Element 12 (as per Doc 9303 MRZ).
14	M	Check digit — *Composite check digit*	1	F	N	As per Doc 9303 MRZ.

Data Element	Optional or Mandatory	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
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 Appendix 1, A13.3,* 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 Appendix 1, A13.3* 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 Appendix 1, A13.3* 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 Appendix 1,* for details on encoding. Data Element may recur as defined by DE 01.
DATA GROUP 4: Encoded identification features — IRIS(ES)						
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 Appendix 1* for details on encoding. Data Element may recur as defined by DE 01.
03	M *If encoded eye(s) feature included*	Eye biometric data encoding(s)	99999 Max	Var	A,N,S,B	See *Normative Appendix 1* 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.

Data Element	Optional or Mandatory	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
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/IEC 10918-1 or ISO/IEC 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		Var		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/IEC 10918-1 or ISO/IEC 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 Element	Optional or Mandatory	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
DATA GROUP 9: Encoded security features — STRUCTURE FEATURE(S)						
01	M *If encoded structure feature included*	Number of structure features	1	F	N	1 to 9, identifying number of unique 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 GROUP 10: 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 *Iif 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 12.1.2]						
DATA GROUP 12: Additional document detail(s)						
See Data Element Directory — Additional document detail(s) [see 12.1.3]						

Data Element	Optional or Mandatory	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
DATA GROUP 13: Optional detail(s)						
See Data Element Directory — Optional detail(s) [see 12.1.4]						
DATA GROUP 14: Reserved for future use						
Reserved						
DATA GROUP 15: Active Authentication Public Key Info						
Active Authentication Public Key Info as specified in Section IV to this volume: “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 12.1.5]						

12.1.2 *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

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**
06	O	Full date of birth				
		Date of birth	8	F	N	CCYYMMDD
07	O	Telephone				
	M, if DE 07 included	*Telephone*	99 Max	Var	N,S	Free-form text
08	O	Profession				
	M, if DE 08 included	*Profession*	99 Max	Var	A,N,S	Free-form text
09	O	Title				
	M, if DE 09 included	*Title*	99 Max	Var	A,N,S	Free-form text
10	O	Personal summary				
	M, if DE 10 included	*Personal summary*	99 Max	Var	A,N,S	Free-form text
11	O	Proof of citizenship		Var		
	M, if DE 11 included	*Citizenship detail*	9999999 Max	Var	B	Image of citizenship document formatted as per ISO/IEC 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, If DE 13 included	*Custody information*	999 Max	Var	A,N,S	Free-form text

12.1.3 *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/IEC 10918-1.
07	O	Image of back of MRTD				
		Image of MRTD (back)	9999999 Max	Var	B	Formatted as per ISO/IEC 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

12.1.4 *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

12.1.5 *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 16 included*	Number of persons identified	2	F	N	Identifies number of persons included in the Data Group.
02	M, *If DG 16 included*	Date details recorded	8	F	N	Date notification date recorded; Format = CCYYMMDD
03	M, *If DG 16 included*	Name of person to notify *Primary and secondary identifiers*		Var	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

13. Security principles

13.1 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 Section IV, *PKI*.

HEADER AND DATA GROUP PRESENCE INFORMATION

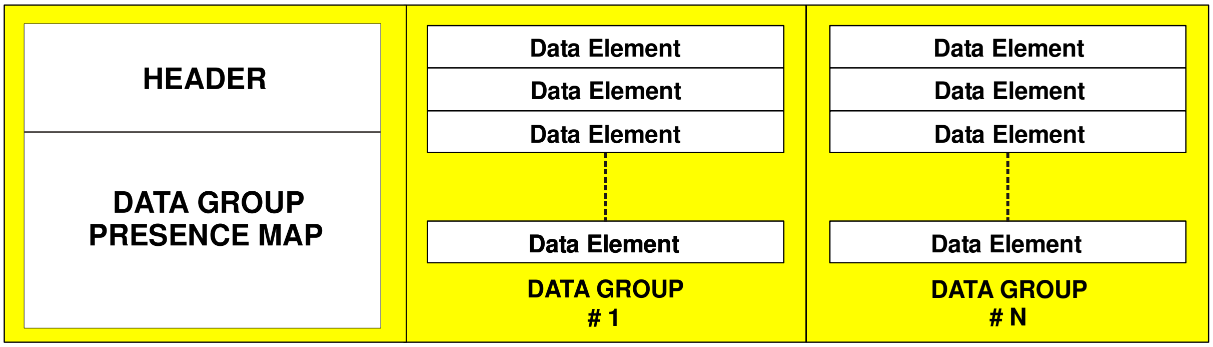


Figure III-3. Mandatory header and Data Group presence information

14. Mapping principles for contactless IC data expansion technology

14.1 *Ordering of LDS.* Only the Random Ordering Scheme is permitted for international interoperability. It is described in Normative Appendix 1 to this Section.

14.2 *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. Variable length Data Elements are encoded as *Length|Value* and lengths are specified in ASN.1 notation.

A *mandatory* Header and Data Group Presence Map is included. This information is stored in EF.COM. Refer to Appendix 1.

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

APPLICATION IDENTIFIER (AID)
LDS VERSION NUMBER
UNICODE VERSION NUMBER

14.2.2 *LDS version number.* The LDS version number defines the format version of the LDS[8]. The exact format to be used for storing this value will be defined in the technology mapping Appendix. 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.

[8] 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.

14.2.3 *Unicode version number*[9]*.* The Unicode version number identifies the coding method used when recording alpha, numeric and special characters, including national characters. The exact format to be used for storing this value will be defined in the technology mapping Appendix. The standardized format for a Unicode version number is “aabbcc”, where:

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

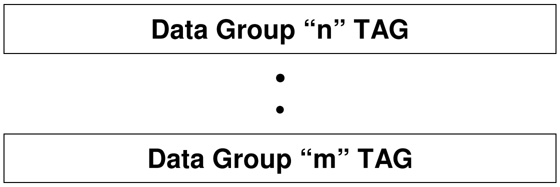
“bb” = number identifying the **minor version** of the Unicode standard (i.e. character additions or more significant normative changes, published as a **technical** report); and

“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 programme 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.

14.3 *Data Group presence map*. The Data Group presence map (DGPM) contains information which enables a receiving State or approved receiving organization to determine which Data Groups are present in the block of data recorded by the issuing State or organization.

14.3.1 The DGPM used with integrated circuit implementations 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 Appendix 1.



Presence of TAG = Data Group present
Absence of TAG = Data Group not present

14.4 *Data Element Presence Maps:* 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 Maps (DEPM) are located at the start of those specific Data Groups that allow optional expansion as illustrated in Figure III-4.

Data Groups requiring the use of a Data Element Presence Map are specified in Appendix 1.

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

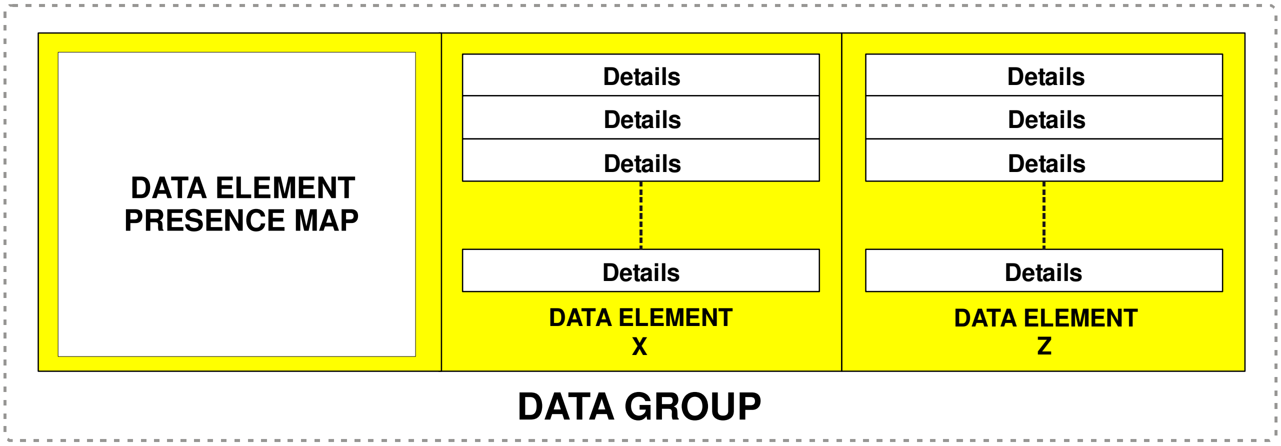


Figure III-4. Data element presence map

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

14.4.2 The 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.

Data Element "n" TAG

•
•

Data Element "m" TAG

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 Normative Appendix 1 to Section III.

Normative Appendix 1 to Section III

MAPPING OF LDS
USING RANDOM ACCESS REPRESENTATION
TO CONTACTLESS INTEGRATED CIRCUITS (IC(s))

A.1 *Scope*. Appendix 1 defines the current specifications 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 Appendix 1 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*. Refer to Section III.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 to 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 Section IV, *PKI*.

- 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.

A.3.1 To provide interoperability Appendix 1 defines:

- Initializations, anticollisions and transmission protocol;

- Command set;

- The use of commands including security references;

- The file structure for the ICAO MRTD LDS application;
- The Data Element mappings to the files; and
- Character set.[10]

A.4 *Security requirements*. Data integrity and authenticity are needed for trusted international interchange. For detailed specifications refer to Section IV, *PKI*.

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 III.2.

A.6 *Definitions*. Refer to Section III.3.

A.7 *Physical characteristics*. The physical characteristics of the document shall adhere to the physical characteristics specified in Volume 1.

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 protocol*. 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.

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 (ATQA) or Answer to Request — Type B (ATQB), as appropriate.

A.10.3 *Application selection*. IC cards shall support at least one machine readable travel document (MRTD) application, 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 Section IV, *PKI*, for detailed information.

[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,” 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.

- The second application, not supported in this edition of Doc 9303, Part 1, 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 Appendix.

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 Section IV, *PKI*.

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 are 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 (DFs) and elementary files (EFs). Dedicated files (DFs) contain elementary files or other dedicated files. An optional[11] master file (MF) may be the root of the file system.

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) and Data Group 2, the encoded face, are 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. EFs shall be addressed by short file ID as shown in Table IIIA-1. The EFs shall

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

have file names for these files that shall be according to the number n, EF.DGn, where n is the Data Group number. The name of the EF containing the security data is EF.SOD. See Figure IIIA-1 for a graphical representation of the file structure.

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 Appendix 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 Doc 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.

Table III-A1. Mandatory 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’

Data Group	EF Name	Short EF identifier	FID	Tag
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'

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

— SELECT
— READ BINARY

The command parameters that are mandatory and optional are specified in A.17 to this Appendix. Paragraph A.23 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 A.22 of this Appendix.

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 Section IV, *PKI*. Such commands are outside the scope of this interoperability specification, but may include:

— GET CHALLENGE
— EXTERNAL AUTHENTICATE
— 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.

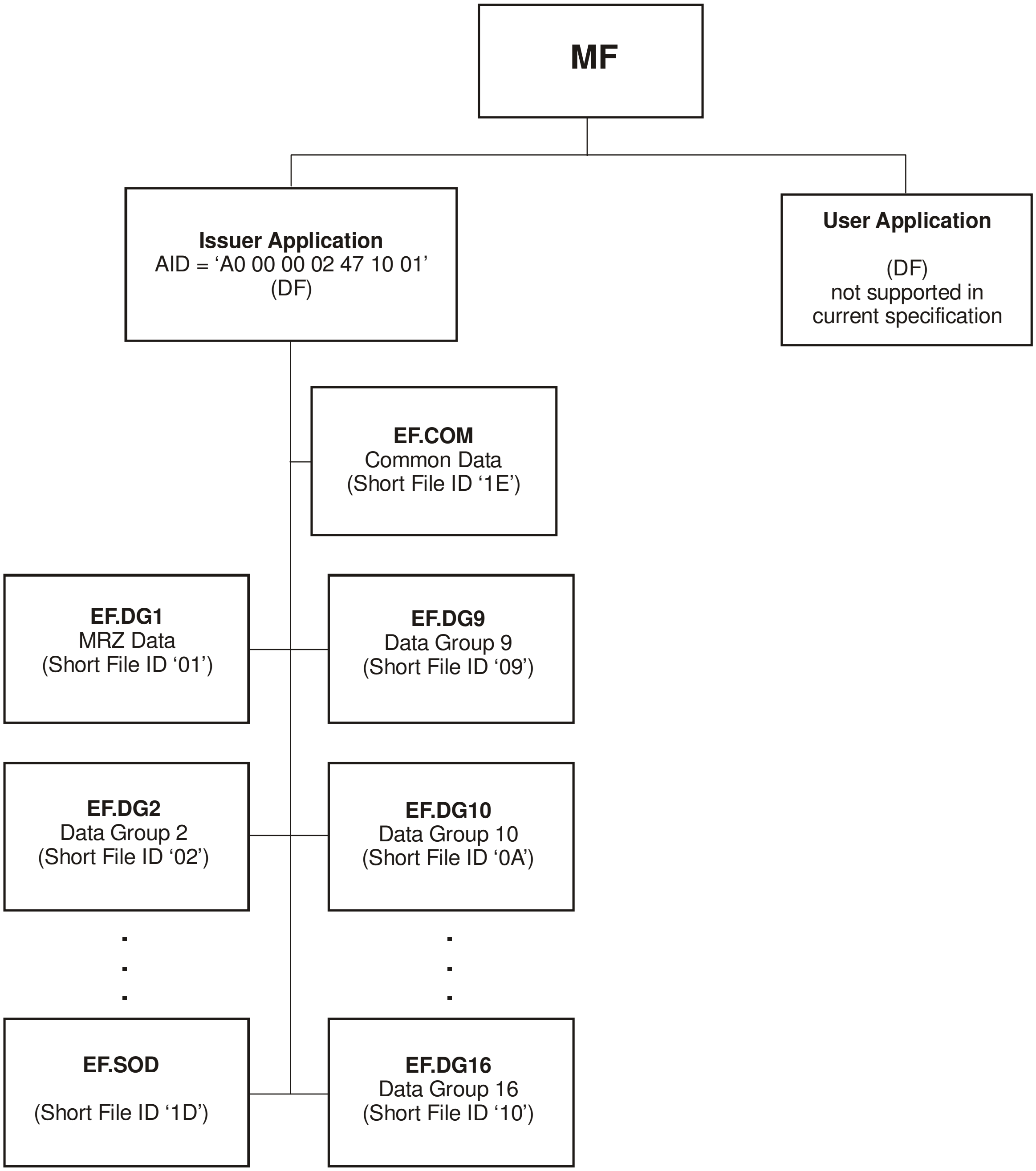


Figure IIIA-1

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

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

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

The example would read in full hexadecimal representation as:

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

A hypothetic LDS Version 15.99 would be encoded as:

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

or hexadecimal:

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

A.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 that 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[12]	M	F 39ANS	Smith<<John<T	5B
4	Document number	M	F 9ANS[13]	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)	5F57
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	F14ANS	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

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<HMD7406222M10123130121<<<<<
<<<<<54

Another example,

‘61’ *‘5B’* **‘5F1F’** *‘58’*
P<NLDMEULENDIJK<<LOES<ALBERTINE<<<<<<<<<<<<<XA00277324NLD7110195F0610010123456782
<<<<<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.

[12] Refer to Volume 1 for truncation rules for names longer than 39 characters.

[13] 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.

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/IEC JTC1/SC37 internationally interoperable biometric data block. Refer to Section II.

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 '0101' (Optional) — Version of the CBEFF patron header format
				'81'	'01-03'		Biometric type (Optional)
				'82'	'01'		Biometric subtype (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**			
			'A1'	X	Biometric Header Template (BHT)		
				Tag	**L**	**Value**	
				'80'	'02'	ICAO header version '0101' (Optional) — Version of the CBEFF patron header format	
				'81'	'01'	Biometric type (Optional)	
				'82'	'01'	Biometric subtype (Optional for DG2, mandatory for DG3, DG4.)	
				'83'	'07'	Creation date and time (Optional)	
				'85'	'08'	Validity period (from through) (Optional)	
				'86'	'04'	Creator of the biometric reference data (PID) (Optional)	
				'87'	'02'	Format owner (Mandatory)	

Tag	L	Value				
				‘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 12 642 bytes (‘3162’ bytes), encoded using a device with a PID of ‘00 01 00 01’, using format type ‘00 04’ owned by template provider ‘00 0A’ was captured on 15 March 2002 (no UTC offset) and is valid from 1 April 2002 through 31 March 2007. ICAO patron template Version 1.0 is being used.

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

```
‘75’ ‘82319EC’
   ‘7F61’ ‘823199’
     ‘02’ ‘01’ ‘01’
     ‘7F60’ ‘823191’
           ‘A1’ ‘26’
                ‘80’ ‘02’ ‘0101’
                ‘81’ ‘01’ ‘02’
                ‘83’ ‘07’ ‘20020315133000’
                ‘85’ ‘08’ ‘2002040120070331’
                ‘86’ ‘04’ ‘00010001’
                ‘87’ ‘02’ ‘000A’
                ‘88’ ‘02’ ‘0004’
           ‘5F2E’ ‘823162’ ‘… 12642 bytes of biometric data …’
```

A.13.4 *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 2 000 bytes. The length of the template is 2 008 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/IEC 10918, JFIF option
Displayed Finger	ANSI/NIST-ITL 1-2000
Displayed Signature/usual mark	ISO/IEC 10918, JFIF option

A.13.5 *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.13.6 *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 Doc 9303 rules
'A0'	'X'	Content-specific constructed data object of names
'02'	01	Number of other names
'5F0F'	X	Other name formatted per Doc 9303. The data object repeats as many times as specified in the '02' element.
'5F10'	X	Personal number
'5F2B'	04	Full date of birth yyyymmdd (BCD encoded)
'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.13.7 *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’	‘04’	Date of issue. yyyymmdd (BCD encoding)
‘A0’	X	Content-specific constructed data object of other people
‘02’	‘01’	Number of other people
‘5F1A’	X	Name of other person formatted per Doc 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
‘5F55’	‘07’	Date and time of document personalization yyyymmddhhmmss
‘5F56’	X	Serial number of personalization system

The following example contains the Issuing Authority (United States of America), the date of issue (31 May 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.13.8 *EF.DG13 Optional Details*

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

A.13.9 *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 Section IV, *PKI*

A.13.10 *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'	'04'	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.13.11 *EF.SOD LDS Security Data, Tag = '77'*

This EF contains a signed data structure conforming to RFC3369.

Tag	L	Value
'77'	X	Refer to Section IV PKI

A.14 *Receiving State application*

Not supported by the LDS in this edition of Doc 9303, Part 1.

A.15 *Tags used*

15.1 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 notify
'5F52'	Telephone	Telephone number of person to notify
'5F53'	Address	Address of person to notify

Tag	*Definition*	*Where Used*
‘5F55’	Date and time document personalized	Additional document details
‘5F56’	Serial number of personalization system	Additional document details
‘60’	Common Data Elements	EF.COM
‘61’	Template for MRZ Data Group	
‘63’	Template for finger biometric Data Group	
‘65’	Template for digitized facial image	
‘67’	Template for digitized signature or usual mark	
‘68’	Template for machine assisted security — Encoded data	
‘69’	Template for machine assisted security — Structure	
‘6A’	Template for machine assisted security — Substance	
‘6B’	Template for additional personal details	
‘6C’	Template for additional document details	
‘6D’	Optional details	
‘6E’	Reserved for future use	
‘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

15.2 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 — Date of birth	Part of MRZ
‘5F06’	Check digit — Expiry date	Part of MRZ
‘5F07’	Check digit — Composite	Part of MRZ
‘5B’	Name of document holder	Part of MRZ

Tag	*Definition*	*Where Used*
‘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
‘5F57’	Date of birth (6 digit)	Part of MRZ

15.3 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	

A.16 *Minimum requirements for interoperability.* The following are the minimum requirements for interoperability of proximity (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;[14]
- 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, refer to the Section II.

A.17 *Commands and command parameters that may be used by the interface device*

A.17.1 The following is a 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 value 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.

[14] Note this implies that readers (Proximity Coupling Devices) must be capable of reading Type A and B.

- The PCD shall detect and resolve any collision that may occur if multiple documents are within the operating field.

- Compliance with 7816 commands shall be indicated by
  - — Type A: SAK (Select Acknowledge) bit 6 = 1, bit 3 = 0
  - — Type B: Protocol_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 EFs 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.

A.18 *Details on ISO/IEC 14443 type A initialization and anticollision according to ISO/IEC 14443 type A*

A.18.1 *REQA AND WUPA (Wake-UP Type A).* The Proximity Integrated Circuit Card (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.

A.18.2 *ATQA.* After a REQA command is transmitted by the PCD, all PICCs in the IDLE state shall respond synchronously with ATQA.

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 bytes. According to ISO/IEC 14443-3 the MSB contains only RFU and proprietary bits, so these bytes 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.

A.18.3 *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 an anticollision loop shall be performed.

A.18.3.1 For the select command only the values of ‘93’ (cascade level 1), ‘95’ (cascade level 2) and ‘97’ (cascade level 3) are allowed.

A.18.3.2 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.

A.18.3.3 If Bit 3 is not set, Bit 6 specifies whether the PICC is ISO/IEC 14443-4 compliant. All PICCs used to store LDS data are required to support 14443-4, so this bit must be set.

A.18.4 *Request for Answer To Select (RATS).* After the anticollision and select loop is performed, an 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 scheme.

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’.

A.18.5 *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.

The interface bytes are followed by the historical bytes. They contain general information about the PICC and should not be evaluated by compliant software.

A.19 *Details on ISO/IEC 7816 command formats and parameter options*

A.19.1 *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.

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

A.19.2 *Selection of Master File:*

CLA	**INS**	**P1**	**P2**	**Lc**	**Data**	**Le**
‘00’	‘A4’	‘00’	‘00’	–	Empty	–

A.19.3 *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	–

A.20 *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	–

A.21 *Reading data from the EF*

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

A21.1.1 ***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

A21.1.2 *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

A.22 Examples for ISO/IEC 7816 usage with LDS

A.22.1 *Reading MRZ data using File Selection*

The following sequence can be used to read the data of Data Group 1 (MRZ).

CLA	INS	P1	P2	Lc	Data	Le	Remark
‘00’	‘A4’	‘04’	‘0C’	‘07’	‘A0 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

A.22.2 *Reading Data Group 2*

A.22.2.1 The following sequence can 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.

A22.2.2 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’	‘A0 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’	:

A22.3 When reading more than one Data Group consecutively, the Issuer Application has to be selected only once (before reading the first file).

A.22.4 *Reading MRZ data using global SFI*

CLA	INS	P1	P2	Lc	Data	Le	Remark
‘00’	‘B0’	‘81’	‘00’	–	–	‘00’	Direct Read of 256 bytes

A22.5 *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’	:

A.23 *EFs larger than 32 767 bytes*

A.23.1 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’

A23.2 The subsequent READ BINARY commands shall specify the offset in the Data field. The final READ BINARY command should request the remaining data area.

A.24 *ASN.1 BER 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.

A.24.1 Examples 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 (1 000) would be encoded as ‘8203E8’ in hexadecimal representation.

A.25 *Biometric sub-feature encoding:* The following table indicates the scheme for the encoding of sub-features:

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

SECTION IV

PKI FOR MACHINE READABLE TRAVEL DOCUMENTS OFFERING ICC READ ONLY ACCESS

1. SCOPE

1.1 This Section provides specifications to enable States and suppliers to implement the authentication scheme involving a specific infrastructure for the application and usage of modern public key infrastructure (PKI) schemes for the implementation and use of digital signatures for machine readable travel documents ("MRTDs") offering ICC read-only access.

1.2 Based on the premise that effective implementation will have to be possible in the year 2006, the specifications do not try to prescribe a full implementation of a complicated PKI structure within each country. It is intended rather to provide a way of implementation in which States are able to make choices in several areas (such as active or passive authentication, anti-skimming and access control, or automated border crossing), thus having the possibility to phase in implementation of additional features without being incompliant to the framework.

2. ASSUMPTIONS

2.1 It is assumed that the reader is familiar with the concepts and mechanisms offered by public key cryptography and public key infrastructures.

2.2 Whilst the use of public key cryptography techniques adds complications to the implementation of integrated circuit-enabled passports, such techniques add value in that they will provide front-line border control points with an additional measure to determine the authenticity of the passport document. It is assumed that their use is the sole measure for determining authenticity and it SHOULD NOT be relied upon as a single determining factor.

2.3 The digitally stored image of the face is assumed not to be privacy-sensitive information. The face of the MRTD holder is also printed in the MRTD and can be readily perceived.

2.4 The digitally stored image of the finger(s) and/or iris are additional biometric features which States MAY choose to apply for national use. They are generally considered to be privacy-sensitive and therefore need to be protected under the issuing State's national legislative framework.

2.5 It is not feasible that ICAO, or any other single, central organization assign, maintain or manage secure private keys for any State. Despite many strategic alliances among participants this will not be recognized as a trusted solution.

2.6 In the event that the data from the chip cannot be used, for instance as a result of a certificate revocation or an invalid signature verification, or if the chip was left intentionally blank (as described in 7.1.1 of this Section), the MRP is not necessarily invalidated. In such case a receiving State MAY rely on other document security features for validation purposes.

2.7 The use of Certificate Revocation Lists (CRLs) is limited to country signing CA certificates and document signer certificates. CRLs are not applicable for individual Document Security Objects and document specific Active Authentication key pairs.

3. TERMINOLOGY

3.1 The key words “SHALL”, “REQUIRED”, “SHOULD”, “RECOMMENDED”, and “MAY” in this Section are to be interpreted as described in [R4], *RFC 2119, S. Bradner, “Key Words for Use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997*.

3.2 In case OPTIONAL features are implemented, they SHALL be implemented as described in this Section.

3.1 CAs, keys and certificates

The following keys and certificates are relevant within the scope of this Section:

Name	**Abbreviation**	**Comments**
Country Signing CA	CSCA	
Country Signing CA Certificate	C_{CSCA}	Issued by CSCA (self-signed). Carries the Country Signing CA Public Key (KPu_{CSCA}). Stored in the inspection system.
Country Signing CA Private Key	KPr_{CSCA}	Signing the Document Signer Certificate (C_{DS}). Stored in an issuing State’s (highly) secured environment.
Country Signing CA Public Key	KPu_{CSCA}	For verification of the authenticity of the Document Signer Certificate (C_{DS}).
Document Signer	DS	
Document Signer Certificate	C_{DS}	Issued by Country Signing CA (CSCA). Carries the Document Signer Public Key (KPu_{DS}). Stored in the inspection system and/or in the MRTD’s chip.
Document Signer Private Key	KPr_{DS}	Signing the Document Security Object (SO_D). Stored in an issuing State’s (highly) secured environment.
Document Signer Public Key	KPu_{DS}	For verification of the authenticity of the Document Security Object (SO_D).
Document Security Object	SO_D	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hashed LDS Data Groups. Stored in the MRTD’s chip. MAY carry the Document Signer Certificate (C_{DS}).

Name	**Abbreviation**	**Comments**
Active Authentication Private Key	KPr_{AA}	OPTIONAL. Signature calculation in Active Authentication mechanism of the MRTD's chip. Stored in the chip's Secure Memory.
Active Authentication Public Key	KPu_{AA}	OPTIONAL. Signature verification in Active Authentication mechanism of the MRTD's chip.
Document Basic Access Keys	K_{ENC} and K_{MAC}	OPTIONAL. To obtain access to public MRTD data and to secure communications between MRTD's chip and inspection system.

3.2 Abbreviations

Abbreviation	
APDU	Application Protocol Data Unit
BLOB	Binary Large Object
CA	Certification Authority
CRL	Certificate Revocation List
DO	Data Object
ICAO	International Civil Aviation Organization
ICC	Integrated Circuit Card
IFD	InterFace Device
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
NTWG	New Technologies Working Group
PICC	Proximity Integrated Circuit Card
PCD	Proximity Coupling Device
PKI	Public Key Infrastructure
PKD	Public Key Directory
SM	Secure Messaging
TAG	Technical Advisory Group

4. REFERENCE DOCUMENTATION

The following documentation serves as reference to this Section:

PKI Threat Assessment, ICAO-NTWG, Sept 03 Final.3 October 2003.

Technical Report: PKI Digital Signatures for Machine Readable Travel Documents, version 4.

Technical Report: Development of a Logical Data Structure — LDS for optional capacity expansion technologies.

RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

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

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

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

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

FIPS 186-3, Federal Information Processing Standards Publication (FIPS PUB) 186-3, Digital Signature Standard.

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

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

ISO/IEC 7816-8, Identification cards — Integrated circuit cards — Part 8: Commands for security operations.

RFC 3369, Cryptographic Message Syntax, August 2002.

ICAO Doc 9303, Machine Readable Travel Documents, Fifth Edition — 2003.

ISO/IEC 3166, Codes for the representation of names of countries and their subdivisions — 1997.

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

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

5. GENERAL OUTLINE

5.1 The principles of PKI schemes have evolved in their use to become highly complex in their application to modern scenarios. Their prime use is in Internet transactions, where keys are to be trusted across a broad range of users and agencies; this has resulted in elaborate systems of key certificates, where public keys are issued in "certificates" which are digitally signed by trusted issuing organizations called certificate authorities (CAs). The trust in these CA organizations is further being verified by higher level CAs in a trust hierarchy, each one in the hierarchy issuing the key and signed certificate for the one beneath it in the hierarchy. The highest level in such a hierarchy is the so-called "Root CA". Different hierarchies cross-certify each other to establish trust in the keys issued by each with the other.

5.2 A complicating factor is the need for Certificate Revocation Lists (CRLs), indicating where a key (certificate) has lost its validity for whatever reason. In fact, by revoking a certificate and publishing this revocation in a CRL, the certificate's issuer informs receiving parties that the contents can no longer be trusted. The need to verify certificates for each and every transaction often implies multiple accesses to CA records and to CRL records in different databases. This is a complex requirement.

5.3 The operating environment of ICAO-standard MRTDs is different from the above-mentioned commercial environments, where the question of public key revocation does apply in a different way (compared to individual users), since the unlikely event of a compromise of any State's private key used during some period to sign many MRTDs cannot deny that documents were indeed signed using that key. These (valid) documents are still in use by their holders for travel purposes. The digital signatures applied are meant to last for the validity period of the MRTD and are not intended for everyday transaction purposes. In the case of key compromise, a caution mechanism SHALL be used to warn States to view those documents more closely.

5.4 As a consequence, this volume of Doc 9303 presents a customized approach that will enable the MRTD community to fast-track implementation of this application for MRTDs with ICC read-only access, and take advantage of its benefits without attempting to address larger PKI policy issues and complex hierarchies. Certificates are used for security purposes, along with a proposed methodology for public key (certificate) circulation to member States, and the infrastructure is customized for ICAO purposes.

5.5 Responsibilities

The ICAO PKI application operates in a completely peer-based user environment, with each State independent and autonomous in the matter of MRTDs and security. Nonetheless it is integral to the programme to have an efficient and commonly accepted means of sharing and updating the set of public keys in effect for all non-expired MRTDs in existence for all participating States at any time.

5.5.1 Issuing States

Each participating State SHALL install its own secure facilities to generate key sets for different periods of time; such key sets SHALL be used to compute the digital signatures to be applied for signing certificates. These systems or facilities SHALL be well protected from any outside or unauthorized access through inherent design and hardware security facilities.

Country Signing CA

The CA hierarchy, in which the key generation will be embedded, is only relevant to this Section as far as it involves the Certificates that are distributed to receiving States. The highest level certificate that is distributed SHALL act as the trust point for the receiving State. In this Section this certificate is referred to as the Country Signing CA Certificate (C_{CSCA}). The Country Signing CA Certificate (C_{CSCA}) SHALL be self-signed and issued by the Country Signing CA (CSCA).

It is RECOMMENDED that Country Signing CA Key Pairs (KPu_{CSCA}, KPr_{CSCA}) be generated and stored in a highly protected, off-line CA infrastructure by the issuing State.

Country Signing CA Certificates (C_{CSCA}) SHALL be distributed by strictly secure diplomatic means (out-of-band distribution).

Each Country Signing CA Certificate (C_{CSCA}) generated by each State SHALL also be forwarded to ICAO (for the purpose of validation of Document Signer Certificates (C_{DS})).

The Country Signing CA Private Key (KPr_{CSCA}) is used to sign Document Signer Certificates (C_{DS}).

Appendix 1 specifies the Certificate Profiles.

Document Signer

It is RECOMMENDED that Document Signer Key Pairs (KPu_{DS}, KPr_{DS}) be generated and stored in a highly protected CA infrastructure by the issuing State.

Each Document Signer Certificate (C_{DS}) generated by each State SHALL be forwarded to ICAO and MAY be stored in the MRTD's chip.

The Document Signer Private Key (KPr_{DS}) is used to sign Document Security Objects (SO_D).

Each Document Security Object (SO_D) generated by each State SHALL be stored in the corresponding MRTD's chip.

Appendix 1 specifies the Certificate Profiles.

Certificate Revocation

Issuing States can revoke certificates in case of an incident (like a key compromise). Such a revocation SHALL be communicated bilaterally to all other participating States and to the ICAO Public Key Directory within 48 hours.

In case of absence of incidents issuing States SHOULD distribute "routine" CRLs bilaterally and to the ICAO Public Key Directory at least every 90 days.

5.5.2 ICAO Public Key Directory (PKD)

In order to efficiently share the Document Signer Certificates (C_{DS}) of all States, ICAO will develop and provide a Public Key Directory (PKD) Service to all participating States. This service SHALL accept information on public keys from States, store them in a directory, and make them accessible to all other States.

Access for updating the certificate lists to be stored in the PKD SHALL be restricted to participating States.

There SHALL NOT be access control for reading the PKD (e.g. for the purpose of downloading PKD information).

Country Signing CA Certificates

Country Signing CA Certificates (C_{CSCA}) are not part of the ICAO PKD service. The PKD however SHALL use Country Signing CA Certificates (C_{CSCA}) to verify the authenticity and integrity of the Document Signer Certificates (C_{DS}) received from participating States, before publishing.

ICAO does not allow access to the Country Signing CA Certificate (C_{CSCA}).

Document Signer Certificates

The ICAO PKD is intended as the repository for all Document Signer Certificates (C_{DS}) used by all participating States at any time. This includes certificates actively being used at any time for signing purposes as well as those no longer being used but still in effect for issued MRTDs.

The ICAO PKD will be the primary distribution mechanism for all these Document Signer Certificates (C_{DS}) and therefore SHALL be populated and maintained up-to-date by all participating States.

Public Key information from a certain issuing State stored in the PKD SHALL also be available for other parties (other than participating States) that need this information for validating the authenticity of digitally stored MRTD data.

Certificate Revocation Lists

The PKD will also be a repository for all Certificate Revocation Lists (CRLs) issued by each participating State. Although States SHALL primarily distribute CRLs bilaterally, they SHALL also communicate CRLs to the PKD. Thus the ICAO PKD will be the secondary distribution mechanism for CRLs.

5.5.3 Receiving States

Users of the PKD service SHALL access the ICAO PKD service on a regular basis and download new key certificate information for storage and use by their internal border systems.

Similarly, it is a receiving State's responsibility to maintain a current CRL cache, namely a current set of CRLs, which SHALL be part of the downloaded information from the ICAO PKD.

Each receiving State SHALL take care of the internal distribution of Country Signing CA Certificates (C_{CSCA}), Document Signer Certificates (C_{DS}) and CRLs to its inspection systems.

It is a State's responsibility to store the Country Signing CA Certificates (C_{CSCA}), as trust points, in a secure way in their border inspection systems.

5.5.4 Other parties

Everyone who has the appropriate equipment is able to read the chip contents of the MRTD, but only the parties that are provided with the appropriate public key certificates and Certificate Revocation Lists will be able to verify the authenticity and integrity of the chip contents. These parties MAY obtain this information from the ICAO Public Key Directory, although they will have to obtain the set of Country Signing CA Certificates (C_{CSCA}) by other means as these are not published in the ICAO PKD.

5.6 Data Authentication

5.6.1 Passive authentication

In addition to the LDS Data Groups, the chip also contains a Document Security Object (SO_D). This object is digitally signed by the issuing State and contains hash representations of the LDS contents (see 7 of this Section.).

An inspection system, containing the Document Signer Public Key (KPu_{DS}) of each State, or having read the Document Signer Certificate (C_{DS}) from the MRTD, will be able to verify the Document Security Object (SO_D). In this way, through the contents of the Document Security Object (SO_D), the contents of the LDS is authenticated.

This verification mechanism does not require processing capabilities of the chip in the MRTD. Therefore it is called “passive authentication” of the chip contents.

Passive authentication proves that the contents of the Document Security Object (SO_D) and LDS are authentic and not changed. It does not prevent exact copying of the chip content or chip substitution.

Therefore a passive authentication system SHOULD be supported by an additional physical inspection of the MRTD.

Passive authentication is specified in 7.2.2.

5.6.2 Active Authentication

An issuing State MAY choose to protect its MRTDs against chip substitution. This can be done by implementing an Active Authentication mechanism.

If supported, the Active Authentication mechanism SHALL ensure that the chip has not been substituted, by means of a challenge-response protocol between the inspection system and the MRTD’s chip.

For this purpose the chip contains its own Active Authentication Key pair (KPr_{AA} and KPu_{AA}). A hash representation of Data Group 15 (Public Key (KPu_{AA}) info) is stored in the Document Security Object (SO_D) and therefore authenticated by the issuer’s digital signature. The corresponding Private Key (KPr_{AA}) is stored in the chip’s secure memory.

By authenticating the visual MRZ (through the hashed MRZ in the Document Security Object (SO_D)) in combination with the challenge response, using the MRTD’s Active Authentication Key Pair (KPr_{AA} and KPu_{AA}), the inspection system verifies that the Document Security Object (SO_D) has been read from the genuine chip, stored in the genuine MRTD.

Active Authentication requires processing capabilities of the MRTD’s chip.

Active Authentication is specified in 7.2.2.

5.7 Access control

Comparing a MRTD that is equipped with a contactless chip with a traditional MRTD shows two differences:

- The data stored in the chip can be electronically read without opening the document (skimming).
- The unencrypted communication between a chip and a reader can be eavesdropped within a distance of several metres.

While there are physical measures possible against skimming, these do not address eavesdropping. Therefore, it is understood that States MAY choose to implement a Basic Access Control mechanism, i.e. an access control mechanism that in effect requires the knowledge of the bearer of the MRTD that the data stored in the chip is being read in a secure way. This Basic Access Control Mechanism prevents skimming as well as eavesdropping.

This recommended Best Practice is intended to protect privacy and recognize the rights of travelers to such protection through prevention of skimming and eavesdropping.

This access control mechanism is OPTIONAL. Descriptions and specifications in this Section on Basic Access Control and Secure Messaging apply only to MRTDs and inspection systems that support this option. If supported, this mechanism SHALL ensure that the contents of the chip can only be read after the bearer has knowingly offered his MRTD.

A chip that is protected by the Basic Access Control mechanism denies access to its contents unless the inspection system can prove that it is authorized to access the chip. This proof is given in a challenge-response protocol, where the inspection system proves knowledge of the chip-individual Document Basic Access Keys (K_{ENC} and K_{MAC}) which are derived from information from the MRZ.

The inspection system SHALL be provided with this information prior to being able to read the chip. The information has to be retrieved optically/visually from the MRTD (e.g. from the MRZ). It also SHALL be possible for an inspector to enter this information manually in the inspection system in case machine-reading of the MRZ is not possible.

Additionally, after the inspection system has been authenticated successfully, it is REQUIRED that the chip enforce encryption of the communication channel between the inspection system and the MRTD's chip by Secure Messaging techniques.

Assuming that the Document Basic Access Keys (K_{ENC} and K_{MAC}) cannot be obtained from a closed document (since they are derived from the optically read MRZ), it is accepted that the passport was knowingly handed over for inspection. Due to the encryption of the channel, eavesdropping on the communication would require a considerable effort.

The access control mechanism is specified in 7.2.2.

5.8 Security for additional biometrics

The personal data stored in the chip as defined to be the mandatory minimum for global interoperability are the MRZ and the digitally stored image of the bearer's face. Both items can also be seen (read) visually after the MRTD has been opened and offered for inspection.

Besides the digitally stored image of the face as the primary biometric for global interoperability, ICAO has endorsed the use of digitally stored images of fingers and/or irises in addition to the face. For national or bilateral use, States MAY choose to store templates and/or MAY choose to limit access or encrypt this data, as to be decided by States themselves.

Access to this more sensitive personal data SHOULD be more restricted. This can be accomplished in two ways: extended access control or data encryption. Although these options are mentioned in this Section, ICAO is not proposing or specifying any standards or practices in these areas at this time.

5.8.1 Extended Access Control

The OPTIONAL Extended Access Control mechanism is similar to the Basic Access Control mechanism already described, however for Extended Access Control a document extended access key set is used instead of the Document Basic Access Keys (K_{ENC} and K_{MAC}).

Defining the (chip-individual) Document Extended Access Key set is up to the implementing State. The Document Extended Access Key set MAY consist of either symmetric keys, e.g. derived from the MRZ and a National Master key, or an asymmetric key pair with a corresponding card verifiable certificate.

Extended Access Control requires processing capabilities of the MRTD's chip.

5.8.2 Encryption

Restricting access to the additional biometrics MAY also be done by encrypting them. To be able to decrypt the encrypted data, the inspection system SHALL be provided with a decryption key. Defining the encryption/decryption algorithm and the keys to be used is up to the implementing State and is outside the scope of this document.

6. SECURING ELECTRONIC DATA IN MRTDS (SUMMARY)

Beside passive authentication by digital signatures, States MAY choose additional security, using more complex ways of securing the chip and its data. The options given in Table IV-1 can be suitably combined to achieve additional security according to existing ISO/IEC standards.

Table IV-1. Baseline Security Method

Method	**Issuer**	**Insp. System**	**Benefits**	**Deficiencies**
Passive Authentication (5.6.1)	**M**	**M**	Proves that the contents of the SO_D and the LDS are authentic and not changed.	Does not prevent an exact copy or chip substitution. Does not prevent unauthorized access. Does not prevent skimming.
ADVANCED SECURITY METHODS				
Comparison of conventional MRZ(OCR-B) and chip-based MRZ(LDS)	N/A	O	Proves that chip content and physical MRTD belong together	Adds (minor) complexity. Does not prevent an exact copy of chip and conventional document.
Active Authentication (5.6.2)	O	O	Prevents copying the SO_D and proves that it has been read from the authentic chip. Proves that the chip has not been substituted.	Adds complexity. Requires processor-chips.
Basic Access Control (5.7)	O	O	Prevents skimming and misuse. Prevents eavesdropping on the communications between MRTD and inspection system (when used to set up encrypted session channel).	Does not prevent an exact copy or chip substitution (requires also copying of the conventional document). Adds complexity. Requires processor-chips.
Extended Access Control (5.8.1)	O	O	Prevents unauthorized access to additional biometrics. Prevents skimming of additional biometrics.	Requires additional key management. Does not prevent an exact copy or chip substitution (requires also copying of the conventional document). Adds complexity. Requires processor-chips.
Data Encryption (5.8.2)	O	O	Secures additional biometrics. Does not require processor-chips.	Requires complex decryption key management. Does not prevent an exact copy or chip substitution. Adds complexity.

MRTDs issued by States choosing to use advanced security methods will be fully ICAO compliant and deemed to meet global interoperability standards.

7. SPECIFICATIONS

7.1 MRTD production and personalization

7.1.1 MRTD production and personalization are the issuing State's responsibility.

However, it is RECOMMENDED that States implement measures to secure transport and storage of chips, the embedding of the chips in MRTDs, and the personalization process.

This edition of Doc 9303, Part 1, Volume 2 is based on the assumption that MRTDs will not be written to after personalization. Therefore the personalization process SHOULD lock the chip as a final step.

In the event that a State's PKI infrastructure is not available to sign MRTD data as part of personalization, and the issuance of the document(s) cannot be delayed, it is RECOMMENDED that the MRTD's chip be left blank and be locked. The passport book SHOULD contain an appropriate printed caveat to this effect. This is expected to be an exceptional circumstance.

7.1.2 Information stored in the chip

Schematically, the contents of the MRTD's chip are as follows:

```
MF
|
|---------DF — LDS                                REQUIRED
    |
    |---------$K_{ENC}$                            OPTIONAL
    |
    |---------$K_{MAC}$                            OPTIONAL
    |
    |---------$KPr_{AA}$                           OPTIONAL
    |
    |---------EF — COM                             REQUIRED
    |
    |---------EF — $SO_D$                          REQUIRED
    |
    |---------EF — Datagroup_1 (MRZ)               REQUIRED
    |
    |---------EF — Datagroup_2 (Encoded Face)      REQUIRED
    //
    |---------EF — Datagroup_n                     OPTIONAL
```

K_{ENC} , K_{MAC}

The (OPTIONAL) Document Basic Access Keys (K_{ENC} and K_{MAC}) are stored in the DF. Derivation of these keys from the MRZ is described in 7.2.2.

KPr_{AA}

The (OPTIONAL) Active Authentication Private Key (KPr_{AA}) is stored in the DF.

EF-COM

See Section III, *LDS.*

EF-Data Group 1-n

See Section III, *LDS.*

EF-SO_D

The EF-SO_D contains the Document Security Object (SO_D). The Document Security Object (SO_D) contains the hash values of the LDS Data Groups that are being used. (This structure is called the LDS Security Object (SO_{LDS}.)) The specification of the Document Security Object (SO_D), including an ASN.1 formatted example of the LDS Security Object (SO_{LDS}) can be found in Appendix 3.

7.2 Inspection

7.2.1 Inspection system

In order to support the required functionality and the defined options that can be implemented on MRTDs that will be offered, the inspection system will have to meet certain pre-conditions.

For MRTD Basic Access Control

Although the described Basic Access Control is OPTIONAL, inspection systems supporting it SHALL meet the following pre-conditions:

1. The inspection system is equipped with an MRZ reader or a form of manual input device (e.g. a keyboard) to derive the Document Basic Access Keys (K_{ENC} and K_{MAC}) from the MRTD.

2. The inspection system's software supports the protocol described in 7.2.2, in the case that an MRTD with Basic Access Control is offered to the system, including the encryption of the communication channel with Secure Messaging.

For Passive Authentication

To be able to perform a passive authentication of the data stored in the MRTD's chip, the inspection system needs to have knowledge of key information of the issuing States:

1. Of each participating issuing State, the Country Signing CA Certificate (C_{CSCA}) SHALL be stored in the inspection system.

2. Of each participating issuing State, the Document Signer Certificate (C_{DS}) SHALL be stored in the inspection system.

For Active Authentication

Support of Active Authentication by inspection systems is OPTIONAL.

If the inspection system supports the OPTIONAL Active Authentication, it is REQUIRED that the inspection system have the ability to read the visual MRZ.

If the inspection system supports the OPTIONAL Active Authentication, the inspection system's software SHALL support the Active Authentication protocol described in 7.2.2.

For Extended Access Control to additional biometrics

The implementation of the protection of the OPTIONAL additional biometrics depends on the State's internal specifications or the bilaterally agreed specifications between States sharing this information.

For Decryption of additional biometrics

The implementation of the protection of the OPTIONAL additional biometrics depends on the State's internal specifications or the bilaterally agreed specifications between States sharing this information.

7.2.2 Inspection process flow

This paragraph describes the flow of the inspection process steps in order of occurrence. Both OPTIONAL and REQUIRED steps are described.

MRTD Basic Access Control (OPTIONAL)

When a MRTD with OPTIONAL Basic Access Control mechanism is offered to the inspection system, optically or visually read information is used to derive the Document Basic Access Keys (K_{ENC} and K_{MAC}) to gain access to the chip and to set up a secure channel for communications between the MRTD's chip and the inspection system.

An MRTD chip that supports Basic Access Control SHALL respond to unauthenticated read attempts (including *selection* of (protected) files in the LDS) with "Security status not satisfied" (0x6982). To authenticate the inspection system the following steps SHALL be performed:

1. The inspection system reads the "MRZ_information" consisting of the concatenation of Document Number, Date of Birth and Date of Expiry, including their respective check digits, as described in paragraphs 9 and 15 of Doc 9303, Part 1, Volume 1, from the MRZ using an OCR-B reader. Alternatively, the required information can be typed in; in this case it SHALL be typed in as it appears in the MRZ. The most significant 16 bytes of the SHA-1 hash of this "MRZ_information" are used as key seed to derive the Document Basic Access Keys using the key derivation mechanism described in Appendix 5.1.

2. The inspection system and the MRTD chip mutually authenticate and derive session keys. The authentication and key establishment protocol described in Appendix 5.2 SHALL be used.

3. After successful authentication, subsequent communication SHALL be protected by Secure Messaging as described in Appendix 5.3.

Passive Authentication (REQUIRED)

The inspection system performs the following steps:

1. The Document Security Object (SO_D) (OPTIONALLY containing the Document Signer Certificate (C_{DS})) is read from the chip.

2. The Document Signer (DS) is read from the Document Security Object (SO_D).

3. The digital signature of the Document Security Object (SO_D) is verified by the inspection system, using the Document Signer Public Key (KPu_{DS}). The Document Signer Certificate (C_{DS}) for this key is stored in the inspection system as downloaded from the ICAO PKD and MAY also be stored in the MRTD's chip. This ensures that the Document Security Object (SO_D) is authentic, issued by the authority mentioned in the Document Security Object (SO_D), and unchanged. Thus the contents of the Document Security Object (SO_D) can be trusted and SHOULD be used in the inspection process.

4. The inspection system reads relevant Data Groups from the LDS.

5. By hashing the contents and comparing the result with the corresponding hash value in the Document Security Object (SO_D) it ensures that the contents of the Data Group are authentic and unchanged.

The biometric information can now be used to perform the biometrics verification with the person who offers the MRTD.

Active Authentication (Optional)

When a MRTD with the OPTIONAL Data Group 15 is offered to the inspection system, the Active Authentication mechanism MAY be performed to ensure that the data are read from the genuine chip and that the chip and data page belong to each other.

The inspection system and the chip perform the following steps:

1. The entire MRZ is read visually from the MRTD's data page (if not already read as part of the Basic Access Control procedure) and compared with the MRZ value in Data Group 1. Since the authenticity and integrity of Data Group 1 have been checked through Passive Authentication, similarity ensures that the visual MRZ is authentic and unchanged.

2. Passive Authentication has also proved the authenticity and integrity of Data Group 15. This ensures that the Active Authentication Public Key (KPu_{AA}) is authentic and unchanged.

3. To ensure that the Document Security Object (SO_D) is not a copy, the inspection system uses the MRTD's Active Authentication Key pair (KPr_{AA} and KPu_{AA}) in a challenge-response protocol with the MRTD's chip as described Appendix 4, A4.2.

After a successful challenge-response protocol, it is proven that the Document Security Object (SO_D) belongs to the data page, the chip is genuine and chip and data page belong to each other.

Extended Access Control to additional biometrics (OPTIONAL)

The implementation of the protection of the OPTIONAL additional biometrics depends on the State's internal specifications or the bilaterally agreed specifications between States sharing this information.

Decryption of additional biometrics (OPTIONAL)

The implementation of the protection of the OPTIONAL additional biometrics depends on the State's internal specifications or the bilateral agreed specifications between States sharing this information.

7.2.3 Additional command set

The minimum command set SHALL at least contain the commands:

SELECT (See ISO/IEC 7816-4)
READ BINARY (See ISO/IEC 7816-4)

Implementation of the recommendations defined as OPTIONAL in this Section requires support of the following additional commands:

EXTERNAL AUTHENTICATE (See ISO/IEC 7816-4)
INTERNAL AUTHENTICATE (See ISO/IEC 7816-4)
GET CHALLENGE (See ISO/IEC 7816-4).

8. ALGORITHMS

8.1 Overview

States SHALL support the same algorithm for use in their Country Signing CA, Document Signing keys and, where applicable, Active Authentication Key Pairs, although different key sizes may be required depending on the algorithm selected.

States SHALL support all algorithms at points where they wish to validate the signature on passport documents and where they exchange key management with other States.

The recommendations on key sizes here assume the maximum recommendations for key issuing periods and a ten-year maximum document validity.

For signature generation in the Active Authentication mechanism, States SHALL use ISO/IEC 9796-2 Digital Signature scheme 1 ([R17], *ISO/IEC 9796-2, Information Technology — Security Techniques — Digital Signature Schemes giving message recovery — Part 2: Integer factorisation based mechanisms, 2002.*).

For use in their Country Signing CA, Document Signing keys and, where applicable, Document Security Objects States SHALL support one of the algorithms below.

8.2 RSA

Those States implementing the RSA algorithm for signature generation and verification of Certificates and the Document Security Object (SO_D) SHALL use RFC3447 ([R7], *RFC 3447, J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003*). RFC 3447 specifies two signature mechanisms, RSASSA-PSS and RSASSA-PKCS1_v15. It is RECOMMENDED to generate signatures according to RSASSA-PSS, but receiving States SHALL also be prepared to verify signatures according to RSASSA-PKCS1_v15.

It is RECOMMENDED that the minimum size of the modulus, n, for Country Signing CA Keys using RSA be *3 072 bits*.

It is RECOMMENDED that the minimum size of the modulus, n, for Document Signer Keys using RSA be *2 048 bits*.

It is RECOMMENDED that the minimum size of the modulus, n, for Active Authentication Keys using RSA be *1 024 bits.*

8.3 DSA

Those States implementing the DSA algorithm for signature generation or verification SHALL use FIPS 186-2 ([R9], *FIPS 186-2, Federal Information Processing Standards Publication (FIPS PUB) 186-2 (+ Change Notice), Digital Signature Standard, 27 January 2000. (Supersedes FIPS PUB 186-1 dated 15 December 1998)*).

The current specification for DSA FIPS186-2 only supports 1 024 key lengths. A new version of the standard FIPS186-3 is being trialled but no date for its availability could be ascertained at this time.

It is RECOMMENDED that the minimum size of the moduli, p and q, for Country Signing CA Keys using DSA be *3 072 and 256 bits*, respectively.

It is RECOMMENDED that the minimum size of the moduli, p and q, for Document Signer Keys using DSA be *2 048 and 224 bits*, respectively.

It is RECOMMENDED that the minimum size of the moduli, p and q, for Active Authentication Keys using DSA be *1 024 and 160 bits,* respectively.

8.4 Elliptic curve DSA

Those States implementing the ECDSA algorithm for signature generation or verification SHALL use X 9.62 ([R11], *X9.62, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", 7 January 1999*). The elliptic curve domain parameters used to generate the ECDSA key pair SHALL be described explicitly in the parameters of the public key, i.e. parameters SHALL be of type ECParameters (no named curves, no implicit parameters) and SHALL include the optional co-factor. ECPoints SHALL be in uncompressed format.

It is RECOMMENDED that the minimum size for the base point order for Country Signing CA Keys using ECDSA be *256 bits.*

It is RECOMMENDED that the minimum size for the base point order for Document Signer Keys using ECDSA be *224 bits*.

It is RECOMMENDED that the minimum size for the base point order for Active Authentication Keys using ECDSA be *160 bits.*

8.5 Hashing algorithms

SHA-1, SHA-224 (Draft), SHA-256, SHA-384 and SHA-512 are all permitted hashing algorithms. See [R8], *FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB) 180-2, Secure Hash Standard, August 2002*.

An appropriately sized hashing algorithm SHOULD be selected for the signature algorithm chosen. For example:

- SHA-1 with RSA 1024;
- SHA-224 with ECDSA 224.

9. KEY MANAGEMENT

9.1 Overview

Issuing States SHALL have at least two key types, called:

- Country Signing CA Keys
- Document Signer Keys

Issuing States MAY have additional key types:

- Active Authentication Keys

The Country Signing CA Keys and the Document Signer Keys are issued using X.509 certificates (RFC3280, see [R6], *RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002*) and the public keys contained within them are used to validate Document Signer Keys (in the case of Country Signing CA Keys) or Document Security Objects (SO_D) issued by that State (in the case of Document Signer Keys).

All certificates issued by States SHALL conform to the certificate profile in Appendix 1.

States SHALL issue a Certificate Revocation List on a periodic basis, see 9.5 on revocation.

9.2 Active Authentication Keys

The OPTIONAL Active Authentication Key Pairs (KPr_{AA} and KPu_{AA}) SHALL be generated in a secure way.

Both the Active Authentication Public Key (KPu_{AA}) and the Active Authentication Private Key (KPr_{AA}) are stored in the MRTD's chip. After that, no Key Management is applicable for these keys.

9.3 Document Signer Keys

Document Signer Certificates (C_{DS}) are used to verify the validity of Document Security Objects (SO_D). Therefore, to accept an electronic passport from another State, the receiving State SHALL already have placed into some form of trust store a copy of the originating States Document Signer Certificates (C_{DS}).

It is RECOMMENDED that the Document Signer Certificate (C_{DS}) be stored in the Document Security Object (SO_D). See Appendix 3 for details.

The Document Signer Certificate (C_{DS}) could be read from the MRTD's chip if the issuing State supports the storage of this certificate in the chip.

Document Signer Key Lifetime

The life time, i.e. the certificate validity period, of the Document Signer Key is determined by concatenating the following two periods:

- The length of time the key will be used to issue passports, with;
- The [longest] validity period of any passport issued under that key.[15]

The Document Signer Certificate (C_{DS}) SHALL be valid for this total period to enable the authenticity of passports to be verified. However the key SHOULD only be used to issue documents for a limited period; once the last document it was used to issue has expired itself, the Public Key is no longer required.

Once the last document has been produced it is RECOMMENDED that States erase the private key in an auditable and accountable manner.

Document Signer Key issuing period

When deploying their systems States may wish to take into account the number of documents that will be signed by any one individual Document Signer Key. A State which issues a large number of documents per day and only uses one Document Signer Key may wish to use a short issuing period in order to minimize business continuity costs in the event of the Document Signer Key being revoked (see 9.5). Alternatively, a State may also choose to use a large number of signing keys to reduce the overhead on any single key.

However, if a State issues only a small number of certificates, there is no necessity for the issuing period of the Document Signer Key to be as short and therefore MAY be longer.

It is therefore RECOMMENDED that the maximum period the Document Signer Key is used to sign passport documents be three months. For States that generate large numbers of MRTDs, several current document signing keys MAY be issued at any given time.

9.4 Country Signing CA Keys

Country Signing CA Certificates (C_{CSCA}) are used to verify the validity of Document Signer Keys. Therefore, to accept an electronic passport from another State, the receiving State SHALL already have placed into some form of trust store, accessible by their border control system, a copy of the originating State's Country Signing CA Certificate (C_{CSCA}).

Country Signing CA Key Lifetime

The lifetime, i.e. the certificate validity, of the Country Signing CA Key is determined by concatenating the following periods:

[15] Some States may issue passports before they become valid, for instance on a change of name upon marriage. The effect of doing this is to extend the validity period by the longest period it is possible to pre-issue the passport.

- The length of time the Country Signing CA Key will be used to issue Document Signer Certificates (C_{DS}); and,
- The Key Lifetime of Document Signer Keys, this is made up of:

  — The length of time the key will be used to issue passports;
  — The longest validity period of any passport issued under that key.

Country Signing CA Key Issuing Period

The issuing period for the Country Signing CA Key is a delicate balance between:

- In the unlikely event of a State's Country Signing CA Key being compromised, then the validity of all the passports issued using Document Signer Keys issued under the Country Signing CA Key in question are called into doubt. Consequently States MAY wish to keep the issuing period quite short;
- Keeping the issuing period very short, however, leads to having a very large number of Country Signing CA Keys present at any one time. This can lead to a complex certificate management within the border processing systems;
- If Country Signing CA Key rollover is too infrequent, it is possible that this will make it more difficult for States due to lack of knowledge or facilities.

It is therefore RECOMMENDED that a State's Country Signing CA Key be replaced every three to five years.

Country Signing Re-key

Country Signing CA Keys provide the trust points in the whole system and without these the system would collapse. Therefore States SHOULD plan the replacement of their Country Signing CA Key carefully. Once the initial signing period has elapsed, a State will always have at least two Country Signing CA Certificates (C_{CSCA}) valid at any one time.

States SHALL give 90 days' notification that their CSCA certificate is about to change and then distribute their new CSCA certificate bilaterally. To authenticate their new certificate States should also confirm their new CSCA certificate using an out-of-band method.

States MAY additionally produce link certificates to support backwards compatibility with previously issued CSCA certificates. Where States choose to issue link certificates, they do not have to issue CSCA certificates using an out-of-band method.

States should refrain from using their CSCA certificate for the first two days after issuance.

9.5 Revocation

All national authorities that issue Document Signer Certificates (C_{DS}) SHALL produce periodic revocation information in the form of Certificate Revocation Lists (CRL). Issued CRLs SHALL conform to the profile as defined in Appendix 2.

States SHALL produce at least one CRL every 90 days. States MAY choose to produce a CRL more frequently than every 90 days but not more frequently than every 48 hours.

Revocation notification

When a State wishes to revoke a Document Signer Key, it does not need to wait until the next update period in the current CRL is due to issue a new CRL. It is RECOMMENDED that a new CRL be issued within a 48-hour period of revocation notification.

Country Signing CA Key Revocation

Revocation of a Country Signing CA Key is both extreme and difficult. Upon informing a relying State that a Country Signing CA Key has been revoked, all other keys issued using that key are effectively revoked.

Where a State has used an old Country Signing CA Key to authenticate a new Country Signing CA Key (see “Country Signing re-key” in 9.4) revoking the old Country Signing CA Key SHALL also revoke the new Country Signing CA Key.

To issue new documents the issuing State basically SHALL revert to bootstrapping its authentication process all over again by establishing bilaterally the new Country Signing CA Certificates (C_{CSCA}) it issued by using the out-of-band method.

10. CERTIFICATE AND CRL DISTRIBUTION

States need to plan their certificate rollover strategies for both Country Signing CA Keys and Document Signer Keys in order to enable propagation of certificates and CRLs into receiving States’ border control systems in a timely manner. Ideally propagation will occur within 48 hours, but some receiving States may have remote and poorly connected border outposts to which it may take more time for certificates and CRLs to propagate out. Receiving States SHOULD make every effort to distribute these certificates and CRLs to all border stations within 48 hours.

Country Signing CA Certificate distribution

Issuing States should expect that Country Signing CA Certificates (C_{CSCA}) will be propagated by receiving States within 48 hours.

Document Signer Certificate distribution

Issuing States should expect that Document Signer Certificates (C_{DS}) will be propagated within 48 hours.

Issuing States can ensure the timely propagation of Document Signer Certificates (C_{DS}) by including the Document Signer Certificate (C_{DS}) within the Document Security Object (SO_D).

CRL distribution

States SHOULD make every attempt whether electronically or by other means to act upon those CRLs issued under exceptional circumstances.

For CRL distribution, see also 5.5.2.

10.1 Distribution through ICAO PKD

For Document Signer Certificates (C_{DS}) the primary distribution channel will be the ICAO Public Key Directory. For CRLs, the PKD is the secondary channel. Country Signing CA Certificates (C_{CSCA}) are not published and not accessible in the PKD, but are used by the PKD to verify Document Signer Certificates (C_{DS}) that are offered to it for publication.

Communications

All communications with the ICAO Public Key Directory SHALL be based on server side authenticated SSL. For this purpose ICAO SHALL obtain a single server key (per site) from a commercial party.

Directory update

Public Keys SHALL be sent to the PKD as X.509-format certificates, signed by the issuing State using that State's Country Signing CA Key. These Certificates SHALL meet the requirements in Appendix 1.

Updates SHALL be performed using the LDAP protocol, where the directory is altered by changes forwarded. Since it is essential that ICAO exercise some due diligence over the process, the PKD SHALL consist of a "Write Directory", where proposed certificate and CRL updates are sent, and a "Read Directory" which is used to contain new certificates after the due diligence process and which is accessed by the MRTD community to download this information.

The certificates and CRLs are by nature signed by the issuing State. This signature SHALL be verified by ICAO before the Certificate or CRL is published in the "Read Directory".

Directory download

The PKD will be set up as a X.500 directory. The estimated size of the PKD will be 15 – 20 MB.

Because the PKD is relatively small it is RECOMMENDED that States download the entire PKD on a daily basis.

Read access to the PKD SHALL NOT be limited to participating States. The PKD will be a totally open and Internet-enabled resource, also available for read-only access to its services (for download) to airlines and the like.

10.2 Distribution by bilateral means

For CRLs and Country Signing CA Certificates (C_{CSCA}), the primary distribution channel will be bilateral exchange between participating and user States.

States generally have bilateral agreements and ways of exchanging information bilaterally (e.g. e-mail or LDAP service). States SHOULD use these existing channels for the exchange of Certificates and CRLs.

States that currently do not have bilateral agreements or ways of exchanging information bilaterally SHOULD establish such agreements and communication channels with other participating States.

NORMATIVE APPENDIX 1

CERTIFICATE PROFILE

Those States conforming to the specification SHALL issue certificates that conform to this profile. All security objects SHALL be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

The following profile uses the following terminology for each of the fields in the X.509 certificate:

m mandatory — the field SHALL be present
x do not use — the field SHOULD NOT be populated
o optional — the field MAY be present
c critical — the extension is marked critical, receiving applications SHALL be able to process this extension.

A.1.1 Certificate Body

Certificate Component	**Section in RFC 3280**	**Country Signing CA Certificate**	**Document Signer Certificate**	**Comments**
Certificate	4.1.1	m	m	
TBSCertificate	4.1.1.1	m	m	See next part of the table
SignatureAlgorithm	4.1.1.2	m	m	Value inserted here dependent on algorithm selected
SignatureValue	4.1.1.3	m	m	Value inserted here dependent on algorithm selected
TBSCertificate	4.1.2			
version	4.1.2.1	m	m	SHALL be v3
serialNumber	4.1.2.2	m	m	
signature	4.1.2.3	m	m	Value inserted here SHALL match the OID in signatureAlgorithm
issuer	4.1.2.4	m	m	See A1.5
validity	4.1.2.5	m	m	Implementations SHALL specify using UTC time until 2049 from then on using GeneralisedTime
subject	4.1.2.6	m	m	See A1.5
subjectPublicKeyInfo	4.1.2.7	m	m	
issuerUniqueID	4.1.2.8	x	x	
subjectUniqueID	4.1.2.8	x	x	
extensions	4.1.2.9	m	m	See next table on which extensions SHOULD be present

A1.2 Extensions

Extension name	Paragraph in RFC 3280	Country Signing CA Certificate	Document Signer Certificate	Comments
AuthorityKeyIdentifier	4.2.1.1	o	m	Mandatory in all certificates except for self-signed Country Signing CA Certificates
SubjectKeyIdentifier	4.2.1.2	m	o	
KeyUsage	4.2.1.3	mc	mc	This extension SHALL be marked CRITICAL
PrivateKeyUsagePeriod	4.2.1.4	o	o	This would be the issuing period of the private key
CertificatePolicies	4.2.1.5	o	o	
PolicyMappings	4.2.1.6	x	x	
SubjectAltName	4.2.1.7	x	x	
IssuerAltName	4.2.1.8	x	x	
SubjectDirectoryAttributes	4.2.1.9	x	x	
BasicConstraints	4.2.1.10	mc	x	This extension SHALL be marked CRITICAL
NameConstraints	4.2.1.11	x	x	
PolicyConstraints	4.2.1.12	x	x	
ExtKeyUsage	4.2.1.13	x	x	
CRLDistributionPoints	4.2.1.14	o	o	If States choose to use this extension they SHALL include the ICAO PKD as a distribution point. Implementations may also include relative CRL DPs for local purposes; these may be ignored by other States.
InhibitAnyPolicy	4.2.1.15	x	x	
FreshestCRL	4.2.1.16	x	x	
privateInternetExtensions	4.2.2	x	x	
other private extensions	N/A	o	o	If any private extension is included for national purposes then they SHALL NOT be marked. States are discouraged from including any private extensions.
AuthorityKeyIdentifier	**4.2.1.1**			
keyIdentifier		m	m	If this extension is used this field SHALL be supported as a minimum
authorityCertIssuer		o	o	See A1.5
authorityCertSerialNumber		o	o	
SubjectKeyIdentifier	**4.2.1.2**			
subjectKeyIdentifier		m	m	
KeyUsage	**4.2.1.3**			
digitalSignature		x	m	
nonRepudiation		x	x	
keyEncipherment		x	x	
dataEncipherment		x	x	
keyAgreement		x	x	
keyCertSign		m	x	
cRLSign		m	x	
encipherOnly		x	x	

Extension name	Paragraph in RFC 3280	Country Signing CA Certificate	Document Signer Certificate	Comments
decipherOnly		x	x	
BasicConstraints	**4.2.1.10**			
cA		m	x	TRUE for CA Certificates
PathLenConstraint		m	x	0 for New Country Signing CA Certificate, 1 for Linked Country Signing CA Certificate
CRLDistributionPoints	**4.2.1.14**			
distributionPoint		m	x	
reasons		m	x	
cRLIssuer		m	x	
CertificatePolicies	**4.2.1.5**			
PolicyInformation				
policyIdentifier		m	m	
policyQualifiers		o	o	

A1.3 SignatureAlgorithm

The Object Identifiers specified in section 2.2 of [R5], *RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002* and section A.2 of [R7], *RFC 3447, J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003*, SHALL be used for those algorithms identified in 8 of Section IV.

A1.4 SignatureValue

The signature structures stored in the SignatureValue field SHALL be as specified in section 2.2 of [R5], *RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002*, for those algorithms identified in 8 of Section IV.

A1.4 SubjectPublicKeyInfo

The subjectPublicKeyInfo fields for the algorithms specified in 8 of Section IV SHALL be populated in line with section 2.3 of [R5], *RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002*.

A1.5 Certificate and Naming conventions

The following naming and addressing conventions for Issuer and Subject fields are RECOMMENDED, in both CSCA and DS Certificates, and the Issuer field in Certificate Revocation Lists.

The following Attributes SHOULD be used:

- country (country codes SHALL follow the format of two letter country codes, specified in [R16], *ISO/IEC 3166, Codes for the representation of names of countries and their subdivisions — 1997.*).
- organization;
- organizational-unit;
- common name.

Additionally some countries MAY use:

- serial number.

States wishing to use existing PKI infrastructures to support their passport issuing systems may be bound by existing naming conventions.

NORMATIVE APPENDIX 2

CRL PROFILE

The following profile uses the following terminology for each of the fields in the X.509 Certificate Revocation List:

m mandatory — the field SHALL be present
x do not use — the field SHOULD NOT be populated
o optional — the field MAY be present
c critical — the extension is marked critical, receiving applications SHALL be able to process this extension.

Certificate List Component	**Section in RFC 3280**	**Country Signing CA CRL**	Comments
CertificateList	5.1.1	m	
tBSCertList	5.1.1.1	m	See next part of the table
signatureAlgorithm	5.1.1.2	m	Value inserted here dependent on algorithm selected
signatureValue	5.1.1.3	m	Value inserted here dependent on algorithm selected
tBSCertList	5.1.2		
version	5.1.2.1	m	SHALL be v2
signature	5.1.2.2	m	Value inserted here dependent on algorithm selected
issuer	5.1.2.3	m	UTF8 Encoding REQUIRED
thisUpdate	5.1.2.4	m	Implementations SHALL specify using UTC time until 2049 from then on using GeneralisedTime
nextUpdate	5.1.2.5	m	Implementations SHALL specify using UTC time until 2049 from then on using GeneralisedTime
revokedCertificates	5.1.2.6	m	
crlExtensions	5.1.2.7	m	

Extension Name	**Section in RFC 3280**	**Country Signing CA CRL**	**Comments**
authorityKeyIdentifier	5.2.1	m	This SHALL be the same value as the subjectKeyIdentifier field in the CRL Issuer's certificate.
issuerAltName	5.2.2	x	
cRLNumber	5.2.3	m	
deltaCRLIndicator	5.2.4	x	
issuingDistributionPoint	5.2.5	x	
freshestCRL	5.2.6	x	
CRL Entry Extensions			
reasonCode	5.3.1	x	

Extension Name	Section in RFC 3280	Country Signing CA CRL	Comments
holdInstructionCode	5.3.2	x	
invalidityDate	5.3.3	x	
certificateIssuer	5.3.4	x	

Note.— It is possible that the CRL contains other revocation information, for example concerning system operator or registration authority certificates.

NORMATIVE APPENDIX 3

DOCUMENT SECURITY OBJECT

The Document Security Object is implemented as a SignedData Type, as specified in [R14] *RFC 3369, Cryptographic Message Syntax, August 2002.* All security objects SHALL be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

A3.1 Signed Data Type

The processing rules in RFC3369 apply.

m mandatory — the field SHALL be present
x do not use — the field SHOULD NOT be populated
o optional — the field MAY be present
c choice — the field contents is a choice from alternatives

Value		Comments
SignedData		
version	m	Value = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-ldsSecurityObject
eContent	m	The encoded contents of an ldsSecurityObject.
certificates	o	States may choose to include the Document Signer Certificate (C_{DS}) which can be used to verify the signature in the signerInfos field.
Crls	x	It is recommended that States do not use this field.
signerInfos	m	It is recommended that States only provide 1 signerinfo within this field.
SignerInfo	m	
version	m	The value of this field is dictated by the sid field. See RFC3369 Section 5.3 for rules regarding this field.
Sid	m	
issuerandSerialNumber	c	It is recommended that States support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	Producing States may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by receiving States except to verify the signature value.
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the

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

A3.2 ASN.1 Profile LDS Security Object

```
LDSSecurityObject {iso(1) identified-organization(3) icao(ccc) mrtd(1) security(1)
ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

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

-- Constants

ub-DataGroups INTEGER ::= 16

-- Object Identifiers
id-icao                    OBJECT IDENTIFIER ::= {2.23.136}
id-icao-mrtd               OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security      OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 1}

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {V0(0)}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier


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

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

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

Note.—

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

NORMATIVE APPENDIX 4

ACTIVE AUTHENTICATION PUBLIC KEY INFO

A4.1 Active Authentication Public Key Info

The OPTIONAL Active Authentication Public Key is stored in the LDS Data Group 15. The format of the structure (SubjectPublicKeyInfo) is specified in [R6], *RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002*. All security objects SHALL be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

ActiveAuthenticationPublicKeyInfo ::= SubjectPublicKeyInfo

```
SubjectPublicKeyInfo ::= SEQUENCE {
        algorithm           AlgorithmIdentifier,
        subjectPublicKey    BIT STRING }

AlgorithmIdentifier ::= SEQUENCE {
        algorithm           OBJECT IDENTIFIER,
        parameters          ANY DEFINED BY algorithm OPTIONAL }
```

A4.2 Active Authentication Mechanism

Active Authentication is performed using the ISO/IEC 7816 INTERAL AUTHENTICATE command. The input is a nonce (RND.IFD) that SHALL be 8 bytes. The ICC computes a signature, when an integer factorization based mechanism is used, according to ISO/IEC 9796-2 Digital Signature scheme 1 ([R17], *ISO/IEC 9796-2, Information Technology — Security Techniques — Digital Signature Schemes giving message recovery — Part 2: Integer factorisation based mechanisms, 2002.*).

M SHALL consist of M1 and M2, where M1 SHALL be a nonce of length c — 4 bits and M2 is RND.IFD. The trailer option 1 SHALL be used in case of SHA-1, if not SHA-1 then option 2 SHALL be used.

The result of the signature computation SHALL be signature σ without the non-recoverable message part M2.

In more detail, IFD (inspection system) and ICC (MRTD's chip) perform the following steps:

1) The IFD generates a nonce RND.IFD and sends it to the ICC using the INTERNAL AUTHENTICATE command.

2) The ICC performs the following operations:
   a) Create the header
   b) Generate M1
   c) Calculate h(M)
   d) Create the trailer
   e) Calculate the message representative F
   f) Compute the signature σ and send the response to the IFD.

3) The IFD verifies the response on the send INTERNAL AUTHENTICATE command and checks if the ICC returned the correct value.

NORMATIVE APPENDIX 5

BASIC ACCESS CONTROL AND SECURE MESSAGING

A5.1 Key Derivation Mechanism

The computation of two key 3DES keys from a key seed (K_{seed}) is used in both the establishment of the Document Basic Access Keys (K_{ENC} and K_{MAC}) and the establishment of the Session keys for Secure Messaging.

A 32 bit counter c is used to allow for deriving multiple keys from a single seed. Depending on whether a key is used for encryption or MAC computation the following values SHALL be used:

- c = 1 (i.e. '0x 00 00 00 01') for encryption.
- c = 2 (i.e. '0x 00 00 00 02') for MAC computation.

The following steps are performed to derive two key 3DES keys from the seed K_{seed} and c:

1. Let D be the concatenation of K_{seed} and c ($D = K_{seed} || c$).
2. Calculate H = SHA-1(D) the SHA-1 hash of D.
3. Bytes 1..8 of H form key K_a and bytes 9..16 of H form key K_b.
4. Adjust the parity bits of keys K_a and K_b to form correct DES keys.

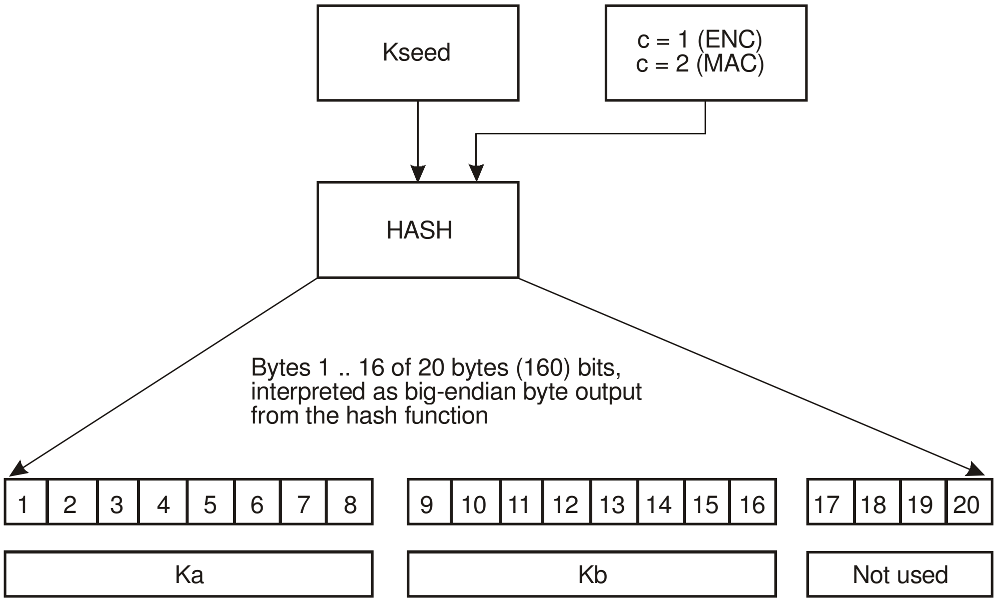

Kseed
c = 1 (ENC)
c = 2 (MAC)
HASH
Bytes 1 .. 16 of 20 bytes (160) bits, interpreted as big-endian byte output from the hash function
1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
17 18 19 20
Ka
Kb
Not used

Figure IV-5-1. Compute keys from key seed scheme

A5.2 Authentication and Key Establishment

Authentication and Key Establishment is provided by a three pass challenge-response protocol according to ISO/IEC 11770-2 Key Establishment Mechanism 6 using 3DES as block cipher. A cryptographic checksum according to ISO/IEC 9797-1 MAC Algorithm 3 is calculated over and appended to the ciphertexts. The modes of operation described in Appendix 5.4 SHALL be used. Exchanged nonces SHALL be of size 8 bytes, exchanged keying material SHALL be of size 16 bytes. Distinguishing identifiers SHALL NOT be used.

In more detail, IFD and ICC perform the following steps:

1) The IFD requests a challenge RND.ICC by sending the GET CHALLENGE command. The ICC generates and responds with a nonce RND.ICC.

2) The IFD performs the following operations:
   a) Generate a nonce RND.IFD and keying material K.IFD.
   b) Generate the concatenation S = RND.IFD || RND.ICC || K.IFD.
   c) Compute the cryptogram E_IFD = E[K_ENC](S).
   d) Compute the checksum M_IFD = MAC[K_MAC](E_IFD).
   e) Send a MUTUAL AUTHENTICATE command using the data E_IFD || M_IFD.

3) The ICC performs the following operations:
   a) Check the checksum M_IFD of the cryptogram E_IFD.
   b) Decrypt the cryptogram E_IFD.
   c) Extract RND.ICC from S and check if IFD returned the correct value.
   d) Generate keying material K.ICC.
   e) Generate the concatenation R = RND.ICC || RND.IFD || K.ICC
   f) Compute the cryptogram E_ICC = E[K_ENC](R).
   g) Compute the checksum M_ICC = MAC[K_MAC](E_ICC).
   h) Send the response using the data E_ICC || M_ICC.

4) The IFD performs the following operations:
   a) Check the checksum M_ICC of the cryptogram E_ICC.
   b) Decrypt the cryptogram E_ICC.
   c) Extract RND.IFD from R and check if ICC returned the correct value.

A5.3 Secure Messaging

After a successful execution of the authentication protocol both the IFD and the ICC compute session keys KS_ENC and KS_MAC using the key derivation mechanism described in Appendix 5.1 with (K.ICC xor K.IFD) as key seed. All further communication SHALL be protected by secure messaging in MAC_ENC mode.

A5.3.1 *Message Structure of SM APDUs*

The SM Data Objects SHALL be used according to Table IV-1 in the following order:

- Command APDU: [DO‘87’] [DO‘97’] DO‘8E’.
- Response APDU: [DO‘87’] DO‘99’ DO‘8E’.

All SM Data Objects SHALL be encoded in BER TLV as specified in ISO/IEC 7816-4. The command header SHALL be included in the MAC calculation, therefore the class byte CLA = 0x0c SHALL be used.

The actual value of Lc will be modified to Lc’ after application of secure messaging. If required, an appropriate data object may optionally be included into the APDU data part in order to convey the original value of Lc. In the protected command APDU the *new Le* byte SHALL be set to ‘00’.

Table IV-1. Usage of SM Data Objects

	DO‘87’	**DO‘97’**	**DO‘99’**	**DO‘8E’**
Meaning	Padding-content indicator byte (‘01’ for ISO-Padding) followed by the cryptogram	Le (to be protected by CC)	Processing status (SW1-SW2, protected by MAC)	Cryptographic checksum (MAC)
Command APDU	Mandatory if data is sent, otherwise absent.	Mandatory if data is requested, otherwise absent.	Not used	Mandatory
Response APDU	Mandatory if data is returned, otherwise absent.	Not used	Mandatory, only absent if SM error occurs.	Mandatory if DO‘87’ and/or DO‘99’ is present.

Figure IV-5-2 shows the transformation of an unprotected command APDU to a protected command APDU in the case *Data* and *Le* are available. If no *Data* is available, leave building DO ‘87’ out. If *Le* is not available, leave building DO ‘97’ out.

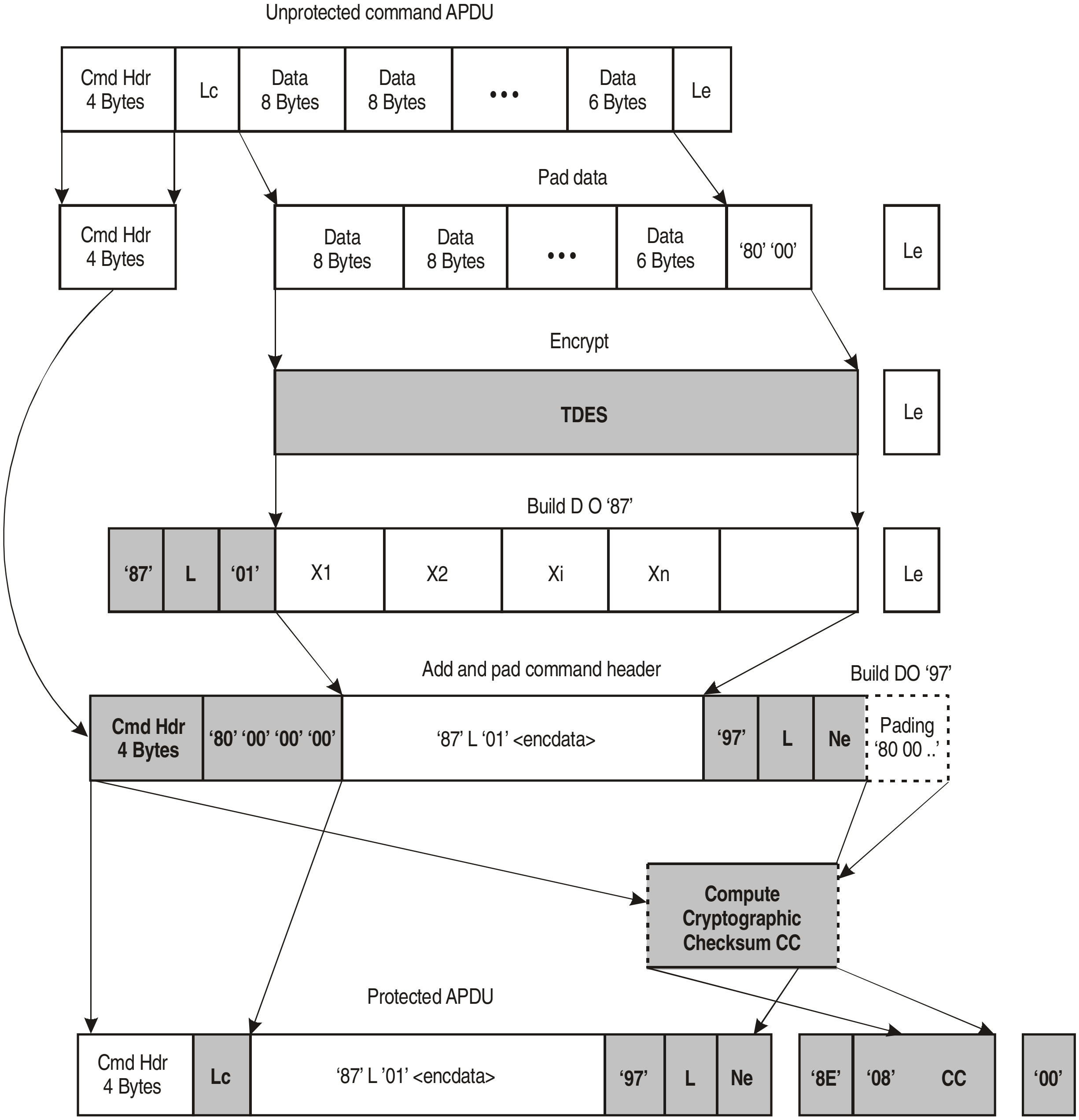


Figure IV-5-2. Computation of a SM command APDU

Figure IV-5-3 shows the transformation of an unprotected response APDU to a protected response APDU in case *Data* is available. If no *Data* is available, leave building DO ‘87’ out.

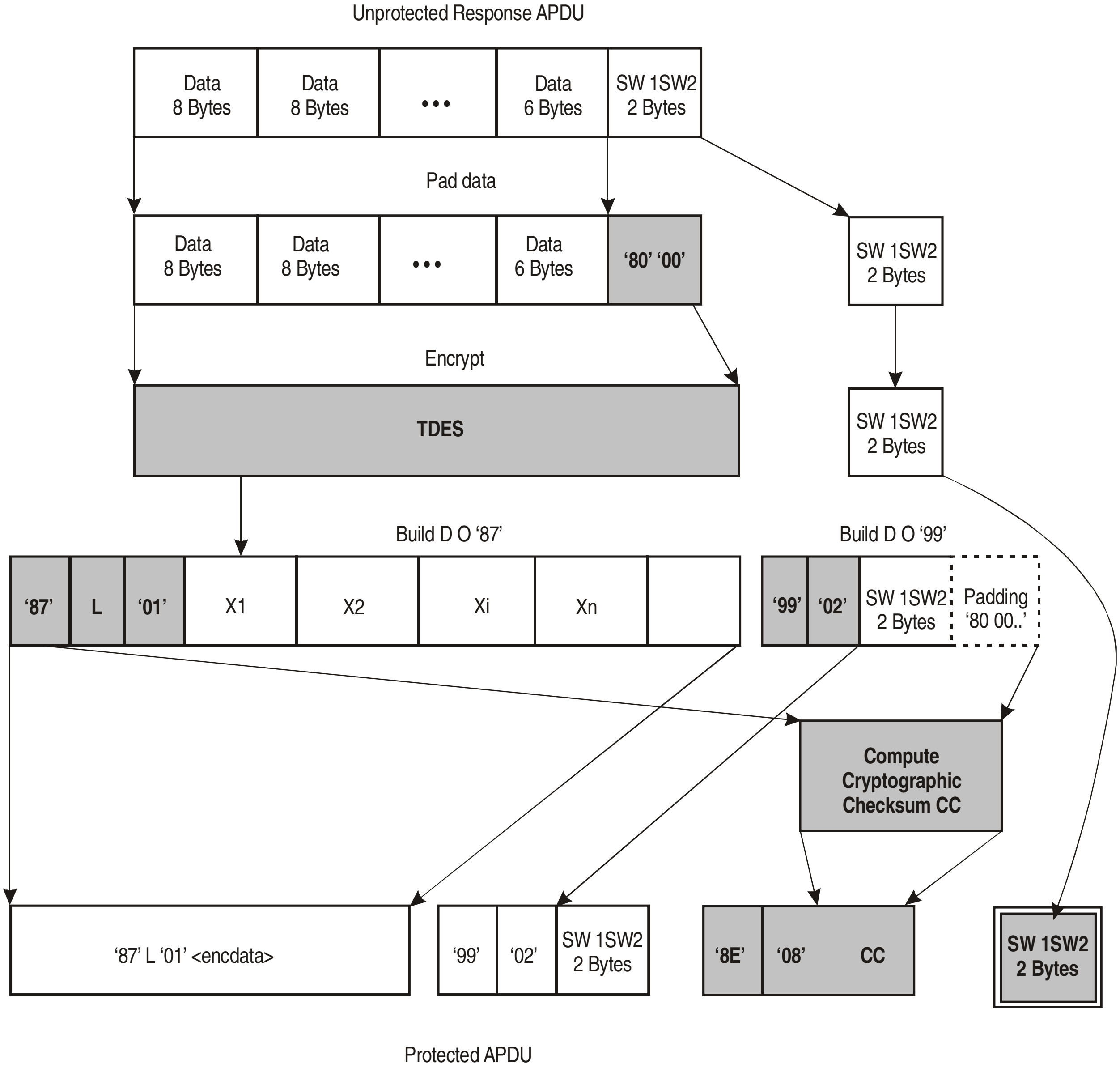


Figure IV-5-3. Computation of a SM response APDU

A5.3.2 *SM errors*

When the ICC recognizes an SM error while interpreting a command, then the status bytes must be returned without SM. In ISO/IEC 7816-4 the following status bytes are defined to indicate SM errors:

- ‘6987’: Expected SM data objects missing
- ‘6988’: SM data objects incorrect

Note.—Further SM status bytes can occur in application specific contexts. When the ICC returns status bytes without SM DOs or with an erroneous SM DO the secure session is aborted. The session will not be aborted on correct error handling.

A5.4 3DES modes of operation

A5.4.1 *Encryption*

Two key 3DES in CBC mode with zero IV (i.e. 0x00 00 00 00 00 00 00 00) according to ISO 11568-2 is used (see Figure IV-5-4). No padding for the input data is used when performing the MUTUAL AUTHENTICATE command. During the computation of SM APDUs, padding according to ISO/IEC 9797-1 padding method 2 is used.

A5.4.2 *Message authentication*

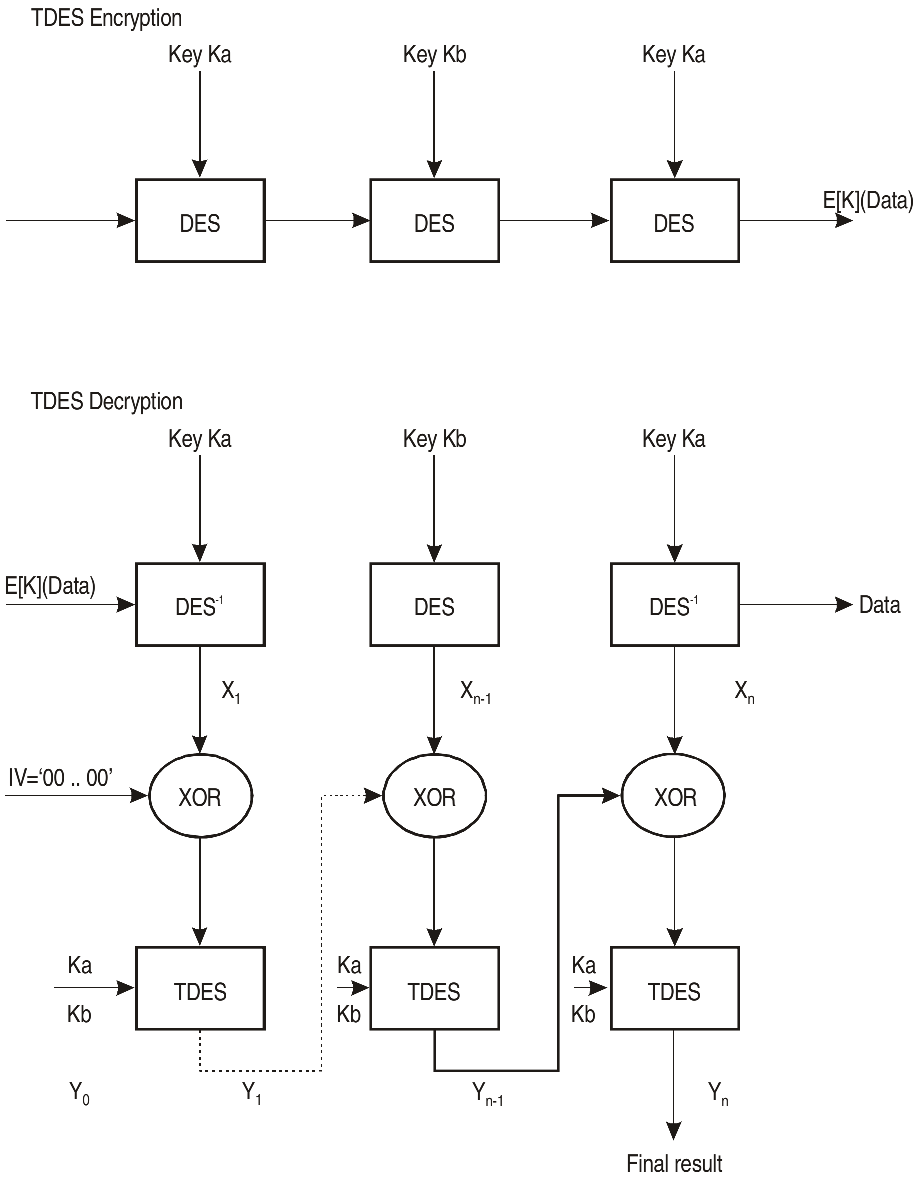
Cryptographic checksums are calculated using ISO/IEC 9797-1 MAC algorithm 3 with block cipher DES, zero IV (8 bytes), and ISO/IEC 9797-1 padding method 2. The MAC length SHALL be 8 bytes (see Figure IV-5-5).

After a successful authentication the datagram to be MACed SHALL be prepended by the Send Sequence Counter. The Send Sequence Counter is computed by concatenating the four least significant bytes of RND.ICC and RND.IFD, respectively:

SSC = RND.ICC (4 least significant bytes) || RND.IFD (4 least significant bytes).

The Send Sequence Counter is increased every time before a MAC is calculated, i.e. if the starting value is x, in the next command the value of SSC is x+1. The value of the first response is then x+2.

For MUTUAL AUTHENTICATE the initial check block Y_0 SHALL be set to zero ‘0000000000000000’.



IV = zero initialization / vector

‘X_1II ... II$^{X}_{n}$’ = plain text (message to encrypt) where each block X_1 is 64-bit long

‘Y_1II ... II$^{Y}_{n}$’ = resulting cryptogram (encrypted message) where each block Y_1 is 64-bit long

Figure IV-5-4. DES Encryption/Decryption in CBC Mode

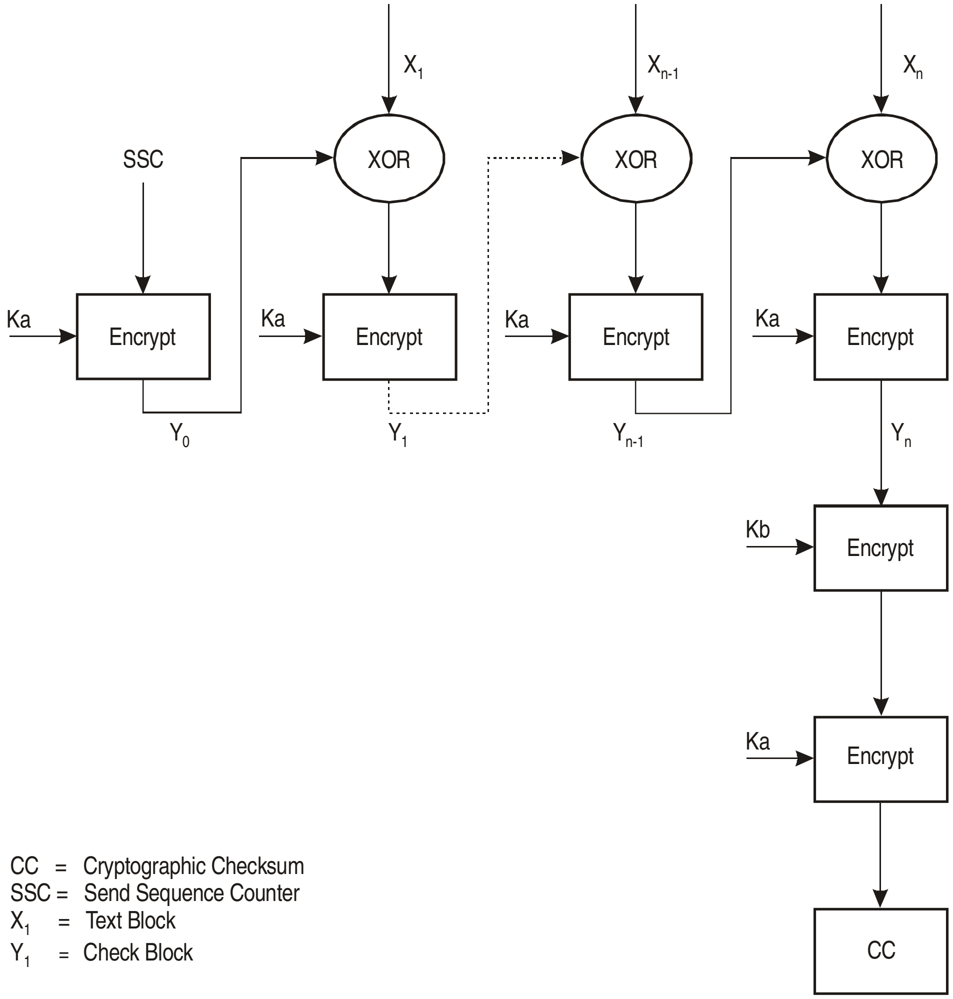


Figure IV-5-5. Retail MAC calculation

INFORMATIVE APPENDIX 6

WORKED EXAMPLES

A6.1 Command sequences

A6.1.1 *MRZ-based Basic Access Control and Secure Messaging*

Compute keys from key seed (K_{seed})

Input:

K_{seed} = ‘239AB9CB282DAF66231DC5A4DF6BFBAE’

Compute encryption key (c = ‘00000001’):

1. Concatenate K_{seed} and c:
   D = ‘239AB9CB282DAF66231DC5A4DF6BFBAE00000001’

2. Calculate the SHA-1 hash of D:
   H_{SHA-1}(D) = ‘AB94FCEDF2664EDFB9B291F85D7F77F27F2F4A9D’

3. Form keys K_a and K_b:
   K_a = ‘AB94FCEDF2664EDF’
   K_b = ‘B9B291F85D7F77F2’

4. Adjust parity bits:
   K_a = ‘AB94FDECF2674FDF’
   K_b = ‘B9B391F85D7F76F2’

Compute MAC computation key (c = ‘00000002’):

1. Concatenate K_{seed} and c:
   D = ‘239AB9CB282DAF66231DC5A4DF6BFBAE00000002’

2. Calculate the SHA-1 hash of D:
   H_{SHA-1}(D) = ‘7862D9ECE03C1BCD4D77089DCF131442814EA70A’

3. Form keys K_a and K_b:
   K_a = ‘7862D9ECE03C1BCD’
   K_b = ‘4D77089DCF131442’

4. Adjust parity bits:
   K_a = ‘7962D9ECE03D1ACD’
   K_b = ‘4C76089DCE131543’

Derivation of document basic access keys (K_{ENC} and K_{MAC})

1. Read the MRZ:

   MRZ = P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
   L898902C<3UTO6908061F9406236ZE184226B<<<<<14

2. Construct the ‘MRZ_information’ out of the MRZ:

   Document number = L898902C<, check digit = 3
   Date of birth = 690806, check digit = 1
   Date of expiry = 940623, check digit = 6
   MRZ_information = L898902C<369080619406236

3. Calculate the SHA-1 hash of ‘MRZ_information’:

   H_{SHA-1}(MRZ_information) = ‘239AB9CB282DAF66231D
   C5A4DF6BFBAEDF477565’

4. Take the most significant 16 bytes to form the K_{seed}:

   K_{seed} = ‘239AB9CB282DAF66231DC5A4DF6BFBAE’

5. Calculate the basic access keys (K_{ENC} and K_{MAC}) using Appendix 5.1:

   K_{ENC} = ‘AB94FDECF2674FDFB9B391F85D7F76F2’
   K_{MAC} = ‘7962D9ECE03D1ACD4C76089DCE131543’

Authentication and establishment of session keys

Inspection system:

1. Request an 8 byte random number from the MRTD’s chip:

   Command APDU:

CLA	INS	P1	P2	LE
00h	84h	00h	00h	08h

   Response APDU:

Response data field	SW1SW2
RND.ICC	9000h

   RND.ICC = ‘4608F91988702212’

2. Generate an 8 byte random and a 16 byte random:

   RND.IFD = ‘781723860C06C226’
   K_{IFD}= ‘0B795240CB7049B01C19B33E32804F0B’

3. Concatenate RND.IFD, RND.ICC and K_{IFD}:

   S = ‘781723860C06C2264608F91988702212
   0B795240CB7049B01C19B33E32804F0B’

4. Encrypt S with TDES key K_{ENC} as calculated in Appendix 5.2:

   E_{IFD} = ‘72C29C2371CC9BDB65B779B8E8D37B29
   ECC154AA56A8799FAE2F498F76ED92F2’

5. Compute MAC over E_{IFD} with TDES key K_{MAC} as calculated in Appendix 5.2:

   M_{IFD} = ‘5F1448EEA8AD90A7’

6. Construct command data for MUTUAL AUTHENTICATE and send command APDU to the MRTD’s chip:

   cmd_data = ‘72C29C2371CC9BDB65B779B8E8D37B29ECC154AA
   56A8799FAE2F498F76ED92F25F1448EEA8AD90A7’

   Command APDU:

CLA	INS	P1	P2	LC	Command data field	LE
00h	82h	00h	00h	28h	cmd_data	28h

MRTD’s chip:

7. Decrypt and verify received data and compare RND.ICC with response on GET CHALLENGE.

8. Generate a 16 byte random:

   K_{ICC} = ‘0B4F80323EB3191CB04970CB4052790B’

9. Calculate XOR of K_{IFD} and K_{ICC}:

   K_{seed} = ‘0036D272F5C350ACAC50C3F572D23600’

10. Calculate session keys (KS_{ENC} and KS_{MAC}) using Appendix 5.1:

    KS_{ENC} = ‘979EC13B1CBFE9DCD01AB0FED307EAE5’
    KS_{MAC} = ‘F1CB1F1FB5ADF208806B89DC579DC1F8’

11. Calculate send sequence counter:

    SSC = ‘887022120C06C226’

12. Concatenate RND.ICC, RND.IFD and K_{ICC}:

    R = ‘4608F91988702212781723860C06C226
    0B4F80323EB3191CB04970CB4052790B’

13. Encrypt R with TDES key K_{ENC} as calculated in Appendix 5.2:

    E_{ICC} = ‘46B9342A41396CD7386BF5803104D7CE
    DC122B9132139BAF2EEDC94EE178534F’

14. Compute MAC over E_{ICC} with TDES key K_{MAC} as calculated in Appendix 5.2:

    M_{ICC} = ‘2F2D235D074D7449’

15. Construct response data for MUTUAL AUTHENTICATE and send response APDU to the inspection system:

    resp_data = ‘46B9342A41396CD7386BF5803104D7CEDC122B91
    32139BAF2EEDC94EE178534F2F2D235D074D7449’

    Response APDU:

Response data field	SW1SW2
resp_data	9000h

Inspection system:

16. Decrypt and verify received data and compare received RND.IFD with generated RND.IFD.

17. Calculate XOR of K_{IFD} and K_{ICC}:

    K_{seed} = ‘0036D272F5C350ACAC50C3F572D23600’

18. Calculate session keys (KS_{ENC} and KS_{MAC}) using Appendix 5.1:

    KS_{ENC} = ‘979EC13B1CBFE9DCD01AB0FED307EAE5’
    KS_{MAC} = ‘F1CB1F1FB5ADF208806B89DC579DC1F8’

19. Calculate send sequence counter:

    SSC = ‘887022120C06C226’

Secure Messaging

After authentication and establishment of the session keys, the inspection system selects the EF.COM (File ID = ‘011E’) and reads the data using secure messaging. The calculated KS_{ENC}, KS_{MAC} and SSC (previous steps 18 and 19) will be used.

First the EF.COM will be selected, then the first four bytes of this file will be read so that the length of the structure in the file can be determined and after that the remaining bytes are read.

1. Select EF.COM

   Unprotected command APDU:

CLA	INS	P1	P2	LC	Command data field
00h	A4h	02h	0Ch	02h	01h 1Eh

a. Mask class byte and pad command header:
CmdHeader = ‘0CA4020C80000000’
b. Pad data:
Data = ‘011E800000000000’
c. Encrypt data with KS_{ENC}:
    EncryptedData = ‘6375432908C044F6’
d. Build DO‘87’:
    DO87 = ‘8709016375432908C044F6’
e. Concatenate CmdHeader and DO87:
M = ‘0CA4020C800000008709016375432908C044F6’

f. Compute MAC of M:

i. Increment SSC with 1:

SSC = ‘887022120C06C227’

ii. Concatenate SSC and M and add padding:

N = ‘887022120C06C2270CA4020C80000000
8709016375432908C044F68000000000’

iii. Compute MAC over N with KS_{MAC}:

CC = ‘BF8B92D635FF24F8’

g. Build DO‘8E’:

DO8E = ‘8E08BF8B92D635FF24F8’

h. Construct and send protected APDU:

ProtectedAPDU = ‘0CA4020C158709016375432908C0
44F68E08BF8B92D635FF24F800’

i. Receive response APDU of MRTD’s chip:

RAPDU = ‘990290008E08FA855A5D4C50A8ED9000’

j. Verify RAPDU CC by computing MAC of DO’99’:

i. Increment SSC with 1:

SSC = ‘887022120C06C228’

ii. Concatenate SSC and DO‘99’ and add padding:

K = ‘887022120C06C2289902900080000000’

iii. Compute MAC with KS_{MAC}:

CC’ = ‘FA855A5D4C50A8ED’

iv. Compare CC’ with data of DO‘8E’ of RAPDU.

‘FA855A5D4C50A8ED’ == ‘FA855A5D4C50A8ED’ ? YES.

2. Read Binary of first four bytes:

Unprotected command APDU:

CLA	INS	P1	P2	LE
00h	B0h	00h	00h	04h

a. Mask class byte and pad command header:

CmdHeader = ‘0CB0000080000000’

b. Build DO‘97’:

DO97 = ‘970104’

c. Concatenate CmdHeader and DO97:

M = ‘0CB0000080000000970104’

d. Compute MAC of M:

i. Increment SSC with 1:

SSC = ‘887022120C06C229’

ii. Concatenate SSC and M and add padding:

N = ‘887022120C06C2290CB00000
800000009701048000000000’

iii. Compute MAC over N with KS_{MAC}:

CC = ‘ED6705417E96BA55’

e. Build DO‘8E’:

DO8E = ‘8E08ED6705417E96BA55’

f. Construct and send protected APDU:

ProtectedAPDU = ‘0CB000000D9701048E08ED6705417E96BA5500’

g. Receive response APDU of MRTD's chip:
RAPDU = `'8709019FF0EC34F992265199029000 8E08AD55CC17140B2DED9000'`

h. Verify RAPDU CC by computing MAC of concatenation DO'87' and DO'99':
i. Increment SSC with 1:
SSC = `'887022120C06C22A'`
ii. Concatenate SSC, DO'87' and DO'99' and add padding:
K = `'887022120C06C22A8709019F F0EC34F99226519902900080'`
iii. Compute MAC with KS_{MAC}:
CC' = `'AD55CC17140B2DED'`
iv. Compare CC' with data of DO'8E' of RAPDU:
`'AD55CC17140B2DED' == 'AD55CC17140B2DED'` ? YES.

i. Decrypt data of DO'87' with KS_{ENC}:
DecryptedData = `'60145F01'`

j. Determine length of structure:
L = '14' + 2 = 22 bytes

3. Read Binary of remaining 18 bytes from offset 4:

Unprotected command APDU:

CLA	INS	P1	P2	LE
00h	B0h	00h	04h	12h

a. Mask class byte and pad command header:
CmdHeader = `'0CB0000480000000'`

b. Build DO'97':
DO97 = `'970112'`

c. Concatenate CmdHeader and DO97:
M = `'0CB0000480000000970112'`

d. Compute MAC of M:
i. Increment SSC with 1:
SSC = `'887022120C06C22B'`
ii. Concatenate SSC and M and add padding:
N = `'887022120C06C22B0CB00004 800000009701128000000000'`
iii. Compute MAC over N with KS_{MAC}:
CC = `'2EA28A70F3C7B535'`

e. Build DO'8E':
DO8E = `'8E082EA28A70F3C7B535'`

f. Construct and send protected APDU:
ProtectedAPDU = `'0CB000040D9701128E082EA28A70F3C7B53500'`

g. Receive response APDU of MRTD's chip:
RAPDU = `'871901FB9235F4E4037F2327DCC8964F1F9B8C30F42 C8E2FFF224A990290008E08C8B2787EAEA07D749000'`

h. Verify RAPDU CC by computing MAC of concatenation DO'87' and DO'99':
i. Increment SSC with 1:
SSC = `'887022120C06C22C'`

ii. Concatenate SSC, DO‘87’ and DO‘99’ and add padding:
K = `‘887022120C06C22C871901FB9235F4E4037F232 7DCC8964F1F9B8C30F42C8E2FFF224A99029000’`

iii. Compute MAC with KS$_{MAC}$:
CC’ = `‘C8B2787EAEA07D74’`

i.v Compare CC’ with data of DO‘8E’ of RAPDU:
`‘C8B2787EAEA07D74’ == ‘C8B2787EAEA07D74’` ? YES.

i. Decrypt data of DO‘87’ with KS$_{ENC}$:
DecryptedData = `‘04303130365F36063034303030305C026175’`

RESULT:

EF.COM data = `‘60145F0104303130365F36063034303030305C026175’`

A6.1.2 Passive Authentication

Step 1. Read the Document Security Object (SO$_D$) (optionally containing the Document Signer Certificate (C$_{DS}$)) from the chip.
Step 2: Read the Document Signer (DS) from the Document Security Object (SO$_D$).
Step 3: The inspection system verifies SO$_D$ by using Document Signer Public Key (KPu$_{DS}$)
Step 4: The inspection system verifies C$_{DS}$ by using the Country Signing CA Public Key (KPu$_{CSCA}$).

If both verifications in step 3 and 4 are correct, then this ensures that the contents of SO$_D$ can be trusted and SHOULD be used in the inspection process.

Step 5: Read the relevant Data Groups from the LDS.
Step 6: Calculate the hashes of the relevant Data Groups.
Step 7: Compare the calculated hashes with the corresponding hash values in the SO$_D$.

If the hash values in step 7 are identical, this ensures that the contents of the Data Group are authentic and unchanged.

A6.1.3 Active Authentication

This worked example uses the following settings:

1. Integer factorization based mechanism:	**RSA**
2. Modulus length:	**1 024 bits (128 bytes)**
3. Hash algorithm:	**SHA1**

Inspection system:

1. Generate an 8 byte random:
RND.IFD = `‘F173589974BF40C6’`

2. Construct command for internal authenticate and send command APDU to the MRTD’s chip:

   Command APDU

CLA	INS	P1	P2	LC	Command data field	LE
0xh	88h	00h	00h	08h	RND.IFD	00h

MRTD’s chip:

3. Determine M_2 from incoming APDU:
   M_2 = `‘F173589974BF40C6’`

4. Create the trailer:
   T = ‘BC’ (i.e. SHA1)

5. Determine lengths:
   a. $c = k - L_h - 8t - 4 = 1024 - 160 - 8 - 4 = 852$ bits
   b. $L_{M1} = c - 4 = 848$ bits

6. Generate nonce M_1 of length L_{M1}:
   M_1 =

```
‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8’
```

7. Create M:
   $M = M_1 \mid M_2$ =

```
‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8F173589974BF
40C6’
```

8. Calculate SHA1 digest of M:
   H = SHA1(M) =

```
‘C063AA1E6D22FBD976AB0FE73D94D2D9
C6D88127’
```

9. Construct the message representative:
   F = ‘6A’ | M_1 | H | T =

```
‘6A9D2784A67F8E7C659973EA1AEA25D9
5B6C8F91E5002F369F0FBDCE8A3CEC19
91B543F1696546C5524CF23A5303CD6C
98599F40B79F377B5F3A1406B3B4D8F9
6784D23AA88DB7E1032A405E69325FA9
1A6E86F5C71AEA978264C4A207446DAD
```

```
               4E7292E2DCDA3024B47DA8C063AA1E6D
               22FBD976AB0FE73D94D2D9C6D88127BC’
```

10. Encrypt F with the Active Authentication Private Key to form the signature:

```
S =           ‘756B683B036A6368F4A2EB29EA700F96
               E26100AFC0809F60A91733BA29CAB362
               8CB1A017190A85DADE83F0B977BB513F
               C9C672E5C93EFEBBE250FE1B722C7CEE
               F35D26FC8F19219C92D362758FA8CB0F
               F68CEF320A8753913ED25F69F7CEE772
               6923B2C43437800BBC9BC028C49806CF
               2E47D16AE2B2CC1678F2A4456EF98FC9’
```

11. Construct response data for INTERNAL AUTHENTICATE and send response APDU to the inspection system:

    Response APDU:

Response data field	SW1SW2
S	9000h

Inspection system:

12. Decrypt the signature with the public key:

```
F =           ‘6A9D2784A67F8E7C659973EA1AEA25D9
               5B6C8F91E5002F369F0FBDCE8A3CEC19
               91B543F1696546C5524CF23A5303CD6C
               98599F40B79F377B5F3A1406B3B4D8F9
               6784D23AA88DB7E1032A405E69325FA9
               1A6E86F5C71AEA978264C4A207446DAD
               4E7292E2DCDA3024B47DA8C063AA1E6D
               22FBD976AB0FE73D94D2D9C6D88127BC’
```

13. Determine hash algorithm by trailer T*:
    T = ‘BC’ (i.e. SHA1)

14. Extract digest:

```
D =           ‘C063AA1E6D22FBD976AB0FE73D94D2D9
               C6D88127’
```

15. Extract M_1:

```
M1 =          ‘9D2784A67F8E7C659973EA1AEA25D95B
               6C8F91E5002F369F0FBDCE8A3CEC1991
               B543F1696546C5524CF23A5303CD6C98
               599F40B79F377B5F3A1406B3B4D8F967
               84D23AA88DB7E1032A405E69325FA91A
               6E86F5C71AEA978264C4A207446DAD4E
               7292E2DCDA3024B47DA8’
```

16. Header indicates partial recovery but signature has modulus length so concatenate M_1 with known M_2 (i.e. RND.IFD):

```
M* =        ‘9D2784A67F8E7C659973EA1AEA25D95B
             6C8F91E5002F369F0FBDCE8A3CEC1991
             B543F1696546C5524CF23A5303CD6C98
             599F40B79F377B5F3A1406B3B4D8F967
             84D23AA88DB7E1032A405E69325FA91A
             6E86F5C71AEA978264C4A207446DAD4E
             7292E2DCDA3024B47DA8F173589974BF
             40C6’
```

17. Calculate SHA1 digest of M*:

```
D* =        ‘C063AA1E6D22FBD976AB0FE73D94D2D9
            C6D88127’
```

18. Compare D and D*:
    D is equal to D* so verification successful.

A6.2 Life times

The following examples demonstrate the explanations on how to calculate the key life times as described in 9.

A6.2.1 *Example 1*

The first demonstrates a system where the State wishes to keep to a minimum the total life time of all its certificates. The State’s passports are valid for five years, and as the State issues a relatively large number of passports per year it has decided to keep its key issuing periods to a minimum.

Period	**Elapsed Time**	
Document Signer Key Issuing		1 month
Passport Validity	5 years	—
Document Signer Certificate Validity	5 years	1 month
Country Signing CA Key Issuing	3 years	—
Country Signing CA Certificate Validity	8 years	1 month

The consequences of this example are by the time the first Country Signing CA Certificate becomes invalid at least 36 document signing keys will have been issued (one for each one-month period) and in the last few months of this Country Signing CA Key there will be at least two other Country Signing keys valid for signature verification.

A6.2.2 *Example 2*

The second example demonstrates a system where the State takes a slightly more relaxed approach. The passports are valid for ten years; the State has decided to keep to average issuing periods for all keys.

Period	**Elapsed Time**	
Document Signer Key Issuing		2 months
Passport Validity	10 years	—
Document Signer Certificate Validity	10 years	2 months
Country Signing CA Key Issuing	4 years	—
Country Signing CA Certificate Validity	14 years	2 months

The consequences of this example are by the time the first Country Signing CA Certificate becomes invalid at least 24 Document Signer Keys will have been issued, and in the last few months of the Country Signing CA Key there will be at least three other Country Signing CA Keys valid for signature verification.

A6.2.3 *Example 3*

The final example demonstrates a system where the State has decided to use the maximum limits advised by this framework. The passports are valid for ten years, the Country Signing CA Key is replaced every five years and Document Signer Keys are replaced every three months.

Period	**Elapsed Time**	
Document Signer Key Issuing		3 months
Passport Validity	10 years	—
Document Signer Certificate Validity	10 years	3 months
Country Signing CA Key Issuing	5 years	—
Country Signing CA Certificate Validity	15 years	3 months

The consequences of this example are by the time the first Country Signing CA Certificate becomes invalid at least 20 Document Signer Keys will have been issued, and in the last few months of the Country Signing CA Key there will be at least three other Country Signing CA Keys valid for signature verification.

INFORMATIVE APPENDIX 7

PKI AND SECURITY THREATS

A7.1 Key management

A7.1.1 *Country signing CA and document signer keys*

To protect the private keys it is RECOMMENDED to use secure hardware devices for signature generation (Secure Signature Creation Device — SSCD), i.e. the SSCD generates new key pairs, stores and destroys (after expiration) the corresponding private key securely. To protect against attacks on the SSCD including Side-Channel Attacks (e.g. timing, power consumption, EM emission, fault injection) and attacks against the random number generator, it is RECOMMENDED to use SSCDs that are successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High.

When distributing self-signed Country Signing CA Certificates by diplomatic means, extreme care must be taken to prevent insertion of a rogue Country Signing CA Certificate. Furthermore, it is RECOMMENDED that States store the received Country Signing CA Certificates securely, accessible by the reader devices in a secure manner. To protect against attacks on the CAD, it is RECOMMENDED to use CADs that are successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High.

A7.1.2 *Active Authentication keys*

It is RECOMMENDED to generate key pairs for Active Authentication in a secure manner. As the private key is stored on the chip in secure memory, and the chip hardware has to resist attacks for the whole validity period of the MRTD, it is RECOMMENDED to use chips that are successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High.

The available chip technology influences the maximum key length of keys used inside the chip for Active Authentication. Many chips currently do not support key lengths that exceed a security level of 80 bits, which was the reason for choosing this value as recommended minimum. This is a relatively low level of security compared to their validity period of the MRTD. Therefore, it is RECOMMENDED to use longer keys, if supported by the chip.

States that make use of the Active Authentication mechanism to validate a foreign MRTD should also be aware that no revocation mechanism has been specified for compromised Active Authentication keys.

A7.1.3 *Denial of service attacks*

Denial of service attacks have to be considered when States rely on the directory for distribution of Document Signer Certificates and CRLs. Those attacks cannot be prevented. It is therefore RECOMMENDED that the Document Signer Certificate required to validate the Document Security Object be also included in the Document Security Object itself. Receiving States SHOULD make use of a provided Document Signer Certificate.

To distribute CRLs bilaterally it is RECOMMENDED to establish multiple channels (e.g. internet, phone, fax, mail, etc.) with other States and to confirm reception of received CRLs.

A7.2 Cloning threats

Compared to paper-based MRTDs, copying the signed data stored on the RF-Chip is easily possible in general. States concerned about the possibility of having data of their citizens copied to another chip SHOULD implement Active Authentication that prevents this to a certain extent.

A7.2.1 *Passive Authentication*

Passive authentication does not prevent copying the data stored on the chip. As a consequence, it is possible to substitute the chip of a MRTD against a fake chip storing the data copied from the chip of another MRTD. Receiving States SHOULD verify that the data read from the chip indeed belongs to the presented MRTD. This can be done by comparing DG1 stored on the chip to the MRZ printed on the datapage of the MRTD. If DG1 and the MRZ compare and the Document Security Object is valid, and the presented MRTD has not been tampered with (is not counterfeited), then the MRTD and the data stored on the chip can be considered to be belonging together.

A7.2.2 *Active Authentication*

Active Authentication makes chip substitution more difficult, but not impossible. The MRTD presented by the attacker to the inspection system could be equipped with a special chip. This chip works as proxy for a genuine chip located in a remote place: the chip communicates with the attacker, the attacker communicates with another attacker, and the other attacker (temporarily) gains access to the genuine chip. The inspection system is not able to notice that it has authenticated a remote chip instead of the presented chip. This attack is called Grandmaster Chess Attack.

A7.3 Privacy threats

A7.3.1 *No access control*

The use of proximity chips already minimizes privacy risks as reader devices have to be very close to the chips, therefore skimming is not considered to be a serious threat. However eavesdropping on an existing communication between a chip and a reader is possible from a larger distance. States wishing to address this threat SHOULD implement Basic Access Control.

A7.3.2 *Basic Access Control*

The Basic Access Keys used to authenticate the reader and to set up session keys to encrypt the communication between chip and reader are generated from the 9-digit document number, the date of birth, and the date of expiry. Thus, the entropy of the keys is relatively low. For a 10-year valid MRTD the entropy is 56 bits at maximum. With additional knowledge (e.g. approximate age of the bearer, or relations between document number and date of expiry) the entropy is lowered even more. Due to the relatively low entropy, in principle an attacker might record an encrypted session, calculate the Basic Access Keys by Brute-Force from the authentication, derive the session keys and decrypt the recorded session. However this still requires a considerable effort compared to obtaining the data from other sources.

A7.3.3 *Active Authentication (Data traces)*

In the challenge-response protocol used for Active Authentication, the chip signs a bit string that has been chosen more or less randomly by the inspection system. If a receiving State uses the current date, time and location to generate this bit string in an unpredictable but verifiable way (e.g. using secure hardware), a third party can be convinced afterwards that the signer was at a certain date and time at a certain location.

A7.4 Cryptographic threats

The recommended minimal key lengths have been chosen so that breaking those keys requires a certain (assumed) effort, independent of the chosen signature algorithm:

Type of Key	Level of Security
Country Signing CA	128 bits
Document Signer	112 bits
Active Authentication	80 bits

A7.4.1 *Mathematical advances and non-standard computing*

According to Moore's Law computation power doubles every 18 months. However, the security of the signature algorithm is not only influenced by computing power; advances in mathematics (cryptanalysis) and the availability of new non-standard computation methods (e.g. quantum computers) also have to be taken into account.

Due to the long validity periods of keys it is very difficult to make predictions about mathematical advances and the availability of non-standard computing devices. Therefore, the recommendations for key lengths are mainly based on the extrapolated computing power. States SHOULD review the key lengths for their own but also for received MRTDs often for reasons mentioned above.

Generating key pairs of a special form may improve the overall performance of the signature algorithm, but may also be exploited for cryptanalysis in the future. Therefore, such special key pairs SHOULD be avoided.

A7.4.2 *Hash collisions*

While it is computationally infeasible to find another message that produces the same hash value as a given message, it is considerably easier to find two messages that produce the same hash value. This is called the Birthday Paradoxon.

In general all messages to be signed are produced by the Document Signer itself. Therefore, finding hash collisions does not help an attacker very much. However, if photographs provided by the applicant in digital form are accepted by the Document Signer without additional randomized modification, the following attack is possible:

- Two persons share their digital photos. Then they repeatedly flip a small number of bits at random in each photo until two photos produce the same hash value.

- Both persons apply for a new MRTD using the manipulated photo. Either person can now use the MRTD of the other person provided that it is possible to replace the digital photo in the chip (e.g. by chip substitution).

The hash function SHA-1 only provides 80 bits of security against hash collisions. Thus, it is considerably easier to find a hash collision than to break the Document Signer Key which provides 112 bits of security. Therefore, whenever hash collisions are of concern (e.g. as described above), it is RECOMMENDED not to use SHA-1 as hash function.

— END —