International Civil Aviation Organization

WORKING PAPER

TAG-MRTD/18-WP/3
22/4/08
English only

TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS (TAG-MRTD)

EIGHTEENTH MEETING

Montréal, 5 to 8 May 2008

Agenda Item 1: Activities of the NTWG
Agenda Item 1.2 Guidelines on e-MRTDs & Passenger Facilitation

GUIDELINES on e-MRTDS & PASSENGER FACILITATION

Presented by the New Technologies Working Group (NTWG)

1. INTRODUCTION

1.1 At TAG-MRTD 16 held in Montreal from 26 to 28 September 2005 a proposal for a Technical Report on Automated Border Control Systems was presented.

1.2 The TAG suggested that this report will be better identified as a “guideline” and that it should broaden the scope to include systems based on e-passport functionality and not just on enrolment. The group also suggested such guidelines could eventually be included in Chapter 6 of Annex 9.

1.3 This Working Paper informs the TAG about the final version of the guidelines.

2. BACKGROUND

2.1 The strategy to improve facilitation and expedite low-risk travellers through (automated) inspection controls while achieving a high level of compliance was already set out in WP/12, presented during TAG-MRTD-11.

2.2 Due to the impact of several international terrorism actions and the heavy workload of the introduction of the e-passport, the NTWG was unable to work on a solution on improvement of facilitation for border control.

2.3 With the introduction of the ICAO standards for e-passports, many States have already implemented the necessary infrastructure, to issue e-passports.

2.4 Meanwhile some States have introduced, or are planning Automated Border Control schemes, in the context of today's demands where security, privacy and confidentiality play an important role along with travel facilitation.

2.5 Since the e-passport contains standard electronic information and biometric identifiers which are globally interoperable and highly secure, the goal of ICAO is to promote the use of e-passports as the token for the automated border control clearance system.

2.6 Taken in consideration that today more then 50% of the issued passports are already compliant with the ICAO e-standard., these new e-travel documents are an excellent tool in an automated border control environment.

3. PROGRESS TO DATE

3.1 Since TAG 16 a sub working group of the NTWG of experts in the field of Automated Border Clearance Systems has been formed.

3.2 The sub working group had several meetings in The Hague, London and at Schiphol Amsterdam Airport

3.3 An outline of the issues to be considered in implementing ABC systems has been completed.

3.4 Draft guidelines version 0.4 was presented to the members of the NTWG.

3.5 This draft received a positive reaction from the members of the NTWG and one member even indicated that his organization had already used parts of the document for the establishment of a trial ABC system.

3.6 Today the guidelines are sufficiently advanced for presentation to the members of the TAG .

4. ACTION BY TAG/MRTD

4.1 NTWG invites the TAG/MRTD

a) take note of the work that has been done by the members of the sub-working group on the guidelines for e-MRTDS & Passenger Facilitation;

b) to agree with the outline and content of the guideline;

c) to approve to start the necessary steps for publication.

— — — — — — — —

APPENDIX

GUIDELINES

electronic - Machine Readable Travel Documents & Passenger Facilitation

Version – 1.0
Date – April 17, 2008

Presented by the New Technologies Working Group (NTWG)

File	: Guidelines on e-MRTDs & Passenger Facilitation
Lead	: J.M.J. Broekhaar for ICAO-NTWG

Release Control

Release	Date	Description
0.1		
0.2	20th July 2006	Following first ad hoc Meeting in Netherlands April 27. and the contribution of the members requested per the action paragraph split decided by Sjef in his DOC dated May 10, 2006
0.3	1st Sept 2006	Revised following meeting in London and further input from the working group. New sections added and first edit for overall continuity.
0.32	1st Jan 2007	Revised following meeting at Schiphol-Amsterdam on 18 October 2006 and further input from members working group
0.57	22nd Jan 2008	Culmination of ongoing edits plus addition of API/APP information
0.58	04th Feb 2008	Paragraphs added
0.59	06th Feb 2008	Additional content from CH added
0.60	11th March 2008	Additional text in 4.11.2 ** and 4.11.5
0.62	14th March 2008	Incorporation of Rapid example in Annexe A (0.61)
0.63	27th March 2008	Further additions and revisions
0.64	31st March 2008	Further contributions added and layout checked
0.65	09th April 2008	Additional text
0.66	11th April 2008	Additional text in 3.4.4
0.67	16th April 2008	General tidying up of document
1.0	17th April 2008	Release of version 1.0 for TAG 18

Release note

Changes, made on version 1.0, resulting in this version 1.1:

Subject	Description	Reference

Preamble

The strategy to improve facilitation and expedite the movement of low-risk travellers through (semi automated) inspection controls while still achieving a high level of compliance has already been set out in WP 12, presented during TAG 11.

Faced with the constant growth in international passenger traffic (air)port operators, control authorities and carriers are seeking new ways to efficiently process passengers with minimum intrusion into individual privacy while at the same time ensuring integrity of border controls.

Recent developments have seen the introduction of a new generation of travel documents which contain, in addition to visible information, an embedded chip in which additional information may be stored and subsequently retrieved via a secure electronic reading process. Within this document, we shall hereinafter refer to such documents as electronic machine readable travel documents (e-MRTDs). Since the introduction of the ICAO standards for e-MRTDs, many states are implementing, or considering the implementation of, the necessary infrastructure in order to issue and read e-MRTDs.

A properly configured and issued e-MRTD enables enhanced border security through robust document security and identity verification capabilities. In addition, the image of the holder that is stored electronically within the document, can be used to improve facilitation through full or partial automation of the border clearance process. Furthermore, in time, other biometric features, such as fingerprints, will undoubtedly appear within e-MRTDs, providing further options for the future.

It is also widely acknowledged that the vast majority of passengers are low risk, often frequent travellers, who pose no risk to the integrity of border controls. The e-MRTD can assist border control agencies in identifying who the low risk passengers are, as well as facilitating their clearance through the border clearance process. It is these passengers that automated border clearance facilities should target and facilitate, since they represent a significant proportion of those using port and airport facilities.

To achieve such a goal, the border control infrastructure needs to be updated by linking the required hardware and software components to the appropriate government IT systems.

During the Technical Advisory Group on Machine Readable Travel Documents meeting, number 16 in Montreal, 26 – 28 September 2005 a proposal for a Technical Report on Automated Border Control Systems was presented. The TAG suggested that this report will be better identified as a “guideline” or a “blueprint”, and that it should broaden the scope to include systems based on e-MRTD functionality as well as pre enrolment programmes. The group also suggested such guidelines be eventually included in Chapter 6 of Annex 9. The Tag considered this proposal and subsequently endorsed it, assigning this task to NTWG.

The Guidelines document presents an outline of an Automated Border Control System (ABC) and how the e-MRTD may become an accepted international token within such an environment, as well as addressing the manual use of such documents.

This Guideline document is the result of contributions from the members of a sub-working group of the ICAO - NTWG. Without their contributions and input to the various discussions it would not have been possible to create this Guideline document in such a short period of time. The members of this sub-working group are detailed below.

ICAO - NTWG sub working group on e-MRTDs & Passenger Facilitation		
Julian Ashbourn (editor)	International Biometric Foundation	United Kingdom
Marcel van Beek	Amsterdam Airport Schiphol	The Netherlands
Sjef Broekhaar (lead)	International Organization for Migration	The Philippines
Chris Hurrey	Home Office / Border & Immigration Agency	United Kingdom
Ellen Brophy	Australia Customs Service	Australia
Jean Salomon	ISO – WG3	France
Terry Wall	Australia Customs Service	Australia

Table of contents

1. EXECUTIVE SUMMARY

The aim of these guidelines is to illustrate how e-MRTDs may be used for an assisted (i.e. "semi-automated") or even fully automated border inspection process, in order to promote expedited passenger flows within airports, seaports or at land borders. The scope consequently includes generic suggestions for immigration and border control procedures at such points of entry and exit.

The first generation of e-MRTDs designed according to the specifications of ICAO (described in Doc 9303, Part 1, Volume 2) have been in circulation since October 2005. International requirements, such as the EU Council regulation Nr. 2252/2004 of 13 December 2004 (on standards for security features and biometrics in passports and travel documents issued by Member States) and the new demands on participants in the US Visa Waiver Programme led more then 40 States to issue e-MRTDs by the end of 2007. Further e-MRTDs will include refugee and alien passports, as well as identity cards.

Electronically enabled machine readable passports, e-Passports / e-MRTDs, will be capable of being scanned by any suitably equipped receiving State, retrieving a greatly increased amount of data relating to both the e-MRTD and its holder. This will include mandatory globally interoperable biometric data which may be used as an input to facial recognition systems and, optionally, to fingerprint or iris recognition systems. For practical reasons, in many countries the provision of biometric data may follow a phased approach and not necessarily be fully implemented upon initial introduction of the document. For an automated border control system using the e-MRTD, no pre-enrolment by the border control agency is required, as all the necessary information on the bearer and the document will have been enrolled by the issuing authority and is incorporated in the chip.

To ensure that Inspection Authorities are aware of the new possibilities that e-MRTDs present, this document will cover subjects like the positioning of the e-MRTDs electronic components, e-MRTD reading devices, the use of biometrics and the architectural design of automated border control systems (ABC systems).

The guidelines are designed for those States or Inspection Authorities who would like to be able to use the e-MRTD in their processes in an assisted or fully automated manner. The guidelines may be used as a blueprint in order to support policy makers, process developers and IT support personnel during the design phase of projects. The guidelines are written by experts in these areas who have themselves implemented operational systems in many countries throughout the world.

The stakeholders should be limited to those who are actually required to trust the e-MRTD as part of a secure border clearance process. This will include immigration officers, border police, port authorities and travel carriers as necessary to meet their respective legal obligations. The primary stakeholder is of course the document holder and full consideration should be given to factors such as ease of use, privacy and accommodating those with disabilities.

e-MRTDs as specified by ICAO offer another possibility: if entry may be granted to distinct classes of passengers (e.g. citizens of the European Union, non-citizen permanent residents) as well as those individually enrolled then border control authorities may make additional savings. For example, if eligibility alone confers rights of entry or exit without detailed examination, then the e-MRTD (with its biometric information) may be all that is required to allow a passenger to proceed.

There are a number of considerations for an e-MRTD system if it is to be used in this way:

- The state accepting the document must be satisfied that the issuing state's document production, application and issue procedures are of a high standard and are not susceptible to fraud.

- The accepting state must be satisfied that the nationals of countries holding e-MRTDs are not a high risk from a crime, smuggling or illegal migration perspective.

- The system must only allow passage to eligible travellers and prevent fraudulent use such as use by multiple persons (tailgating) or climbing over or under an unsupervised barrier.

- The system should also fall back to a safe (e.g. closed) mode in the event of electronic or mechanical failure so that border security is not compromised.

- The system must be able to allow young, elderly or disabled persons to use it without difficulty or prejudice
- There should be adequate training for new passenger users, guidance in multiple languages is desirable and assistance on hand in case of difficulties.

- The system should be able to detect e-MRTDs which are legitimate, defective, have been tampered with or which have been revoked by the issuing authority via a trusted PKD.

- The system should keep secure the personal or document data it handles, both within the mechanism and within links to other systems.

- The system should be proof against spoofing of the biometric required to complete the identity check and the false accept rate needs to be minimized to an acceptable level.

- The system may need additional input from a passenger aside from presentation of a passport and a biometric. It may be necessary for the passenger to make a declaration by pressing keys or a screen area in response to specific questions

- Operational processes and systems performance must be equivalent across nodes. This has been mentioned in various parts of this document and is further stressed here. Without such equivalence, the confidence we might have in any such application will be significantly diminished.

- It is essential that users have confidence in the system, both from an operational perspective and, especially, from a security perspective. In this respect, careful consideration must be given to the security of both systems and attendant operational processes in addition to overall facilitation.

2. INTRODUCTION

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

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

In 1997, the TAG/MRTD commenced a comprehensive revision of Doc 9303, Parts 1, 2 and 3. In this revision process, the structure and organization of the three parts were harmonized. The sixth edition of Part 1 represents the first stage of a new revision process; as a result there are some changes in format from the previous generation of the Parts of Doc 9303.

By the mid-1990's, the TAG/MRTD had established three Working Groups. The New Technologies Working Group (NTWG) was tasked with planning and implementing the long term development of MRTD's. The Document Content and Format Working Group's role was to review and edit future editions of Doc 9303, while the Education and Promotion Working Group undertook the task of providing information and guidance to States on the implementation of MRTD schemes.

In 1998, the NTWG began work to establish the most effective biometric identification system and associated means of data storage for use in MRTD applications, particularly in relation to document issuance and immigration considerations. The bulk of the work had been completed by the time of the events of September 11th 2001, which caused greater emphasis to be paid to the security of a travel document and the identification of its holder. The work was quickly finalised, endorsed by the TAG/MRTD and the Air Transport Committee and the results published as a standard in Volume 2 of Part 1 in the sixth edition of Doc 9303.

2.1 Purpose and Audience

The purpose of this document is to offer guidelines regarding the effective use of e-MRTDs within both a national and international interoperable environment. The expected audience includes policy makers, control authorities, port and airport authorities, technology suppliers and integrators, and other agencies as may become applicable.

2.2 Scope

The aim of these guidelines is to offer suggestions as to the use of an e-MRTD within a semi or even fully automated inspection process, in order to facilitate enhanced passenger flows within airlines, airports, seaports or at land borders. The scope consequently includes official immigration and border control procedures at such points of entry and exit.

2.3 Drivers

As of October 2005, documents designed according to the specifications of ICAO described in Doc 9303, Part 1, Volume 2 have been in circulation. Due to international requirements, like the EU Council regulation Nr. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, and the new demands on participants in the US Visa Waiver Programme led more then 40 States to issue e-MRTDs by the end of 2007. Further e-MRTDs will include refugee and alien passports, as well as identity cards in addition to passports.

Electronically enabled machine readable passports, so-called e-Passports / e-MRTDs, will be capable of being used by any suitably equipped receiving State, in order to read from the document a greatly increased amount of data relating to both the e-MRTD and its holder. This will include mandatory globally interoperable biometric data which may be used as an input to facial recognition systems and, optionally, to fingerprint or iris recognition systems. For practical reasons, in many countries the provision of biometric data may follow a phased approach and not necessarily be fully implemented upon initial introduction of the document.

To ensure that inspection authorities are aware of the new possibilities the e-MRTDs present, this document will cover subjects like the positioning of the e-MRTDs electronic components, e-MRTD reading devices, the use of biometrics and the architectural design of automated border control systems.

The guidelines are designed for those States or Inspection Authorities who would like to be able to use the e-MRTD in their processes in a semi or fully automated manner. The guidelines may be used as a blueprint in order to support policy makers, process developers and IT support personnel in their decision making processes during the design phase of associated projects. The guidelines are written by experts in these areas who have themselves implemented operational systems in many countries throughout the world.

2.4 Stakeholders

The stakeholders should be limited to those who are actually required to issue and use the e-MRTD as part of the border clearance process. Responsibility for the issue of an e-MRTD lays with the Issuing Authority of a given state / country. Those responsible for the border clearance process will include Immigration officers, Border police, Customs officers, port authorities and travel carriers as necessary to meet their respective legal obligations. The primary stakeholder is of course the document holder and full consideration should be given to factors such as ease of use, privacy and accommodating those with disabilities.

2.4.1 Roles and Responsibilities

It is important that, with regard to e-MRTDs, we maintain a clear understanding of roles and responsibilities among the various control authorities and that there is no overlap or function creep between them. This is particularly important from the perspective of the document holder, who needs to understand who is responsible for what and under what conditions. In general terms we may state that:

- Immigration policy and control is the responsibility of the appropriate appointed authorities.
- Depending on administrative arrangements within each State, the border control authority may be an Immigration, Customs, Border Guard, Police or other government agency or a combination of such agencies.
- Port authorities are responsible for document checks in situations where legislation requires it.
- Travel carriers (airlines, shipping companies, railways and road transport) are responsible for undertaking document checks as required by legislation.

Beyond such responsibilities, as necessary to support mandatory legislation, there should be no requirement whatsoever to use the document. The document holder should be made specifically aware of such legislated requirements via proper communication at the time of issue or renewal. Similarly, the document holder should be advised, at all border crossing points of presence, of the correct and legal use of the travel document, including who might legally request to examine or automatically read the document. There should be no ambiguity on these points.

2.5 Assumptions

The following assumptions have been made: That states will introduce e-MRTDs. The associated technology will continue to evolve. That border control authorities, airport operators and airlines will continue to use e-MRTDs in support of processes around legal obligations. The introduction of e-MRTDs should be orchestrated in such a way that they will be clearly beneficial to society. That e-MRTDs will be designed and refined to reach optimum interoperability. That e-MRTDs will remain as physical documents and continue to be the primary identity document within this operational environment. That the MRZ and chip are simply additional elements designed to facilitate automation. That the physical document will be used in a conventional manner and remain valid under fallback procedures in the case of chip failure.

2.6 Other considerations

It should be noted that there is a strong possibility of making assumptions around the use of the document beyond its legally prescribed use. The e-MRTD is a specific document for a specific purpose. Such purpose should be clearly articulated by the issuing authority, including attendant roles and responsibilities. It should be made clear to the document holder that any use, or suggested use, outside of this declared purpose is beyond that required by legislation and, if entered into, would be done so on a purely voluntary basis by the document holder. Under no circumstances should the document holder be required, or pressed into using the document for any other purpose than that prescribed by the issuing authority.

We must equally beware of making assumptions around the value and use of a biometric in association with the document. A biometric verification check, while providing an enhanced confidence that the document is being presented by the individual to whom it was originally issued,

does not prove or validate the identity of that individual. Due to the potential for genuine MRTDs to be falsely obtained, passing such a check does not necessarily mean that the individual in question is who you think they are or is of no societal risk. Similarly, failing such a check does not necessarily mean that the individual is not who they claim to be and therefore represent a risk. There are many reasons why an individual may fail a biometric identity verification check at a particular point in time through no fault of their own. The value of a biometric identity verification check needs to be understood in context, especially by immigration and border police officials. Whilst the addition of a biometric to a document adds another level of security, immigration and border officials need to remain alert to the potential for genuine documents to have been issued to fraudulent applicants.

We must additionally beware of making assumptions around individual transaction times where an automated use of the document is being considered. An automated document check is not necessarily going to be any faster or slower than a manual check. There are many systems related factors, aside from the biometric check, which will have an influence upon transaction times, and these should be properly evaluated and understood. Transaction time in a "self service" style automated system will also be influenced by the user interaction issues while complying with the transaction steps, including his experience in using the system. Indeed, it is likely that, especially in the early stages of implementation, an automated check may take longer than the existing manual procedure. There may also be unexpected technology failures at a given point of presence which could take time to recover from. It is therefore important to provide an appropriate level of human assistance and back up in the case of difficulties or failure of the gate. This will ensure that delays are quickly dealt with

Factors such as operational continuity and disaster recovery should also be taken into consideration within any aspiration for the deployment of automated border controls, as should health and safety in relation to flow control. Automated border control systems may allow a number of gates to be supervised by one single official with consequent benefits to border control administration, such as redeployment of staff to dealing with higher risk travellers, however assumptions should not be made in this context prior to operational experience.

2.7 How to read this document.

It may not be necessary for every reader to read this document in a linear manner from beginning to end. For those who already have a thorough understanding of certain topics, they may prefer to use the index in order to identify areas of more immediate interest. However, certain sections will assume a fundamental understanding of the broader area.

3. THE e-MRTD CONCEPT

3.1 General outline

The primary benefit associated with e-MRTDs is the provision of an electronic IC (chip) secure storage area where user related data, including biometric data, may be stored and subsequently retrieved for identity verification purposes via either a manual or automated process. As e-MRTDs become widely issued, the provision of automated border clearance processes, for those with the appropriate entitlements, may become an increasingly attractive proposition. However, such propositions must be carefully considered from a sustained and scalable operational perspective.

3.2 e-Machine Readable Travel Document

With respect to the development of an Automated Border Control System, it is advisable to use the most recent version of Doc 9303, together with the latest Supplement. These documents will give a complete and detailed outline of the structure and content of MRTDs and e-MRTDs.
We are currently at the 6th published version of Part 1 of Doc 9303, which consists of 2 volumes.

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.

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.

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.

3.2.1 How to recognize an e-MRTD?

ICAO has developed an e-symbol which must be visible on a compliant e-MRTD where the travel document also meets the following requirements:

1. That the e-MRTD contains a contactless microchip, with a data storage capacity of at least 32kB,
2. That it is encoded in accordance with the Logical Data Structure with, as a minimum, the MRZ data in Data Group 1 and a facial image as specified in Data Group 2, the whole data being secured with a digital signature.

Unless an e-MRTD conforms to these minimum requirements, it may not be described as an e-passport or display the e-passport symbol. The symbol shall appear on the front cover of the e-passport / e-MRTD either near the top or the bottom of the cover.

The e-passport symbol

The image, as shown above, is a positive, i.e. the black part of the image above shall be printed or otherwise imaged. The symbol shall be included in the foil blocking or other image on the front cover. Equipment suppliers may also like to consider the use of the symbol on fully compliant hardware, in order to assist identification by control authorities and users alike.

3.2.2 The Contactless Chip

The flexibility to implement biometric facial recognition and, optionally, biometrics for finger and iris, comes at the expense of the data storage capacity required. After careful examination, the NTWG decided to select a contactless integrated circuit (IC), conforming to ISO/IEC 14443. This technology involves communication between the IC module (the IC attached to an aerial coil), contained within the e-MRTD, and a reader situated within a distance of 10 cm (3.9 in). The technology offers the following advantages:

- It has been proven in other fields.
- There are a significant number of manufacturers of suitable ICs of various data capacities, and integrators who can construct the IC module.
- There are several methods available for incorporating the IC module into the book, either in the cover or in a specially reinforced page within the book.
- The use of ISO/IEC 14443 technology does not demand accuracy of positioning of the MRP on the reader, compared to a contact chip, but the close read distance means there is little risk of unauthorized reading of the data stored on the IC, provided suitable electromagnetic screening is used within the reader and associated secure communications are implemented.

The data storage capacity of the IC is specified to be a minimum of 32 kb, which is large enough to store the mandatory facial image and, also mandatory, a duplication of the MRZ data. However, the optional storage of more than one facial image and/or fingerprint/iris images requires a considerably larger data capacity. Some States are planning to use ICs with much larger data capacities to allow for future expansion and options. ISO/IEC 14443 specifies two alternative types of IC; A and B; the

specifications allow either type to be used, necessitating the use of a reader at the point of presence capable of operating with an IC of either type. Issuing authorities are consequently encouraged to consider possible future requirements when specifying IC capacity, especially where multiple biometrics may be used.

3.2.2.1 Position of the contact less chip

The ICAO specifications give several options where to place the contactless IC and its associated antenna in an e-MRTD. Specified are the following options:

- Between the front cover and the front end paper;
- Between the rear cover and the rear end paper;
- Integrated in the biographical data page;
- Located in the centre of the passport booklet'
- As a special added page in the booklet.

It is important to understand that the contact less IC and its antenna is not on one location in the passport. Certainly when e-readers have to be purchased or developed for the ABC system, one has to understand that the ergonomics also play an important role for this purpose. The ergonomics of the e-reader has to facilitate the process, have to deal with all location options of the contact less chip and may have no impact on the durability of the e-MRTDS.

3.2.2.2 Data structure (LDS)

In order to achieve globally interoperability, it is important that information is stored in a standard way in the contact less chip. For that purpose ICAO developed the Logical Data Structure (LDS). The LDS consist today out 16 data groups and the data groups have again been divided into data elements. There are mandatory and optional data groups.

To achieve globally interoperability the following four data groups or data elements are mandatory:

1. Data group 1, which contain the content of the MRZ of the e-Passport;
2. Data group 2, which contain the encoded image of the face of the e-Passport holder;
3. EF.COM, containing version information and tag list
4. EF.SOD, containing data integrity, authenticity information.

The other data groups are optional for use by an issuing State or organization.

Data groups 17 till 19 have been prepared for future use. Especially data group 17 is of interest for the readers of this document, because it is dedicated to Automated Border Clearance. The idea is that in the near future this data group can be used or by the issuing State or organization to store the right information for usages of the system. It can also be used by a receiving State to write information to this data group in the contactless IC to allow the bearer of the e-passport to make use of the ABC system in that State.

3.2.2.3 Content

As mentioned before in order to get a globally interoperability e-passport system it is important to create structure and definition. The Logical Data Structure of ICAO recognizes two options in the use of the LDS, namely mandatory and optional data groups and data elements. The mandatory fields have been mentioned here fore. Issuing States or organization can use the other data groups for there own conveniences.

It is important to know that several States already used other data groups for own or general use. Some States have used DG 11 to place the rest of the surname and given names when these are not completely displayed in the MRZ or repeat these. Other data that can be stored in this data group is for example the place of birth. Other states have used DG 7 for an image of the signature. In 2009 many States in the European Union starts to use DG 3 to store two images from the left and right index finger or other fingers if these are not available.

It is up to organizations who develop an Automated Border Control system how to use the additional data in their data stream and for which purpose.

3.2.3 The Machine Readable Zone

The existing OCR based machine readable zone will continue to be featured on e-MRTDs and will provide a valuable level of flexibility around how the document might be used within varied operational environments. It will also serve, under the requirements of basic access control (BAC), as a mechanism with which to effectively 'unlock' the chip, allowing chip resident data to be read accordingly. Indeed, it may be some considerable time before a critical mass of border crossing points are equipped to read the IC chip within e-MRTDs. Furthermore, a large number of travel documents without embedded ICs will continue to be in circulation, necessitating the continuance of the visible MRZ and associated optical reading equipment.

3.3 Interoperability

The term 'interoperability' may be interpreted in several ways. There is the simple technical interoperability which requires that e-MRTDs from different issuing authorities must be able to be read electronically across all points of presence equipped to do so. This requires a relatively straightforward compliance to published standards for both the e-MRTD and associated document readers, coupled to properly conceived test strategies in order to verify such a compliance.

There is a broader interoperability however, which embraces both operational process and environmental design, ensuring that, especially in the context of automated systems, the user experience is roughly equivalent between nodes. As realised performance is directly influenced by user prior experience, this is an important consideration. If significant differences in operational process occur across nodes, users will become confused and may consequently fail to interact with the associated systems in the expected manner. This, in turn, would have a negative impact upon realised systems performance and anticipated throughput. It is hoped that principles of best practice will evolve and be communicated between States in order to facilitate this broader interoperability.

3.4 Access to chip and data

3.4.1 Privacy and Data Protection

The concept of data protection and privacy remains important to citizens across the world. There are various factors to take into account in this context.

Firstly, with regard to the e-MRTD and how it is read by suitable equipment, it must be possible to demonstrate a resilience to 'skimming' or 'eavesdropping' whereby data might be read from the chip by non-authorised equipment within the vicinity. Technology supplier's claims alone are not sufficient to provide confidence in this respect, and trials should be undertaken in order to ascertain such susceptibility under field conditions.

Secondly, there is the much broader issue of what happens to the data after it has been read, who might have access to it and for what purpose. There has been an increasing trend to blur immigration control with law enforcement in many countries. This is a potentially serious issue as, on the one hand we are dealing with the legitimate person seeking rights to cross a border, while on the other we are dealing with criminal activity. If this distinction is not properly understood and catered for, there is a risk of citizens becoming disenchanted with the process and losing confidence in the government agencies and control authorities involved. There are perhaps two areas where reassurances might usefully be created. Firstly, by making it easy for document holders to see exactly what is encoded within the chip of their e-MRTD (as recommended by ICAO) and, secondly, the provision of clear statements as to exactly how that data is used, with whom it is shared and for what purpose. Furthermore, such a statement should cover factors such as data retention, access control and associated factors.

It should be noted, that current activities around the provision of traveller's data to third parties does not sit comfortably with the principles of many in place data protection acts. If the scope of such activities increases further, as has often been suggested, then the provisions of these data protection acts will become effectively meaningless. Such a development could significantly, and possibly irrevocably, impact the trust model between citizen and state. This is an area which will require careful thought and attention.

In the context of privacy and data protection, it will be important to maintain an absolute clarity of purpose around any aspirations for border control using the e-MRTD. As stated elsewhere, the passport or travel document is a specific instrument for a specific purpose. This purpose must not become obscured or misunderstood.

3.4.2 Basic Access Control (BAC)

The function of Basic Access Control is to reduce the possibility of an unauthorized system or person reading the chip contents over a (short) distance *"Skimming"*. A conventional (non electronic) MRTD has to be handed over and *opened* by a inspector before the personal and document details can be read and its content examined. Similarly, BAC also enforces the initial *opening* of the document before it is possible to get access to the personal and document details of the bearer stored in the chip.. The keys, necessary to get access to the chip, are generated from a limited number of fields in the MRZ. As a consequence the visual MRZ has to be read optically (e.g. the e-MRTD book has to be opened) first in order to generate the access keys for electronic reading (*opening*) of the chip. BAC is a both a security mechanism and a privacy measure. It is important to understand this method because it can be used for several design solutions of an automated border control system.

Another privacy concern is eavesdropping, whereby data resident within an IC chip is intercepted by an intruder while it is being read via an authorized reader. BAC incorporates a *secure messaging* feature which prevents eavesdropping by encrypting the messages passing between the reader and the chip. The message may only be deciphered via a decryption 'key' which is derived from specific data within the MRZ.

3.4.3 Write protection of the chip

With the first generation of ICAO's e-MRTDs, it was not possible to write to the embedded contactless chip after personalization. Consequently, producers of e-MRTDs locked the chip as a

final step in the personalization process. With the current generation of documents, the principle of WORM (Write Once Read Many) is utilised. Although the Logical Data Structure includes data groups which may be written to, this is understood as a feature to facilitate future options.

More research is required in order to fully understand the implications of receiving states having the possibility to write to the chip. Perhaps a logical future application might be the ability to electronically stamp the e-MRTD.

3.4.4 Extended Access Control (EAC)

ICAO's mandatory requirement as the globally interoperable biometric is the face. Therefore, within the e-MRTD contactless chip, data group 1 (a copy of the MRZ) and data group 2 (encoded image of the face) are always populated. For privacy reasons access to these data groups is restricted via the Basic Access Control mechanism. Issuing States have also the possibility to add additional or secondary biometrics. As secondary biometrics ICAO identifies the fingerprint and the iris as the most suitable biometrics in a travel document scheme. It is acknowledged that the secondary biometrics represent more sensitive personal data than the face. Therefore, access to this data should be more restricted.

One of the solutions to accomplish this is to use Extended Access Control (EAC). Today EAC is not yet an ICAO standard, but has to be implemented in e-MRTDs of member states of the European Union before 28 June 2009. The use of EAC in the EU scheme is based on the authorisation of inspection systems by e-MRTD issuers, proven via the possession of certificates. These certificates are exchanged via a Public Key Infrastructure. The EU PKI scheme requires a rather complex infrastructure and certificate distribution scheme, but on the other hand it provides a high level of protection of the sensitive biometric data and privacy of the bearer of an e-MRTD.

If an inspection system is not authorized to read the images of the fingerprint of the bearer of an e-MRTD, the system won't see or be able to download this data. Furthermore strong session keys encrypt the communications to prevent eavesdropping. This is achieved by using two advanced security mechanisms. First of all Chip Authentication. This provides strong session encryption and enables the inspection system to verify that the chip is genuine. Secondly Terminal Authentication, this enables the chip to verify that the inspection system is entitled to access the sensitive data. An EAC compliant e-MRTD supports a non EAC compliant inspection system in order to guarantee interoperability.

It is important for an operator of an ABC system to understand the concept of EAC thoroughly, since the readers (inspection systems) have to be authorized to access the sensitive data. This is achieved via a dedicated PKI and the issuance of Country Verifying CA Certificates, a Document Verifier Certificate and authorizing Inspection System Keys. As a consequence, an Inspection system should contain a certificate chain of each State using the EAC protocol.

The PKI, required for Terminal Authentication, providing EAC, consists of the following entities:

1. Country Verifying CAs (CVCA), issuing Document Verifier Certificates
2. Document Verifiers (DV), issuing Inspection System Certificates
3. Inspection Systems, accessing e-MRTD chips.

The Country Verifying Certificate Authority (CVCA) acts as a single trust-point of an issuing State. The CVCA determines access rights to the e-MRTD chips, issued by that State, for Document

Verifiers. These access rights are granted to a Document Verifier by issuing a DV Certificate to it. The DV Certificate contains the DV's public key and is signed by the CVCA.

A DV manages inspection systems by issuing Inspection System Certificates, and is therefore a CA authorized by the national CVCAs.

An Inspection System is authorized to access sensitive data stored on a State's e-MRTD through the certificate chain, starting with the CVCA Certificate, issued by the MRTD issuer's CVCA and ending with the Inspection System certificate. In adopting this scheme, the Inspection System (document reader) becomes an important mechanism with which to access sensitive data and, consequently, an attractive target for misuse. To diminish the potential risk of lost or stolen Inspection Systems, the IS Certificates will have a relatively short validity period.

The use of sensitive biometric data, as contained within an e-MRTD, in an ABC system environment requires careful management of keys and consultation with issuing States whose citizens are entitled to use this facility. In order to be able to support such a scheme, a structure to manage the certificates, keys, policies and attendant procedures must be embedded within the organization concerned.

3.5 Data Security

3.5.1 Passive authentication

Passive authentication is a mechanism to detect alteration of the data stored in the contactless chip embedded in the e-MRTD. Each data item stored on the chip adheres to a so-called Logical Data Structure (LDS), which groups the data in a logical order. The LDS consists of several data groups, each of which comprises a certain type of information. Data group 1 contains data relating to the MRZ, while data group 2 contain data relating to the facial image of the bearer. If, these data groups are to be used to verify a person's identity, we will need to establish that:

- the data is authentic, and stored in the LDS by the issuing authority;
- data integrity has been preserved since the data was issued.

The Document Security Object (DSO) was introduced to facilitate these verification requirements. The DSO is stored on the chip and consists of a data structure that stores a hash representation (a very compact, yet unique representation) of each data group being used. In other words, if the chip contains the minimum recommended features (MRZ and Facial Image) DG1 and DG2 will be in use, and the Security Object will contain hash representations for DG1 and DG2. Then the issuing state has to sign the Security Object using a digital signature. By verifying this digital signature, the inspection system is able to establish the authenticity and integrity of the Security Object and as a consequence, the LDS data. According to ICAO specifications, the use of Passive Authentication is mandatory.

3.5.2 Active Authentication

The function of Active Authentication is to confirm that the data has been read from the original embedded chip in the e-MRTD. Active Authentication requires the chip to perform several specific cryptographic calculations. As such, Active Authentication is based on a documents own key pair. This key pair is generated during the personalisation process and stored in the secure memory of the

chip, which cannot be accessed or changed by an external system. The secure memory is used to perform the cryptographic calculations. The Public Key is stored in LDS Data group 15.

By reading the MRZ data on the biographical data page and comparing it to the MRZ data stored in the LDS, the inspection system is able to establish that the biographical data page and the LDS belong together. As the authenticity of the LDS content can be established by means of Passive Authentication, it can be proved that the physical MRZ is authentic. But it is still possible that the physical end electronic MRZs are copies. Since the Active Authentication Public Key is stored in the LDS data group 15, its authenticity and integrity are implicitly established by means of the Passive Authentication check. The inspection system uses this (trusted) Public Key to encrypt a randomly generated number ands sends a so-called challenge to the chip. The chip decrypts the challenge and returns a so-called response to the inspection system. By comparing the response to the challenge, the inspection system is able to establish that the Public and the Private Key form a pair.

As the Private Key cannot be separated from the chip and the Public Key has been proven to be genuine, the above challenge-response sequence establishes that the chip is genuine (and that its contents have not been copied). Now it is established that the chip is authentic, that the Document Security Object (and therefore the LDS) is linked to the chip, and that the chip belongs to the biographical data page.

By using Active Authentication in the electronic part of the MRTD, border control authorities are able to determine if a chip embedded in the E-MRTD belongs to that document and is not cloned chip. But crucial in this process is that the border control authorities have incorporated the software in the inspections systems to perform the necessary calculations and checks which come with the use of Active Authentication.
According to ICAO specifications is the use of Active Authentication optional, which means that not every e-MRTD contains this provision.

3.6 Public Key Infrastructure (PKI)

The principles and potential benefits of a PKI are understood and yet the technology is not perhaps as widely used as many anticipated it would be within our ‘information age’. The primary reason for this may be due to operational challenges and the relative complexity of managing a PKI on an ongoing basis, especially when implemented upon a broad scale. Any weaknesses associated with such a management, can easily result in chaos from the users perspective, together with compromised security. Furthermore, the support costs of managing a PKI can increase dramatically if any such weaknesses exist or develop over time. We must therefore think very carefully about the benefits we expect a PKI to deliver, together with the roles and responsibilities associated with its implementation, usage and ongoing support. Anything less than absolute clarity in this respect will fail. We should also acknowledge that implementing a practical PKI represents a long term commitment.

If we contemplate a situation whereby individual issuing authorities maintain key pairs which might be subject to change on an ongoing or ‘scrolling’ basis, then it is likely that, over time, documents will exist, issued by the same authority, with differing authentication requirements. If we additionally wish to endow hardware (capable of reading the document’s chip) with keys, which might also be subject to change, then we have a potentially complex situation to manage, especially when one considers the number of issuing authorities worldwide and the potential number of document reading points of presence. The certificate authority (CA) responsible for overseeing this

PKI must therefore pay close attention to the issue and dissemination of keys (certificates), in close cooperation and coordination with issuing authorities.

An additional challenge exists at locations (i.e. ports and border crossing points) where the documents will be used and the chips within them read by machines. Each such reading device must ideally be capable of accurately authenticating and reading every e-MRTD in circulation. Maintaining this capability, both as new documents are issued from existing e-mrtd equipped authorities, and other authorities introduce their own e-MRTDs, will require careful management. The certificate authority must therefore anticipate these and other related challenges, ensuring that well-defined processes are in place accordingly.

3.6.1 Key dissemination

The certificate authority (CA) must devise and maintain a method for disseminating keys to all those with legitimate reason to use them. They must also maintain an accurate log of precisely which keys (including subsequent versions from the same issuing authority) have been distributed (or accessed from a repository) when, and to whom. They must also understand when new keys are required by a given issuing authority and exactly when these new keys will be used. In addition, they must maintain a key / certificate revocation list and ensure that it is permanently available to all who need to access it.
It follows then that issuing authorities and those producing document reading hardware must liaise closely with the certificate authority if a practical PKI is to be maintained. Establishing an effective and workable PKI globally will take some time, and this should be taken into consideration.

3.6.2 ICAO Public Key Directory

From the foregoing it is evident that ePassport validation is an essential element to capitalise on the investment made by States in developing ePassports to contribute to enhance aviation security while facilitating passenger processing. Because the benefits of ePassport validation are collective, cumulative and universal, the broadest possible implementation of a scheme or schemes of ePassport validation is desirable.

The exchange of PKI certificates (and the exchange of the certificate revocation lists that are the essential recovery layer in the system) must be reliable and timely. This exchange cannot be achieved by other than electronic means. The system of ePassport validation must operate on an open ended, indefinite basis.

The ICAO PKD has been established to support the global interoperability of ePassport validation to act as a central broker to manage the exchange and update certificates and certificate revocation lists. This central role is critical to minimise the volume of certificates being exchanged, to ensure timely uploads and to manage adherence to technical standards to ensure interoperability is maintained.

ICAO, as the global agency responsible for travel document standards, is well placed to perform this role to achieve a workable, sustainable global scheme.

The ICAO Public Key Directory has been operational since March 2008.

Updated information on the ICAO PKD is available at: http://mrtd.icao.int/content/view/47/251/

4. THE POTENTIAL for the use of e-MRTDs for AUTOMATED BORDER CONTROL

4.1 Introduction

Ports of entry around the world are handling increasing numbers of passengers and crew, making it more difficult for border control authorities to meet public waiting time expectations while maintaining security. Higher throughput traditionally means more staff, more service positions and larger border control accommodation areas.

The increased scrutiny of passengers by border control authorities in many countries in the last few years means that processing transaction times have increased.

There is an opportunity to examine how the new electronic travel documents, which are now being issued by many countries, might be used in order to enhance security, improve facilitation and possibly refocus resources. The documents are subject to ICAO standards and it should be possible for commercially available reading equipment to handle almost all of them.

Many countries operate border control in such a way that the possession of the necessary entitlement will allow quick and relatively unrestricted admission and exit. In other cases passengers still need to be examined individually by border control officers or to make declarations prior to being granted entry or exit. In the latter case, e-MRTDs are used typically to verify identity and citizenship and, where applicable, to provide data for a watch list check or other control authority purposes.

4.2 Working Definitions

Automated Border Control system

"*A fully automated system which authenticates the eMRTD, establishes that the passenger is the rightful holder of the document, queries border control records, then automatically determines eligibility for border crossing according to pre defined rules.*"

Example: a State could deploy an ABC programme for all its citizens and legal residents who hold e-MRTDs.

e-MRTD Assisted Border Clearance

"*A system which assists the border control officer to authenticate the eMRTD via the use of a suitable document reader, establish that the passenger is the rightful holder of the document and query border control records. The officer himself determines eligibility for border crossing"*

Example: a conventional border control system for all e-MRTD holders who require clearance from a border control officer to cross the border.

The e-MRTD is a more secure document and can provide greater assurance of the identity of the holder, provided that the image (face and/or fingerprint) that is electronically stored on the e-MRTD is verified to that of the holder and that the cryptographic element operates as expected.

The rapidly increasing circulation of e-MRTDs that meet ICAO specifications affords the opportunity for border agencies to develop interoperable automated border control systems. The biometric data contained within the e-MRTD allows border agencies to automate the face-passport identity check normally undertaken manually. The fact that the biometric and biographical data contained within the passport can be read during the process may reduce the border agencies need to collect, store and secure large amounts of personal information.

4.3 Advantages of e-MRTDs

The rapidly increasing circulation of e-MRTDs that meet ICAO specifications affords the opportunity for border agencies to develop standard and interoperable automated border control systems. The biometric data contained within the e-MRTD allows border agencies to automate the face-passport identity check normally undertaken manually. The fact that the biometric and biographical data is portable and contained within the passport may reduce the border agencies' need pre-clear or pre-enrol large numbers of low-risk passengers.

In addition, border control agencies may be able to collect more relevant information about travelers without extra manual processes.

Automated border control systems can be quick, non-intrusive and simple to use, in order to appeal to a wide range of travellers from diverse backgrounds (families, business travellers, people with special needs, multiple languages etc).

ABCs have the potential to reduce queuing and waiting times in arrivals halls by diverting low-risk passengers through additional lightly supervised exits. They also introduce an element of 'self service' which may reduce the negative feelings some passengers have about airports and passenger processes. While providing benefits to the travelling public, ABC systems must not introduce new programme integrity risks to participating states. ABCs processes should be at least as robust as traditional procedures undertaken at the border.

There may be other, related processes at ports or border crossing points where the e-MRTD may prove useful in terms of identity verification. However, it is important to understand roles and responsibilities within these operational environments and distinguish between legislated and non-legislated requirements. Furthermore, such a distinction must be made absolutely clear to travellers.

4.4 Border Control Considerations and Caveats

4.4.1 Checking Document Authenticity and Validity

It is essential for border agencies to check that the e-MRTD presented is genuine, within its declared validity and not tampered with since issue. This can be done through examination of the face of the document (through image processing and a database of passport security features) or by a check of the integrity of the chip contents, or reference to a central passport issue database, or any combination of these. No system should be planned without this key requirement and suppliers' solutions should be independently tested.

4.4.2 Identification and/or identity verification

Clearly border control agencies will wish to identify each e-MRTD holder to a high degree of confidence. The biographical/biometric data may be cross-checked against other elements in the document and against issuer databases. See section on biometric matching.

4.4.3 Checking of watch lists and profiles

While passengers with e-MRTDs may be eligible to enter without formal clearance by a border control officer, some may still be of interest to law enforcement or security agencies. It will be necessary, as part of the ABC process, to send data from e-MRTDs to national watch lists. This may add extra seconds to the total transaction time. Consideration must be given to what response the system will give to a passenger who is positively matched or whose name is similar to a person of interest.

4.4.4 Determination of Eligibility

Once a passenger's nationality, identity and risk have been satisfactorily established, there needs to be a rule-based system which determines whether or not that person may be admitted without examination by a border control officer. This might be based purely upon nationality (for example citizens of the European Economic Area/European Union or countries with which the operating state has close political ties) or upon the existence of a residence permit or other permission to reside or where the passenger is in possession of a valid electronic visa. Consideration needs to be given to which passenger nationalities or classes of resident would be eligible for admission by ABC.

4.4.5 Passenger Declarations

Some states require passengers to make declarations about intentions, previous conduct or customs-dutiable goods. Consideration should be given to whether an ABC can handle such a process and what response the system would give if the passenger gave an incorrect or insufficient declaration. Again, transaction times will also be an important factor.

4.4.6 Passenger movement logging

In some states it may be lawful for border control agencies to record details of passengers (both biographic and biometric) who enter and exit. Consideration should be given to how much of the data contained in e-MRTDs is essential to border control and national security and whether legal powers exist to capture, store and use such data.

4.5 Implementation objectives

Assuming that certain port and border crossing point processes may be streamlined and enhanced as a result of the introduction of e-MRTDs, this should theoretically ease the flow of travellers through these particular processes. However, it must be acknowledged that such processes represent only a part of the overall port and border crossing experience. There are many other operational factors which need to be taken into consideration. Consequently, the overall movement of travellers through a given port or border crossing point depends upon a combination of these factors. It would be incorrect to assume that the introduction of e-MRTDs will make a material difference to this situation.

In time, as e-MRTDS become commonplace and associated processes become embedded, it may indeed be possible to moderately enhance the flow at specific points, such as passport control for example, providing that the necessary technical infrastructure is in place and operating reliably. For this to be the case, we must ensure equivalence of operational performance as well as equivalence of process across nodes. When this is achieved, the percentage of travellers able to successfully use automated facilities will increase, allowing respective authorities to focus more effectively upon the exceptions, providing of course that local legislation allows for this. However, this is unlikely to reduce the staffing requirement significantly as there will be a raft of new issues associated with the new processes, as well as the requirement to maintain an adequate manual fall-back position. Furthermore, throughput will only be enhanced for travellers falling into certain groups who are entitled to use such facilities. Therefore, bearing in mind the other operational processes involved, the overall movement of travellers through ports will be little changed, although certain official processes may be enhanced as a consequence of the introduction of e-MRTDs.

4.6 Caveat / Risk assessments

States need to consider carefully the risks, cost and benefits of e-MTRD-based admission systems and ensure that negative reaction from customers and stakeholders are minimised.

Clearly the first priority must the integrity of the state's border control. Passengers must not pass unchecked through automatic gates and this requires robust and accurate biometric comparison systems and accurate watch list checking. States should decide at the start of the project how passengers who fail either a biometric or watch list check should be treated: they may be quite innocent. Supervision of the system must be close and constant, to prevent fraud and to assist stranded passengers.

States should also consider the risks presented by the type of passenger who is allowed to use the system. Passengers who are no threat to Immigration controls may nevertheless be risky as far as Customs or Police authorities are concerned. The views of these organisations and other security agencies may need to be taken into account.

States may restrict the system to use by its own citizens, or by citizens of neighbouring countries or from political entities formed of separate countries.

If the privilege of using such controls is based upon a passenger fee or levy, the economics of the proposal should be carefully examined as they may conflict commercially with schemes devised by airlines and port operators.

Finally, states should consider what would happen to airport traffic if the system were to fail: there should be enough staff on hand to roll back to manual processing.

4.7 Different border control models

There may be potential for slightly different models according to geographic location and local policies, coupled to specific localized requirements. However, it would be pertinent to strive for an equivalence of operational process wherever possible in order to provide consistency of experience for the traveller. This, in turn, would promote consistency in operation, especially with regard to automated or semi-automated systems where user psychology plays an important part in realised performance. Clarity of purpose and simplicity of process will be important factors in this respect, and these should be the guiding principles of any such design.

4.8 Environmental considerations

There are many environmental issues to take into consideration. Some of these are obvious, such as the effects of temperature and humidity upon physical equipment, including capture devices. Some should be obvious to any experienced operator, including the effects of lighting and lighting variations upon any system relying upon optics for capturing information, for example as would be the case for facial identity verification.

There are some environmental considerations which are rather less obvious, but nonetheless very important with regard to the successful implementation of automated or semi-automated systems. Good signage and passenger flow fall into this category and are factors which are often not sufficiently taken into consideration. Similarly, the perceived comfort and overall efficiency of the environment is very important, especially where automated processes are envisaged. In such systems, fall-back procedures should also be made very apparent to passengers, ensuring that they are not unduly delayed if the system is not working for them. This is very important. It is a factor which, if not properly considered, will result in much higher than anticipated transaction times and attendant congestion.

Another less obvious environmental consideration lies in the area of underlying systems infrastructure. The infrastructure must be robust, scalable and properly maintained and supported at all times. There should be disaster recovery processes in place and the management of data should comply with the most stringent data protection and privacy acts. It should be understood that weaknesses in the underlying infrastructure can bring any such system to a total standstill. If this were to coincides with control authority staff minimisation or redeployment, then sever congestion will result.

4.9 Types of Biometrics

Within this document it is considered inappropriate to provide a technical overview of biometric technology in general, or details of each technique. Such information is readily available from a variety of sources if required. Suffice it to say that, in the context of e-MRTDs, the agreed biometrics are face, fingerprint and iris, with face mandated by ICAO as the primary biometric. In many instances, e-MRTDs will be issued initially with face biometric data, with other biometrics added at a later stage as and if required. It should be noted that, when using the term ‘biometric’ we are referring to image data rather than an algorithmically derived digital code. This has some implications for both processing and perceived privacy which should be understood.

4.10 Reference programs

Many countries have developed automated border control systems which utilise biometric technology to facilitate the movement of the traveller across the border. These systems are largely enrolment based whereby ‘trusted travellers’ must pre-register to use the system. These systems either use a token (passport, enrolment card) to retrieve an enrolment record and undertake a one to one biometric identity verification match, or, use the live capturing of biometric data to facilitate a one to many biometric check against a central database. (Appendix A)

4.11 Implementation Issues

The implications and consequences of introducing each layer of functionality enabled by the e-MRTD must be carefully considered. The ability to do so will depend largely upon the available infrastructure at a given point in time, coupled to in place operational processes. If the two become misaligned, then we shall experience difficulties.

In this respect, issuing authorities and agencies wishing to make use of the e-MRTD technology might like to consider a phased approach, whereby existing and future processes run in parallel until such time that future processes are proven reliable and all-encompassing. Such a desirable state of affairs may not be practically realizable in the short term, and this should be acknowledged.

Similarly, where a proposed new process requires the cooperation of third parties, for example port authorities and carriers, then it should be acknowledged that similar infrastructural and operational constraints exist in those areas and will need to be taken into consideration. Progress will be made via careful cooperation and coordination between all parties involved at a given location. However, on a global basis, this will take time and we should acknowledge this reality. Similarly, we should acknowledge that, especially in the early days, mistakes will be made and fallback / exception handling procedures will need to be maintained in full.

There will be a public-facing element to implementation which will need to be allowed for in associated plans and carefully managed accordingly. This will include fundamentals such as clear and timely communication, instruction and equally clear signage at physical points of presence.

There are many implementation issues to consider. Some of the primary issues are illustrated at a high level within this document. However, it is beyond the scope of this document to cover every issue in sufficient depth to ensure a seamless and trouble-free implementation in each eventuality. Those responsible for implementation must develop their own detailed plans according to their particular situation and aspiration. Suffice it to say that, depending upon the aspiration, implementation is likely to be non-trivial in the majority of cases, and this should be understood.

4.11.1 Working with suppliers

With respect to any operational, technical or process change which involves third parties, it is important to have an in place Service Level Agreement (SLA) which clearly defines the responsibilities and associated levels of performance expected from all parties involved. Typically, there will be a number of SLAs associated with a particular service, depending upon the scope and complexity of that service and how many distinct suppliers or collaborators are involved.

With regard to the use of e-MRTDs, there are several processes where SLAs may be appropriate. These include:

- The enquiry and registration process, where equipment and possibly operational or administrative services may be supplied by others.
- The operational process for immigration agencies, where both primary equipment and access to remote services may be supplied by others.
- The operational process for carriers and port security agencies, where primary equipment and related services may be supplied by others.
- Other processes as may be required by legislation or operational efficiency.

In all such cases, SLAs should be produced for all pertinent aspects of the overall service and agreed between the various parties involved. The scope of such SLAs should cover all operational conditions with exceptions noted where appropriate. SLAs should be written in plain language and include a glossary for any technical terms or other locally or operationally specific terms not in common language usage. Completed SLAs should be signed by senior and accountable representatives of the agencies and organisations involved, with copies kept by all parties. Any revision to an SLA should be subject to a change process, including re-signing by the original signatories.

Some examples of where an SLA might be appropriate include:

- Where equipment is supplied in order to read the e-MRTDs. Such equipment will be expected to perform according to a recognised level and with an acceptable level of reliability. Furthermore, if maintenance is required, it should be carried out to an agreed standard, by verified personnel and within an agreed time period following notification. All of these factors may be clearly defined within the SLA, including a full technical specification covering connectivity and interoperability as appropriate.
- Where a supporting technical service is supplied, such as electronic communications or the use of shared infrastructure. Such services should be clearly defined with respect to performance, existing capacity, scalability and availability. Furthermore, processes for requesting changes to such services should be clearly articulated. The technical support, maintenance and associated response times should all be clearly defined within such an SLA.
- Where access to a relevant external system, such as a database for example, is required. Such access will be expected to be available on a 24 hour 365 day basis and with defined response times. The applicable process for notification of planned maintenance should be included, together with an agreed maximum system outage in terms of hours per period or percentage of operational time. In this context, it will be important to clarify responsibilities and ensure that SLAs identify and include all parties involved in the ultimate presentation of the service.
- Where a managed service is supplied in order that a specific process may be outsourced to a third party. In the case of a managed service, the service supplier must clearly state the precise and inclusive nature of the service, together with any exceptions envisaged. The SLA should reflect this and include agreed performance levels for all aspects of the service. In addition, penalties for failing to deliver the service, or any part thereof, should be clearly stated and agreed.

There are many other areas where an SLA will be appropriate, but the above examples provide an understanding of the general concept.

Having defined where SLAs are required and establishing them accordingly, it will be important to ensure that they are properly maintained. Within a given agency, the responsibility for this should be clear, with any processes required developed and implemented. This responsibility may ultimately fall under a contracts or procurement department, but should have an input from operational personnel who are experienced in the area concerned. Furthermore, the provisions of such SLAs should be adequately communicated to operational personnel and, where appropriate, reflected in their everyday processes, in order to ensure compliance on all sides. Given the importance of these operational processes and the likelihood of an increased use of technology, it is important that SLAs cover all appropriate areas of operation.

4.11.2 Operational Considerations

e-MRTDs as specified by ICAO offer another possibility: if entry may be granted to classes of passengers - as well those individually enrolled - then border control authorities may possibly make additional savings. For example, if nationality alone (or the possession of a valid electronic visa)

confers rights of entry or exit without detailed examination, then the e-MRTD (with its biometric information) may be all that is required to allow a passenger to proceed.

There are a number of requirements for an e-MRTD system if it is to be used in this way:

- The state accepting the document must be satisfied that the issuing state's document production, application and issue procedures are of a high standard and are not susceptible to fraud.

- The accepting state must be satisfied that the nationals of countries holding e-MRTDs are not a high risk from a crime, smuggling or illegal migration perspective.

- The passengers using e-MRTDs must satisfactorily identify themselves to the receiving system through something which only they have (a biometric) or know (a personal identification number or code)

- The system must only allow passage to eligible travellers and prevent fraudulent use such as use by multiple persons ("tailgating") or climbing over or under an unsupervised barrier.

- The system must be positioned in secure, supervised and well-lit area and supervised to an extent that border control or other officials can effectively and confidently monitor admissions and exits and react to exceptions.

- The system should also fall back to a safe (e.g. closed) mode in the event of electronic or mechanical failure so that border security is not compromised.

- The system must not harm or injure passengers and if the system fails with a passenger trapped within barriers there should be an escape mechanism or warning device by which assistance can be summoned.

- There must be simple procedures for dealing with passengers trapped within the booth/gates or rejected by the system.

- The system must be able to allow young, elderly or disabled persons to use it where practicable, unless special facilities are provided.

- There should be adequate training for new passenger users, guidance in multiple languages and assistance on hand in case of difficulties.

- The system should be able to detect e-MRTDs which are defective, have been tampered with or which have been revoked by the issuing authority. A fallback process is required to deal with passengers who have not been recognised or have been rejected.

- The system should be able to cope with all ICAO-compliant types of travel document and as many types of biometric as the operating state required and is satisfied are reliable

- The system should keep secure the personal or document data it handles, both within the mechanism and within the links to other systems.

- The system should be proof against spoofing of the biometric required to complete the identity check and the false accept rate needs to be minimized to an acceptable level.

- The system may need additional input from a passenger aside from presentation of a passport and a biometric. It may be necessary for the passenger to make a declaration by pressing keys or a screen area in response to specific questions – e.g. 'Do you have any goods or valuables to declare to Customs on this occasion?'

- The system may consist of one process (identify, authenticate, admit) or more (e.g. identify, authenticate… get authority to enter on a ticket… present ticket for admission), depending on the policy of the owner.

- Operational processes and systems performance must be equivalent across nodes. This has been mentioned in various parts of this document and is further stressed here. Without such equivalence, the confidence we might have in any such application will be significantly diminished.

4.11.2.1 Human Factors

It is important to fully acknowledge human factors within the design or aspiration for any such application. Human factors are diverse and include obvious requirements, such as the need to cater for people with physical disabilities, and non-obvious requirements such as understanding user psychology. Such matters become especially important where the use automated or semi-automated systems is envisaged and the variability between individuals becomes increasingly important. An example lies in the area of non-obvious disabilities whereby, for various reasons, an individual may find it difficult to interact properly with the required procedure, resulting in an abnormally high incidence of rejection.

Similarly, it will be important to acknowledge language and other cultural distinctions which might impact the successful operation of an automated system. In this respect, it is easy to underestimate the role that a human operator plays in existing processes and consequently make incorrect assumptions around the value of automated processes. A workable balance must be achieved in this area.

It is also important to understand the implications around ageing, sickness and ethnicity with regard to the use of an automated system. This is a relatively complex area, but must be taken into consideration with respect to automated or semi-automated systems.

4.11.2.2 Bulk enrolment if validated by risk assessment

The ABC may provide for the bulk enrolment of identities from a trusted source (called 'reference identities'). This will reduce the number of enrolment processes the traveller has to endure to take advantage of the ABC as well as reducing the establishment and maintenance cost of the reference identities. The bulk enrolment processes must address both initial establishment and periodic updates from the source.

The process for establishing that the source can be trusted must include an appropriate risk assessment and be guided by appropriate quality standards and/or accreditation. A suitable governance and audit regime should be established to maintain public confidence in the reference identities.

4.11.2.3 Improved return against manual procedures

The ABC must demonstrate an improved return against manual procedures via an agreed set of performance indicators. The indicators should be such that the administrative overhead in acquiring them is minimised. Where possible the indicators used should reflect return characteristics that include the ability to redirect manual efforts to high risk areas.

4.11.2.4 Environmental Factors, location and location requirements

There are some obvious environmental factors to take into consideration, such as the avoidance of excessive temperature, humidity and direct sunlight, which will need to be balanced against the realities of construction, available space and overall flow. However, the operational environment from the users perspective, will undoubtedly have an impact upon realised performance and the extent to which facilitated operation will be required. In this context, factors such as perceived space, good signage, an attractive and welcoming presentation, the provision of current information and intuitive operation will be paramount.

In terms of location, ABC facilities should ideally be placed within a logical flow as travellers make their way to and from the point of embarkation / disembarkation. They should be positioned in such a way as to accommodate the highest levels of anticipated traffic without appearing to be overly congested – an area in which many current facilities fail badly. This will naturally be a product of throughput, good design and collaboration with the port authorities and carriers in order to devise the most practical and timely flow.

The chosen location should also take into account support factors such as exception handling, technical support, manual fallback procedures and associated remediation, ensuring that such support may be provided quickly and efficiently if and when required. This suggests an integrated overall design which anticipates worst case scenarios and plans accordingly.

From a technical perspective, the ABC location should be adequately supported with the provision of regulated power, communications connectivity and an agreed degree of spare capacity. All connections should be according to standards and should be secured. Lighting should be appropriate to the specific location and should be integrated with signage and information display requirements in order to remain unobtrusive and efficient.

All of the above should be considered with respect to future capacity requirements. If these are thought to increase over time, then capacity expansion should be designed in at source, without the need to compromise or confuse the current operation.

4.11.2.5 Flexible and compliant to accommodate flow changes (Flexible configuration)

The ability to be able to adapt the ABC to changes in the physical environment or demands on it will enhance the utility of it. Consideration should be given to design characteristics that facilitate ease of installation, relocation and/or replacement within the constraints of the adopted standards for the equipment.

Flexibility also includes the ability to enhance individual components such as a reader and maintain the operational capability of the overall ABC. This means that the approach to component integration should facilitate their interchange as far as is practically possible.

4.11.2.6 User Acceptance of given Biometrics and/or Procedure

While one might take the view that users must simply comply with local legislative requirements, the manner in which such requirements are implemented will have an impact upon user perception and, consequently, the overall flow through the process and hence realised performance of the overall system.
The rule of thumb in this respect is to implement the barest minimum of biometric processing and associated procedure, necessary to satisfy local legislation. In most cases, simply matching the user's biometric against the stored reference on the document should be sufficient from an identity verification perspective. Other checks, such as document validity etc., should be transparent to the user. The overall process should appear logical, slick and efficient from the user's perspective, with good guidance as to what is expected at the identity checking stage.

The broader question of which biometric might be more or less acceptable to the user is somewhat academic as de facto standards are emerging, based upon local requirements. A more pertinent question is whether the background processing of any such information is clear to the user and whether such processing is considered as necessary to the task at hand. In terms of border control, many will consider that live comparison with the stored reference on the document is all that is necessary. Any additional capture or storage of the biometric will be of concern to many citizens. In this context, implementing authorities should be open and honest as to exactly how they are using, or propose to use, any biometric or otherwise personal information. Anything less will erode confidence and could be damaging to the relationship between citizen and state. Furthermore, unauthorised or obscure use of such data will increase the possibility of data related errors and incorrect assumptions. A reality which serves no-one.

User acceptance of the overall process implies an agreement between citizen and state as to appropriate levels of border control. Consequently, it is based upon understanding and trust. Implementing agencies should therefore strive to promote such an understanding and thus engender trust. Roles and responsibilities must be clearly defined and precise details of how personal information, including a biometric, is being used must be openly provided.

4.11.2.7 Scalability

There are various aspects of scalability to consider. Firstly, technical scalability. In theory, this is easy to provide for as one can simply add infrastructure in order to accommodate increased loads. However, there comes a point of diminishing returns when the various systems and sub-systems are operating at levels for which they were not really designed. This is particularly relevant with respect to databases and information processing, especially where there are operational rules to take into consideration. Such questions should be addressed right at the start of any relevant ABC design. Furthermore, in many cases, there will be a dependency upon in-place infrastructure which might be supported by third parties. This should be understood at the start and form an integral part of the overall design. There will always be a limiting factor, or 'bottleneck' to capacity and this should be identified and understood. If third parties own or otherwise provide elements of the infrastructure, then clear service level agreements (SLAs) should be drawn up which allow for agreed levels of scalability. The entire technical design should be fully documented and such documentation maintained. This will be necessary, in any event, to satisfy information security and compliance requirements.

Another form of scalability lays in physical architecture and the provision of the operational process. This is a part of the overall port or airport design and is often orchestrated by the port authority. However, it would be appropriate for a tight coordination between port authority, border control agencies and carriers in order to understand scalability and potential future requirements.

This is a potentially complex area and it would be useful to produce and maintain clear documentation which could be shared between the relevant parties.

Yet another form of scalability is the efficiency with which biometric identity verification systems may be maintained and intelligent decisions made upon transactional results. A small system with three or four points of presence may be maintained with relevant ease, providing trained personnel are available. Such maintenance will include the setting of biometric matching thresholds and the monitoring of realised transactional performance in order to refine such settings, ensuring an equivalence of performance, and therefore reasonable interpretation, across nodes. A larger system, perhaps with ten or twenty points of presence, makes such maintenance and interpretation of results more problematic. A very large or linked system, with perhaps many tens of points of presence, raises a completely different set of requirements, especially if any equivalence of realised performance is to be hoped for.

4.11.3 Technical Considerations

4.11.3.1 Transaction Times

With regard to automated identity verification transaction times, there is a distinction between 'verification' – a 1 : 1 comparison of the live biometric with a stored template, and 'identification' – a 1 : many search among templates in order to match the live biometric. The latter approach typically requires a longer processing time and greater computational power, depending upon the chosen biometric and the size of template database being used. e-MRTDs have the capability to store the biometric reference template within the document, thus negating the need for a separate database and facilitating a 1 : 1 match within a reasonable processing time. In this context, research suggests that within 3 seconds is an acceptable processing time within which to match the biometric. This objective should be easily realized in practice using the on-board biometric template of the e-MRTD within a properly configured system.

4.11.3.2 Success and matching rates

Understanding error rates in the context of biometric matches is a complex undertaking. Firstly, we can only readily identify false rejections (where the individual has been incorrectly rejected by the system), as false acceptances (where an impostor has been incorrectly accepted) will not be detected in real time. Furthermore, there are three main blocks of factors which directly affect realised performance. These are:

- Technical factors, including total systems performance and equivalence of performance across nodes
- Environmental factors, including temperature, humidity, lighting and 'soft' factors such as signage, traffic density and ergonomics
- User factors, including user psychology, understanding and habituation.

Of these, user factors can have a more dramatic affect upon perceived performance than is often acknowledged. In many implementations, the reality of this will be learned over time. Environmental factors may, in some instances, be harder to control than expected due to the multi-user tenancy of many port environments. Technical factors may, in some instances, also be harder to control than expected due to shared infrastructures and the lack of centralised control.

As a consequence of these multiple factors, it would be naive to assume a given biometric matching performance based upon device manufacturer's proposed figures alone. Proper testing in a

representative environment with a representative user base will provide a better understanding of what might be expected in this context.

It will be additionally important to implement a methodology with which to maintain performance across nodes, in a manner which is measurable against defined targets. This will entail the real-time monitoring of *perceived* performance at each point of presence, together with the ability to adjust configuration parameters as necessary to maintain performance at a given level.

As indicated, the qualification of biometric matching performance is a complicated affair. In depth understanding of all the related issues is not commonplace. In most instances, training will be required for those implementing such systems. In general terms, acceptable error rates are often quoted as 1 % for 2D facial recognition, 0.05 % for fingerprint, and 0.0001% for iris recognition. However, how such targets are realized in practice and measured on an ongoing basis is a matter for careful consideration.

4.11.3.3 Liveness detection

Liveness detection is an understandable aspiration for real-world biometric processes. Clearly, there is a possibility that attempts would be made to fool such systems with fake credentials such as false fingers, iris prints or deliberately altered facial features or masks. Biometric device manufacturers continue to develop techniques with which to combat this possibility. To date, these have included the detection of movement, the detection of temperature, the detection of a regular pulse and other measures. However, liveness detection does represent a technical challenge and it is likely that it will continue to be developed over time, in order to combat increasingly sophisticated attempts to undermine such systems.

4.11.4 Systems Considerations

4.11.4.1 Integrity

Maintain systems integrity throughout the entire operational chain and in compliance with ICAO 9303 (ref)

4.11.4.2 Adjust respective trust levels of system components

An e-MRTD may contain more than one type of biometric data. The ability for ICAO countries to configure access to public key information for their needs would be advantageous.

4.11.4.3 Resilience

Resilience of the technology incorporated into the e-MRTD would have to be considered within the systems design with regard to:

- Damage from reasonable wear and tear
- Damage from atmospheric variables such as heat, cold and ambient moisture
- Deliberate tampering or attempts to access data via:
- Physical interaction/reverse engineering, or
- Electronic data ‘skimming devices’

4.11.4.4 Backwards Compatibility

As take up of the e-MRTD's increases and technology evolves, careful consideration should be made to existing standards and technology that are in use by ICAO participating countries. New advances in the capturing, storage and verification of biometric data should not render previous or existing technology solutions obsolete. Operational processes must also accommodate all existing standards.

4.11.4.5 System Security

The security for the e-MRTD and supporting systems infrastructure should be no less than for existing border control systems and procedures. Minimum-security protocols would have to be established to assure integrity across all ICAO participants.

4.11.4.6 Equivalence of performance

Performance should be measured against existing processes (both manual and IT systems). Benchmarks should be established for gauging performance of key components such as e-MRTD readers, biometric capture and verification hardware (lighting, cameras etc), and user interaction devices. This must also be coupled with the setting of acceptable processing times across the end to end biometric validation and verification cycle (such as FRR, passenger facilitation rates, passenger cycle times, and efficiency gains). Furthermore, an equivalence of perceived performance should be maintained across all operational nodes in order to ensure a consistency of both performance and user experience. Without such an equivalence, confidence in the operation of the system overall will be significantly compromised.

4.11.5 Privacy

It is important that proper consideration is given to all aspects of privacy when dealing with travellers and their personal information. There are various elements of privacy to consider in this context.

Firstly, data privacy. Naturally, all in place data protection and privacy legislation should be complied with. Such legislation may vary slightly in detail from country to country, although general principles apply almost universally. These include the prohibition of passing personal data to third parties without explicit permission from the individual concerned, using personal data for purposes other than that required to facilitate the task at hand, storing personal data after the event, and so on. It would be good practice to produce a data protection and privacy leaflet with respect to every border control implementation, in order that both travellers and border agency personnel are fully aware of requirements, roles and responsibilities.

Another aspect of privacy concerns physical privacy throughout the border control process. Efforts should be made to ensure that the user has private space while undertaking the border control transaction, whether fully automated, partly facilitated or fully manual. Such a practice promotes good security as well as respecting the privacy of the individual.

4.11.6 Interoperability

4.11.6.1 Interoperability overview.

Interoperability is a word often misused and even more frequently misunderstood. True interoperability is not simply an issue of technical compatibility, but rather encompasses a raft of both technical and process related issues.

From a technical perspective, we need compatibility not just at the front end device layer, but throughout the entire end to end system. Furthermore, a given transaction may need to reference multiple systems, some of which have interoperability requirements beyond the scope of, and possibly in conflict with, those of the transaction. Establishing the complete chain of interoperability as required to support a given process from end to end, including any variances to that process, is likely to become quite complex. It may well entail translation layers between protocols, physical interfaces, network infrastructures and more.

Assuming we achieve complete technical interoperability, as outlined above, the overall end to end transaction may still be rendered ineffective if the attendant operational processes are not similarly aligned. If, for example, a different interpretation is based upon the value of a biometric identity check, then the user experience may be quite different at specific points within the overall transaction (either side of a border crossing for example). If registration processes are not aligned, then confidence levels with regard to documents from different issuing authorities will be similarly misaligned. This might result in different user experiences (and subsequent interpretation) at different points of presence, accentuated perhaps by different levels of hardware configuration.

True interoperability, from both a users and administrative perspective, will only be achievable if both technical infrastructures and operational processes are aligned on an international scale. This will additionally require an equivalence of operational performance between nodes, without which, any interpretation placed upon authentication at multiple points will be invalid.

4.11.6.2 The transition between manual processes and the introduction of automated or semi-automated systems (ABC systems).

When planning the introduction of an automated border control system, it is essential to understand the transition from current processes and what this entails for both supporting staff and users. In both cases, there will be a learning curve while individuals familiarise themselves with the new operational system and associated processes. In this context, it will be necessary to provide proper training for border agency personnel and mount a communications programme for users who, especially in the early days of implementation, will likely require a good deal of assistance. Consequently, the provision of hands-on assistance and good signage / general information will be paramount in the early days of a successful implementation.

Related experience to date suggests that, for frequent travellers, an assimilation period of around three months would be required while, for less frequent travellers, twenty four months or more might be required. This will need to be accommodated within the overall implementation plan, including provision of the necessary human resources in order to support such a transition.

If this factor is not adequately attended to, the realised performance from the ABC system is more likely to be inconsistent from both the operator and user perspective.

4.12 Fallback Procedures and Exception Handling

4.12.1 Fallback/fail over procedures

Good system design, coupled with robust business continuity planning, is key to ensuring border integrity is not lost in the event of system failure of the automated border processing system.

Software systems must ensure that at the point of failure, or loss of data communications, all automated border processing ceases and passengers are referred for normal manual processing. Hardware design must also allow for gates to be secured but trapped passengers allowed to retreat back into the arrivals hall for manual processing.

System monitoring is required to alert system administrators and border control staff of degradation of performance levels of the system as whole and by component. It should also provide the ability to set configurable performance thresholds and be notified automatically when these are not met. This allows for remediation work to commence prior to matters escalating, or in the event of unforeseen component failure, instant diagnosis of the issue.

Business continuity plans and procedural statements must also clearly outline the steps needed to be undertaken by border agency staff in the event of system failure and progress redial action will ensure the integrity of the border is not compromised.

4.12.2 Exception Handling

Countries should ensure that those passengers failing any component of the system checking undertaken by the ABC system (identity verification, watch list checks, non compliant passport, chip integrity check) should not be further processed by the system. These passengers should be referred for manual border processing and should receive preferential or priority processing facilities.

Countries should also make sure that appropriate staff members are alerted immediately if the system fails to admit a passenger for any reason or the passenger fails to respond to system prompts within a reasonable time.

5. ARCHITECTURAL DESIGN CONSIDERATIONS

5.1 Introduction

The architectural design of any ABC system is important from many perspectives if the implementation is to prove successful and sustainable over time. Some of the fundamental requirements are outlined below;

- The overall design must be technically compatible with associated standards of operation and communication, while allowing ongoing flexibility to accommodate developments in this area.
- Wherever possible, the architectural design should be modular using COTS components, allowing for easy re-configuration or expansion in a vendor agnostic manner
- The design should support systems redundancy and fall-back in order to maintain operation in the event of host component failure
- The physical configuration, including signage, should conform to accepted best practice in order to present consistent user interfaces
- The design should accommodate scalability and should not be limited in this respect
- The design should meet the requirements and obligations of the hosting administration with standard components and should not be bespoke
- The architectural design should be easily supported by third party support organisations and should not be vendor specific

Due to the commonality of operational requirements across countries, it is likely that a fairly generic high level design may evolve, at least as far as it is perceived by both travellers and border control personnel. Such a design will nevertheless allow for distinctions in individual components and flexibility in deployment and scalability, while remaining intuitive in use. This is desirable, as policy and process should take precedence over the mechanics of delivering it.

5.2 Physical design and ergonomic considerations

5.2.1 Overview

The following points summarise the requirements for the physical design of an ABC point of presence.

- The overall design should remain intuitive with a minimal learning curve
- The physical design should be attractive and welcoming
- The operational environment should remain comfortable and enhance personal privacy
- Attention should be paid to signage and instruction
- The physical and technical environment should remain consistent and sustainable
- The physical design should support, and be aligned to, the operational process

5.2.2 Design considerations

An ABC system design should not be undertaken in isolation, neither should it attempt to simply replicate the existing border crossing process by automated or semi-automated means.

A more robust approach would be to firstly ensure that the current processes, together with any perceived issues, are properly understood and documented. Secondly, an exercise should be undertaken to translate these processes into an automated or semi-automated model, noting how they may be improved upon or made more robust within the new system. Perceived ease of use from the user's perspective will, in part, determine the success of the system.

Factors such as anticipated transaction times, throughput, usability, resource requirements and signage should all be taken into consideration and a margin for error incorporated into the design. Similarly, attention should be paid to sustainability, the support model and future scalability.

5.2.3 Attractiveness of design

It is important that the physical design of the ABC point of presence be perceived as attractive and welcoming by the user. This is important whether participation in the scheme is voluntary or mandatory, as it will directly affect the usability and hence realised performance of the system.

Particular attention should be paid to colour schemes, lighting, signage (in appropriate languages), operational space and the intuitiveness of the overall design, in order to ensure that users should feel relaxed and confident as they interact with the system.

5.2.4 User experience and psychology

It is natural that users, when confronted by a new process or system, will initially feel a little apprehensive and unsure of themselves. This will particularly be the case if they are required to undertake the process in a busy public environment, where they may be concerned that their own lack of experience may cause delays for others. For some users, this will represent a very stressful situation, especially when unfamiliar technology is involved. The more stress a user feels, the more likely they are to make mistakes or be inconsistent in the way they interact with the system.

This situation may be alleviated by a combination of good systems design, a comfortable and intuitive operating environment and helpful assistance from the operational staff on hand. With good signage, guidance and a friendly interaction with local staff, users may quickly acclimatise themselves to the new operation. If any of these factors are poorly implemented, then it is likely that a negative user experience will translate directly into poor operational systems performance.

5.3 Electrical design and safety considerations

Within the broader context of an ABC implementation, attention should naturally be paid to the physical and logical architectural design. Where such design involves electrical components and sub-systems, it is important that, at every level, the design complies with the relevant electrical standards, including in areas of electromagnetic radiation, earthing, specification of cables and connections, general safety considerations and so on. Furthermore, in order to provide the necessary levels of assurance, such systems should be tested and documented against a defined and agreed test schedule. Such documentation should form part of the eventual hand-over to the implementing agency.

Any subsequent changes to the systems architecture should be similarly evaluated for compliance, tested and documented accordingly.

5.4 IT design and infrastructural considerations

5.4.1 Introduction

In order to realise the potential benefits offered by the e-MRTD, it will be necessary that an appropriate supporting infrastructure is in place at each point of presence where the documents might be used. This infrastructure will include front end components such as document readers, biometric capture devices, user interfaces and physical barriers, as well as background IT processing, the use, where appropriate, of databases and the necessary communications infrastructure.

Within the context of a given transaction, the use of this entire infrastructure will determine the realised performance. It is this 'realised' performance which is most important both to traveller flow and accuracy of automated process. The potential benefits of the e-MRTD will only be realised when the entire supporting infrastructure is optimised for the in-place process. This, in turn, requires that such process is properly considered and fine tuned to work with both current and previous technology, as well as delivering the accuracy of processing required. Furthermore, this should be achieved without undue inconvenience to the traveller, to whom such processes should be largely transparent.

The following paragraphs provide an overview of some of the salient points to be considered within the context of using the new e-MRTDs. However, we should remain conscious that this process must accommodate, no doubt for some considerable time to come, a wide variety of travel documents and those individuals presenting them. We are, after all, dealing with an evolving situation and our underlying infrastructure and supporting technologies must reflect this reality. In this respect, it is pertinent to mention the situation with regards to API, APP and the provision of passenger information as currently understood. We therefore start with an overview of API and APP before considering software and hardware infrastructure.

5.4.2 Advance Passenger Information (API)

API in the travel environment allows border authorities to undertake checks on passengers prior to arrival in the country of destination. The data requirements for API normally include flight number, expected date of arrival and biodata which is available on the passport data page.

The advantage for a border control agency to receive API is that resources can be allocated to passengers who present the highest risk and therefore require intervention, while the majority of passengers will be able to proceed through the arrivals process with minimal delay. API can also include extra data such as intended address in the country, visa status and other relevant data required to comply with legislation.

Accurate API normally includes the use of a passport reader by an airline to collect the data, thus minimising keying errors. API can be sent during the check-in process, or when the aircraft leaves the ground as a complete record of an aircrafts passengers on board. API can also be used in the departure process, thus allowing for an exit control system which will complete the passengers movement record and indicate whether a passenger has met all visa conditions of their visit, such as compliance with a length of stay.

5.4.3 Advance Passenger Processing (APP)

APP, also sometimes known as interactive API or iAPI, allows airlines to verify a passenger's travel authority at check-in. It also allows collection of passenger data at check in and transmission of that data to border agencies prior to arrival of the aircraft. This facilitates an effective authority to carry process. For example, API is sent from the airline to immigration to check on the immigration status of the traveller, including the visa requirements, whether the passport is lost or stolen and returns a message to the airline as to whether they should allow the check-in process to continue or cease.
The result is an "immigration pre-clearance" or an "okay to board", depending on the receiving countries immigration process.

With APP, border agencies are able to offer an unparalleled level of service delivery to passengers, airlines and industry.

The benefits include:

- A one-stop client service for industry
- Best practice passenger management through faster clearance for passengers at airports.
- Quantifiable reduction in undocumented arrivals
- Reducing the risk of fines to airlines for carrying illegal passengers
- More effective allocation of staff through pre-arrival risk assessment of passengers using API.
- Improved border security.

5.4.4 APP/API and automated border processing

APP provides a significant advantage for border agencies wishing to automated the immigration clearance element of border processing as the process can considerably reduce the risk associated with automated clearance as all passengers who have undergone and APP process will have effectively been pre-cleared and will have had their visa validated.

5.4.5 Software

When using e-MRTDs within an automated or semi-automated process, it is typically necessary that the document leads to an authorisation which can be used to control a portal or gate of some description. In order to transform data that's read from the document into such an authorisation, many rules in separate software components may need to be evaluated and various software modules or routines may need to be accessed in the process. The following outlines some of these factors.

Reader software. For both optical and RF readers, the appropriate software drivers are necessary.

Security software. For gaining access to the chip, authenticating or even decrypting the data it is necessary to use security software components.

Authorisation software. To cross-reference data within either black-list and/or white-list systems or against separate authorisation rules. For example; the use of an automated border control based upon the nationality of the presented document in combination with the outcome of referencing a relevant database.

Authentication software. Specific software components to determine the authenticity of the presented document. This component does not seek to authenticate the data contained within the document, but verifies authenticity against understood visual security features.

Verification software. Specific software components to determine whether the presenter of the document is the same person to whom it was originally issued. This is undertaken via a comparison of the reference biometric data held within the document, with live biometric data supplied by the document holder. In addition to the necessary biometric matching algorithms, such software might usefully include a liveness detection capability.

Control software, combines the outcomes of all the software components described above and maintains the status of both the overall system and its immediate environment. For example it may monitor inputs from associated systems such as fire alarms, providing an over-ride to controls where appropriate. It may have the added capability of monitoring critical infrastructure components and being able to pinpoint failures accordingly.

Software should also monitor and maintain an equivalence of performance across operational nodes. This should be a real-time process, ensuring that in place processes are adequately supported by technical performance. If such an equivalence is not achieved, the confidence that can be placed upon the results from any such system will be significantly diminished.

5.4.6 Hardware

There will typically be a variety of hardware associated with the use of e-MRTDs within a travel environment. The precise combination of hardware at a particular point of presence, may however depend upon the operational requirements at that particular point. For example, domestic as opposed to international arrivals and departures at ports. Furthermore, there may be various degrees of automation in place at different points of presence. Again, we must bear in mind that we are dealing with an evolving situation in this respect and that the precise hardware complement at a given point may be subject to change. Similarly, as technology itself evolves, different hardware requirements may present themselves. Such factors serve to highlight the need for robust capacity planning and the provision of a flexible and scalable supporting infrastructure. Indeed, this will largely determine the ability to roll out the desired capability in line with aspirations. The following outlines some of the pertinent hardware elements.

Document readers. Familiar components which shall need to evolve in order to accommodate the e-MRTDs. Furthermore, their physical form and configuration may need to evolve in order to co-exist within other components, such as kiosks for example. To ensure a successful read in an automated process the reader my also have to be designed to hold the e-MRTD in place during the optical and RF read, or even taken from the traveller and released when reading is completed.

Biometric capture devices. Such devices must be fit for purpose within the pertinent operational environment. There is room for evolution in this respect, for equipment featuring all ICAO supported biometric techniques (finger, face and iris). Again, consideration should be given to the physical integration within other components such as kiosks, manned booths and so on.

Local processing devices. At the point of presence, there will typically be a data processing capability in order to coordinate inputs from other devices, undertake cross-references with other systems and, often, to provide a user interface. This may take the form of a computer terminal, a kiosk or processing power embedded within another sub-system.

Physical barriers. There will, depending upon the degree of automation, often be physical barriers such as turnstiles or other controlled portals. These will typically be controlled by inputs from the local system (which may reference external systems) and will incorporate fail-safe mechanisms in order to meet the requirements for health and safety.

Data routing devices. In order to position a local point of presence within a larger infrastructure, a data-communications layer will be necessary. This layer will contain a variety of routers, switches, firewalls, load-balancers and other devices as necessary to support the transaction levels anticipated. This layer should of course be scalable to meet increasing levels of demand as the broader infrastructure evolves.

Back end data sources. In many instances, local processes may wish to reference off-site databases for specific purposes. In such cases, the remote databases (or distributed nodes thereof) will have been designed according to their own infrastructural requirements. It may be necessary to revisit these requirements if substantially increased access is required.

There will be a raft of other technical and non-technical hardware required in order to support the overall process. This will include that required for channelling throughput as well as appropriate signage. Indeed, any substantially increased or otherwise altered operational process, is likely to require a significant investment in supporting hardware, together with its installation, commissioning and ongoing maintenance. Such factors should not be overlooked when designing enhanced processes to support the e-MRTD.

5.4.7 Additional Design Considerations

For the physical design the major consideration is whether there will be supervision or not during the operational time of an automated border or access control installation.

5.4.7.1 Unmanned installation

For an unmanned installation there is no form supervision at all, at least not enough to prevent fraud handling and / or passing the installation as in a normal procedure. There are two possibilities of an unmanned situation; the one where there is camera surveillance where fraud or unauthorized passing cannot be prevented but is seen and recorded, so the person(s) involved is known. Other one is the situation were there is no surveillance at all or not close enough to the installation.

In the last case the installation should be designed based on high end security components. That means it is necessary to have an access control installation with a separated zone in which only one person is allowed to step in and step out. In this separated zone the biometric verification should be installed so that it is not possible to transfer an authorisation to another person and help him through the installation on another identity.

In the situation were there is enough video surveillance it is possible to use another access control gate, although it still is necessary to regulate one person going through the installation and prevent transferring an authorisation or be sure that in that case alarms will be activated.

In both cases it is advised to use a form of biometric and type of capture device that have a strong form of authenticating the live image, with live and / or fake detections and algorithms.

5.4.7.2 Manned installation

The business drivers for a manned situation are different for those in an unmanned installation. Most of the time these installations will result in a more efficient way of working for border police or security officers.

In these manned situations two kinds of operational process should be considered. The first situation reflects a 100% self service process including biometric verification, the other situation is where authorisation and / or authentication of the token is self service and verification is fully manual without the use of biometrics, or possibly semi automated using biometrics, but with an officer analysing the outcome and undertaking verification. In the latter situation, the installation doesn't need any specific access control requirements other then those that are related to the desk where the officer is undertaking identity verification.

In the case were the whole process is self service it is still necessary to have a separate verification zone although it doesn't need to be fully closed as in an unmanned situation. In the design of these installations the main consideration is to create a neat process and overview on the process for the supervising officer. In cases where fingerprint or iris pattern verification is used a strong live and / or fake detection is necessary because the supervisor cannot detect fraudulent attempts with a gummy finger or printed lenses from a distance.

5.4.7.3 Compliance

It is of course necessary to design an installation that is compliant with all in place security and safety regulations. Security regulations influence all aspects of the overall design: physical, electronics and control, systems and data security. With regard to security, it is important to have the same level of integrity throughout the system.
With regard to compliance with safety regulations, much depends upon the choice of physical access control hardware, in combination with the controlling electronics and overall operational process.

5.4.8 IT Infrastructure

Mention has already been made of some of the software and hardware required for the supporting IT infrastructure. It should be remembered that, as previously stated, realised performance depends upon the entire infrastructure (as required to support a specific process) and its correct operation. This reality should be taken into consideration during the design of any enhanced process to support the use of e-MRTDs.

Overall network and data security should also feature prominently within our design and associated processes. Factors such as access control, transaction rollback, audit trails and disaster recovery should form an integral part of any such design. In addition, the means to test for vulnerabilities across the entire infrastructure should be incorporated at the outset, together with an appropriate process to ensure that proper responsibility is taken by the appropriate department. The design of any such system, dealing with the personal information of citizens, should be subject to external scrutiny and auditing. Processes and accountabilities should be established in order to be able to demonstrate data flow and an appropriate use of personal information, including the destruction of that information when no longer needed to facilitate the overall process.

Specific and broader network security should also be considered, especially when external input or read access is envisaged. For example, off-site access may be permitted to some systems in order that other authorities, or even the traveller themselves, may be able to input data. If such external access is to be considered, then network security becomes paramount. This includes the exchange of

data between systems and how such data may, where applicable, be normalized and aggregated for a specific purpose, and what happens to it after that purpose is satisfied.

In short, it is easy to focus predominantly on the front end, point of presence components. However, the operational system will typically consist of much more than this, and equal consideration should be given to the broader infrastructure, how it functions, its performance and, most importantly, its relative security.

5.4.9 User Interfaces

The on-site user interface may be supporting a control authority operator or the traveller themselves, or perhaps both parties. There may also be off-site user interfaces to some elements of the overall system. In any event, there are some common requirements, as articulated below.

The user interface should be attractive and intuitive, enabling the user to easily and quickly understand precisely where they are in the process and what the next steps are.

The interface should be available in multiple languages and associated character sets, which should be user selectable at the start of the process and can also be selected automatically based on the nationality of the e-MRTD. Where appropriate, commonly understood symbology may reinforce the textual content.

Where user-facing, the interface should accommodate disabilities such as sight defects or hearing difficulties as well as limitations of physical dexterity, where it is practical to do so. It may be appropriate to configure special channels, for example for wheelchair access.

Fall-back procedures should be incorporated wherever possible into the user interface in order to offer guidance for users, even if communication with other systems components is interrupted.

The user-facing interface includes appropriate signage in order to identify correct channels and terminals. This should follow similar rules of being attractive, intuitive and un-ambiguous.

Where users are required to interface with biometric capture devices, special consideration should be given to factors such as physical alignment and step by step procedures, including clear fall-back procedures should the process not complete or return an unexpected result.

If users are required to present their travel document as part of an automated process, then special consideration should be given to advising on document orientation, selection of the correct page and step by step procedures to guide the user through the process. Commonly understood diagrams and symbology may be of value in this context.

In conclusion, all aspects of the user interface should be attractively designed and intuitive in operation, featuring the least number of steps required in order to complete the process.

5.4.10 Performance

As previously mentioned, realised performance depends upon the successful operation of the entire infrastructure, as required to support the operation in question. This performance may be usefully sub-divided into transaction time and informational accuracy. Individual transaction time will be constrained by the weakest link within the technical infrastructure, coupled to the extent of human intervention required. As such it will typically be variable across a nominal distribution, with exceptions falling outside of this range. However, the exceptions and longer transaction times may

be cumulative within a given channel, leading to unexpected congestion, especially at peak times. Increasing levels of automation will not necessarily lessen the requirement for human resources, especially in the early days of a given implementation, featuring mostly non-habituated users and untested local infrastructures.

With regard to individual transaction times, it is possible that automated processes will increase the transaction times, sometimes considerably. This should be taken fully into account in process engineering and overall design.

With regard to informational accuracy, much will depend upon how we configure systems within both the local and broader infrastructure. Some situations may be satisfied by a binary result, such as whether an individual is present within a list. Other situations may not be. The combination of several such factors may introduce uncertainties which, outside of the diligence of a trained and experienced official, may be incorrectly interpreted by the system. This is a serious factor which may not be universally well understood. An example revolves around the biometric matching process and the importance of providing an equivalence of performance across nodes. Without such an equivalence, the overall process immediately becomes inconsistent and unreliable. This is also not well understood. It is consequently recommended that a proper risk assessment be undertaken in relation to each such process, taking such uncertainties and inconsistencies fully into account.

The introduction of new and automated processes in support of the e-MRTDs does not render traditional skills redundant. On the contrary, control authority personnel will require enhancements to their existing skills in order to understand the implications of the new technology. It is likely that, for a given situation, human resource requirements will be accentuated, especially within the early stages of a given implementation.

5.4.11 System Dependencies

The underlying infrastructure and its secure operation is paramount to the successful operation of a given implementation. It follows therefore, that there shall be various interfaces and dependencies within this broader infrastructure, all of which represent a potential point of failure. It is outside the scope of this document to cover all eventualities in this context. Suffice it to reiterate the importance of understanding the broader infrastructure and exactly how it is working, including all ancillary components.

There is an additional factor here around responsibility. Who is responsible for what and who takes responsibility for the support and maintenance of which elements of the infrastructure. Typically, one would like to see a coordinating element which can quickly respond to and resolve any technical or operational difficulties associated with a given design. This requirement should be considered at the early stages of design and followed through to implementation and beyond.

6. e-MRTD READERS and BIOMETRIC CAPTURE DEVICES

The logical development of e-MRTDs is based on several aims and assumptions. First of all the need to enhance document security in the endurance race against forgers. Furthermore the growing usage of travel documents. And in that regard the need to speed up border clearance processes. An associated benefit lies in the potential for automated document handling, by enabling the capture of relevant biographic data of the document holder to facilitate further data retrieval and processing. The development and design of e-MRTD readers is essential to facilitate such an approach.

6.1 Reading types

Where new generation travel documents have two types of data storage (visual and electronic) both types may be read in a different way. It will be important to retain this flexibility into the foreseeable future, in order to accommodate the wide variety of legacy travel documents in circulation. The following provides an overview of optical and RF reading techniques.

6.1.1 Optical reading

Optical reading will remain necessary whether it is for authenticating optical features or for reading data in order to facilitate access to the chip, a specific technique to prevent unauthorised reading of information held therein.

Between 1980 and 1988, the progressive merging between separate ICAO and ISO early standardization efforts led to the common adoption of Optical Character Recognition (OCR), using the printed OCR-B font character set to display the primary traveller's bio-data. As OCR was already an established data capture technology, this approach held potential for automated capture of traveller bio-data via the appropriate OCR readers.
The first generation of MRTD readers were designed to automatically decode the OCR-B characters, which became an integral part of the Travel Document, via the Travel Document MRZ (Machine Readable Zone), wherein two lines of human readable OCR-B characters display traveller and document related data. These early OCR readers were operating as line scanners enabling character-by-character recognition, and therefore adding mechanical motion complexity to associated equipment.

Modern readers capture OCR data in a similar manner to that of the familiar office document scanner, by capturing from a dual MRTD page a high resolution digital bitmap via the equipment CCD. Subsequent analysis of the captured image enables the separation of text zones and image or background areas. Finally, high speed software conversion of the OCR characters provides ready-to-be-used data for further processing, as required by the application. Typical processing time is around one second.

6.1.2 RF reading

RFID (Radio Frequency Identification) is a means of non-contact and out-of-line-of sight data retrieval via electromagnetic transmission to/from an RF compatible integrated circuit (IC) device.

RFID systems typically consist of the following components:

- An RF reader, including an antenna, which is the device used to emit the electromagnetic energy enabling data to be read and/or written from RFID IC's.

- An IC chip (with its own antenna) able to be activated by the radiated RF signal in order to transmit data to a reader or receive data from it.
- The communication between the base components is initiated and energized by the RF reader, which uses a defined radio frequency and associated protocol in order to transmit and receive data from the chip.

In the case of e-MRTDs, data is read from the chip using a standardised communication protocol, ISO-14443, which operates at a frequency of 13.56 MHz. Being a contact less method of reading data, the immediate RF environment surrounding the reader/e-MRTD combination (other chips, metals, other RF source) could have an influence over the quality of the data being transferred. Operational environments must therefore be controlled in order to ensure data quality as well as data privacy during transmission. According to this standard for RF-reading, embedded chips may be read up to a distance of 10cm (4") from the reader (although longer reading distances may be possible).

The development of e-MRTDs and associated readers, seeks to combat document fraud and enhance security. Within this context, ICAO has acknowledged the desirability of incorporating a digital image of the document bearer's face within the machine readable chip, as a logical continuation of existing processes which utilize the document holders portrait on the human readable page of the document.

The choice for chip-enabled e-MTRDs was logical in order to provide an upwardly scalable processing capability, together with sufficient memory for storing biometric data. In addition, readily available encryption algorithms using fast chip co-processors and native smart card operating systems, were already firmly established in other operational environments.

The potential benefits of using contact-less technology include ease of use via a controlled short reading distance, enabling simultaneous data exchange with the chip while the optical examination of the MRTD is being undertaken.

The existence of established contact less chip standards, namely ISO 14443, using RFID at 13,56 MHz, were also well documented and proven within synergistic application areas, lending confidence to the choice of this technology for e-MRTDs.

6.2 Reader types

There are several types of readers which are able to read e-MRTDs. A significant distinction lies in the way the MRTD is to be handled, i.e., in a one step or two step operation. The following types of readers are described:

- **Swipe readers**
  - Swipe readers with RF
- **Full page readers**
  - Full page optical readers with document authentication
  - Full page optical readers with RF
  - Full page optical readers with RF and document authentication

6.2.1 Swipe readers

Swipe readers are typically low cost and very common as PC keyboard accessories. Their use involves the MRTD (held vertically by the operator) being manually swiped across a pair of plastic

guides at the back of the keyboard, during which the MRZ OCR characters are read and transferred as ASCII characters to the running application.

In many cases, the same reader is also able to swipe and read magnetic cards and or magnetic airline tickets. Such readers are also often found as table top stand alone units, directly connected to the application PC via a cable. They are used today as the standard MRZ input interface to retrieve the passenger PNR (reservation and flight data) and, where applicable, to assist in the collection of mandatory bio-data at the departing airport (API - Advance Passenger Information, a data transfer to inform the destination country about the traveller's identity and final destination, and, if necessary, to identify un-authorised passengers).

6.2.2 Swipe readers with RF

A large installed base of swipe readers exist at most of the worlds airports. With the progressive deployment of e-MRTD's, a possible trend will be to append, at the back of the counter OCR keyboard, or close to the table-top OCR swipe reader, an RF reader module, the role of which will be to read the e-MRTD data contained in the chip and enable the application to perform all subsequent verification tasks.
Typically, the e-MRTD may be inserted in a kangaroo-like pocket stuck to the back of the OCR keyboard (or of the stand alone reader) or may also be laid down flat on a separate RF reader.
It is worth noting that such add-ons require two steps to access the e-MRTD data. Since most countries will use the BAC (Basic Access Control) approach, the chip data will only be read after the MRZ is read, as a part of the key to unlock the chip. Such a mode of operation thus requires two successive hand movements in order to read the e-MRTD, however at a much reduced equipment cost. Such dual operations are more likely to be successfully performed by agents than by unassisted travellers at self-service kiosks.

6.2.3 Full page readers

Full page readers may be installed with basic or advanced features and functionalities, according to application requirements at the point of presence. Various options are discussed below.

6.2.3.1 Optical readers

Reading the full data page of the document. In case of an ID-3 format this includes reading the MRZ, several data fields and optical security features. In case of an ID-1 format the MRZ is on the other side of the document, which means a 2-step procedure for reading and authenticating the document. Full page readers have many options for reading data, the sequence of reading and the use of several security features for authenticating the document. Therefore these full-page readers are configurable.

These OCR readers are typically used at document control stations, either by the Immigration Officer, or in the back room site, when secondary checks have been required. The document to be read is placed open, either face up or down depending upon the type of reader. OCR reading is performed by extracting the two line MRZ zone from the bio-data page. But the entire data page can be optically scanned at the same time. Additional checks can thus involve matching the two line MRZ data decoding with the other data elements digitised from the MRTD data page, as a rapid sanity check for the overall MRTD validity.

Full page readers may potentially be used within an automated passenger handling process, typically at self-service kiosks or perhaps at an automated border control point.

6.2.3.2 RF Readers

Reading Radio Frequency (RF) is possible with a reader based on the ISO 14443 protocol in combination with several sizes of antenna. Consequently, it is often considered beneficial that reader and antenna should be independent from each other, in order to promote maximum flexibility of configuration. Optimal reader configuration will promote communication reliability and performance. The antenna should be selected upon its characteristics in combination with the environment. For example, considerations around accommodation space, metallic materials in the surrounding area, other RF sources in the surrounding area and other influencing factors should be taken into account. Important characteristics for the antenna are its size, shape and the strength of the magnetic field which powers both the chip and the communication medium. Most RF reader suppliers offer versatile, modular packages with varied functionality, either within proprietary housings or OEM packages. Some suppliers offer these packages in combination with optical reading modules, for example as separate RF 'piggy bags'. The latter type might be installed as operational add-ons to an existing base of OCR readers or OCR keyboards.

6.2.3.3 Full page optical readers with document authentication

Additional features have been progressively added to MRTD reader specifications in order to support the broadening scope of travel document validity authentication, in line with the evolving features of MRTD's themselves, eventually leading to automated document authentication behind the scenes.

UV and near IR illumination were incorporated in order to confirm hidden security document backgrounds, verify the presence of security features such as non visible inks, metallic inserts inside of laminates, or the texture of guilloche templates. Similarly, some MRTD authenticator providers developed advanced authentication databases, enabling the specific matching of these features, plus others (e.g. holograms, kinegrams) against authentic travel document templates, including 'classical' faked travel documents from most countries worldwide.

In summary, MRTD readers continue to evolve in order to deliver additional resources to a combined ID and document authentication mission, via the OCR-B triggered MRZ reading, up to and including the local machine-assisted, database inspection software for forged or otherwise invalid travel documents. This type of reader is typically used by immigration officers.

6.2.3.4 Full page optical readers with RF

Many traditional full page MRTD readers are now proposing an RF extension via the integrated electronics on board of the reader body, with single or dual antennas, integrated around and below the reader's glass field of view, on which the e-MRTD is placed flatly or inclined, and which enables the concomitant one step capture of the document's MRZ followed by the immediate chip access and data extraction following the proper secure process for accessing this data (re BAC, Active Authentication, etc.).

6.2.3.5 Full page optical readers with RF and document authentication

This type of full fledge, full page MRTD readers would be mostly utilized by expert Immigration Officers or at back-office government fraud teams, when suspicious newly obtained e-MRTD's would be referred for secondary inspection.

6.3 Reader integration

The successful usage of MRTD readers may depend partly upon proper integration into available on-site equipment such as kiosks, turnstiles, portals etc., which may, in turn, feature biometric identity verification and other capabilities designed to facilitate passenger flow. In this context, the use of e-MRTD's may have advantages over other tokens and techniques such as bar coded boarding passes, RF-enabled frequent flyers cards and so on.

To read the data from the chip it is most convenient to integrate an optical reader with an RF-reader. With such a combination, it is possible to read the protected data in one routine. There are solutions where swipe readers are integrated with RF readers. In these solutions the document is stopped or placed in a position to the RF reader after it is swiped. In other solutions a RF reader is integrated in a full page reader. In all of these solutions the position of the reader antenna to the document is a design issue, especially when both ID-1 and ID-3 documents need to be read with the same integrated device. The percentage of magnetic field (flux) that goes from the reader-antenna through the document antenna is proportional to successful and stable reading.

MRTD reader integration may be utilised for the benefit of automating, securing and possibly streamlining passenger flow, whether at border control, security check-points, to bolster unattended airport procedures such as completing check-in at self-service kiosks, or even to perform automated self-boarding with largely reduced supervision manpower. However, such possibilities must be carefully aligned with responsibilities and legal requirements, as much as with the potential for passenger facilitation.

In addition, as authenticated breeder documents, eMRTDs offer the possibility, where appropriate, to verify the traveller's most up-to-date security profile and threat status, by accessing, on line Government security databases, including the most recently posted lost passport or faked visas black lists.

An integrated e-MRTD reader may also facilitate 1-to-1 identity verification, via matching the biometric of the traveller against the stored biometric on the document. This may be useful at various points of presence within the overall border control process. For example, it may guard against last minute traveller substitution during boarding processes (whereby two individuals may swap their boarding documents and perceived identities in order to travel to different destinations, one domestic, one abroad, which is one of the perennial problems faced by Immigration Agencies). Another example of a particular use of e-MRTD's is in Automated Border Crossing, which will be described elsewhere.

6.4 Biometric Capture Devices

In this section the characteristics and associated requirements for capture devices are discussed.

6.4.1 Devices for Face capture

6.4.1.1 2D devices

The primary benefit of 2Dimensional capture devices for face recognition lies in their inherent simplicity. Conventional CCTV-cameras may be used for 2D facial recognition. An important characteristic is the number of pixels utilised by the capture device, which affects image resolution and must be compatible with the chosen matching algorithm.

6.4.1.2 3D devices

Typically, 3Dimensional face recognition capture devices fall into two groups. Firstly, there are fully integrated devices which incorporate, together with the necessary software, two internal camera modules, aligned at an appropriate angle to provide a 3D perspective. The second group consist of two or more camera modules which may be deployed separately in order to provide an optimal field of view for 3D image capture. Such configurations often feature continuous operation in order to capture multiple images of the face, regardless of pose. The associated software may then construct the optimal three dimensional image to facilitate facial recognition.

6.4.2 Devices for Fingerprint capture

Fingerprint capture devices also fall into two broad groups. Those which use electronic sensors (capacitive) and those which use optical sensors (image capture).

6.4.2.1 Electronic capture devices

Electronic capture devices detect the presence of a finger-tip at multiple points across the sensor. The device measures resistance or capacity according to the pattern of ridges in contact with the sensor, constructing an image from this information. Some electronic devices feature a 'liveness' test, as they are able to distinguish between live and synthetic tissue and/or the presence of a pulse. Certain sensors also read beneath the immediate surface layer of the finger, providing resilience against the presence of minor blemishes.

6.4.2.2 Optical capture devices

Optical capture devices simply capture an image of the fingerprint offered up to them via the transparent contact surface. However, optical alignment and illumination need to be precisely managed. Such devices may also offer a degree of 'liveness' testing via the sensing of temperature.

Both types of fingerprint capture technology continue to be developed in order to enhance performance and service reliability.

6.4.3 Devices for Iris recognition

Iris recognition systems may operate either at a short range (approx 10"), typically focusing on a single eye, or at a longer range (up to 40") typically focusing on both eyes. Devices which focus upon both eyes may exhibit a shorter learning curve with respect to a given individual, thus enhancing performance. However, those focusing upon a single eye at a shorter distance may be less affected by variances in ambient light.
The software for iris recognition systems is very much standardized with regard to matching algorithms, although other operational functions may differ between suppliers. The algorithm, having effectively distinguished between iris and sclera, organises the iris pattern into 256 segments arranged in concentric circles surrounding the pupil, each of which may be analysed separately. Consequently, a wealth of information is available with which to verify an individual iris, leading to very high matching performance, subject to optical resolution and environmental conditions.

Iris recognition devices broadly fall into two cost related groups.

6.4.3.1 Low cost devices

Iris cameras for the consumer market differ from those targeting the B2B sector. Typically, they are less robust in construction and may exhibit lower overall resolution which, in turn, may constrain ultimate performance. However, such characteristics must be balanced against cost.

6.4.3.2 High end devices

High end iris cameras tend to be robust in construction and offer higher overall performance. Furthermore, they have been well proven across a wide range of real-world operational environments.

This section has provided an overview of the data capture devices typically used within the design of a broader border control system. It should be acknowledged however that the type of capture device does not itself denote a particular level of operational performance. Realised performance is a product of the data capture transaction (including the accuracy of the capture device), the configuration of the matching algorithm (where biometrics are used) and the real-time performance of the overall system. Furthermore, we might make a distinction between the theoretical technical performance at a specific point of presence and overall systems performance, which will take into account the overlying objectives of the operation, user profile and psychology, equivalence of performance across nodes, operator experience and associated capabilities and other factors.

7. MARKETING and COMMUNICATIONS

Having designed a suitable ABC system and paid attention to the environmental issues around deployment at a given location, it will be important to consider marketing and communications to prospective users in order that they understand both their own requirements for interaction and the underlying purpose of the deployment. Perceived 'user-friendliness' will be an important factor in relation to any such system, not just in relation to operational parameters, but in general understanding. Consequently, effective marketing and communications are crucially important and will be the hallmark of a successful implementation.

The following factors should be included within a marketing and communications plan:

- Overview of why the system is being introduced and what the benefits will be, both to the administering state and the individual
- A clear statement as to the requirements for compliance with the new system from the travellers perspective (i.e., registration, documentation and so on) and how to go about becoming compliant, including relevant contact information
- The provision of specific user training during the registration process, in order that users may understand the operational system and how to interact with it
- A simple instruction leaflet which guides the user through interaction with and operation of the in-place system. This should be bold and clear with an emphasis upon graphics
- A simple statement of roles and responsibilities in connexion with the new system, including full contact details of the authorities and operating agencies concerned
- Details of an information hot-line where users may ask relevant questions or check their understanding of the new system, how it operates and why it is there
- Details of a remediation hot-line where users may address issues and complaints appertaining to use of the system (including false rejection)
- Announcements and press releases via relevant local media channels in order to advise of the new system and the changes it will introduce
- Announcements to carriers who might deliver travellers to the port in question, detailing relevant requirements and go-live dates
- Ongoing announcements and press releases covering the introduction of the new system, how it may scale in the future and repeating relevant contact information

While the above points do not represent an exhaustive list, they may serve to form a framework for a more comprehensive plan. Such a plan will be essential if a smooth transition between existing and future systems is to occur. Without such a plan, an implementing agency may find itself overwhelmed with questions and issues which could have been addressed in advance. Furthermore, it may be considered a matter of common courtesy to ensure that all those affected by such a change are properly advised in advance. Such attention to detail will pay dividends with regard to the successful introduction of an ABC system.

8. e-MRTD TECHNOLOGY in the FUTURE

8.1 Next ICAO e-MRTD Passport Specifications

The e-MRTDs will of course evolve over time in order to realise enhanced functionality facilitated by the architectural design of the document and embedded chip. The first e-MRTD passports, both in their BAC and most recent EAC versions, do not allow for any data to be written onto the chip once the e-passport has been personalized and delivered to the traveller. However, provision was made within the e-MRTD design which could allow for subsequent extension of the LDS, which might allow for such write operations as well as other extended functionality. Such an extended use would of course need to be carefully considered and designed, both from a technical operational perspective and, especially, from a usability perspective. We must also acknowledge that it is not always advisable or practical to use every aspect of technology simply because it is possible to do so and, instead, ensure that any proposed extended or otherwise enhanced use of the e-MRTD has a specific purpose and quantifiable benefit in mind.

8.2 Other (National) MR Travel Documents

Similarly, we might usefully acknowledge the co-existence of other machine readable documents within this application space. These might range from less sophisticated book type passports, identity cards to various tokens and chip cards associated with bespoke systems, many of which incorporate ICAO compliant technology. It is inevitable that there will be a period within which a variety of such documents will be in active use, due to the manner in which border control thinking and technology has evolved. This reality may have implications for international ports where e-MRTDs and associated systems are being introduced subsequent to other, more bespoke initiatives. Such a situation will of course be resolved over time. An important consideration in this respect will be the quality and timeliness of communications, both with relevant government agency personnel and end users

8.3 Juxtaposed Border Crossing

Juxtaposed border crossings already exist today to decongest immigration lines. For example, US Immigration is routinely performed in Dublin before US carriers take off to their destinations. The arrival process is expedited, since it is limited to Customs clearance. France and the UK operate juxtaposed controls on the Channel Tunnel.

Trans-border crossing between Canada and the US is another existing example, which would get worse, once passport usage become mandatory for both Canadian and US citizens to cross their mutual border. One of the ways to absorb this large inspection overflow may be the extension of existing Registered Traveller Programs to incorporate biometric identity verification, facilitated by the use of e-MRTD's as part of ABC solutions.

As a general rule, immigration lines are time consuming, costly and manpower intensive. Ongoing global security problems may possibly lead to a complete rethink of emigration procedures, according to which MRTD and visa checking may become as extensive for emigration as they are for immigration.

Many large airports worldwide, especially large domestic carrier terminals in the US, do not have the in-place infrastructure to permit such a Security paradigm shift. Some present DHS driven programs are trying to assess this difficulty. Here again, the use of e-MRTD's with biometrics, and

an airport-by-airport custom premises flow optimisation, with signage, streamlined light obstacles (one way doors, IR sensors, etc.), may bring some relief to the present situation. New variations of 'fast track' programme may have to be considered, building perhaps on previous registered traveller programmes, should they still maintain adequate background check security status.

As a summary for this emerging application, one of the potential benefits of e-MRTD's lies in the anticipated extension of registered traveller programmes, to enable participants with carefully checked backgrounds to pass quickly through both emigration and immigration processes subject to the proper e-MRTD reader-assisted identity verification at appropriate points.

8.4 Extension to e-Visas reading

Many countries (US and the EU) have already decided to use e-visas mainly consisting of pointers into their own country visa database. Thus, the visitor's biometrics collected at the consulate of origin will be retrieved on line and matched against the visitor's own MRTD while performing a biometrics collection during the visitor's immigration process. In this case, the e-Visa verification procedure could also utilize the existing e-MRTD of the traveller, should he indeed already possess one.

To the extent that the receiving country will only use ICAO- compliant e-visa OCR paper stickers when welcoming its visitors, the already existing OCR reader infrastructure could be used without further complication.

The potential use of chip-bearing e-visas, if and when utilized (most certainly only as a separate document from the e-Passport), would necessitate further application development to be embedded into the MRTD readers by the receiving country, which, of course, would be limited to the reader base installed at the immigration lines of all its ports of entries. While no conflict between the simultaneous occurrence of e-visa chip and e-passport chip is anticipated (they are on separate documents), the receiving country would have to make sure their own particular e-visa authentication application procedure using their MRTD reader installed base is itself not impacting the rest of the other countries e-MRTD verifications.

8.5 Extension to other e-Documents

As national ID programs develop in the coming years, the choice made by many countries to use the same RF technology and infrastructure should permit a reasonably easy implementation of e-ID usage in all airport MRTD equipped infrastructures, wherever deemed acceptable, for example thanks to bi-lateral agreements. Should, for example, the use of an e-National ID's as the minimum e-MRTD document be acceptable, say for passenger biometric identity verification through an automated turnstile in a domestic (or Schengen) flight, the equipment already in place for e-MRTD driven facilitated flow should perform equally well.

8.5.1 e-Administration

As more e-MRTD's are issued, there will be an increased need for citizens to verify the information held within the chip, after the official e-MTRD has been delivered to them. This will lead to inspection-only readers for public use. The first ones are already in place in some German city halls and in all the UK's Passport Offices. This trend will develop in the EU and elsewhere, and will include embedded display systems in a large number of public self-service kiosks, which are anticipated to be part of the future e-Administration infrastructure.

8.5.2 e-Commerce

As e-Commerce continues to grow, ICAO should continue to monitor associated technical breakthroughs which may potentially be of interest in relation to its own goals. e-Commerce tried and (sometimes !) successfully implemented, advanced and secure data communication and infrastructure technologies, which were submitted to intensive hacking, thus filtering the more stable technologies.

Progress to upgrade and further develop solutions by the-Commerce community should, thus, not remain under ICAO's radar.

Annex A Existing ABC and Registered Traveller Programs

Introduction

Where admission is dependent upon a pre-existing entitlement, e-MRTDs may assist control authorities to divert a significant number of low-risk passengers through automated channels so that control staff can concentrate their time and efforts in examining higher risk traffic.

A number of states are using biometrics to identify passengers who have enrolled into a 'fast track' or 'frequent traveller' scheme. The use of a facial image, fingerprint or iris pattern (or a combination of these) allows border control authorities to select certain passengers for expedited entry. Such a scheme may require the use of a token (a smart card or machine-readable passport) in order to verify the identity of the passenger via the comparison of a live biometric to one contained in the token or, alternatively stored within a central database.

Such systems typically require pre-enrolment during which passengers are examined by trained border control staff in order to counter fraud. The systems are generally not interoperable so enrolment in one system cannot confer membership of any other system. Initiatives of this kind also require investment in terms of staff and dedicated enrolment facilities, tokens and associated systems technology.

A number of States have already implemented an Automated Border Control system, some as pilot initiatives and some intended as ongoing operational systems. Various tokens and infrastructures have been trialled within these initiatives. It is interesting to compare the different implementations and a standard presentation template is used to facilitate this, providing much associated detail. Currently, few systems are using the e-MRTD as the token. However it is expected that, with the wider adoption of e-MRTDs, more states will decide to use the e–MRTD as a token in future semi or fully automated border control systems.

Readers should bear in mind that the implementations reflected on the following pages serve as early examples, the details of which are subject to change as experience is gained and the supporting technology refined. Agencies seeking to implement similar systems in an operational / decision making environment are advised to make contact with the indicated authorities in order to understand both the current configuration and points learned from their experience to date.

Existing programs

A listing of example programs follows. These are presented in no particular order.

PRIVIUM

Location	Schiphol-Airport Amsterdam, The Netherlands
Introduction date	1st October 2001
ABC or semi ABC	Fully automated with intervene option immigration service
Responsible authority	Airport Authority in cooperation with Ministry of Justice, IND and Royal Marechaussee
Target group	Frequent Flyers with an EU-nationality
Fee	Yes
Enrolment centre	Yes
Entry control	Yes
Exit control	Yes
Number of gates	3 exit, 2 transfer, 5 entry and 3 Schengen transit points
Biometric used	Iris recognition
Token	Smart card
Storage biometric	On smart card as a template
Average process time	10 – 15 seconds
Description system	
Upon application, an enrolment record is created and biographical and iris biometric data collected. A smart card containing the iris template is then issued to the traveller.	
Description process	
On arrival at the airport, travellers are asked to present the card to the automated border control system and look into a camera so a live iris scan can be collected. The iris template is retrieved from the card and compared to live iris scan to verify the card holders identity. This process takes approximately 10-15 seconds to complete. If system is unable to verify the travellers identity then they are referred to manual processing.	
Additional information	
www.privium.nl	
Content updated	01 January 2007 Version Template: 1/2006

IRIS (Iris Recognition Immigration System)

Location	London-Heathrow Terminals 1, 2, 3, 4 & 5 Gatwick North and Gatwick South Manchester Terminals 1 & 2 and Birmingham
Introduction date	3rd January 2006
ABC or semi ABC	IRIS barriers are fully automated
Responsible authority	UK Border Agency
Target group	Frequent Flyers, Business Travellers, Returning Residents and Visa Holders
Fee	None
Enrolment centre	Enrolment Stations available at all the above ten airport terminals
Entry control	Yes
Exit control	No
Number of gates	7 at LHR, 2 at LGW, 2 at MAN, 1 at BHX
Biometric used	Iris recognition
Token	No
Storage biometric	In secure database
Average process time	20 - 25 seconds to pass through the IRIS barrier

Description system

The IRIS system was introduced in order to expedite the clearance of bona fide, pre-registered travellers through the United Kingdom Border Control.
Enrolment onto the scheme takes place in the IRIS Enrolment Stations situated in the airside departure lounges of the participating airport terminals.

Enrolment is carried out by forgery trained Immigration Officers. Procedures for enrolment mirror those carried out on the primary arrivals control.

At enrolment there is a 1: many search of the IRIS database and a portrait photograph of the traveller is taken together with their iris patterns. This information is linked to their passport data and immigration status in the UK provided at the time of enrolment.

Description process

On arrival at the airport and as long as their entitlement to use the scheme is still valid, enrolled travellers may use the IRIS automated barriers to enter the United Kingdom, by looking into an iris recognition camera, which performs a 1:many search against the database and provides a response within 6 seconds depending on network availability.

If the traveller's registration is valid, the landside glass doors of the barrier open to allow the traveller to enter the United Kingdom without the need to be seen by an Immigration Officer.

The entire transaction, from first entering the IRIS barrier to exiting the landside glass doors into the United Kingdom takes approximately 20 - 25 seconds.

Additional information

Heathrow T5 opened with 2 IRIS barriers and an Enrolment Station on 27th March 2008 and has proved very popular with the second highest usage of the barriers of the 10 airports.

www.iris.gov.uk

Content Updated	15 April 2008 Version Template: 1/2006

SMARTGATE

Location	SmartGate Series 1 was initially implemented at Brisbane and Cairns International Airports in Australia and will be made progressively available at all Australian International Airports
Introduction date	August 2007
ABC or semi ABC	Fully automated
Responsible authority	Australian Customs Service
Target group	Initially Australian ePassport holders; extended to New Zealand ePassport holders in December 2007. SmartGate Series 1 will be made progressively available to a broader range of ePassport holders as SmartGate implementation progresses
Fee	No
Enrolment centre	Not applicable
Entry control	Yes
Exit control	No
Number of gates	8 kiosks and 4 gates at Brisbane International Airport and 4 kiosks and 2 gates at Cairns International Airport. Further expansion at Brisbane and other Australian International Airports is underway or planned
Biometric used	Face recognition
Token	ICAO ePassport
Storage biometric	On smart chip
Average process time	30 seconds at the kiosk; 15 seconds at the gate
Description system	
SmartGate Series 1 is automated border processing developed and implemented by the Australian Customs Service that utilises facial recognition biometric technology. It is a secure and simple process that performs the customs and immigration checks usually made by a Customs officer upon arrival in Australia	
Description process	
SmartGate is a two-step process involving a kiosk and a gate. Step 1, undertaken at the kiosk, checks if a traveller can use the automated option. Step 2, undertaken at the gate, performs the identity and clearance check	
Additional information	
www.customs.gov.au ('travellers' section)	
Content Updated:	31st March 2008 Version Template: 1/2006

MiSensePlus Trial

Location	London- Heathrow Terminal, 3 United Kingdom
Introduction date	November 2006
ABC or semi ABC	Trial System with elements of manual intervention around background and routine checks
Responsible authority	United Kingdom Immigration Service
Target group	European Economic Area Travellers (and visa nationals with leave to enter beyond period of trial)
Fee	None
Enrolment centre	Yes
Entry control	Yes
Exit control	Yes
Number of gates	3 plus (1 arrivals 2 ticket presentation 6 portable devices for boarding)
Biometric used	Finger print (all 13 bio's captured at enrolment)
Token	2nd Generation ICAO Passport Smartcard
Storage biometric	Encrypted images on Card
Average process time	12 - 17 Seconds at arrivals gate (to be confirmed at end of trial)

Description system

The system is a Registered Traveller system design to expedite passenger travel through a port terminal– Passengers are assessed for eligibility and travel documents scrutinised – at enrolment 13 biometrics captured and subjected to background and routine checks against watch lists and database records – card is tested with passenger and card issued – passenger's card is activated following successful background checks and maintained subject to successful routine checks.

Description process

Enrolled passengers arrive at an automated arrivals gate, their card is scanned, their biometrics taken from the chip in the card and verified against their fingerprint (1:1) to verify their identity. A check is also made against the core system to verify their registered traveller card is activated. If a match is not found the passenger is referred to manual processing.

Additional information

www.misense.org

Content Updated:	14 April 2008	Version Template: 1/2006

eIACS (enhanced Immigration Automated Clearance System)

Location	▪ Changi Airport, Singapore ▪ Budget Terminal, Singapore ▪ Singapore Cruise Center, Singapore ▪ Tanah Merah Ferry Terminal, Singapore ▪ Tuas Checkpoint, Singapore ▪ Woodlands Checkpoint, Singapore
Introduction date	26 March 2006
ABC or semi ABC	ABC
Responsible authority	Immigration & Checkpoints Authority (ICA), Singapore
Target group	Passport-Based Automated Clearance ▪ Singapore Citizens Smart Card-Based Automated Clearance ▪ Singapore Permanent Residents ▪ Singapore Long-Term Pass holders ▪ Selected Frequent Travellers to Singapore
Fee	Smart Card : $30
Enrolment centre	▪ ICA Building ▪ Changi Airport, Singapore ▪ Tuas Checkpoint, Singapore ▪ Woodlands Checkpoint, Singapore
Entry control	Yes
Exit control	Yes
Number of gates	88
Biometric used	Fingerprint
Token	▪ Singapore Passport ▪ Smart Card
Storage biometric	Backend databases
Average process time	12 seconds

Description system

The Immigration Automated Clearance System (IACS) was introduced in 1997 to provide efficient and secure immigration clearance at checkpoints. IACS authenticates the identity of travellers through the matching of live fingerprints with that stored in a smart card. In 2006, ICA implemented the enhanced IACS (eIACS) which enables Singapore Citizens who have already registered their fingerprints with ICA and issued with valid passports to clear immigration via the automated lanes using their passports.

Description process

Under the system, a Singaporean only needs to scan his passport at the self-service kiosk located before the automated lane. The system will read the Machine Readable Zone (MRZ) of his passport to retrieve his fingerprint record from the backend databases for authentication purpose. The automated gate will open for the holder to pass through once the system authenticates the holder's fingerprint. Feedback received was generally positive, as the users found that clearance was fast, secure and convenient.

Additional information

-

Content updated	Version Template: 1.4/2007

Automated Passenger Clearance (APC) System (also known as e-Channel)

Location	• Hong Kong International Airport • Border Control Points, namely Lo Wu, Hung Hom, Lok Ma Chau, Lok Ma Chau Spur Line, Man Kam To, Sha Tau Kok, Shenzhen Bay • Harbour Control Points, namely China Ferry Terminal, Macau Ferry Terminal, Tuen Mun Ferry Terminal
Introduction date	16 December 2004
ABC or semi ABC	Fully automated
Responsible authority	Hong Kong Immigration Department
Target group	All Hong Kong permanent residents and the majority of non-permanent residents aged 11 or above holding Smart Identity Cards
Fee	No
Enrolment centre	No enrolment is required. Qualified residents are eligible to use their Smart Identity Cards for self-service clearance
Entry control	Yes
Exit control	Yes
Number of gates	174 departure, 166 arrival
Biometric used	Fingerprint verification
Token	Smart Identity Card
Storage biometric	On chip of Smart Identity Card as a template
Average process time	10 – 12 seconds
Description system	
The Automated Passenger System (e-Channel), a self-service passenger clearance facility, has been implemented at our border control points. The self-service facility is equipped with a smart card reader, a fingerprint scanner and is powered by an Industry PC housed in a clearance channel so as to dispense with visual inspection by immigration control officers. APC e-Channel is developed and implemented by the Hong Kong Immigration Department that utilized fingerprint verification biometric technology. Eligible Hong Kong residents holding Smart Identity Card may enjoy secure and efficient automated passenger clearance upon arrival at and departure from Hong Kong.	
Description process	
Passenger firstly inserts his smart identity card into the card reader of the e-Channel. The system will retrieve the personal particulars and fingerprint template from the chip of the card after mutual authentication which guards against invalid and forged identity cards. After entering the auto-gate, passenger just needs to place his thumb onto a fingerprint scanner with custom-made liveliness detection capability. His live thumbprint will be captured for verification with the retrieved fingerprint template. If the matching is affirmative and online immigration record check is cleared, the exit door will open automatically and the arrival or departure record will be captured. If verification fails, an alert together with real-time passenger's data will be transmitted to the Gate Officer's PDA through wireless network for follow-up action.	
Additional information	
http://www.immd.gov.hk/ehtml/20041216.htm	
Content updated	20 September 2007

Automated Vehicle Clearance (AVC) System (also known as e-Channel)

Location	Border Vehicular Control Points, namely Lok Ma Chau, Man Kam To, Sha Tau Kok and Shenzhen Bay
Introduction date	21 April 2005
ABC or semi ABC	Fully automated
Responsible authority	Hong Kong Immigration Department
Target group	All Hong Kong permanent residents and the majority of non-permanent residents who are cross-boundary drivers and Smart Identity Cards holders
Fee	No
Enrolment centre	No enrolment is required. Cross-boundary drivers can use their Smart Identity Cards to perform self-service clearance
Entry control	Yes
Exit control	Yes
Number of gates	27 departure, 27 arrival
Biometric used	Fingerprint verification and face recognition
Token	Backend database/Smart Identity Card
Storage biometric	On chip of Smart Identity Card as a template
Average process time	9 – 10 seconds

Description system
The Automated Vehicle Clearance System (vehicular e-Channel), a self-service driver clearance facility, has been implemented at our border control points. The self-service facility is equipped with a smart card reader, a fingerprint scanner, cameras and is powered by an Industry PC housed in a clearance kiosk so as to dispense with visual inspection by immigration control officers. AVC e-Channel is developed and implemented by the Hong Kong Immigration Department that utilized fingerprint verification and face recognition biometric technology. Eligible cross-boundary drivers holding Smart Identity Card may enjoy secure and efficient automated vehicle clearance upon arrival at and departure from Hong Kong.
Description process
Before a cross-boundary vehicle enters into the e-Channel, its license plate number is recognized by the Automated Vehicle Recognition System (AVRS) which is equipped with infra-red/ day light camera. The system then retrieves the driver's personal particulars as well as fingerprint template from the database, meaning that the driver even needs not to insert his smart identity card for data retrieval. When the vehicle stops inside the e-Channel, the checking station, with the aid of the Vehicle Height Detecting Unit (VHDU), will automatically adjust to the appropriate position to facilitate the driver for performing identity verification process. The driver simply places his thumb onto the fingerprint scanner of the checking station and looks at the camera for identity verification. Once the fingerprint or the facial image matches with the database, the movement record will be instantly captured. The driver will then be notified by the LCD display of the Checking Station and the LED display board at the exit of the e-Channel that the clearance process has been completed.
Additional information
http://www.immd.gov.hk/ehtml/20041216.htm

Content updated	20 September 2007

Immigration Autogate – Department of Immigration Malaysia

Location	Airport – KLIA, LCCT, Penang, Kota Kinabalu, Miri, Kuching, Langkawi (Peninsular and East Malaysia) Land port – Tambak Johor, Second Link, Bukit Kayu Hitam, Rantau Panjang, Padang Besar
Introduction date	2nd August 2000
ABC or semi ABC	ABC
Responsible authority	Malaysia Immigration Department
Target group	Malaysian Citizens
Fee	None
Enrolment centre	Immigration Offices and National Registration Service Centre
Entry control	Yes
Exit control	Yes
Number of gates	53
Biometric used	Fingerprint
Token	e-Passport and e-ID (MyKad)
Storage biometric	In e-Passport and e-ID (MyKad) Smart Chip
Average process time	9-12 seconds to pass through the Autogate Barrier

Description system

The Autogate system was introduced in August 2000 to expedite the clearance of bona fide Malaysian e-passport passengers through the automated lanes at Kuala Lumpur International Airport. The system consist of a barrier with RF reader and LCD to display the information read out from the chip and authenticating the identity of the e-Passport holder through the matching of live fingerprints with the stored template in the e-Passport.

Description process

The process starts with passenger stepping into the barrier, place the electronic passport on the RF reader, system check the passport chip contents and display photo and name, send record to watch list database, extract image from live fingerprint scanning, verify against stored template and display results on the LCD screen. Passenger is prompted to take passport and exit the barrier if pass, if fail, system will prompt passenger to exit via the entry flap and refer to the counter for manual processing or assistance. Entire process takes 9-12 seconds. An average of 300,000 passengers breeze through the autogate at Kuala Lumpur International Airport monthly.

Additional information

Http://www.imi.gov.my

Content updated	15 October 2007.	Version Template: 1.4/2007

RAPID (Automatic Identification of Passengers Holding Traveling Documents)

Location	Main Airport in Lisbon, other airports are Faro, Funchal and Porto.
Introduction date	May 2007
ABC or semi ABC	ABC
Responsible authority	Serviço de Estrangeiros e Fronteiras (SEF) (Portuguese Immigration)
Target group	EU Citizens, EEA citizens and citizens from CH older than 18
Fee	No
Enrolment centre	No enrollment required
Entry control	Yes
Exit control	Yes
Number of gates	Lisbon Airport 24 (14 terminal 1 and 6 terminal 2) Faro – 10 Funchal - 8
Biometric used	Face
Token	e-Passports
Storage biometric	Contact less chip in travel document
Average process time	15 seconds

Description system

This is the first system worldwide to allow an automatic control of passengers who hold electronic passports, thereby removing the need for human action. This system combines the operations of reading and checking electronic passports with an innovating feature for assessing the biometric data which operates an automatic door opening device. This feature checks, on a first instance, the genuineness of the electronic passports and validates all data stored in the chip and check the Schengen and Internal Database (Restrict Measures), and, on a second instance, it appraises the passenger's identification by establishing a comparison between the photo stored in the chip and the image of the passenger in loco, automatically opening the passage door when the features of both images are coincident. RAPID was made secure by an intelligent system that allows the entry of one passenger alone and automatically adjusts the reading camera to his / her height. After that, it performs a live match-to- chip verification of facial biometrics, therefore providing passengers a quick and simple way to get clearance at the border.

Description process

This system combines the operations of reading and checking electronic passports with an innovating feature for assessing biometric data which operates an automatic gate opening device. This device checks on a first phase the genuineness of electronic passports and validates all data stored in the chip and, on a second phase, appraises the passenger's identification by establishing a comparison between the photo stored in the chip and the information of the passenger in loco, automatically opening the border gate when the features of both images are coincident. RAPID was made secure by an intelligent system that allows the entry of one single passenger each time and automatically adjusts the reading camera to his / her height. This innovating system will permit a highly rationalized management and a significant boost to the efficiency of means at border control. By reducing the process of border crossing to an average of less than 15 seconds it will speed up the movement of passengers at border control significantly.

Additional information

We aimed to install e-gates in all border Posts until the end of this year.
www.sef.pt; or http://tv.sef.pt; or www.rapid.sef.pt

Content updated	February 2008	Version Template: 1.4/2007

Annex B Terminology

Within this document, the reader may encounter various terms and abbreviations with which they may not be familiar. A list of abbreviations is offered below for clarification, together with a list of reference documentation which provides additional background. The reader should refer to these aids as required.

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.

Automated Border Control system - *"A fully automated system which authenticates the eMRTD, establishes that the passenger is the rightful holder of the document, queries border control records, then automatically determines eligibility for border crossing according to pre defined rules."*

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 scanned 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 enrolee 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 enrolee 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 enrolee 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.

e-MRTD – An MRTD with an contacless IC (chip) embedded which is designed and the mandatory data stored, according to ICAO standards, in order to facilitate identity verification via either a manual or automated process

e-MRTD Assisted Border Clearance - *"A system which assists the border control officer to authenticate the eMRTD via the use of a suitable document reader, establish that the passenger is the rightful holder of the document and query border control records. The officer himself determines eligibility for border crossing"*

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.

Enrolment – 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.

Enrolee – 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 enrol or compare that potential user.

Failure to Enrol – The inability of a biometric system to obtain the necessary biometric sample of a user sufficient to enrol 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.

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 enrol 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 traveller (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 enrolee, 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 enrol 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 enrolee whose identity is being claimed, to determine whether it matches the enrolee'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.

Annex C Abbreviations

Abbreviation	
ABC	Automated Border Control system
BAC	Basic Access Control
CA	Certification Authority
CRL	Certificate Revocation List
CSCA	Country Signing CA
DG	Data Group
DO	Data Object
DS	Document Signer
ICC	Integrated Circuit Card
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
PKD	Public Key Directory
PKI	Public Key Infrastructure
RF	Radio Frequency
SM	Secure Messaging
TAG	Technical Advisory Group

Annex D Reference Documentation

The following documentation served as reference for this Technical Report:

[R1] *Technical Report: Biometrics Deployment of Machine Readable Travel Documents, version 2.0.*

[R2] *Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Revision – 1.7*

[R3] *Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version: 1.1.*

[R4] *Doc 9303, Part 1, Machine Readable Passports , 6th edition 2006, volume 1, Passports with Machine Readable Data Stored in Optical Character Recognition Format*

[R5] *Doc 9303, Part 1, Machine Readable Passports, 6th edition 2006, volume 2, Specifications for Electronically Enabled Passports with Biometric Identification Capability.*

— END —