MACHINE READABLE TRAVEL DOCUMENTS

MACHINE READABLE TRAVEL DOCUMENTS (MRTDs): HISTORY, INTEROPERABILITY, AND IMPLEMENTATION

Version: Release 1
Status: Draft 1.4
Date: March 23, 2007

INTERNATIONAL CIVIL AVIATION ORGANIZATION

File	: MRTDs: History, Interoperability and Implementation
Author	: ISO/IEC JTC1 SC17 WG3/TF1 for ICAO-NTWG

Release Control

Release	Date	Description
0.1	30-Dec-2005	First draft
0.2	Apr-2006	Draft as first effort after the Rome NTWG
0.3	Jun-2006	Internal review
0.4	Sept-2006	To serve as discussion document for Kingston NTWG
0.5	Sept-2006	Internal review
0.6	22-Sept-2006	Produced after discussion at NTWG/Kingston
1	29-Sept-2006	First version released to NTWG for review
1.1	09-Nov-2006	Draft incorporating all comments received after above review
1.2	25-Nov-2006	Refinement of the above draft to release for final review
1.3	07-Dec-2006	Draft posted for comment
1.4	23 March 2007	Graphic updates.

Table of Contents

SECTION 1. EXECUTIVE SUMMARY

The International Civil Aviation Organization (ICAO) is the United Nations agency created to promote aviation understanding, facilitation and security through cooperative multilateral regulation. In carrying out these broad responsibilities, ICAO establishes international standards for travel documents, in accordance with the Chicago Convention. The ICAO began to explore different approaches for machine readable travel documents (MRTDs) in meetings during 1969, culminating in 1980 with the publication of the first edition of Document 9303, titled "A Passport with Machine Readable Capability." Since that time, ICAO has worked to further the concepts of machine readable travel documents, broaden the use of such documents and to enhance the documents themselves to serve better the corollary goals of facilitation and security. This paper will trace those activities over the past decade that have led to the development and publication of standards for electronic travel documents, and in particular, passports (through 9303 Part 1, Passports/Sixth Edition), that allow for the storage of biometric data using contactless chips as the storage medium.

This paper replaces the ICAO Technical Report, "Biometrics Deployment in Machine Readable Travel Documents" and is intended to provide information regarding the thought processes and multilateral deliberations that occurred from 1995 through 2006 with the publication of 9303 Part 1, Passports/Sixth Edition. It serves as a companion to the 9303 specifications and the Technical Reports published by ICAO. In that regard, it seeks to provide background into the "why" and the "what" with respect to travel document technology choices, particularly those associated with biometrics and Integrated Circuit contactless chips. The paper is to be viewed as a summary guide and a pointer to other ICAO documents; it is NOT to be viewed as a replacement for the Standards themselves. In that context, this paper is intended for an audience composed of individuals generally interested in the history and evolution of travel documents as well as those who are responsible for the issuance, inspection or other non-travel use of machine readable travel documents. It has been written to address the wide variety of issues and considerations regarding travel document programs and as a compendium of the history and background of current travel document specifications.

In 1995, ICAO clearly recognized the desirability of pursuing the use of biometrics in travel documents as the single best way to link the document and its rightful "owner." To accomplish this, ICAO acknowledged the need to be able to store more data in a machine readable travel document, which led to a comprehensive examination of data storage technologies. Accordingly, much of this paper is focused on the fundamental ICAO decisions and the reasons for those decisions that have charted these fundamental travel document directions, especially those regarding contactless chips and facial recognition biometrics. In addition to historical and technical perspectives on chips and biometrics, in

serving as a summary and guide, this paper highlights related areas of focus, such as the need to insure that travel document systems employ sound means of internal control to assure system integrity. Similarly, it discusses operational considerations and implementation strategies to assist in clarifying some of the approaches in deploying travel document programs, including the characteristics of the documents themselves. This latter area covers a variety of issues regarding materials and document qualitative factors and provides guidance regarding the need for and development of testing programs. Finally, this paper concludes with two Appendices, one that provides a summary of the references used in document 9303 and the other a collection of definitions and terms.

SECTION 2. INTRODUCTION

The International Civil Aviation Organization (ICAO) has long played a major role in establishing the specifications and best practices for the issuance of passports and other travel documents, among numerous other responsibilities associated with global air travel matters. Standardization of document formats and contents has facilitated international travel and enhanced national security by enabling nations to determine more quickly and accurately the validity of travel documents. Over the years, ICAO has issued specifications and guidance for the layout of the passport data page, size and shape of travel documents, and inclusion of security features, as well as for other aspects of travel document production and issuance. An issuing officer or border inspector can now visually determine whether a document contains any of a variety of security features (i.e., thereby reducing counterfeiting), or whether it might have been tampered with (such as by photo substitution) when using those security features designed to be tamper-evident.

An important aspect of international border security is the need to establish that a traveler presenting a passport and/or visa is the person to whom the document was legitimately issued. A first step in this direction was the creation of standards for the printing of the machine readable zone (MRZ). This is a set of two lines of data on a passport (two or three on a visa, depending on size) that are printed using a standard format and font (called OCR-B). The MRZ replaces typed or handwritten personalized information, which might easily be altered, with a standardized representation for the holder's name, date of birth, and other details as well as arithmetically derived security verifying check digits. This allows inspectors and other authorized document examiners to use a special reader that interprets these characters and directly passes them to a computerized system, thereby reducing errors in entering information into inspection and lookout systems. By standardizing the size and location of the photo on the data page, an inspector can now easily compare that picture to the person presenting the document. Documents conforming to these specifications are called machine readable travel documents (MRTDs).

As significant as these advances were, there still was the need to confirm more accurately the validity of the traveler as the rightful "owner" of the documents and to further enhance document integrity and security. ICAO's New Technologies Working Group (NTWG) began examining various technologies to accomplish this objective in the late 1990s. As a result of that effort, the NTWG developed specifications for an enhanced MRTD—one including an embedded integrated circuit (IC) chip encoded with biometric information. A passport containing such a chip with stored biometric information conforming to ICAO specifications is called an e-passport. It includes advanced security features (further reducing the possibilities of counterfeiting or alteration), and by containing biometric data from the rightful holder, it allows the document examiner to verify that data against biometric information collected from the person presenting the document. Those persons examining these chip-enabled passports can be assured that the biometric data stored on the passport were placed there by the Issuing State through the use of special electronic

"document signing" information that can be validated and associated only with that Issuing State. The verification of this "digital signature" is performed using modified Public Key Infrastructure (PKI) techniques. PKI relies upon complex algorithms to create a key-pair—a "private key" for the Issuing State to digitally sign the information on the chip and a "public key" that is used by a Receiving State to verify that the Issuing State was the true signer of the data. These keys are uniquely paired, and knowledge of the public key does not allow replication of the private key.

With the decision to adopt integrated circuit (IC) technology and to employ a PKI scheme to ensure that data on the chip are secure, there still remained the major task of achieving global interoperability, or ensuring that this technology could be produced by nations around the world, and that the e-passport any nation produces would be readable by systems employed by other nations when checking those documents. The ICAO Work groups, reporting to the TAG, have developed the specifications for electronic MRTDs (e-MRTDs), specifically with the major focus on global interoperability for passports and visas. For purposes of this paper, the use of the term MRTD refers to the full scope of machine readable travel documents, including passports, visas, and other official travel documents. Generally, throughout the paper, however, the primary emphasis is on the e-passport.

2.1 SCOPE AND PURPOSE

This document is designed to be a summary of the key decisions ICAO has made for travel documents. It is written for individuals with an interest in the development and deployment of technologies needed to achieve globally interoperable MRTDs, with an emphasis on e-passports. It describes the changes required in policies and procedures by States moving towards the production and reading of ICAO-compliant, internationally interoperable MRTDs. To provide the rationale for the decisions ICAO has made, it pulls information from various technical reports issued by the NTWG, as well as from other sources. This document is <u>not</u> designed to provide detailed specifications for e-passports—the actual specifications themselves are incorporated into various sections of ICAO's Document 9303. The purpose of this document, therefore, is to serve as a guide in using the other Technical Reports, the Supplement, the 9303 specifications, and other relevant documents and references. This Technical Report is not in any way intended to be construed as a stand-alone reference and must be viewed in concert with the other documents cited.

This document will address the following and related concepts, in view of the technologies involved with e-passports and the requirements in ICAO standards:

- Global Interoperability – specifying how the technologies are to be deployed and used in a universally interoperable manner. This also includes the issue of backward compatibility.

- Uniformity – minimizing, via specific standard-setting, to the extent practical, the different solution variations that may potentially be deployed by member States.
- Technical Reliability – providing 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 and reliable verification at their end.
- Practicality –ensuring that recommended standards can be implemented by States unambiguously to avoid having to introduce a plethora of disparate systems and equipment to ensure they meet all possible variations and interpretations of the standards.
- Quality – to insure that the contents of the data captured in travel documents, both electronic as well as visually displayed are of the highest quality possible in order to use the documents with confidence and reliability.

SECTION 3. ICAO HISTORY AND BACKGROUND

Travel documents such as passports have been used for centuries as a basis for establishing the bearer's identity and for affording civil and diplomatic protection when crossing borders or traveling in foreign jurisdictions. The fact that passports initially took a variety of forms—from a sovereign's letter of recommendation written on large size parchment to "safe conduct" passes—did not create much difficulty at a time when international travel was infrequent and was limited mostly to official, trade, and privileged classes. However, with the rise of large-scale tourism and the increase in international commerce, governments became concerned with the bottlenecks created by complex administrative control procedures at border-crossings, and with the burden of verifying the authenticity of passports and other identity documents issued according to a variety of standards and patterns by foreign States. The first multilateral Conference, convened for this purpose in 1920, adopted standard passport and visa formats for all signatory States, with uniform provisions governing their layout, content, validity, and issuing fees. A second international Conference, convened in 1926, endorsed the main recommendations of the 1920 Conference, setting forth additional specifications for and improvements to the standard international passport format.

3.1 CREATION OF ICAO

The dissolution of the League of Nations ended the Post World War I movement toward standardization, but the principle of its desirability had been established. With the end of the Second World War, the movement was revived with the creation of ICAO in 1946 as a specialized agency under the United Nations. ICAO's mandate to develop standards and specifications stems from the 1944 Chicago Convention, which created ICAO and covered the full range of requirements for the efficient and orderly operation of international civil aviation worldwide, including provisions for clearance of persons through border controls. From its beginning in 1944, ICAO has grown to an organization with, at the time of this writing, 189 Contracting States. ICAO's aim is the safe and orderly development of all aspects of international civil aeronautics. It provides the forum whereby requirements and procedures in need of standardization may be introduced, studied, and resolved.

ICAO's mandate to develop travel document standards is provided by Articles 22 (*Facilitation of formalities*), 23 (*Customs and immigration procedures*), and 37 (*Adoption of international standards and procedures*) of the Chicago Convention, which oblige Contracting States to develop and adopt international standards for customs, immigration, and other procedures to facilitate the border-crossing processes involved in international air transport. A fundamental precept in the development of standards under Annex 9 to the Chicago Convention (Facilitation) is that, if public authorities are to comply with the requirements, they must have confidence in the reliability of travel documents and in the effectiveness of inspection procedures. The production of standardized specifications for travel documents aims at ensuring that confidence. Hence,

Annex 9 covers such issues as travel documents (including formats, issuance and control procedures), immigration and customs procedures and systems, and, the prevention and handling of document fraud cases and other security matters.

ICAO has been leading international efforts to develop standards-based, interoperable MRTDs (e.g., passports and visas). A passport is a document issued to an individual by one's State of citizenship. It identifies the individual and his or her citizenship entitlement and is used by the issuing nation to grant re-entry into the country. A visa is a document issued by a nation to permit entry to a foreign national. Typically, a visa document is inserted into an individual's passport. ICAO has been addressing issues such as document durability and security, data storage capacity, data content and format, optical character recognition (OCR) capability, biometrics, contactless chip technology, and privacy with respect to national laws. ICAO standards are now becoming the basis for a variety of identity-related documents and systems.

ICAO's work on what are now known as MRTDs began in 1968 with the establishment of a Panel on Passport Cards. That panel produced a set of recommendations that included the adoption of optical character recognition (OCR) as the machine reading technology of choice due to its maturity, cost-effectiveness, and reliability. In 1980, the specifications and guidance material developed by the Panel were published as the first edition of Document 9303, *A Passport with Machine Reading Capability*. Since the original publication of Document 9303, which became the basis for the initial issuance of machine readable passports (MRPs) by Australia, Canada, and the United States, Document 9303 has been expanded to cover a family of MRTDs. Now included in that family are Passports (ID-3 size), Visas in Format A (sized to fit in an ID-3 Passport), Format B Visas (ID-2 size), Travel Document 1 Cards (ID-1 size), and Travel Document 2 Cards (ID-2 size).

3.2 ORGANIZATION OF ICAO

Standards for MRTDs are developed by ICAO's TAG/MRTD, an advisory group appointed by the Secretary General of ICAO. The TAG provides its advice through the Facilitation Section of the Air Transport Bureau of ICAO. TAG/MRTD is currently made up of experts from several ICAO member States.

The TAG/MRTD drafts and adopts specifications (i.e., detailed technical requirements) for the design of MRTDs, and the specifications are published by ICAO in Document 9303. The TAG also publishes guidance material to assist States in implementing its specifications, as well as Technical Reports, the 9303 Supplement, and Information Papers to guide States and private industry on present and future aspects of its work.

To the extent possible, TAG/MRTD bases its standards to comply with those developed by the International Organization for Standards (ISO) and the International Electrotechnical Commission (IEC) and other standards-making organizations. The chart in Figure 1 shows some of the relationships between TAG/MRTD and Subcommittees within ISO/IEC Joint

Technical Committee 1 (JTC 1). Under the responsible subcommittees, the chart also shows several of the standards referenced within Document 9303.

Up until the New Zealand meeting in December 2004, NTWG had special working groups to deal with biometrics, PKI, and Logical Data Structure (LDS). After the work products were formalized, NTWG asked ISO/IEC to assign to Task Force 1 the responsibility of updating the specifications as needed.

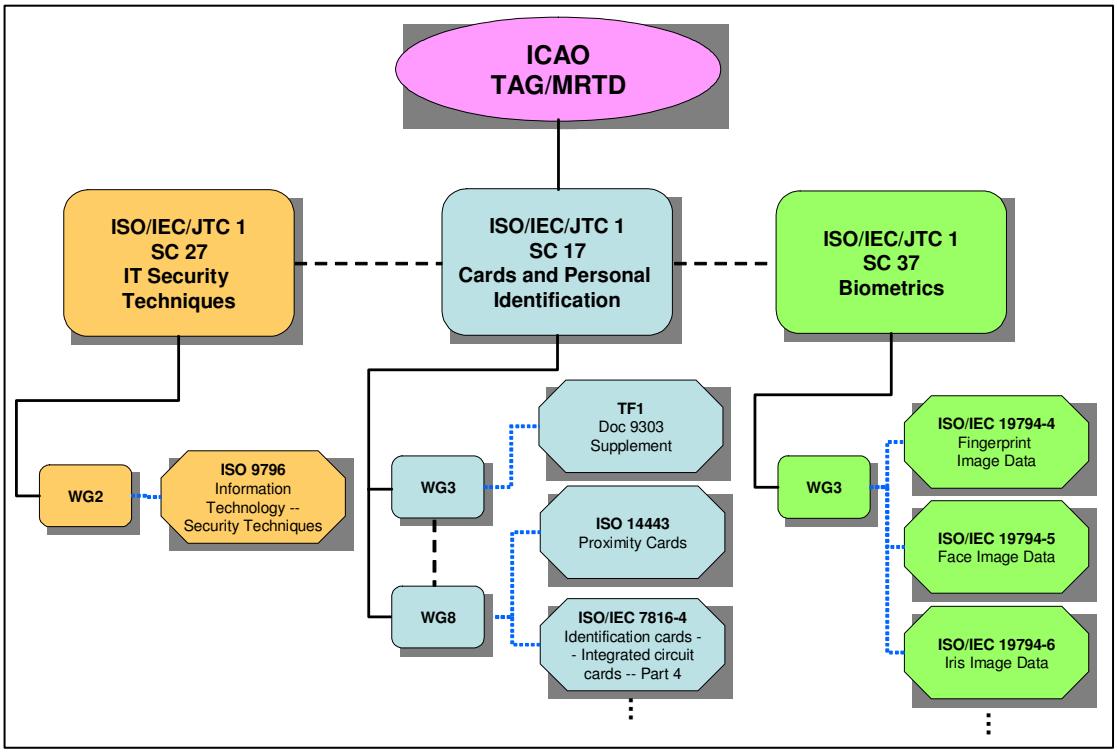

Figure 1. Representation of the relationships between ICAO TAG/MRTD and the relevant ISO/IEC JTC1 subcommittees

SECTION 4. TECHNICAL SPECIFICATION FOR MRTDS

As illustrated in Figure 2, the latest version of Document 9303 contains Parts 1, 2, and 3. Part 1, which is in its sixth edition, provides specifications for Machine Readable Passports (MRPs). Part 2 provides specifications for Machine Readable Visas (MRVs). Part 3 provides specifications for the various types of visas and other official travel identity documents.

Figure 2. Components of Document 9303

Parts 1 and 3 are now each provided in two volumes, with Volume 1 providing specifications for documents without additional storage and Volume 2 providing specifications for documents with additional storage and biometric identification capabilities. The titles for Parts 1 and 3 volumes are as follow:

- Part 1, Volume 1 is entitled *Machine Readable Passports without Additional Data Storage*, 2005
- Part 1, Volume 2 is entitled *Specifications for Electronically Enabled Passports (E-Passports) with Biometric Identification Capability*, 2005

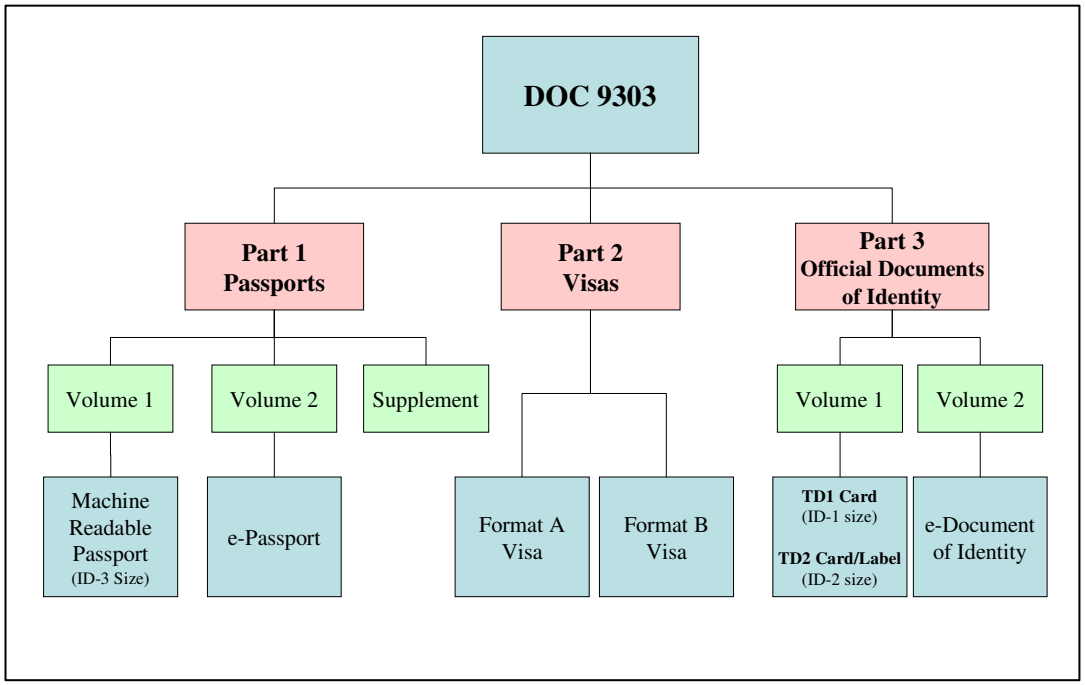

Figure 3. Components of Document 9303

Part 1, Supplement is entitled *Supplement to Doc9303-part 1-sixth edition*

- Part 3, Volume 1 is entitled *Machine Readable Official Documents of Identity without additional data storage*, 2006
- Part 3, Volume 2 is entitled *Machine Readable Official Documents of Identity - Specifications for Electronically Enabled Official Documents of Identity with Biometric Identification Capability*, 2006.

4.1 COMPONENTS OF PART 1

The emphasis of this document is on Part 1. The following subsections describe the components of Part 1 in more detail.

4.1.1 Part 1, Volume 1

Part 1, Volume 1 provides passport specifications for States that do not intend to incorporate the global facilitation for their citizens that will be available with machine assisted biometric identification. The data storage format uses a subset of the OCR-B font characters with specific sizes, ink characteristics, spacing and alignment criteria in order to create the MRZ at the bottom of the passport's data page. The order of the data is pre-specified as is the meaning of certain characters within particular fields within the MRZ.

4.1.2 Part 1, Volume 2

Part 1, Volume 2 contains additional specifications for a globally interoperable system of biometric identification and associated data storage utilizing a contactless IC. Its specifications were drawn up following a detailed study carried out over several years by the ICAO Technical Advisory Group's New Technologies Working Group (NTWG), beginning in 1998. The study examined the different biometric identification systems, concentrating on their relevance to traveler facilitation in applying for and obtaining a biometrically enabled passport and in using that passport for travel between States. Additionally, the NTWG examined very carefully the storage media available to most effectively carry both biometric as well as biographic information. Privacy laws applied by States around the world and the requirement for the biometric to be acceptable to the MRP holder strongly favored the use of the holder's face as the globally interoperable biometric, as the face, in the form of a photograph in a passport, is universally accepted as a means of identification.

Figure 3 displays the structure of Volume 2. Section I of Volume 2 provides an Introduction. Section II, Biometric Deployment, defines the methods of capture and use of the biometric data, and the requirements of the contactless IC used to store the data. Section III, LDS, defines the way the data are to be stored on the IC, and Section IV, Public Key Infrastructure, defines the process and procedures to be used for securing the data on the IC and ensuring that access to the data is appropriately restricted.

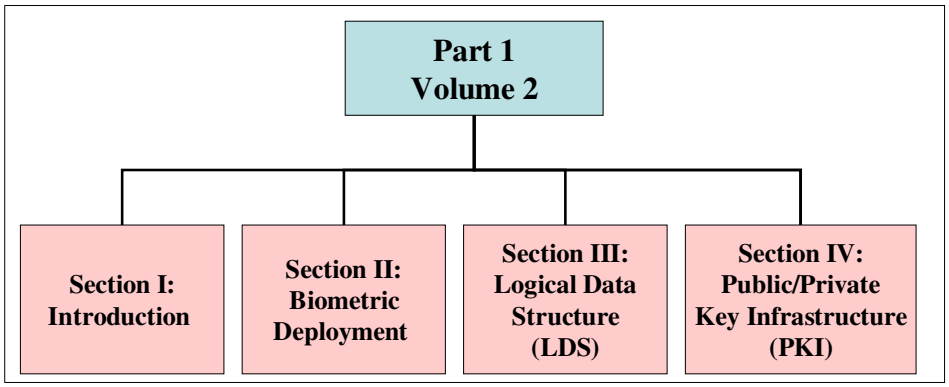

Figure 4. Structure of Document 9303, Part 1, Volume 2

4.1.3 Part 1, Supplement

The Supplement to Doc9303-part 1-sixth edition is intended to serve several purposes. It provides periodic guidance, advice, update, clarification and amplification on travel document issuance. It also serves as a "bridge" between the formal drafting of Standards and Technical Reports and the needs of the travel document community to have timely and official direction on which to rely. Its role is as a maintenance vehicle for 9303 and its content has the full force and effect of 9303 standards. As such, it may augment, clarify, elaborate, amplify or restate the content and interpretation of standards as well as practices. The Supplement is issued on an as-needed basis, generally twice each year.

4.2 ICAO/NTWG SPECIFICATION DEVELOPMENT PROCESS

The first work product associated with the e-passport project was the Technical Report, *Selection of a Globally Interoperable Biometric for Machine-assisted Identity Confirmation with MRTDs* in 2001. The NTWG worked directly with the ISO/IEC to examine various storage technologies that could handle the requirements associated with the recommendation to use facial recognition as the primary biometric.

Specialized work groups established by NTWG produced the following three Technical Reports containing e-passport specifications, which were incorporated into the current version of 9303:

1) Biometrics: *Biometrics Deployment of Machine Readable Travel Documents,* succeeded and replaced by this document
2) Data Protection: *PKI for Machine Readable Travel Documents offering ICC Read-Only Access.*
3) Data Organization: *Development of an LDS – for Optional Capacity Expansion Technologies.*

The contents of the documents were reviewed at each NTWG meeting as they went through development and subsequent revisions. In 2004, the NTWG "froze" the content in order for nations to proceed with interoperability testing of prototype e-passports and

reader systems. The Technical Reports were approved by the ICAO TAG at its meeting in May, 2004. This interoperability testing resulted in the need for clarification on some technical points that could potentially have been interpreted in different ways. The extant ISO/IEC Task Force 1 was called upon to examine these points. This Task Force then issued the first edition of Supplement to Document 9303, which reflects these clarifications.

The intention of the NTWG was to incorporate all of the technical specifications included in these reports into a revised Document 9303. This was accomplished, and the updated version was published in 2006. Up until that point, the totality of the e-passport specifications was spread across Document 9303, each of the Technical Reports mentioned above, and three editions of the Supplement. It should also be noted that the Biometrics report included several annexes that were included after the original publication of that report, and clarifications and updates were documented in the Supplement. In order for nations to proceed with the development of e-passports prior to the final publication of Document 9303, Version 6, ICAO consolidated the NTWG Technical Reports and other related documents into a single website.

SECTION 5. BIOMETRICS IN MRTDS

NTWG has undertaken a program focusing on machine-assisted identity confirmation of persons, both in terms of identification at the time of issuance of travel documents, and in terms of verification for border control purposes. Biometrics—the automated means of recognizing a living person through the measurement of distinguishing physical or behavioral traits - is integral to this program.

The incorporation of biometrics into e-passports required standardization so that the e-passports that each nation produces are readable by systems employed by other nations when checking those documents. NTWG was faced with the challenge of developing specifications to ensure such interoperability.

5.1 KEY CONSIDERATIONS CONCERNING BIOMETRICS DEPLOYMENT

To meet the challenge of deploying biometrics in MRTDs, ICAO assessed the following technical factors when selecting technologies and considering interoperability:

- Compatibility with MRTD enrollment, renewal, and machine-assisted identity verification requirements
- Redundancy (ability to fall back to similar manual methods to support inspection of a person to identify the document holder when the machine-assisted technique fails)
- Durability and reliability specifications
- Performance (speed, accuracy and related attributes)
- Backward compatibility (i.e., for use in environments not having e-passport readers)
- Data protection protocols
- E-passport reader specification and data retrieval standards
- Storage requirements
- Booklet and data format and contents
- Biometric data standards

5.2 PUBLIC PERCEPTION CONSIDERATIONS

In addition to the technical considerations, the NTWG was challenged with developing a set of specifications that would result in an e-passport that would be acceptable to both Issuing States and to the traveling public. The traveling public expects that the new form of passports will be accepted in each of the nations that may be visited. In addition, travelers expect that there will be privacy protection methods incorporated into the e-passport.

In the original 2001 report that reviewed biometrics, ICAO examined the perception of the traveling public for face, signature, finger, hand, voice, and eye biometrics, according to the following major categories:

- Privacy
- Legislative environment
- Health risk / safety
- Cultural impediments
- Ease of use (self evident / minimal training required)
- Benefit to the traveler
- Threat – carrying details on the MRTD
- Threat – storing details in a central database
- Acceptance once familiarized
- Social stigma
- Least fear of misidentification

This evaluation assumed no prior education of the public on biometric techniques.

5.3 SELECTION OF BIOMETRICS MODALITIES FOR E-PASSPORTS

ICAO considered a number of biometric technologies and focused intensively on the following generic types of biometric technologies in its 2001 evaluation: face image, iris, fingerprint, hand geometry, voice, and signature. Retinal features and other biometric technologies were considered, but rejected as impractical means of identity confirmation given the requirements defined for machine-assisted identity confirmation when presenting an MRTD.

In the Technical Report, *Selection of a Globally Interoperable Biometric for Machine-Assisted Identity Confirmation with MRTDs* (2001), the evaluators developed a series of criteria for each of the major categories and evaluated each of the biometrics technologies against those items. The results for each category were consolidated and weighted according to relative importance in accordance with a wide variety of multilaterally determined criteria.

Based on this analysis, ICAO concluded that the six general types of biometric technologies can be separated into three ranking groups, based on their overall ability to meet the comprehensive set of requirements defined for machine-readable identity confirmation with MRTDs, as follows:

Group 1: Face achieves the highest compatibility rating (greater than 65%)

Group 2: Finger(s) and iris emerge into a 2nd level compatibility grouping (near 65%)

Group 3: Signature, hand, and voice emerge in a 3rd level compatibility grouping (less than 50%)

ICAO concluded that "certain biometric technologies are *much more compatible with the comprehensive system requirements established for machine-assisted identity confirmation with MRTDs* than others, and factors other than performance have a strong impact on which biometric technology is the best to standardize for global interoperability."

In the **Berlin Resolution** of June 2002, the NTWG unanimously supported its preference for the use of facial recognition as the globally interoperable biometric, noting that

> "ICAO TAG-MRTD/NTWG endorses the use of face recognition as the globally interoperable biometric for machine assisted identity confirmation with MRTDs. ICAO TAG-MRTD/NTWG further recognizes that Member States may elect to use fingerprint and/or iris recognition as additional biometric technologies in support of machine assisted identity confirmation."

NTWG noted that States optionally can provide additional data input to their (and other States') identity verification processes by including multiple biometrics in their travel documents. 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 a national identification card system.

The Berlin Resolution received wide publication and interest from various countries and groups in terms of the clarification it provided to enable Member States to plan their biometrics deployment strategy. However, it was also noted that some confusion and interpretation difficulties existed with this resolution.

Though facial recognition is the primary globally interoperable biometric element, the NTWG recognized that some States would wish to use more than one biometric element. For example, many States have extensive fingerprint databases, which they might wish to employ to verify the identity of a traveler.

Iris recognition was also identified as a reliable method of identification. Though technically commendable, fingerprint and iris recognition each involve a rather more invasive and time-consuming collection of data, both at the original enrollment and at a port of entry. The NTWG therefore decided that it would recommend that fingerprint and iris data should be optional and secondary means of biometric identification.

5.4 STORAGE TECHNOLOGY

During the revision of Document 9303, TAG/MRTD determined that a State or organization might wish to expand the machine readable data capacity of the MRTD beyond that defined for global interchange (i.e., with OCR-B of the MRZ), for such purposes as providing machine readable access to breeder document information (e.g., birth certificate details), stored personal identity confirmation and/or document authenticity verification details. Since co-existence of an optional machine readable data storage technology with the mandatory OCR technology is critical to ensure global interoperability of the MRTD, specifications were developed governing the location of the capacity

expansion technologies. These specifications have been included in new editions of each Part of Document 9303.

Among the storage technologies that had been considered for use in passports are barcodes, magnetic stripes, optical media, and ICs. Among those, only Contactless ICs were determined to provide the required storage capacity, speed, reliability, and convenience. Consequently, the March 2003 **New Orleans Resolution** advises that "Member States, in their initial deployment of MRTDs with biometrics identifiers, are encouraged to adopt Contactless IC media of sufficient capacity to facilitate on-board storage of additional MRTD data and biometric identifiers." The intent of this part of the Resolution is that States adopt as high a capacity as they possibly can and which is operationally feasible and practicable. Key clarification provided by the New Orleans resolution includes:

- Digitally stored images will be used for global interoperability purposes, and these will be "on-board" (i.e., electronically stored in the travel document)
- These images are to be standardized
- High capacity Contactless IC media is the electronic storage medium endorsed by NTWG as the capacity expansion technology for use with MRTDs in the deployment of biometrics.

The Air Transport Committee of the ICAO Council in May 2003 adopted a four-part "Blueprint" for incorporating biometrics in travel documents. The Blueprint includes:

- Specifications for the face as the primary biometric, mandatory for global interoperability
- The contactless IC chip as the electronic data storage medium
- A logical data structure for programming the chip
- The PKI to secure the data against unauthorized alteration and ensure its authenticity

These specifications are incorporated in the sixth edition of Doc 9303, Part 1 (2006).

5.5 TEMPLATE COMPATIBILITY

Vendors employ different biometric templates, or data representations, usually degrading performance or making interoperability impossible. Therefore, ICAO requires that the full image (or token, a standardized representation of the facial image) be stored for interoperability and backward compatibility.

SECTION 6. BIOMETRICS APPLICATIONS

Biometrics can be used to improve the quality of the background checking performed as part of the passport, visa, or other travel document application and entitlement adjudication processes, and they can be used to increase the strength of the binding between the travel document and the person to whom the document was issued.

States should consider the following when implementing a biometric technology:

- Suitability of a particular biometric technology (face for global interoperability and optionally either finger or eye) to the border crossing application.
- Throughput (e.g., travelers per minute) of either the biometric system or the border crossing system as a whole
- The impact and fit with respect to current processes and the changes, if any, needed to modify those current practices.
- Collecting the "best" biometric samples possible, in order to maximize accuracy under automated biometric recognition.
- Accuracy of the biometric matching functions of the system. Issuing States must encode one or more facial, fingerprint, or iris biometrics on the MRTD as per LDS standards (or on a database accessible to the Receiving State). Given an ICAO-standardized biometric image and/or template, Receiving States must select their own biometric verification software and determine their own biometric scoring thresholds for identity verification acceptance rates – and referral of imposters.

6.1 KEY PROCESSES

Implementing an end-to-end solution for MRTDs involves many considerations and knowledge domains. Interoperability among member States is complicated by the varying levels of compliance (ranging from the minimum displayed portrait and MRZ to an IC chip with multiple biometrics) and the multitude of operational technologies, vendors, and implementation strategies.

The key processes relating to interoperability of the MRTD can be separated into "issuance" and "inspection".

6.1.1 Application and Issuance

The application and issuance processes consist of the initial identification of an individual and the determination of entitlement to ICAO compliant travel documents. States have a large degree of authority and discretion regarding the selection of technologies and the manner in which they issue travel documents to their citizens in the case of passports or to those wishing to visit in the case of visas. The process of identity proofing by utilizing "breeder documents" such as birth certificates to verify a subject's identity is the first key

step of issuance. The applicant's biometrics can be searched against one or more biometric databases (identification) to determine whether the applicant is known to any of the corresponding systems (for example, holding a passport under a different identity, criminal record, holding a passport from another State, etc.). After the background checking and vetting, the acquisition of biographical text data and biometric data from the subject is undertaken by the issuing authority.

Following the printing and production of the MRTD, it is the responsibility of the Issuing State to verify that the MRTD is readable. When the applicant obtains the passport or visa, if done in person, the biometric data can be taken again and verified against the initially captured biometrics. States should as well consider providing a means for citizens to read and verify the data in passports.

6.1.2 Inspection

A principal driver behind the introduction of the e-passports is the ability to verify that the person carrying the travel document is truly the person to whom the document was issued, and that the document is not counterfeit. The ability to capture and compare biometric samples from a person presenting a passport or visa in the ordinary course of an inspection is important. In addition, an important part of the inspection process can be the ability to search, in real time, watch lists containing biometric data on individuals.

States are strongly encouraged to use biometrics to establish or validate a traveler's identity at ports of entry and exit. States need to change the focus of border inspections from merely processing entry/exit to confirming identity and detecting fraud using machine assistance. Each time travelers (i.e., e-MRTD holders) enter or exit a State, their identities can be verified against the biometrics captured at the time their travel documents were 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 of the forms of Advance Passenger Information System (APIS). For example, for people with common names, biometric verification may eliminate the need for a traveler's secondary inspection when the identity of that traveler is quickly established to not be the person on the biographic watch list.

In a two-way check, the traveler's current captured biometric image data can be matched to the biometric data from the travel document (or from a central database) to confirm that the travel document and presenter are an authentic pair. PKI must be used to assure data integrity (e.g., data has not been altered).

In a three-way check, the traveler's current biometric data, the image from the travel document, and the image stored in a central database can be matched to confirm that the travel document has not been altered. This technique matches the person with the passport and with the database recording the data that was put in that passport at the time it was issued.

A fourth confirmatory check, albeit not an electronic one, is visually matching the results of the three-way check with the portrait displayed on the Data Page of the traveler's passport.

Exception-handling procedures must be designed for cases where the biometrics on the e-MRTD do not match the person at the border because the document is not working, the storage medium is damaged or not functioning properly, the verification software does not match the person successfully, the document has been physically tampered with, or the traveler is an imposter. Similarly, inspection officers need to be aware of methods used to attempt to fool the biometric capture devices (i.e., cosmetic surgery, patterned contact lenses, surgical alteration of fingerprints, etc.). If the biometric verification is negative, or if the person is identified as someone on a watch list, the traveler may be sent to secondary inspection for detailed inspection.

6.2 ERGONOMICS

Ergonomics is the science of designing safe and comfortable machines for humans. There are ergonomic issues associated with capturing biometrics with respect to both the operator and the traveler. For example, the user interface, operational environment, feedback, and communication can affect the quality and efficiency of transactions.

Consideration should be given as to where to place fingerprint scanners at issuance and inspection stations so they are at an appropriate height and angle for all subjects without causing discomfort. For face or iris recognition, camera placement should be optimized to accommodate various subject heights. Most biometric ergonomic issues are directly related to image quality and time to acquire a usable biometric.

6.3 USE OF TRAVEL DOCUMENTS FOR OTHER PURPOSES

As an internationally recognized form of identification, the passport has been used for purposes other than for verifying identity and citizenship at the time of entry or exit to/from a nation. For example, many nations require that persons registering at hotels or establishing temporary residence in an area present a passport to the local government representative or to persons (such as hotel staff) authorized to transmit this information to the local government. As another example, financial institutions and other organizations that require proof of identity often rely upon and require passports when opening accounts.

Recognizing the use of passports for these secondary applications, and also to ensure backward compatibility for border crossings without e-passport readers, ICAO determined that the passport must continue to have a data page that includes the traditional MRZ and the Visual Inspection Zone (VIZ) — that is, information could not be stored solely in electronic format.

Many privacy advocates are concerned about the potential for individuals or organizations who are not directly involved with travel document issuance and inspection to obtain and

use data read from an MRTD. One prime consideration, recognizing this dual use of passports, was the protection of the data on the IC chip. The traveler may not wish for certain enterprises to have copies of his/her biometric data especially where those data may be especially sensitive such as the case with fingerprints. Thus, ICAO recommended that if the Issuing State stores fingerprint or iris data, such data should be encoded in a manner that would require a special 'key' to access the information.

ICAO did recommend that the MRZ data and the photograph be stored on the chip with access available to such secondary users, if the passport booklet has been presented by the traveler for such use (i.e., it must be opened and the MRZ accessed using a special optical reader to retrieve the data). To accomplish this, the ICAO best practice is to use the data access protocol known as Basic Access Control (BAC). This technique uses relatively sophisticated encryption algorithms that require the book to be opened, as authorized by the bearer, in order to decrypt the data held within the passport chip.

ICAO recommends that states storing fingerprint and/or iris data on the e-passport utilize Extended Access Control (EAC), possibly with encryption. The technical details of EAC had not been finally determined by ICAO as of the writing of this paper. Encryption standards would be left to the issuing state.

SECTION 7. DOCUMENT CHARACTERISTICS

The basic MRTD, with its OCR medium, is designed for both visual and machine reading. This feature is essential, since the conversion of travel documents to chip-based (or even OCR-based if the document is not already so equipped) machine readable format can only be made gradually as current travel documents expire and are renewed or reissued, and the introduction of machine readability at border-crossing points is only being introduced gradually according to traffic volumes. The Sixth Edition of Doc 9303 Part 1 specifies the one additional machine reading technology, contactless ICs, for global interoperability that is to be carried out by countries seeking additional storage capacity in their various travel documents; however, in addition, OCR will be retained as the basic technology and is mandatory to ensure global interoperability. ICAO requires Contracting States to issue only machine readable passports starting in 2010.

The benefits of adopting the machine readable formats for passports and other travel documents extend beyond the obvious advantages for States that have the machine readers and databases for use in automated clearance systems. Many developing countries have elected to invest resources in the introduction of MRTDs because the physical characteristics and data security features of the documents themselves offer strong defense against alteration, forgery or counterfeit. Moreover, adoption of the standardized format for the visual zone of an MRTD facilitates inspection by airline and government officials, with the result that clearance of low-risk traffic is expedited, problem cases are more readily identified, and enforcement is improved. The optional introduction of biometric identification with data stored on a contactless IC will provide greater ability to identify imposters and enhance security and resistance to fraud as well as bring greater facilitation for the document holder and international travel.

7.1 BOOKLET FORMAT

The passport shall take the form of a book consisting of a cover and a minimum of eight pages, including a data page containing the holder's personal data and period of validity. To expedite and facilitate inspections, the data page must conform to specific edge tolerance and nominal dimensions and shall be part of the passport cover or an inner page in close proximity to an end leaf, so that inspectors know where to find the page. The VIZ and the MRZ, which contain mandatory elements in a standard sequence, represent the minimum requirements for the passport data page.

Although the material choices are at the discretion of the Issuing State, the physical characteristics of the MRTD must be of sufficient quality to ensure that the document will last throughout the period of validity defined by each State (9303, Part 2). The MRTD shall bend (not crease) and be able to be flattened by a reading device. It shall present no toxic hazards and be resistant to chemical effects and deterioration from exposure to light. The MRTD shall remain machine readable at extreme operating temperatures and relative air humidity. (In acknowledgement of differing national practices, with regard to

temporary and emergency passports, these provisions do not necessarily apply to such documents.)

7.2 BOOKLET COVER

A typical layout for the cover of an e-passport is shown in Figure 5a. Because of the grace periods for the validity of existing travel documents and the varying rates of adoption of the IC chip by member States, there must be an indication on the MRTD of the existence of a data storage technology. TAG 15 recommended that the appropriate place for such an indicator (or logo) is on the bottom of the front cover of the passport below the country crest, and below the word "PASSPORT". TAG 15 voted on designs to symbolize the contactless IC, and the winning logo is shown in Figure 5b. States may also place the logo on the Data Page, and/or near the chip. It was also suggested that States may choose to put some text in their passport pertaining to the presence of a chip and its sensitivity to temperature, moisture, and bending.

Figure 5. a) Passport cover; b) logo symbolizing a contactless IC

7.3 PRINTED PORTRAIT

The 45mm × 35mm portrait displayed on the data page must be recognizable by a human inspector. It must accurately represent the holder and may not be occluded by background security and final preparation treatments and may not contain a border or frame. The portrait must have been captured within six months of the issuance date. The portrait must be a centered, frontal view of the full face, in focus from crown to chin and with both eyes open. The head height must comprise 70 to 80 percent of the portrait height. The full range of portrait requirements is included in 9303, Part 1, Volume 1. The printed portrait on the data page of a passport is not in and of itself considered an electronic biometric identifier. Often, the printed photograph is not of sufficiently high quality for effective

biometric identification due to low printing resolution and, in some cases, personalization printing, in addition to certain security features of the passport, which may obscure or distort the picture.

Additionally, the signature or mark must be displayed in its original aspect ratio so that it is recognizable. A single-digit fingerprint may be displayed in a one-to-one replication of the original print.

7.4 PLACEMENT OF THE IC CHIP

The actual placement of the chip and its antenna within the e-passport is a decision of the Issuing State, and this discretionary placement was a key factor in choosing the contactless form of chip for ICAO standardization. Suggested locations for the IC chip include the data page, center of booklet, between end paper and cover, or on a separate sewn-in page (in which case, it is not to be used as a visa page or travel stamp page). The two basic configurations are illustrated in Figure 6. When the booklet is placed on a flat screen reader, with the data page facing the reader panel, the chip is either on the same side of the fold as the data page or it is on the other side of the fold from the data page. This has important implications for an e-passport reader design.

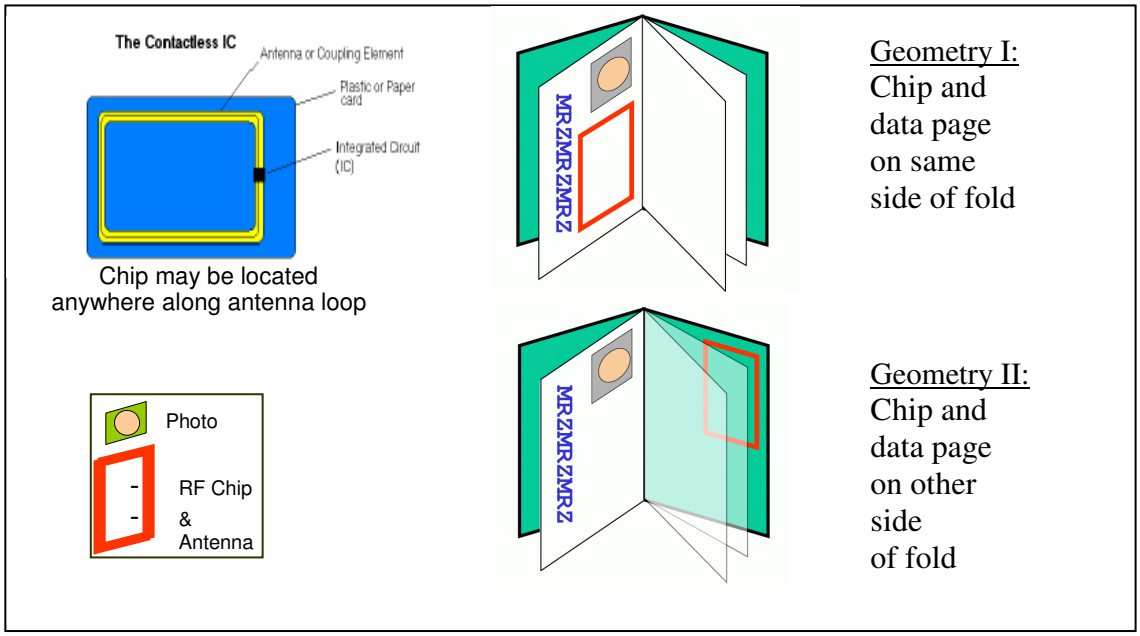

Figure 6. E-passport configurations

Some States have also chosen to shield or encase the Contactless IC in a metal jacket (e.g., aluminum foil) to prevent the chips from being read when the passport is closed. Care must be taken in reading documents that use such shielding. States also need to ensure that

the booklet manufacture process and the personalization process do not introduce unexpected damage to the chip or to its antenna (e.g., image-perforation security features puncturing the antenna; or heat lamination damaging the chip).

SECTION 8. BIOMETRIC DATA FORMATS AND QUALITY

In order for e-passports to serve the requirements of ICAO, the biometric data that is stored in them must be of high quality. This means that there must be common definitions and specifications for the capture and storage of the data. Capture is the automatic acquisition of a biometric sample from the subject via a capture device such as a fingerprint scanner, document scanner, or digital still or video camera. ICAO recognized that if a biometric data sample is incorrectly acquired, its utility is greatly diminished. Certain criteria and procedures for the capture process are needed to ensure that samples are acquired with adequate fidelity and format.

Fortunately, ISO/IEC had been developing a set of standard "Biometric Data Interchange Formats," with a separate section for each major biometric type. The ISO/IEC standards incorporated into the e-passport specifications are:

- Facial Image Format for Interoperable Data Interchange (ISO/IEC 19794-5)
- Iris Image Format for Interoperable Data Interchange (ISO/IEC 19794-6)
- Fingerprint Image Format for Interoperable Data Interchange (ISO/IEC 19794-4)
- Fingerprint Minutiae Format for Interoperable Data Interchange (ISO/IEC 19794-2)
- Fingerprint Pattern Format for Interoperable Data Interchange (ISO/IEC 19794-3)

ICAO has considered whether to store images versus templates on the MRTD. In order to preserve vendor neutrality and backward compatibility, ICAO has made storage of the image mandatory, for each biometric type stored in the MRTD, with storage of an associated template as optional, at the discretion of the Issuing State.

States need to be sure that the data supplied to them is of sufficient quality and integrity to enable accurate verification at their end. Documents need to last up to at least 10 years. ICAO considered the compatibility and ranking of biometric technologies with respect to MRTD enrollment requirements, MRTD renewal requirements, machine-assisted identity verification requirements, redundancy, global public perception, storage requirements, and performance. Face was chosen over finger and iris as the globally interoperable biometric, because, among numerous other considerations, faces are already captured and verified, so there exists legacy face databases, and there would be no changes required for enrollment. Furthermore, faces always acquire and are easy to verify by a human, and children need not appear in person to provide a facial sample.

8.1 FACE

Since the biometric that was accepted for universal use in e-passports was the facial image, considerable effort was focused on this area. ISO/IEC 19794-5 provides a Face Image

Format for face recognition applications requiring exchange of face image data. The typical applications are:

- Human examination of facial images with sufficient resolution to allow a human examiner to ascertain small features such as moles and scars that might be used to verify identity
- Human verification of identity by comparison of persons against facial images
- Computer automated face identification (one-to-many searching)
- Computer automated face verification (one-to-one matching)

8.1.1 Face Image Quality

To enable many applications on a variety of devices, including devices that have limited storage space, and to improve face recognition accuracy, the standard specifies not only a data format, but also scene constraints (lighting, pose, expression, etc), photographic properties (positioning, camera focus etc), and digital image attributes (e.g., image resolution, image size, etc). It is very important that image quality requirements be carefully adhered to and all of those involved in the image capture process, such as photographers, manufacturers of photo-vending machines and others are well informed regarding these specifications.

With respect to e-passports, the face must have been captured within six months of the issuance date and may be in black and white or color. The full frontal face image type is suitable for travel document displayed portraits and storage. It includes the full head with hair, neck, and shoulders and has sufficient resolution for human examination as well as reliable computer face recognition. A variety of considerations need to be taken into account to ensure acceptable image quality. For example, the portrait must be a centered, frontal view of the full face, in focus from crown to chin, with both eyes open. The head height must comprise 70 to 80 percent of the portrait height (ISO/IEC JTC 1/SC 37 N 506).

Adequate and uniform lighting shall be used to capture the full-face frontal pose (i.e., appropriate illumination techniques shall be employed and illumination used to achieve natural skin tones and a high level of detail, and minimize shadows, hot spots, red eye, and reflections, such as sometimes caused by spectacles). Uneven or insufficient lighting can degrade face recognition accuracy. Diffused, multiple light sources can be used to evenly illuminate the face without hot spots or shadows on the face or background. The subject shall be surrounded by a uniform light-colored background.

Because pose and expression are known to strongly affect the performance of automated face recognition systems, the expression must be neutral and non-smiling, with both eyes open and mouth shut, and the rotation of the subject's head must be less than five degrees in any direction (roll, pitch or yaw). While roll (or tilt) is easily corrected using image

processing, similar post-acquisition correction of pitch and yaw are error prone and could introduce substantial distortion to the image.

Because extraneous objects or the absence of facial features can hinder the recognition of expected patterns in face recognition algorithms, obstruction due to eyeglass rims, tint, or glare, bangs, eye patches, head clothing, or eyes closed is not permitted (ISO/IEC JTC 1/SC 37 N 506). The quality of the original captured portrait should be at least comparable to the minimum quality acceptable for photographs, resolution comparable to 6-8 line pairs per millimeter, or 300 pixels per inch (ppi).

Examples of acceptable and unacceptable passport photographs are included in Figure 7. These examples are from *"Guidelines for Taking Photographs to Maximize Facial Recognition Results,"* a report developed originally by Australia that has also been incorporated, in different form, directly into the latest version of ICAO Document 9303.

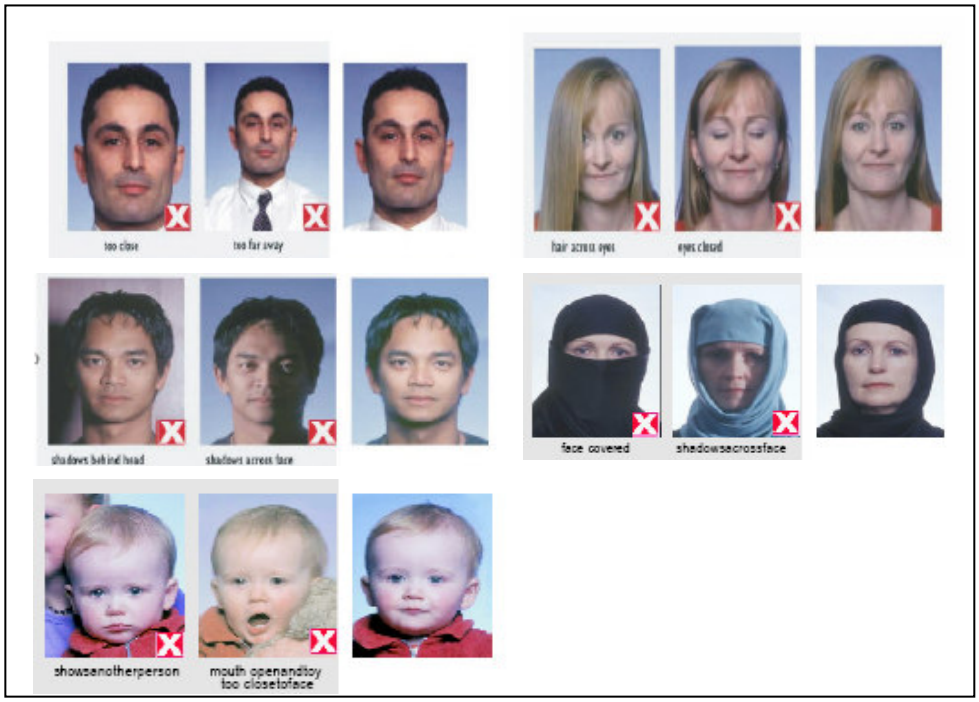

Figure 7. Examples of acceptable and unacceptable passport images

8.1.2 Stored Image Format

The stored image must be identical to the printed image or cropped to enclose the face edge-to-edge and from chin to crown. The facial image shall be stored as a full frontal image or token image in accordance with ISO/IEC 19794-5. Storage of optimally-compressed images is mandatory. The face record format requires that the header and the

entire data structure be CBEFF compatible and the image data be encoded using JPEG[1] or JPEG2000. Compression of the facial image to 15 kilobytes (kB) - 20 kB is recommended for the e-passport. For facial images, an ICAO standard size photograph color scanned at 300 ppi results in an image with approximately 90 pixels between the eyes and a size of approximately 643 kB for 24-bit color.

There should be at least 7 bits of intensity variation, or dynamic range, (at least 128 unique values) in the facial region after conversion to grayscale. The image must reflect natural colors with respect to expected skin tones. The head should be centered in the image with a head width to image width ratio between 5:7 and 1:2. Gradations in skin texture should be visible, with no saturation on the face. There should be at least 90 (and preferably 120) pixels between eyes. The depth of field must be such to maintain better than 2 mm (and preferably 1 mm) of resolution throughout the face—from chin to crown and nose to ears (ISO/IEC JTC 1/SC 37 N 506).

8.1.3 Token Frontal Image

ICAO allows the storage of either the token image or standard full frontal image on the IC chip. A token image is an image that has been adjusted to enable a facial recognition algorithm to operate more quickly— it is *not* a template. The steps involved in the transformation of a full frontal face image to a token image are depicted in Figure 8. Specifically, in the creation of a 240-pixel wide token face image, the original image (a) is rotated to horizontally align the eyes (b). The image is then uniformly scaled so that there are exactly 60 pixels between the centers of the eyes (c). Lastly, the image is translated and cropped (d) such that the first eye coordinate is (89,144) i.e. 89 pixels over and 144 pixels down from the upper left corner of the image (0,0). The black pixels which are padding the borders can be any color, with the best practice being to extend the color used on the border of the original image to the edges of the token image (e).

[1] Joint Photographic Experts Group – a lossy compression technique

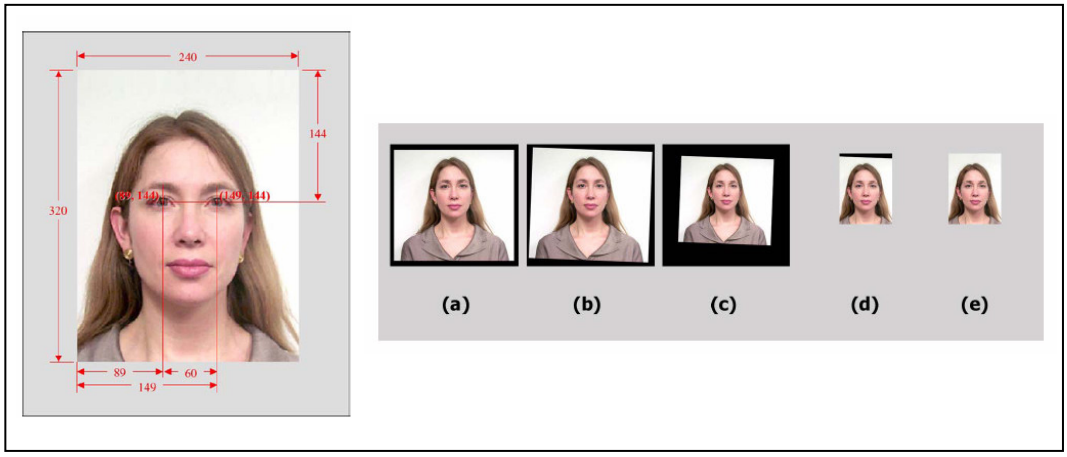

Figure 8. Illustration of the steps in the creation of a Token Frontal Image

8.2 FINGERPRINT

ISO/IEC 19794-4 provides a standard for the capture and transmission of raw or processed fingerprint images to allow interoperability among different implementers and vendors to accommodate images captured from dissimilar devices, with varying image dimensions, resolutions, and levels of grayscale. There are other standard formats used for exchanging lists of fingerprint characteristics such as minutiae, patterns, or other variants, but ICAO requires conformance to ISO/IEC 19794-4.

8.2.1 Fingerprint Image Quality

Fingerprints must be captured in an upright position and centered horizontally in the field of view, scanned left-to-right, flat or rolled. Fingerprint scanners should capture fingerprints at a minimum resolution of 500 ± 5 ppi in both the detector row and detector column directions. Both the white signal-to-noise ratio and black signal-to-noise ratio of the scanner should be greater than or equal to 125. At least 80 percent of the fingerprint images taken with a given scanner must have a grayscale dynamic range of at least 200 gray levels, and at least 99 percent shall have a dynamic range of at least 128 gray levels. Grayscale linearity and uniformity must be verified with test patterns (ISO/IEC JTC 1/SC 37 N 466).

Whatever device may be used for acquisition, fingerprint digital images shall appear to be the result of scanning conventional inked impressions with black ridges. The standard states that a fingerprint quality value between 0 (worst) and 100 (best) must be recorded in the header. Digital fingerprint images must be of sufficient quality for conclusive fingerprint comparison, high performance, and Automated Fingerprint Identification System (AFIS) search reliability. Fingerprint comparison requires a high fidelity image without any banding, streaking, or other visual defects. Finer detail such as pores and incipient ridges are needed along with a sufficient gray-scale dynamic range.

Proper care should be taken in order to deal with people who have abnormal or faint fingerprints. Deterioration of the fingerprints can be due to genetics, disease, or occupation, and both Issuing and Receiving States should have processes and procedures in place to address such cases. Training and information will be essential to prepare staff to deal with these kinds of problems, either at the enrollment station or at border control.

8.2.2 Fingerprint Image Format

Grayscale finger image data may be stored, recorded, or transmitted in either compressed or uncompressed form. Uncompressed images can be recorded in packed or unpacked form. Images with a resolution of 500 ppi (pixels per inch) can be compressed using Wavelet Scalar Quantization (WSQ) with a 15:1 compression ratio or with JPEG at a 5:1 compression ratio. Images with a resolution of 1000 ppi should be compressed with JPEG2000. The optimal compressed size for a fingerprint image was estimated by ICAO to be approximately 10 kB per finger. The pixel depth may range from 1 to 16 bits (ISO/IEC JTC 1/SC 37 N 466).

8.3 IRIS

ISO/IEC 19794-6 proposed a standard for the exchange of iris image information. The standard contains a specific definition of attributes, a data record format for storing and transmitting the iris image and certain attributes, a sample record, and conformance criteria. Currently, exchange of iris information between equipment from different vendors can only be done using a large-scale image of the entire eye, which is expensive in storage and bandwidth. To provide interoperability among vendors, it is necessary to define a standard, compact representation of a human iris.

8.3.1 Iris Image Quality

When capturing an iris image, the head should be held vertical with eyes opened as wide as possible. A pupil diameter of 7 mm or less is desirable, since excessive pupil dilation may affect the quality of enrollment. Eyeglasses, hard contact lenses, and patterned soft contact lenses should be removed. The spatial resolution of the iris imaging system should be at least two line pairs per millimeter (lp/mm) at the object plane with 60 percent modulation. The eye should be illuminated using near-infrared wavelengths between approximately 700 and 900 nm (ISO/IEC JTC 1/SC 37 N 504).

8.3.2 Iris Image Format

The image orientation should be right side up. It can be stored in rectilinear or polar coordinates. Any preprocessing, such as boundary extraction, scan type corrections, assignment of special intensity values to iris occlusions, and orientation correction, should be conducted on the rectilinear image prior to conversion to polar coordinates. The intensity of each polar image sample $p(r, \theta)$ shall be computed using bilinear interpolation. Three levels of image quality (low, medium, high) have been defined for iris images. The minimum requirement is a pixel resolution equal to at least 8.3 pixels per mm. The

optimal compression size for an iris image is 30 kB per eye. If JPEG or JPEG2000 compression is used, a compression factor of 6:1 or less is recommended. The image should have a dynamic range spanning at least 256 gray levels. If specular reflections occur, their intensity should be set to the saturation level. The iris image should have a minimum of 90 gray levels between the iris and sclera and a minimum of 50 gray levels separation between iris and pupil for all color eyes. At least 70 percent of the iris should be visible. The minimum digital iris diameter should be comprised of at least 100 pixels, with 70 pixels between the left or right edge of the iris and the closest edge of the image, and at least 70 pixels between the upper or lower edges of the iris and the closest edge of the image. The iris image should not exhibit effects of optical distortion including spherical aberration, chromatic aberration, astigmatism and coma consistent with standard optical design practices. The signal-to-noise ratio should not be less than 40 dB inclusive of any noise introduced by image compression techniques (ISO/IEC JTC 1/SC 37 N 504).

SECTION 9. DATA STORAGE

9.1 SELECTION OF DATA STORAGE MEDIA (IC CHIPS)

ICAO has determined that the integrated circuit (IC) chip offers the best technical solution for the storage of biometric and other data in an MRTD. Contact IC cards, commonly referred to as "smartcards," are already widely used for varied purposes (e.g., bank and telephone cards). The main disadvantage with contact chip technology is the very explicit placement requirements for the chip in the document which would have required inordinate and generally unacceptable reengineering of the passport blank manufacturing processes. On the other hand, the Contactless IC offers a much more flexible operation with a contactless (RF) transfer of data between the document and the reader, a reasonable amount of data capacity, and a relatively low cost. The Contactless IC can also be produced in a flexible plastic sheet format, so it can be sandwiched or laminated into the cover or pages of an MRP without the explicit positioning requirements associated with contact IC cards.

The Contactless IC chip was determined to be the only Data Storage Technology that meets ICAO's requirements in terms of usability, capacity, and performance.

9.1.1 Usability

Border Authorities have a strong desire for a contactless mode of operation. This data storage technology is the alternative most amenable to the passport booklet format and the easiest for passport holders to manage, because rather than swiping or sensing the electronic data, it is simply retrieved via short-range antennae while the holder places the MRTD on top of a designated reading device. High Density Magnetic Strip, Optical Memory, and Contact IC chips all require direct contact of the technology with a reader. Barcodes require direct, or line-of-sight, contact of the technology with a reader. The only technology that requires neither direct nor line-of-sight contact is Contactless IC Chips.

9.1.2 Capacity

The storage of a high resolution face image, the bearer's biographical data, and document issuer and validity data requires large storage capacity. The minimum size of the JPEG compressed[2] face image that provides high recognition accuracy using contemporary face recognition systems has been shown to be in the interval 12 kB to 20 kB. This need obviates the use of barcodes (typical capacity up to 2.2 kB, though some technologies up to 15.5 kB are available which have potential for deployment in localized travel document applications); and of High Density Magnetic Strip (typical capacity is up to 3,024 bytes

[2] At the time of the capacity analyses, JPEG 2000 had not been authorized as a data compression algorithm; however, it is noted that JPEG 2000 can compress effectively and be used in facial recognition.

gross; 2,328 bytes net of overheads). The only technologies with sufficient capacity are Contact IC chips, Contactless IC Chips and Optical Memory.

9.1.3 Performance

The more data to be retrieved, the slower the retrieval rate for any given technology. The ability to retrieve randomly only the data that is needed, as opposed to serially reading the entire record, also improves performance throughputs. In general, Contactless IC Chip technologies read faster than Contact IC chips. Furthermore, to meet the necessary data retrieval requirements, an operating system on the chip is required, as per ISO/IEC Standard 7816-4.

9.2 IC CHIP REQUIREMENTS

Contactless ICs for use in MRTDs are to comply with ISO/IEC standard 14443 Type A or Type B. The on-board operating system must conform to ISO/IEC Standard 7816-4. The LDS is to be encoded according to the Random Access method with encryption, hashing, and signing. The read range should be up to 10 cm. In accordance with ICAO determinations, the space to encode one photograph plus ancillary data is at least 20 kB; hence, the minimum chip size is 32 kB with the need for high speed of data retrieval. The memory area on a 32 kB chip available to the user is approximately 30 kB.

Issuing States should bear in mind that the new-technology, very high capacity chips (> 64 kB) can have larger overheads in terms of space required for memory management, operating systems and command sets – this can be up to 256 kB for 512 kB and 1024 kB (1 MB) capacity chips. Therefore to facilitate future-proofing and flexibility via high capacity (in excess of 64 kB), it follows that 512 kB or larger is a chip size for States to target towards, guaranteeing 256 kB+ of available user data space that can be used over the life of the e-passport. Data transfer speeds must be carefully considered in terms of the higher capacity chips.

The ISO/IEC standards contain anti-collision procedures that under normal circumstances will overcome problems associated with reading multiple documents within the active range of the machine (RF) reader. Physical interference between the antennae of adjacent Contactless ICs in an e-MRTD may occur, especially if the antennae are the same size and spatial match. In this case, the booklet (if the e-MRTD is an e-passport) must be opened to the page where the Contactless IC is placed in order to eliminate the interference and facilitate reading. The Contactless IC does not need to come into contact with the machine (RF) reader. Contactless ICs can be read within seconds, even in hot, dirty, damp, cold, foggy environments and through material that would be unsuitable for other technologies.

9.2.1 Safety

Under circumstances far different than those for passports, radio frequency waves may have the capacity to cause injury to human beings if the radiation level is too strong. Water or human tissue does not absorb radio waves at 13.56MHz, and the use of this frequency by Contactless ICs complying with ISO/IEC14443 has international acceptance.

The Contactless IC chip also needs to be protected against physical tampering and casual damage including flexing and bending.

9.2.2 Power

More power than the minimum ISO/IEC 14443 specification may be needed to obtain better performance for high capacity data transfer, high speed transactions, and high speed transmission. Given the operating and security requirements for the e-passport chip, the chip will need to be a microprocessor-based chip operating at the mid-power range settings specified in ISO/IEC 14443.

9.2.3 Future Proofing

The data storage medium deployed in an MRTD must last for the life of that MRTD (typically five - to ten years). Advances in data storage techniques, coupled with demand for new multi-purpose applications of smart card technology in particular, have resulted in rapid advances being made in storage capacity and these capacities are expected to continue to increase. Additionally, the speed of data transfer has increased, and continued speed enhancements are another factor in ensuring future proofing.

9.3 LOGICAL DATA STRUCTURE

To ensure global interoperability for machine reading of stored details, TAG/MRTD initiated the development of a standardized organization of data (i.e., LDS) for the recording of details in a capacity expansion technology. As part of that work, unique 'mappings' – ways of storing the LDS - were developed to ensure optimal recording for each capacity expansion technology, as well as compliance with published International Standards specific to that technology. ICAO determined that the predefined, standardized LDS must meet a number of mandatory requirements. It must ensure efficient and optimum facilitation of the rightful holder, protect details recorded in the optional capacity expansion technology, allow global interchange of the data, address the capacity expansion needs of Issuing States and organizations, support a variety of data protection options, allow updating of details, and utilize existing International Standards to the maximum extent possible.

A standardized LDS is required to enable global interoperability. The LDS identifies all mandatory and optional data elements and any prescriptive ordering and/or grouping of data elements that must be followed to achieve global interoperability for reading of details (Data Elements) recorded in a capacity expansion technology (IC Chip). Figure 9 displays the mandatory and optional elements of the LDS.

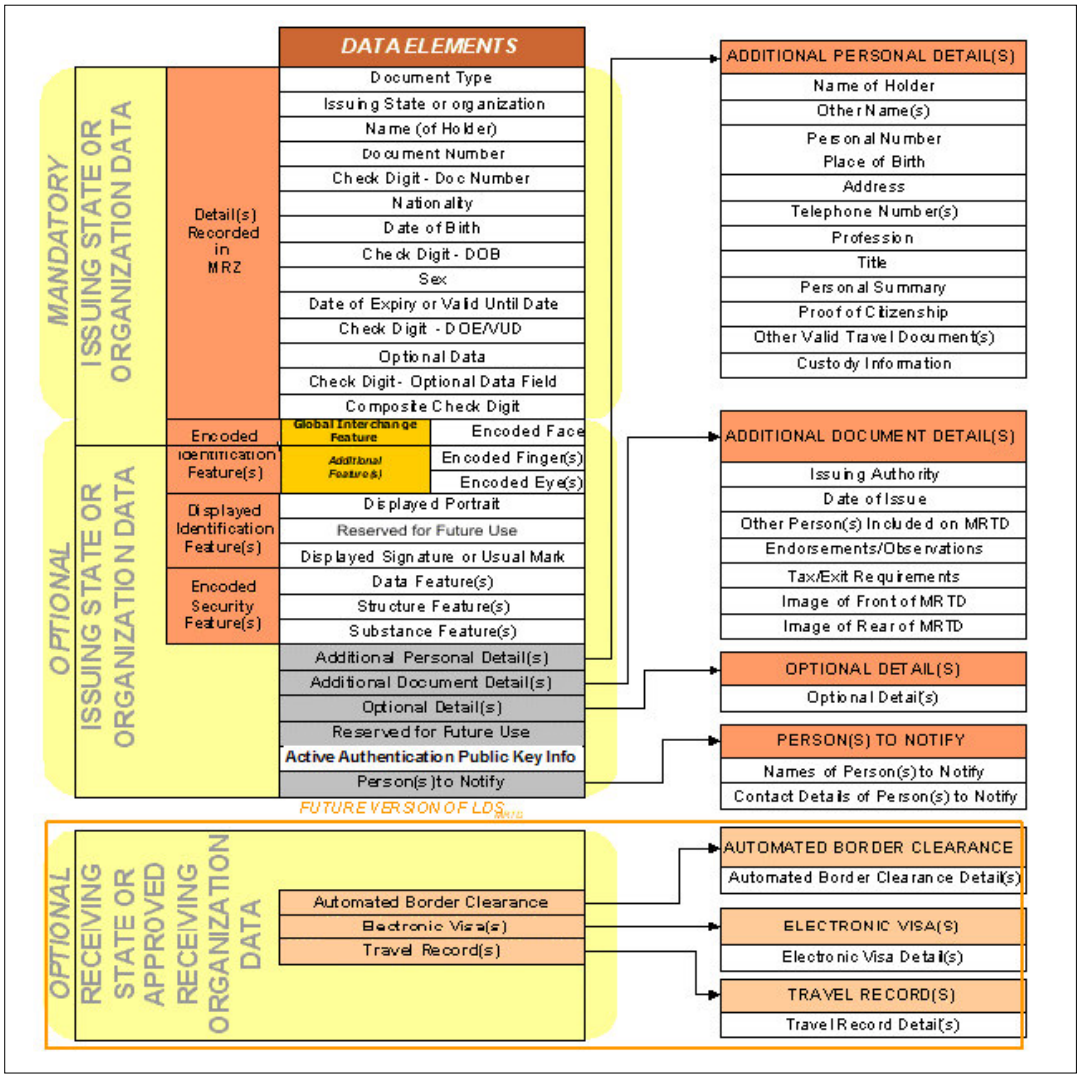

Figure 9. Mandatory and optional elements of the Logical Data Structure

In Figure 9, DG refers to "Data Group." Some data groups may have repeated elements (such as DG3 for fingers). DG1 (information recorded in the MRZ) and DG2 are mandatory. DG2 may be either the displayed portrait or the token image. If DG2 is substantially different from the displayed portrait, the Issuing State may store the displayed portrait in DG5. Otherwise, DG5 need not be encoded. The details of the LDS structure are incorporated into the new version of Document 9303.

To minimize security and data protection complexity, the NTWG has decided for now to not endorse updates of chips in e-passports subsequent to their personalization at the time of issue to the holder (i.e., e-passports will be "write-once"). However, in the future, the LDS may need to support "write-many" applications. While much deliberation will have

to be carried out in terms of the desirability of "write-many" capability, some practical applications for the "write-many" version of the LDS specification will include:

- An Issuing State writing a second biometric measurement into the LDS (e.g., updating a facial biometric as a result of plastic surgery), or adding a different type of biometric at a later date (e.g., future addition of an iris image)
- A Receiving State writing a second biometric into the LDS created by the Issuing State (e.g., adding a verified live image of the passport holder, as captured at an airport)
- Updating visa data
- Updating frequent traveler data
- Storing travel records
- Storing automated border clearance records

9.4 PUBLIC KEY INFRASTRUCTURE

Both the Issuing and Receiving States need to be satisfied that data stored on the IC have not been altered since the data was recorded at the time of issuance of the document. In addition, the privacy laws or practice of the issuing country may require that the data cannot be accessed except by an authorized person or organization. Accordingly, ICAO developed the specifications in Section IV of Part 1, Volume 2 regarding the application and usage of modern encryption techniques, particularly interoperable PKI schemes.

In May 2003, at TAG 14 approved a format for PKI now specified in 9303, Part 1. It provides guidance and advice to States and to suppliers regarding the application and usage of modern encryption techniques, particularly interoperable PKI schemes. The intent of PKI is primarily to augment security through automated means of authentication of e-passports and their legitimate holders internationally.

The NTWG was asked to proceed with specifying the PKI scheme for the MRTD community in more detail and did so with further multilateral work that has been incorporated into 9303, Part 1. The intent of the specifications in this regard is to be as detailed as necessary to enable States to implement the scheme in e-passports offering IC chip read-only access. The aim of the PKI scheme, as described, is mainly to enable e-passport-inspecting authorities to verify the authenticity and integrity of the data stored in the e-passport. In conjunction with the LDS, the PKI specifications are intended to outline how data integrity and data privacy are to be achieved in the context of biometrics deployment in MRTDs.

Authentication, or the ability to confirm that the LDS was created by the Issuing State, is maintained by using PKI, where public keys are issued in certificates which are digitally signed by trusted issuing organizations called Certificate Authorities (CAs). Certificate Revocation Lists (CRLs), which indicate if a key (certificate) has lost its validity, will be

necessary. For passive authentication, the Issuing State must digitally sign a Document Security Object (SOD) on the chip, which, to ensure data integrity, contains hashed representations of the LDS contents. It is recommended that Issuing States use secure hardware devices (known as Secure Signature Creation Devices or SSCDs) for signature generation. The SSCD generates new key pairs and 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, electromagnetic emission, fault injection) and attacks against the random number generator, it is recommended to use SSCDs that are successfully certified/validated under a Common Criteria Recognition Arrangement (CCRA)-compliant certification body, according to a suitable Common Criteria Protection profile as covered in the PKI segments of 9303, Part 1.

To protect against chip cloning or substitution, an Issuing State may chose to implement Active Authentication. This optional mechanism operates by means of a challenge-response protocol between the inspection system and the chip. For this purpose the chip contains its own Active Authentication Key pair. The Active Authentication Public Key is stored in Data Group 15 and the corresponding Private Key is stored in the chip's secure memory.

9.5 ACCESS CONTROL

The chips chosen by ICAO for use in e-passports can be read effectively up to 10 cm of distance. With special equipment, this distance, under certain circumstances, can be increased a bit. This raised the possibility that a person holding an e-passport may be subjected to having the data from the e-passport read surreptitiously, perhaps by another person standing nearby. This may or may not be viewed as a problem. While it is possible under certain very definitive circumstances and using highly specialized equipment to access the chip, measures are outlined in the following specifications to address unauthorized access and to protect data.

9.5.1 Basic Access Control

To protect the data on the chip from being read surreptitiously, Basic Access Control (BAC) can be used and is specified as an ICAO best practice. BAC is a challenge-response protocol where a machine (RF) reader must create a symmetric key by hashing the data scanned from the MRZ in order to read the contactless chip. BAC prevents skimming, because a remote reader will not be able to access data on the passport without the passport being physically opened and scanned.

Another privacy concern is eavesdropping, where data from an IC chip is intercepted by an intruder while it is being read from an authorized reader. BAC prevents eavesdropping by encrypting the communication channel through its *secure messaging* feature, which

encodes the messages between the reader and the chip in a manner that requires knowledge of the 'key' derived from the MRZ to decipher.

9.5.2 Extended Access Control

The only data groups that are required on the chip of an e-MRTD are DG1 and DG2 (the MRZ information and the facial image). ICAO recommends that Issuing States placing additional biometric information on the chip restrict access to this data, which can be accomplished using Extended Access Control (EAC) or Data Encryption.

SECTION 10. OPERATIONAL CONSIDERATIONS

10.1 ISSUANCE AND INSPECTION

The ICAO NTWG acknowledges that issuance is a State responsibility, but inspection requires interoperability between States. This interoperability requires consensus on MRTDs in terms of both technology choices and operations. Beyond the choices of technology, interoperability requires adherence to agreed upon standards, security of systems and data, and agreement on legal and privacy issues. Integrity of each State's issuance systems is critical to providing a basis for reliable identity management and achieving interoperability during inspection.

The rationale for selecting facial recognition as the globally interoperable biometric was the acknowledgment that a large amount of legacy photographic information – some already digitized – existed to support the use of facial recognition. Facial recognition lends itself very well to ease of enrollment from both legacy photographic information and in-person enrollment. A human face always is acquired during enrollment, and people need not be present to be enrolled as this can be done from photographs or other digitized photos. Lastly, operational considerations benefit from the use of facial recognition, as human inspection of the credentials is possible. For border control authorities, this is an important consideration, as manual inspection is a reality in many border crossings. Additionally, criminal watch lists are largely circulated in photographic form, and having travel documents using the facial biometric matches this format. Other biometrics utilized with MRTDs can be utilized if there are bilateral and/or multilateral agreements between and among States

For some States, computer assisted inspection is desired beyond human inspection of travel documents. PKI must be utilized by an issuing State when issuing e-passports, and of course must conform to standards to ensure interoperability. It is a State's responsibility to handle the internal distribution of Country Signing CA Certificates (CCSCAs), Document Signer Certificates, and Certificate Revocation Lists (CRLs) to the State's inspection systems.

Interoperability requirements for inspections are focused on the operations. MRTDs must meet several requirements. An inspection station must have an MRZ reader to derive the Document Basic Access Keys (KENC and KMAC) from the document. Computer-based inspection systems should ensure data security through encryption for the communication channels. For example, if an inspecting State elects to utilize PKI technology, the inspecting State will require knowledge of PKI key information from the Issuing State. Information, such as the issuing country's Signing CA Certificate, must be stored in the "inspecting" State's inspection system. PKI assures the data integrity (i.e., no tampering) and validates the issuing authority. This complements the use of biometrics, which validates the presenter of the MRTD, completing a chain of trust from issuance to inspection.

ICAO has made several recommendations concerning border control inspections. States are encouraged to use biometrics to establish or validate identity at border control points using one-to-one verification systems with future growth into one-to-many systems as appropriate. If biometric verification is negative, meaning identity was not confirmed, the traveler may be sent to a secondary, detailed inspection. These inspections would be "three-way" visual comparisons of the MRTD holder: printed portrait image on the data page, stored digital record read from the IC chip, and stored digital record from a central database. These biometric checks, including other biometrics beyond facial if presented, would be captured at the inspection point of the border control facility. Standard Operating Procedures would need to be developed to handle failures of IT systems, verification software errors – and standing procedures to deal with liveness checking and detection of spoofing. The result of these enhancements would transition border systems from merely processing entrances/exits to automated identity verification systems to uncover fraudulent identities and fraudulent travel documents. Lastly, ICAO recognizes that a large amount of legitimate business is conducted across borders, requiring regular, prompt service to not negatively impact these activities. Any "pre-entry" systems, such as APIS, should be utilized as part of the processing strategy.

10.2 RISK MANAGEMENT

Risk management includes data accuracy concerns, data/privacy security, and operational considerations. The risk of implementing complex biometrics-based systems to current operations can be significant. The accuracy and security of data suggests the strong need to properly design, test, and deploy new issuance and inspection systems to obtain the desired result at points of service. A system that produces many false rejects slows legitimate travel and business – perhaps prohibiting entry to a State to the detriment of both States. This imposes a greater cost to businesses and lost opportunity cost of commerce.

A set of strong Standard Operating Procedures, with robust contingency plans, must exist to deal with inspection cases that result in denials based on failed matching of biometric data. Inspectors must have additional means to distinguish between correct rejects and false rejects from a biometric verification system. Also, these contingency plans must exist to ensure that PKI systems remain online and functional to support inspections. Prompt resolution of these situations is critical to the proper functioning and confidence in these systems.

Adequate protection of information technology systems used for issuance and inspection from cyber attacks of any nature must be sufficiently robust to provide a high level of confidence that they cannot be compromised. Additionally, verification of the competency and integrity of individuals involved with the deployment, maintenance, and administration of these systems must be validated. A strong counter-intelligence system using both computer technology techniques and human behavior analysis should be in place to quickly determine when a breach of security has occurred.

10.3 DATA SECURITY, INTEGRITY

Many States have a legacy database of facial images captured as part of the digitized production of passport photographs that can be encoded into facial templates and verified against for identity comparison purposes. If interoperability includes sharing of templates, then States will have a large vested interest in ensuring data security of their citizens' images and biometric templates in other State systems, and pertinent State laws will require compliance or modification.

The IC chip technology makes uses of wireless technology for contactless operation. Now, in addition to securing existing database and telecommunication technologies in the issuance, inspection (operations), and storage modes, States are required to address the security of information stored on an IC chip which has data security implications in the operations mode. The chip, when used along with a host of other security measures such as those intended to protect the document itself, provides an added dimension to enhance data security and overall protection of the document.

Counterfeiting involves the creation of all or part of a document which resembles the genuine MRTD with the intention that it be used as if it were genuine. Counterfeits may be produced by attempting to duplicate or simulate the genuine method of manufacture and the materials used therein or by using copying techniques. Greater detail concerning methods of preventing counterfeiting of documents can be found in the Informative Annex of ICAO Document 9303. Some methods needing consideration include “fusion readers” that read the Data Page in addition to the Contactless IC chip, making counterfeiting more difficult as both would need to be altered. The security of the Contactless IC chip requires security against logical tampering – including protection, encryption, and authentication of the data. Several methods being evaluated include cryptographic check sums – which is the current recommended strategy, since it has been determined that LDS data such as the MRZ and facial images are not to be encrypted. Digital watermarking is an approach being considered, but the proprietary nature of the approach makes a globally interoperable approach difficult. Another approach requiring a unanimous agreement to the technique would be the use of a unique chip serial number that would be tracked to prevent cloning of chips.

The contactless chip has several mandatory requirements for the standardized LDS. A single LDS has been agreed to by all States to permit common usage among all inspections systems reading e-MRTDs. This LDS is architected to allow for some optional storage requirements. Additionally, future technology advancements in capacity and usage can be made without changing the structure of the LDS. The overriding purpose of the LDS is to ensure efficient and optimum facilitation of the rightful holder when the MRTD is used during inspection.

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

and offered for inspection. Other data, including biometric data, may be present in the e-MRTD. Issuing States may elect to limit access or encrypt this data.

PKI offers a solution to protection of data privacy and integrity by the use of cryptographic methods of authentication and data encryption using symmetric and/or asymmetric public/private keys. This requires an investment of systems, people, and integration into current operations, which is not a trivial task. The combination of encryption, checksums for integrity checking, and the validation of the current status of the issuance provides strong mechanisms to enhancing the trust in a biometrically based inspection process.

PKI must be used to ensure that the IC has not been altered since issuance of the document by matching the checksum of the written data. Cryptographic Threats require minimum key lengths and perhaps expansion of these lengths in the future. The recommended minimal key lengths have been chosen, so that breaking those keys requires a certain (assumed) effort, independent of the chosen signature algorithm. 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 and neural networks) 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 e-MRTDs often for reasons mentioned above.

10.4 PRIVACY

ICAO requires a minimum set of data elements to be present on MRTDs. In the Berlin Resolution of 2002, it was agreed that facial photographs do not disclose information that the person does not routinely disclose to the general public. States may elect (but are not required) to collect other biometrics and information. This puts the burden on countries to ensure that their processes for collecting and distributing data meet the guideline of not disclosing information that is not routinely disclosed to the general public. The photograph, or rather an individual's facial image, is already collected and verified in the MRTD application and is socially and culturally accepted internationally. Since the public is already aware of its capture and use for identity verification, it is deemed acceptable. Additionally, the enrollment of a facial biometric is non-intrusive, as there is only non-contact, minimal interaction of a user with an acquisition system.

Another privacy concern is the possibility that data on the chip could be skimmed or read surreptitiously. Eavesdropping (i.e., clandestinely listening electronically to the communication while the chip is being accessed by an authorized reading device) is also a concern with Contactless IC chips. With Contactless IC chip on the MRTD, any unencrypted data can be eavesdropped within the range of several meters. Issuing States may elect to implement an access control mechanism to eliminate eavesdropping and

skimming. Moreover, the electromagnetic generator in the reader would need to remain within a few centimeters of the e-passport to power the chip and maintain the communication.

10.5 PUBLIC PERCEPTIONS/OUTREACH

There are many layers of public perception that should be recognized and taken into consideration. States are strongly urged to develop and employ means to communicate the purposes and processes of the biometric and associated systems used.. Biometrics in general is new technology to the public's awareness. Many individuals do not understand how it works, what are the costs and risks, and most importantly – what are the benefits.

Within biometrics, there are different issues among the different types of biometrics. According to the Berlin Resolution, the facial image is already socially and culturally accepted internationally. The public is already aware of its capture and use for identity verification purposes. However, not every culture in the world fully embraces the use of photography. Some cultures, although a small minority in the world, have strict prohibitions against capturing images of individuals for religious or societal reasons. In the Islamic world, women are required to wear a headdress at all times, making enrollment of this biometric during issuance or capture at inspection for identity verification difficult. For other biometrics, the public perceptions have other issues. For example, fingerprinting has long been associated with tracking and monitoring criminal activity.

The merging of biometrics into travel documents changes the travel landscape for everyone crossing State borders. Individuals will be better served by understanding the cost and benefits to the merging of biometrics and cryptology software within their travel documents. The benefits of ensuring personal privacy of the personal information on the Contactless IC chip can help individuals understand the need for cryptology on the chip.

10.6 ENVIRONMENTAL/ACCESSIBILITY

Environmental considerations exist with both the issuance and the inspection phases of e-MRTDs. For enrollment, it is more likely that a State will easily be able to field an enrollment station with the proper environmental controls. However, if a State elects to enroll facial images from legacy databases of digitized passport photographs, the environmental conditions may vary widely within the databases leading to some operational issues. For inspection, a greater variety of operational considerations regarding ambient environmental factors such as lighting, temperature, humidity, among others exist.

Different biometrics pose different problems for capture. Face recognition requires good lighting and attention to human factors issues regarding capturing the subject's face image without any obstructions such as head coverings, hair, hats, sunglasses, or other items which may shield the face from the camera. For fingerprint biometrics, temperature and humidity must be within a certain range to produce the best results. Additionally, with current technology, a clean fingerprint sensor surface is necessary in order to achieve

optimal performance in matching captured fingerprints against fingerprint templates stored on the IC chip in the e-MRTD.

The communication between the IC chip and the reader could be susceptible to electrical interference when being read at the inspection point. Damage through normal usage of the e-MRTD could also interfere with the electrical operation of the IC chip.

With the right environmental conditions, enrollment and inspection can be facilitated by improving accessibility for holders of the e-MRTDs. Specifically during inspection, the potential exists for speeding the process of verifying identity and checking electronic records. It is even conceivable to have unmanned stations with automated inspection of e-MRTD, providing appropriate physical access control devices and appropriate contingency plans for handling exceptions or problems.

10.7 SOCIOECONOMIC

Fundamental changes to the technology utilized in MRTDs and the resulting impacts to operations, data integrity, and privacy have impacts in the socioeconomic realm. These changes require expenditures of time and capital. The interoperable nature, being a goal of these implementations, requires a great deal of negotiation and compromise between individual States. The positive result of these programs can result in a changed landscape for travel that ideally improves security via identity verification and speeding transaction time during inspection while solving the issues of data security and privacy. Even with the best possible result being achieved, there will a transitional period where States and individuals become accustomed to the new methods to inspect travel documents and handle the related issues that come with increased efficiency of biometrics and information technology improvements.

One area that has the potential for contention is the potential "digital divide" between nations that can move forward on every "mandatory" requirement and even adopt many of the "optional" requirements issued by ICAO. Some States may elect to operate on this leading edge, while other States may not have the resources or expertise to keep pace. The cost of producing e-MRTDs may be no greater than that of producing conventional documents, though the cost will be higher when biometric identification and electronic on-document data storage become involved.

As traffic volumes grow and more States focus on how they can rationalize their clearance processes with the employment of computerized databases and data interchange, the MRTD will play a pivotal part in modern, enhanced compliance systems. Equipment to read the documents and access the databases may entail a substantial investment, but this can be expected to be returned by the improvements in security, clearance speed, and accuracy of verification which such systems provide. If the gap between the leading and trailing States grows too large, it will be difficult for trailing States to realize the benefits of the modern, enhanced compliance systems. The cost of not participating in those "modern" implementations may drive commerce and tourism away from these "lagging"

States towards States that can afford to make these investments and see them through to completion where the value is realized.

10.8 FACILITIES

Issuing States will be required to build and maintain appropriate facilities for issuance systems, applicant enrollment, and safe storage of the associated data. When a State elects to implement PKI, equipment and facilities to receive, store, and transmit information securely are required. Additionally, the telecommunications necessary to support the deployment and operations of the associated digital systems will for many States necessitate a very significant investment.

For border crossing and enrollment and issuance stations, unique challenges exist regarding predicting traffic levels. For land border crossings where many people cross regularly for commuting purposes, several people may travel in the same vehicle. Additional equipment, such as MRTD OCR-B and/or e-passport readers, may need to be acquired and deployed in existing facilities.

10.9 LEGAL

Several new legal issues have emerged with the changes in MRTDs. Many States have unique laws requiring different approaches regarding privacy. This can come into conflict with the interoperability requirements of MRTD – specifically as biometric data, associated with individuals' names and other personal data are stored in information systems around the world. Law Enforcement groups may have access to digitized travel document information, and differences may exist between States regarding the privacy of such information.

SECTION 11. INTEGRITY OF ISSUANCE SYSTEMS

Each Issuing State is responsible for ensuring that the data that it enters into passports meets or exceeds ICAO specifications. For biometric data, the optimal method to do this is to perform quality analysis at the point of data capture. This may be feasible for certain nations when the applicant must appear in person to submit an application at a central facility. An important point to remember is that not all quality analysis programs are truly predictive of *matcher performance*. ISO/IEC has not yet adopted a standard metric for quality measurement, and thus, such a metric cannot be incorporated into ICAO standards. It is nonetheless encouraged that Issuing States examine each biometric data sample to determine *conformance* to the ICAO specifications to the maximum extent possible prior to issuing the e-passport.

The issuance system should incorporate quality control measures to ensure that supplied face photographs are on photo-quality paper and are compliant with the standards, and that they do not appear to be older than six months. Such quality control could be a combination of human visual inspection and automated image quality assessment software. Assurance is also needed at the issuance stage to make sure that the data on the chip is readable. After personalization of the Contactless IC and completion of printing of the MRTD, the IC chip should be read by a machine (RF) reader, before the MRTD is issued to the holder.

11.1 BREEDER DOCUMENTS

A subject's identity is typically established when the person is registered in the system through the use of breeder documents, such as birth certificates and citizenship certificates. The fundamental integrity of an issuance system depends upon verification of the authenticity of such breeder documents. This is a very difficult problem considering the wide range of breeder documents issued by various States. This limits the ability to standardize an inspection or validation of documents used to populate a travel document. Additionally, the importance of associating and verifying biometric data when these documents are originally issued relies on accuracy of biographical data presented at that time. Special care should be taken to guarantee the validity of breeder documents to avoid the issuance of passports or any official identity document to those who may be attempting to obtain them fraudulently.

11.2 HUMAN RESOURCES

The new initiatives being advanced by ICAO will impact the human resources required for States' issuance and inspection procedures. First, the number of individuals assigned to support these new initiatives will likely grow. Staff with information technology skills will be required to examine the ICAO standards, compare against a State’s current installed infrastructure, and develop architecture plans to meet these new objectives. Varying levels of staff will need knowledge in the areas of telecommunications, biometrics, cryptology,

and systems engineering, supported by project management and policy offices. In addition, as should be the case presently, security offices should perform background checks on staff implementing, managing, and using these new systems. Moreover, checks may be needed on citizens when applying for travel documents to verify questionable breeder documents. Enrollment of citizens' biometrics may require full time staff to prepare that part of the machine readable document.

The collection of biometric samples on a very large scale, such as during the enrollment for passports, visas, or government ID cards, is an unprecedented task, requiring skills and experience that depend greatly on the biometric selected and the public's perception of the purpose of the collection. The interaction of the staff with the public (at enrollment, border control, or other type of station) can create stressful situations, due to difficulties associated with the biometric sample collection process itself, with language barriers, or with queue lengths. Proper care and attention should be taken by States and authorities in order to prevent such stress through proper training of the staff.

For internal control purposes, biometrics can also be used for the issuance staff to confirm that such individuals 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.

11.3 MULTILATERAL COOPERATION

Multilateral cooperation is a critical component to advancing the goal of interoperability. For many items, consistent, homogeneous configuration, operations and policy must be in place to realize the gains of this goal. However, with many varying concerns and issues put forward by States, it is obviously a difficult objective.

The TAG 15 key consideration includes "global interoperability" - the crucial need for specifications defining how the biometrics deployed are to be used in a universally interoperable manner. For PKI, multilateral cooperation is absolutely necessary for the technology to deliver the benefit of verified information. 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 program 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 countries at any time. Issuing States can revoke certificates in case of an incident (like a key compromise). Such a revocation must be communicated bilaterally to all other participating States and to the ICAO Public Key Directory within 48 hours. In order to efficiently share the Document Signer Certificates (CDS) of all States, ICAO will provide a Public Key Directory (PKD) Service to all participating States. This service shall accept information on public keys from all States, store them in a directory, and make this information accessible to all other States.

The ICAO PKD will be the primary distribution mechanism for all these Document Signer Certificates (CDS) and so must 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 (not being participating States) that need this information for validating the authenticity of digitally stored MRTD data.

11.4 INDEPENDENT ASSESSMENT/AUDITING

For many of the facets of MRTD-issuance process, independent assessment must be made to verify that security standards are maintained. For PKI, this is absolutely required to ensure the "confidence" in the system. Today there are no mandates or mechanisms to perform audits and to assess a State's compliance with ICAO initiatives.

However, observations and measurements can be made from the outside. For example, statistical sampling to determine a "rate of fraud" can provide an indirect level of assessment of the reliability of systems and processes.

SECTION 12. IMPLEMENTATION STRATEGIES

12.1 CONTACTLESS IC READERS

The radio frequency (RF) reader provides the power for and communicates with the Contactless IC by means of radio waves. The RF reader contains a high frequency module for transmitting and receiving data, a control module, and an antenna (or coupling element) to connect to the Contactless IC. The RF reader will also usually have an interface to allow it to communicate with a computer system.

Since water or human tissue does not significantly absorb radio waves at 13.56MHz, which is the frequency used by ISO/IEC 14443, the presence of human beings, body parts such as hands, or moisture, in the region between the Contactless IC and the machine (RF) reader will have no adverse impact on the operation. However, the radio waves are sensitive to the presence of metal parts. Encasing the Contactless IC in a metal jacket (e.g., aluminum foil) will prevent reading. Care must be taken in the placement of the machine (RF) reader relative to adjacent metal parts. Because inductive coupling decreases with the sixth order of distance, adjacent systems or other external noise sources are unlikely to adversely affect the reading operation.

There is no standard for a PC to interface to a Contactless Reader. A new Task Force of ISO/IEC SC17/WG4 is working on a standardization of the interface in order to allow a wider selection and easier change-over of card readers and to remove the need for rewriting the interface software each time a different reader is used. Personal Computer/Smart Card (PC/SC) Specification version 2 now contains support for a contactless interface (www.pcscworkgroup.com).

12.1.1 Power Consumption

Early testing revealed that more power than the minimum ISO/IEC 14443 specification may be needed to obtain better performance for high volume data transfer and high speed transactions and transmission. The *Guide to Interfacing e-MRTDs and Inspection Systems* recommended that e-passport readers support a minimum bit rate of 424 kbps to allow greater data throughput. *The Guide* states that the e-passport chips must support 106 kbps (to be compatible with ISO/IEC 14443) but must also support the higher bit rate of 424 kbps. Support for yet higher rates, such as 848 kbps, was noted as highly desirable. The *Guide* addresses field strength issues, noting that in the prototype stage, some chips require more than the minimum of 1.5 Amperes per meter (A/m) to operate, and may require as much as 4 A/m; however, the *Guide* also states that chip manufacturers are to conform to the standard, viz, chips shall operate within field strengths from 1.5 A/m – 7.5A/m.

The outcome of the e-passports/WG8 London Meeting (June 17, 2004) was the following endorsement: “e-passport chips shall support entire power range 1.5 to 7.5 A/m, but to be

on the safe side, e-passport Readers shall supply a field level as much as possible higher than 1.5 A/m to give energy to the present chips in existence."

12.2 INTEROPERABILITY

Interoperability tests carried out in Canberra (AUS), Morgantown (USA), and Sydney (AUS), and Mock Port-of-Entry (POE) tests conducted at the Baltimore-Washington International Airport (BWI), in Tsukuba (Japan), Singapore, and in Berlin (Germany) were held to confirm the progress of reader manufacturers towards achieving global interoperability for the reading of e-passports, based on the specifications set out in the published Technical Reports and other ICAO documents. The results of some of these earlier tests were considered at the ICAO TAG-NTWG meeting in Auckland in December 2004. NTWG concluded that global interoperability for the reading of e-passports had not yet been achieved, and that the necessary functionalities of inspection (border clearance) systems proved insufficient to support the variety of options that may be present in e-passports. NTWG decided that an elaboration of the specifications in the form of a Guide would accelerate the realization of global interoperability for the reading of e-passports. The "*Guide to Interfacing e-MRTDs and Inspection Systems"* was developed as a result.

12.3 TESTING

An Issuing State should conduct three types of tests on e-passport prototypes prior to issuance, specifically:

- Conformance testing - designed to determine whether the chip, inlay, passport paper, inks, bindings, and other components adhere to the specifications outlined in ICAO Document 9303.
- Durability testing - designed to determine if the passport and its components will survive normal rigors of use during its expected lifetime.
- Performance testing - designed to determine whether the e-passports actually can function properly in an inspection environment.

12.3.1 Conformance Testing

The NTWG felt that testing and evaluation of the standards was imperative to ensure that there were no errors or omissions prior to large scale deployments. At its meeting in Glasgow (October 2003), the NTWG brought industry experts together to ensure that the basic structure defined by the NTWG for e-passports was feasible and practical to implement. The consensus from the industry was that since ISO/IEC 14443 was followed, there should be no problems with interoperability. That is, that a chip manufactured by one company can be read by a reader manufactured by another. This would also mean that readers would be capable of reading both 'Type A' and 'Type B' 14443-compliant chips.

Australia hosted the test session in February 2004. The results showed that interoperability did not exist. There was an almost total lack of ability for readers to handle chips with which they were not specifically designed to work, because most applications up until that date had been "closed systems." That is, the chips were used in a single system that employed readers designed to work with them. The chips were not expected to operate in other systems. At the February session, it was also determined that some manufacturers were interpreting ISO/IEC specifications in different ways.

After a series of joint ICAO-ISO/IEC meetings, culminating in a meeting held June 17, 2004 in London, most of the apparent technical issues and specifications were resolved. At that meeting, the US representative from the Department of Homeland Security offered to host a testing session in July for manufacturers and integrators to come together and test whether their interpretations of the standards were, indeed, similar and would allow for interoperability (the ability to have an e-passport produced for one nation read by readers produced by other companies and placed at various locations around the world, and for the readers to read all of the e-passports presented to it). These tests were conducted in Morgantown, West Virginia, USA.

This session provided an opportunity for organizations involved in the production of e-passports and in the development of equipment to access the information from e-passports to come together in a non-competitive environment in order to work towards establishing interoperability of their products. Approximately 130 persons from 18 nations, representing over 50 organizations, were present. Chip and passport integrators provided 128 prototype samples for use in testing chip and passport readers. By the end of the session, the participating organizations were able to establish basic interoperability for a broad set of prototype e-passports and readers.

Australia hosted another test session in August, which was followed by subsequent sessions in Japan, Singapore, and Germany. Each of these sessions offered chip makers, booklet assemblers, operating system coders, reader manufacturers, and governments the opportunity to work together to solve the problems associated with ensuring that e-passports and their readers would work together.

This or a similar approach is considered an integral part of each nation's acceptance tests prior to public issuance of e-passports. Separate from the e-passport specifications, interoperability tests in Canberra Australia (February 2004) and Morgantown, USA (July 2004), as well as the Mock POE simulation hosted by the United States in December 2004 at Baltimore, highlighted the need for commonality in e-passport reader requirements. At the December 2004 meeting of the NTWG in Auckland, New Zealand, the NTWG authorized a special work group to specify these requirements. The resulting document was: "Guide to Interfacing e-MRTDs and Inspection Systems" (February 2005). Those specifications are *not* included in Document 9303, since they do not refer directly to the production of the e-passports themselves, and should be referenced separately.

12.3.2 Durability Testing

Contactless ICs store the data as electrical charge which has the possibility of leaking away, causing data loss. Usually, the electrical charge is refreshed through the use of the Contactless IC by placing the passive device in an active field. It has been found that Contactless ICs will store their charge for at least ten years at 25ºC, and thus will last for the maximum ten-year lifetime of an MRTD. Manufacturer's specifications should be consulted for exact information on data retention.

Most chip applications assume a chip/smartcard validity of two to three years – how such technology will perform over a passport life of five to ten years is yet to be tested in real world applications, as the technology typically has not been deployed with consumers for that length of time. Simulated document aging tests will be needed to assess the durability of e-passports. Because the survival rate of actual e-passports is unknown, some nations have shortened the length of a valid passport to account for the possibility of chip/antenna failure before a full ten-year period has elapsed.

12.3.3 Performance Testing

The two main performance indicators pertaining to IC chips in MRTDs are functional (memory size, security) and operational (range, communication reliability, and speed). Tests designed for the e-passport should assume that the passport book is placed flat on the reader (passport thickness $\leq$ 2 cm); read rate $\geq$ 424 kbps; at least 17 kB of data should be read in test scenarios; the size of end-user chips will likely be $\geq$ 64kB; and LDS DG1 and DG2 will be read at a minimum.

Systems must be able to handle chip operating system, host operating system, and card edge issues (drivers, interface, and synchronization). The interface between the reader and the e-passport chip must be independent of the PC-reader interface.

Readers need to poll for both Type A and Type B chips. Physical and logical anti-collision processes are necessary due to the possibility of multiple chips being present in one passport (e-passport chips must comply with the ISO/IEC 14443 standard for collision detection).

12.3.4 Mock POE Test

The primary goal of the U.S. December 2004 Mock POE test was to determine the operational impact of using new equipment capable of reading e-passports on the primary inspection process. A key insight gained by that exercise was that if technology does not enhance or improve the existing process flow, new reader technology solutions will not be well received by the POE officer/inspector community. In order to conduct the test, sample e-passports were provided by manufacturers using consistent data for 13 test subjects. Legacy travel documents were used by test volunteers. The test included national representatives with sample passports from United States, Sweden, Germany, Australia, France, Belgium, New Zealand, Italy, and Japan.

Inspectors manned the stations using standard procedures, with the only exception being the introduction of e-passport reading capabilities to the process. The following findings emerged from the test:

- The system must be capable of handling both legacy documents and e-passports at the same station (since a family may be comprised of persons holding both types of documents).
- The inspector should not have to perform a 'special' process in order to use e-passports. The reader should be able to detect an e-passport automatically and access the data in an appropriate manner.
- Ergonomics are a key factor for the inspector. The unit must not be too large to fit effectively in the inspection booth. Access to it must be in a natural, non-awkward way.
- The reader should be able to access the chip regardless of where it is placed in the booklet without the inspector having to manipulate the placement of the booklet on the reader.
- If the read access time is perceived to be too long, the inspector may inadvertently break communications by removing the booklet prematurely.

The capture of photographs for automated comparison against the e-passport stored image was also examined. Several different configurations were tested. A key result was that the system should capture an image with as little interaction needed on the part of the inspector as possible. The abilities of various inspectors to capture a good photograph varied considerably. Traveler-operated capture systems fared poorly. Quality control analysis of the photographs was deemed essential.

12.3.5 Live Tests

The Mock POE test was followed by a 'live test' involving the US, Australia, and New Zealand. This occurred in June-September 2005 at Los Angeles and Sydney airports. Non-BAC passports were issued by the three participating nations to airline crew flying between these airports. A key factor that emerged from this test was the importance of training for the inspectors. It was important to note that by this time, sufficient interoperability had been achieved for the test to proceed.

A second live test involved the US, Australia, New Zealand, and Singapore. It was conducted from February to April 2006 using e-passports equipped with BAC. During this test, e-passports presented by travelers from other nations that had begun production were also read and logged. Read access times varied considerably by e-passport type and nation, potentially causing inspectors to prematurely remove slower e-passports from the reader before the data has been completely accessed.

12.3.6 Implementation

The U.S. Visa Waiver Program required that after October 26, 2006 all nations participating in that program issue ICAO-compliant e-passports for travel to the United States under that provision. In addition, the European Union required Schengen-area nations to issue e-passports as of August, 2006. As a result of these two directives, several nations have already started to issue e-passports. Nations not directly affected by these directives have also started to issue e-passports, having recognized the additional security associated with them. Some nations have also installed e-passport readers at ports of entry. The United States was required to have the capability to read e-passports at its ports of entry as of October 26, 2006. Other nations, such as Australia and Singapore have also introduced the capability to read e-passports. More nations are expected to introduce the technology and supporting data systems in the foreseeable future.

APPENDIX 1. DEFINITIONS AND TERMS

The following terms are defined with respect to MRTDs. These definitions were obtained from ICAO references, unless cited otherwise.

Active Authentication – Explicit authentication of the chip. Active authentication requires processing capabilities of the MRTD's chip. The active authentication mechanism ensures that the chip has not been substituted, by means of a challenge-response protocol between the inspection system and the MRTD's chip.

Basic Access Control (BAC) – Challenge-response protocol where a machine (RF) reader must create a symmetric key in order to read the CONTACTLESS chip by hashing the data scaned from the MRZ.

Biometric – A measurable physical characteristic or personal trait used to determine the identity, or verify the claimed identity, of an enrolled individual.

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 enrollee for an MRTD
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 they 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)
5. indicating whether or not an identification or verification of identity has been achieved.

CBEFF (Common Biometric Exchange Formats Framework) – defines a basic structure for standardized biometric information records.

Capture – The process of taking a biometric sample from the user.

Contactless IC – the data carrying unit incorporated into the MRTD, consisting of an integrated circuit or microchip and an antenna.

Doc 9303 – The ICAO standards publication that defines specifications for MRTDs which allow compatibility and global interchange using both visual (eye readable) and machine readable means.

Extended Access Control – EAC – Protection mechanism for additional biometrics included in the MRTD. The mechanism will include State's internal specifications or the bilateral agreed specifications between States, sharing this information.

Eavesdropping – When data from an IC chip is intercepted by an intruder while it is being read from an authorized reader.

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

Enrollee – A human being assigned an MRTD by an Issuing State.

E-passport – An MRTD passport that has a contactless IC chip embedded in it, in accordance with ICAO standards.

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 inability of a biometric system to obtain the necessary biometric sample of a user sufficient to enroll or compare that potential user.

Failure to Enroll – The inability of a biometric system to obtain the necessary biometric sample of a user sufficient to enroll that potential user.

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

Hash – A number generated from a string of text using a formula to ensure that a message has not been tampered with. The sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes (www.webopedia.com).

Holder – A person possessing an MRTD, 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/her 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 common sense notion of personal identity. A person's name, personality, physical body, and history, including such attributes as nationality, educational achievements, employer, security clearances, financial and credit history, etc. 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 MRTD 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 – The digital representation of a biometric as typically captured via a camera or scanning device.

Inspection – The act of a State examining an MRTD presented to it by a traveler (the MRTD 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.

Logical Data Structure (LDS) – Standardized data format common to optional capacity expansion technologies of MRTDs to enable global interoperability for recorded details (travel document data) used during inspection of person and their MRTD).

Machine (RF) Reader – The radio frequency reader which provides power to the Contactless IC and reads and writes to the Contactless IC by means of radio waves.

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

MRP – Machine Readable Passport

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

MRZ – Machine readable zone. The area on a passport containing two lines of data (three lines on a visa) that are printed using a standard format and font

MRV – Machine Readable Visa

Passive Authentication – Verification mechanism that does not require processing capabilities of the chip in the MRTD. Passive authentication proves that the contents of the

Document Security Object (SOD) and LDS are authentic and not changed. It does not prevent exact copying of the chip content or chip substitution.

Public Key Infrastructure (PKI) – Data encryption trust hierarchy that helps to ensure data privacy, security, and integrity.

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

RFID – Radio-frequency identification

Secure Signature Creation Device (SSCD) – Secure hardware device for signature generation.

Skimming – Reading the electronic data in an IC chip surreptitiously with a reader in the vicinity of the travel document.

SOD – (Document Security Object) on the chip, containing a hash representation of the LDS contents to ensure data integrity.

State – A country that issues MRTD, and/or inspects MRTDs at its border.

Template/Reference Template – Usually condensed and vendor-specific data, which represents the biometric measurement of an enrollee, used by a biometric system for comparison against subsequently submitted biometric samples.

Type A Contactless IC – Memory only IC; the machine (RF) reader uses 100% amplitude modulation of the electromagnetic field for communication from the reader to the IC.

Type B Contactless IC – Equipped with a processor IC; the electromagnetic field switches from 100% to 90% amplitude modulation for communication from the reader to the IC.

User – A person who interacts with a biometric system to enroll or have his/her identity checked; sometimes referred to as the subject.

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'.

Visual Inspection Zone (VIZ) – Those portions of the MRTD (data page in the case of MRP), i.e. front and back (where applicable), not defined as the MRZ.

APPENDIX 2. REFERENCES

Annex A - Photograph Guidelines

Annex D - Biometric Data Interchange Formats – Part 5: Face Image Data (ISO/IEC JTC 1/SC 37 N 506)

Annex E - Biometric Data Interchange Formats – Part 6: Iris Image Data (ISO/IEC JTC 1/SC 37 N 504)

Annex F - Biometric Data Interchange Formats – Part 4: Finger Image Data (ISO/IEC JTC 1/SC 37 N 466)

Annex G - Biometrics - Biometric Data Interchange Formats – Part 2: Finger Minutiae Data (ISO/IEC JTC 1/SC 37 N 464)

Annex H - Biometrics Data Interchange Formats – Part 3: Finger Pattern Spectral Data (ISO/IEC JTC 1/SC 37 N470)

Annex I - Use of Contactless Integrated Circuits

Annex J - ICAO May 2003 Press Release

Annex K - ICAO Supplementary Requirements to ISO/IEC14443 -v2

Annex L - E-Passports Data Retrieval Test Protocol

Biometrics Deployment of Machine Readable Travel Documents - ICAO TAG MRTD/NTWG Technical Report, 21 May 2004

Doc 9303 Parts 1 (Passports) and 2 (Visas) are endorsed by ISO/IEC as Std 7501 Parts 1 & 2, 2005

Doc 9303 Part 3 (Travel Documents a.k.a. Cards) endorsed by ISO/IEC as Std 7501 Part 3, 2005

Doc 9303 Part 4 Crew Member Certificates abolished, survives as Annex J to Part 3

ICAO Doc 9303 when endorsed becomes ISO/IEC Standard 7501

Machine Readable Travel Documents – Selection of a Globally Interoperable Biometric for Machine-Assisted Identity Confirmation with MRTDs - ICAO TAG MRTD/NTWG Technical Report, 2001

Output Document of the WG 6 Special Group on Legal Aspects in Section 7.2.3 of the Technical Report 24714-1, ISO/IEC JTC 1/SC 37 N1259, 2005-08-25

PKI for Machine Readable Travel Documents Offering ICC Read-Only Access v1.1, Technical Report, 2004

Structure and Process for Machine Readable Travel Documents – ICAO TAG MRTD/NTWG Technical Report

TAG-MRTD 16th Meeting Report, September 2005

www.pcscworkgroup.com

www.webopedia.com