



**BIOMETRICS DEPLOYMENT
OF
MACHINE READABLE
TRAVEL DOCUMENTS**

ICAO TAG MRTD/NTWG

TECHNICAL REPORT

Version 1.9

*Development and Specification of
Globally Interoperable Biometric Standards for
Machine Assisted Identity Confirmation
using Machine Readable Travel Documents*

TABLE OF CONTENTS

1. DOCUMENTATION HISTORY	4
2. INTRODUCTION.....	5
SCOPE AND PURPOSE.....	5
WHAT ARE BIOMETRICS ?	6
DEFINITIONS AND TERMS	8
WHAT ARE THE KEY PROCESSES WITH RESPECT TO BIOMETRICS ?	11
WHAT APPLICATIONS ARE THERE FOR A BIOMETRICS SOLUTION ?	12
CONSTRAINTS ON BIOMETRICS SOLUTIONS.....	13
3. ICAO'S VISION.....	14
THE VISION	14
THE SELECTION OF BIOMETRICS APPLICABLE TO MRTDs.....	14
THE BERLIN RESOLUTION	15
THE NEW ORLEANS RESOLUTION	17
4. NTWG RELATED TECHNICAL REPORTS.....	18
THE ORIGINAL TAG/MRTD BIOMETRICS SELECTION REPORT	18
THE LOGICAL DATA STRUCTURE (LDS) TECHNICAL REPORT	19
PKI (SECURITY OF ELECTRONIC DATA) TECHNICAL REPORT	19
CONTACTLESS IC CHIP TECHNICAL REPORT.....	20
MINIMUM MRTD ISSUANCE SECURITY STANDARDS TECHNICAL REPORT	20
MINIMUM MRTD SECURITY STANDARDS/FEATURES TECHNICAL REPORT	20
MRTD READER STANDARDS TECHNICAL REPORT	20
5. SELECTION OF A BIOMETRIC	21
POTENTIAL METHODS OF IDENTITY CONFIRMATION	21
KEY CONSIDERATIONS CONCERNING BIOMETRICS DEPLOYMENT	21
MRTD ISSUANCE CONSIDERATIONS	22
BORDER CONTROL CONSIDERATIONS	23
OPERATIONALIZATION CONSIDERATIONS	24
DEPLOYMENT COSTS AND IMPACTS	25
6. USING THE LOGICAL DATA STRUCTURE.....	26
LOGICAL DATA STRUCTURE TECHNICAL REPORT.....	26
LDS DATA UPDATE BY OTHER STATES	26
7. ENABLING GLOBAL INTEROPERABILITY.....	27
IMAGE OR TEMPLATE ?.....	27
MINIMUM DATA ITEMS IN THE LDS THAT MUST BE ASSIGNED VALUES IN A BIOMETRICS DEPLOYMENT OF THE LDS	30
8. DATA STORAGE TECHNOLOGIES.....	31
WHICH DATA STORAGE TECHNOLOGY IS APPROPRIATE FOR A GLOBALLY INTEROPERABLE BIOMETRICS DEPLOYMENT ?	31
WHAT MINIMUM DATA CAPACITY SHOULD BE CHOSEN ?	32
CONTACTLESS IC CHIP RECOMMENDATION.....	34
CONTACTLESS IC CHIP CONSIDERATIONS.....	35
WHERE IS THE CONTACTLESS IC CHIP PLACED IN THE PASSPORT ?.....	37
HOW IS THE CONTACTLESS IC CHIP DATA PROTECTED IN THE PASSPORT ?	38
HOW TO INDICATE IN THE DOCUMENT THAT THERE IS A DATA STORAGE TECHNOLOGY IN THE MRTD ?.....	39
TRAVEL DOCUMENT 10 YEAR VALIDITY CONSIDERATIONS	40

9. VISAS.....	41
10. OTHER INTEROPERABLE USES OF BIOMETRIC-ENABLED MRTDS.....	42
11. SECURITY REQUIREMENTS.....	43
12. TECHNICAL RELIABILITY.....	44
13. INTERIM/TRANSITIONAL STRATEGIES.....	45
DATA PAGE PORTRAIT.....	46
14. DOCUMENT 9303.....	47
15. SUMMARY OF RECOMMENDATIONS.....	48
16. ANNEXES – [SEE THESE CORRESPONDING SEPARATE DOCUMENTS].....	50
A - GUIDELINES FOR TAKING PHOTOGRAPHS TO MAXIMIZE FACIAL RECOGNITION.....	50
RESULTS : PASSPORTS AUSTRALIA BROCHURE.....	50
B - FACIAL IMAGE OPTIMAL STORAGE SIZE STUDY – 1.....	50
C - FACIAL IMAGE OPTIMAL STORAGE SIZE STUDY – 2.....	50
D - FACIAL IMAGE FORMAT FOR INTEROPERABLE DATA INTERCHANGE.....	50
E - IRIS IMAGE FORMAT FOR INTEROPERABLE DATA INTERCHANGE.....	50
F - FINGERPRINT IMAGE FORMAT FOR INTEROPERABLE DATA INTERCHANGE.....	50
G - FINGERPRINT MINUTIAE FORMAT FOR INTEROPERABLE DATA.....	50
INTERCHANGE.....	50
H - FINGERPRINT PATTERN FORMAT FOR INTEROPERABLE DATA INTERCHANGE.....	50

1. Documentation History

Date	Revision	Action
11-Sep-2002	1.1	Conceptual Outline & Project Editing Terry Hartmann, Passports Australia terry.hartmann@dfat.gov.au
11-Oct-2002	1.2	Initial Outline Draft
18-Nov-2002	1.3	Expand Outline Draft - wider range of topics
19-Nov-2002	1.4	Incorporate M1 papers
4-Dec-2002	1.5	Comments arising from Nov US visit by TH
20-Dec-2002 4-Mar-2003	1.6	Review by NTWG Meeting in Rotorua Expansion of text to include detailed content Incorporate suggestions from John Osborne
20-Mar-2003 17-Apr-2003	1.7	Include review comments from NTWG Meeting in New Orleans in March 2003
25-Apr-2003	1.8	Feedback from NTWG Review of version 1.7 and Helsinki WG3 Meeting
19-May-2003	1.9	Feedback from NTWG on 5 May 2003 Feedback from TAG 14 on 5-9 May 2003

2. Introduction

Scope and Purpose

ICAO New Technologies Working Group (NTWG) has, as a key tenet, been undertaking a program focusing on machine assisted identity confirmation of persons, both in terms of identification at the time of initial issue of travel documents, and in terms of verification for border control purposes.

At the core of this program is biometrics, being the way of uniquely encoding a particular physical characteristic of a person into a biometric-identifier (also known as a biometric template) that can be machine-verified to confirm the presenter's identity. In ultimate terms this could enable self-verification of an individual, and as a minimum it can provide assistance for verification personnel as to the potential the person presenting is an impostor.

NTWG has authored a number of Technical Reports, initially specifying face, fingerprint and iris (one or a combination thereof) as the biometrics to be used by States and subsequently resolving that face is the biometric most suited to the practicalities of travel document issuance, with fingerprint and/or iris available for choice by States for inclusion as complementary biometric technologies. Additional NTWG Technical Reports have specified a Logical Data Structure in which to electronically encode the biometric in a travel document, and the use of PKI (Public Key Infrastructure) schemes to protect and authenticate the data so-encoded.

The purpose of this Technical Report is to discuss each of the issues in relation to the deployment of biometrics and to present to ICAO Technical Advisory Group (TAG/MRTD) in May 2003 a series of recommendations for approval as standards in relation to biometrics and how these standards are to be incorporated into Document 9303. The timely specification of standards will enable member States to implement biometrics-related technologies as soon as possible, confident they are ICAO standards compliant.

In so doing, key considerations are:

- **Global Interoperability** – the crucial need for specifying how the biometrics deployed are to be used in a universally interoperable manner
- **Uniformity** – the need to minimise via specific standard setting, to the extent practical, the different solution variations that may potentially be deployed by member States
- **Technical Reliability** – the need for provision of guidelines and parameters to ensure member States deploy technologies that have been proven to provide a high level of confidence from an identity confirmation viewpoint; and that States reading data encoded by other States can be sure that the data supplied to them is of sufficient quality and integrity to enable accurate verification at their end
- **Practicality** – the need to ensure that recommended standards can be operationalized and implemented by States without them having to introduce a plethora of disparate systems and equipment to ensure they meet all possible variations and interpretations of the standards
- **Durability** – that the systems introduced will last the maximum 10 year life of a travel document, and that future updates remain backwards compatible.

What are Biometrics ?

“Biometrics” are the automated means of recognising a living person through the measurement of distinguishing physiological or behavioural traits. A “biometric template” is a machine-encoded representation of the trait created by a computer software algorithm, and enables comparisons (matches) to be performed to score the degree of confidence that separately recorded traits identify (or do not identify) the same person.

In the context of this Technical Report, the biometrics referred to are the physiological ones of

- facial recognition
- fingerprint
- iris

which were selected and endorsed by the ICAO TAG/MRTD in February 2002 in the original *NTWG Biometrics Selection Technical Report*.

Furthermore the purpose of this *Biometrics Deployment Technical Report* is to provide guidelines for States in the introduction and deployment of biometrics with respect to Machine Readable Travel Documents (MRTD) and their holders, border security and border control.

There are three (3) types of MRTD:

- A **passport** asserts the person is a citizen of the issuing State
- A **visa** asserts the State issuing the visa has granted the non-citizen the privilege of entering and remaining in the issuing State for a specified time and purpose.
- **Other travel documents** are essentially special purpose identification/border-crossing cards issued to non-citizens

In biometrics terminology:

- “**verify**” means to perform a **one-to-one** match between proffered biometric data obtained from the MRTD holder now, and a biometric template created when the holder enrolled in the system.
- “**identify**” means to perform a **one-to-many** search between proffered biometric data and a collection of templates representing all of the subjects who have enrolled in the system.

Biometrics can be used to improve the quality of the background checking performed as part of the passport, visa or other travel document application process, and they can be used to increase the strength of the binding between the travel document and the person who holds it.

This *Biometrics Deployment Technical Report* focuses on biometrics in relation to Machine Readable Passports.

Following publication, a subsequent version of it will continue to be updated to include:

- clarification of strategy and guidelines based on:
 - information and techniques determined in related NTWG Technical Reports (in particular the *LDS, PKI and Contactless IC Technical Reports*)
 - feedback from Member States research and development, and pilot programs
 - feedback from other groups and institutions exploring biometrics technology
- new technology developments
- globally interoperable standards developments
- specific information on biometrics deployment with respect to visas and travel cards.

Definitions and Terms

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

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

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

Biometric System – An automated system capable of:

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

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

Comparison – The process of comparing a biometric sample with a previously stored reference template or templates. See also ‘One-To-Many’ and ‘One-To-One’.

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

End User A person who interacts with a biometric system to enrol or have his/her identity checked.

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

Enrollee – A human being, ie natural person, assigned an MRTD by an Issuing State

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 physical characteristics of a user to enrol that potential user.

Failure to Enroll – The inability of a biometric system to enrol a potential user.

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

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

False Match Rate – Alternative to ‘False Acceptance Rate’. Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of ‘False Acceptance’ and ‘False Rejection’.

False Non-Match Rate – Alternative to ‘False Rejection Rate’. Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of ‘False Acceptance’ and ‘False Rejection’.

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

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

Gallery – the database of biometric templates of persons previously enrolled, amongst which you are looking for the Probe

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.

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 video, camera or scanning device.

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

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

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

Live Capture – The process of capturing a biometric sample by an interaction between an MRTD holder and a biometric system.

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

MRTD – Machine Readable Travel Document eg passport, visa

Multiple Biometric – A biometric system that includes more than one biometric system or biometric technology.

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

One-to-Many – Synonym for ‘Identification’.

One-to-One – Synonym for ‘Verification’.

Probe – the biometric template for the person you are looking for

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

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

Score – a number on a scale from low to high, measuring the success that a biometric probe record (the person you are looking for) matches a particular gallery record (a person previously enrolled)

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

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

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

Threshold – a “benchmark” score above which you are interested in the potential of the match, or below which you reject the match, as potentially being the probe person you are looking for

Token – A physical device that contains information specific to the user/holder, eg a passport.

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

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

What are the Key Processes with respect to Biometrics ?

The major components of a biometric system are:

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

These processes involve:

- the *enrolment* process is the *capture* of a raw biometric sample. It is used for each new person (potential MRTD holder), taking biometric samples to establish a new template. This capture process is the automatic acquisition of the biometric via a capture device such as a fingerprint scanner, photograph scanner, live-capture digital image camera, or live-capture iris zooming camera. Each capture device will need certain criteria and procedures defined for the capture process – for example standard pose facing the camera straight-on for a facial recognition capture; whether fingerprints are capture flat or rolled for fingerprint capture; eyes fully open for iris capture.
- The *template creation* process preserves the distinct and repeatable biometric features from the captured biometric sample and is generally via a proprietary software algorithm to extract a template from the captured image which defines that image in a way it can subsequently be compared with another captured image and a comparative score determined. Inherent in this algorithm is quality control, wherein through some mechanism, the sample is rated for quality. Quality standards need to be as high as possible since all future checks are dependent on the quality of the originally captured image. If the quality is not acceptable, the *capture* process should be repeated.
- the *identification* process takes new samples and compares them to saved templates of enrolled users to determine whether the user has enrolled in the system before, and if so, whether in the same identity
- the *verification* process takes new samples of an MRTD holder and compares them to previously saved templates of that holder, to determine whether the holder is presenting in the same identity.

What Applications are there for a Biometrics Solution ?

The key application of a biometrics solution is the identity verification problem of physically tying an MRTD holder to the MRTD they are carrying.

There are several typical applications for biometrics during the enrolment process of applying for a passport or visa:

1. The applicant's biometric template(s) generated by the enrolment process can be searched against one or more biometric databases (identification) to determine whether the applicant is known to any of the corresponding systems (for example, holding a passport under a different identity, criminal record, holding a passport from another state).
2. When the applicant collects the passport or visa (or presents themselves for any step in the issuance process after the initial application is made and the biometric data is captured) their biometric data can be taken again and verified against the initially captured template
3. The identities of the staff undertaking the enrolment can be verified to confirm they have the authority to perform their assigned tasks. This may include biometric authentication to initiate digital signature of audit logs of various steps in the issuance process, allowing biometrics to link the staff members to those actions for which they are responsible.

There are also several typical applications for biometrics at the border:

1. Each time travellers (ie MRTD holders) enter or exit a State, their identities can be verified against the images or templates created at the time their travel documents were issued. This will ensure that the holder of a document is the legitimate person to whom it was issued and will enhance the effectiveness of any Advance Passenger Information (API) system. Ideally, the biometric template or templates should be stored on the travel document along with the image, so that travellers' identities can be verified in locations where access to the central database is unavailable or for jurisdictions where permanent centralized storage of biometric data is unacceptable.
2. Two-way check - The traveller's current captured biometric image data, and the biometric template from their travel document (or from a central database), can be matched to confirm that the travel document has not been altered.
3. Three-way check - The traveller's current biometric image data, the image from their travel document, and the image stored in a central database can be matched (via constructing biometric templates of each) to confirm that the travel document has not been altered. This technique matches the person, with their passport, with the database recording the data that was put in that passport at the time it was issued.
4. Four-way check - A fourth confirmatory check, albeit not an electronic one, is visually matching the results of the 3-way check with the digitised photograph on the Data Page of the traveller's passport.

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

1. Accuracy of the biometric matching functions of the system. Issuing States must encode one or more facial, fingerprint or iris biometrics on the MRTD as per LDS standards (or on a database accessible to the Receiving State). Given an ICAO-standardised biometric image and/or template, Receiving States must select their own biometric verification software, and determine their own biometric scoring thresholds for identity verification acceptance rates – and referral of imposters.
2. Throughput (eg travellers per minute) of either the biometric system or the border crossing system as a whole.
3. Suitability of a particular biometric technology (finger or face or eye) to the border crossing application.

Constraints on Biometrics Solutions

- It is recognised that vendor's implementation of most biometrics technologies are subject to further (rapid) development.
- Many have not been tested over a ten year plus period
- Many have no proven track record confirming identity on a one-to-many basis against a large national database
- Given the rapid state of technology change, any specifications must allow for changes resulting from technology improvements
- The biometrics information stored on travel documents should not (as far as possible) contravene any national data protection laws or cultural practices.

3. ICAO's Vision

The Vision

The ICAO vision for the application of biometrics technology encompasses:

- Specification of a primary interoperable form of biometrics technology for use at border control (verification, watch lists) as well as by carriers and document issuers and specification of agreed supplementary biometric technologies
- Specification of the biometrics technologies for use by document issuers (identification, verification and watch lists)
- Capability of retrieval for maximum ten year validity as specified in Document 9303
- Having no proprietary element to ensure that any States investing in biometrics are protected against changing infrastructure or changing suppliers

The Selection of Biometrics Applicable to MRTDs

It has long been recognised that names and honour are not sufficient enough traits to guarantee that the holder of an identity document (MRTD) assigned to that person by the Issuing State, is guaranteed to be the person purporting at a Receiving State to be the same person to whom that document was issued.

The only way therefore to tie the person irrevocably to their travel document is to have a physiological characteristic of that person associated with their travel document in a tamper-proof manner. This physiological characteristic is, of course, a biometric.

NTWG therefore began investigating some five years ago biometrics as various incarnations of the technology emerged. The first task was to identify biometrics that were applicable to MRTDs and, after an exhaustive analysis, this was achieved with the Biometrics Selection Report endorsed by TAG in February 2002 which recommended the biometrics applicable to MRTDs being

- Face
- Fingerprint
- Iris

and that member States start actively investigating these technologies.

Subsequent to the start of that investigation, the events of September 11, 2001 motivated increased activity in the area of development of various biometrics studies, experiments, pilot programs and products to expedite the inspection process at border crossing points.

The Berlin Resolution

By June 2002, it was clear to NTWG that a guideline was needed to assist States in prioritising their investigations. Consequently at the June 2002 meeting of NTWG in Berlin, the following resolution was unanimously endorsed:

“ICAO TAG-MRTD/NTWG RESOLUTION N001 - Berlin, 28 June 2002

ICAO TAG-MRTD/NTWG endorses the use of face recognition as **the globally interoperable biometric** for machine assisted identity confirmation with machine readable travel documents.

ICAO TAG-MRTD/NTWG further recognizes that Member States may elect to use fingerprint and/or iris recognition as additional biometric technologies in support of machine assisted identity confirmation.

Endorsement: Unanimous”

In reaching this resolution, NTWG observed that for the majority of States the following advantages applied to face:

- Facial photographs do not disclose information that the person does not routinely disclose to the general public
- The photograph (facial image) is already socially and culturally accepted internationally
- It is already collected and verified routinely as part of the MRTD application form process in order to produce a passport to ICAO Document 9303 standards
- The public are already aware of its capture and use for identity verification purposes
- It is non-intrusive – the user does not have to touch or interact with a physical device for a substantial timeframe to be enrolled.
- It does not require new and costly enrolment procedures to be introduced
- Capture of it can be deployed relatively immediately and the opportunity to capture face retrospectively is also available
- Many States have a legacy database of facial images captured as part of the digitised production of passport photographs which can be encoded into facial templates and verified against for identity comparison purposes
- It can be captured from an endorsed photograph, not requiring the person to be physically present
- It allows capture of children’s biometrics without the children having to be present
- For watch lists, face (photograph) is generally the only biometric available for comparison
- It always acquires
- Human verification of the biometric against the photograph/person is relatively simple and a familiar process for border control authorities

At the Berlin Meeting, the NTWG unanimously supported its preference for the use of facial recognition as the globally interoperable biometric, noting that whilst it is recognized that research in this area is not yet complete, there is no evidence to suggest that facial recognition cannot be made to work in both the document issuance and border control environments.

NTWG noted that States optionally can provide additional data input to their (and other States) identity verification processes by including multiple biometrics in their travel documents ie a combination of face and/or fingerprint and/or iris.

This is especially relevant where States may have existing fingerprint or iris databases in place against which they can verify the biometrics proffered to them, for example as part of an id card system.

The New Orleans Resolution

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

Consequently at the March 2003 NTWG Conference in New Orleans, USA, a clarification resolution was proposed and accepted which builds on, and further clarifies, the strategy articulated by the Berlin resolution.

NEW ORLEANS RESOLUTION 21 March 2003

In order to clarify NTWG Resolution N001 of June 28, 2002 (commonly referred to as the "Berlin Resolution"), and taking into account recent developments in data storage technologies, the NTWG hereby resolves:

ICAO TAG-MRTD/NTWG recognizes that Member States currently and will continue to utilize the facial image as the primary identifier for MRTDs and as such endorses the use of standardized digitally- stored facial images as the globally interoperable biometric to support facial recognition technologies for machine assisted identity verification with machine-readable travel documents.

ICAO TAG-MRTD/NTWG further recognizes that in addition to the use of a digitally stored facial image, Member States can use standardized digitally- stored fingerprint and/or iris* images as additional globally interoperable biometrics in support of machine assisted verification and/or identification.

Member States, in their initial deployment of MRTDs with biometrics identifiers, are encouraged to adopt Contactless IC media of sufficient capacity to facilitate on-board storage of additional MRTD data and biometric identifiers.

* subject to the resolution of intellectual property issues

Key additional clarification provided by the New Orleans resolution includes:

- Digitally stored images will be used for global interoperability purposes, and these will be "on-board" ie electronically stored in the travel document
- These images are to be standardized (the *NTWG Biometrics Deployment Technical Report* is the document that in the first instance defines the standards)
- High capacity Contactless IC media is the electronic storage medium endorsed by NTWG as the capacity expansion technology for use with MRTDs in the deployment of biometrics.

4. NTWG Related Technical Reports

The Original TAG/MRTD Biometrics Selection Report

In 2001, TAG/MRTD, published a Technical Report entitled *Machine Readable Travel Documents – Selection of a Globally Interoperable Biometric for Machine-Assisted Identity Confirmation with MRTDs*.

The purpose of this Technical Report on Biometrics was to

"define the current state of investigation in to the compatibility and ranking of the available biometric technologies with the complete set of unique requirements imposed on machine-assisted identity confirmation with MRTDs"

The Technical Report defines the requirements for ranking biometric technologies in MRTD environments, and provides weighted ratings of leading biometric technologies according to this methodology. It then offers an emerging thesis based on this data, and proceeds to define next steps in terms of scenario-based and operational testing.

The Report states as a necessary condition of compatibility with MRTD requirements the ability to support both verification and identification.

The Report cites the following processes in which the use of biometrics must be feasible:

- Initial MRTD issuance
- MRTD renewal
- MRTD document and document-holder inspection for purposes such as border control or airline check-in.

The Technical Report recommended

"It is necessary for scenario evaluations and operational evaluations to be undertaken in the context of MRTD application requirements, in order to obtain meaningful performance data for selected technologies when used in conjunction with enrollment in an MRTD program, renewal of an MRTD and machine-assisted identity verification with an MRTD.

Sufficient data is available from the assessment to advance three (3) of the currently available technologies to more detailed assessment work, ie face, fingerprint and iris. Testing of these technologies should be undertaken by States immediately".

The Logical Data Structure (LDS) Technical Report

During the revision of Doc 9303 TAG/MRTD determined that a State might wish to expand the machine readable data capacity of the MRTD beyond that defined for global interchange (optical character reading of the MRZ Machine Readable Zone), for such purposes as providing machine readable access to breeder document information (eg birth certificate details), stored personal identity confirmation (biometrics) and/or document authenticity verification details.

Since co-existence of an optional machine readable data storage technology with the mandatory OCR technology is critical to ensure global interoperability of the MRTD, specifications were developed governing the location of the capacity expansion technologies (ie IC(s) with contacts, contactless IC(s), optical memory and bar codes) on a MRTD. These specifications have been included in the new editions of each Part of Doc 9303.

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

The LDS Technical Report is a report published in advance of publication of formal specifications for the LDS in future Editions of Doc 9303, and describes in detail “*Development of a Logical Data Structure (LDS) For Optional Capacity Expansion Technologies*”.

PKI (Security of Electronic Data) Technical Report

This Technical Report is intended to provide guidance and advice to States and to suppliers regarding the application and usage of modern encryption techniques, particularly interoperable public key infrastructure (PKI) schemes, to be used by States with their Machine Readable Travel Documents as made in accordance with the specifications set out in ICAO Doc 9303.

The intent of this Technical Report on encryption and PKI technologies is primarily to augment security through automated means of authentication of MRTDs and their legitimate holders internationally. In addition, this Technical Report documents ways and means recommended to implement international MRTD authentication, and provides a path to the use of advanced capability MRTDs, (eg those employing optical zones, smart chips or other advanced technologies), to facilitate biometric or e-commerce applications.

The PKI Technical Report and its associated Addendums represents the recommended direction to be taken by ICAO in the area of increased security through encryption technologies and document authentication, and the potential expansion of MRTD activities into e-commerce services.

The PKI Technical Report, in conjunction with the LDS Technical Report, specifies how data integrity and data privacy is to be achieved in the context of biometrics deployment in MRTDs.

Contactless IC Chip Technical Report

The purpose of the Contactless Integrated Circuit (IC) Technical Report is to provide advice and guidance to States and to potential Suppliers regarding the application and use of Contactless ICs in MRTDs. The report covers each of the issues in relation to the deployment of these Contactless ICs.

The Technical Report advises

- Contactless ICs are to conform to ISO 14443 Type A or Type B
- The LDS is to be encoded according to the Random Access method
- read range should be up to 10cm

Minimum MRTD Issuance Security Standards Technical Report

This Technical Report provides recommended practices to enhance the security of the issuance process for Machine Readable Passports. As such it establishes recommended global practices for use by all States with the objective of minimizing the vulnerabilities that are within every passport handling and issuance process.

The recommendations cover the entire passport process from ordering of the blank documents, to delivery of the issued document to the passport applicant. They also include personnel security issues to help prevent internal fraud, through a robust internal controls program. The Technical Report also contains an introduction to protection against theft and abuse of genuine passports and their components.

Minimum MRTD Security Standards/Features Technical Report

This Technical Report discusses prevention of counterfeiting and alteration of Machine Readable Travel Documents. It has been adopted as an Informative Annex of ICAO Document 9303 – the global machine readable travel document standard.

MRTD Reader Standards Technical Report

This Technical Report describes minimum standards for Machine Readable Travel Document OCRB readers as an aid to States and suppliers of this equipment.

This report will also need to consider fusion readers that read the Data Page as well as the Contactless IC Chip.

5. Selection of a Biometric

Potential methods of Identity Confirmation

There are 3 potential methods of Identity Confirmation with respect to MRTDs.

These methods are:

1. Carried on identity document or card eg the chip in the passport
2. Held by receiving entity eg on their central database of visas issued at embassies in foreign countries
3. Derived from displayed feature resident on the identity document/card eg the photo on the data page of a passport

The best one for the particular application needs to be chosen, having regard to global interoperability considerations.

Key Considerations Concerning Biometrics Deployment

When selecting a biometric, States should have regard to a variety of considerations including:

- The *NTWG Biometrics Selection Technical Report* nominating face, fingerprint and iris
- The Berlin and New Orleans resolutions
- Public acceptability
- Practicality of capture
- Practicality of deployment
- Proprietaryness - protecting investment against changing infrastructure or changing suppliers
- Impact on MRTD issuance process
- Impact on Border Security and Border Control
- Impact on design and manufacture of MRTDs
- Costs of deployment

MRTD Issuance Considerations

From the MRTD issuance point of view, considerations include:

- Business Usage – noting the difference between a passport (open system where interoperability is required) and a visa (closed system where interoperability is not required)
- Which biometric(s) to capture ?
- How to encode the biometric data ?
- What data aspects of the biometric to electronically store ?
- Whether the biometric will be stored physically in the MRTD or accessed via database lookup ?
- How the biometric will be stored in the MRTD ?
- Where to place the biometric in the MRTD ?
- **And above all**, whether the Issuing Authorities procedures and processes ensure that the document is issued to a person to whom it is entitled, for example that a passport is issued to a bona-fide citizen of the State whom the issuing authority has verified as such via use of breeder documents, electronic verification of documentation presented with the issuing authority for that documentation, external database integrity checks, id card database checks etc.

Border Control Considerations

- States are encouraged to use biometrics to establish or validate identity at border control. The use of biometric data does not ensure that a person has provided their correct name, citizenship and other information, but when biometric identity has been confirmed, it does help to prevent the person from using another name in their dealings. Biometric identity should be identified at ports of entry and ideally points of exit.
- If the biometric verification is negative, or there are other actions to be taken determined at the primary port of entry, the traveller may be sent to secondary inspection for detailed inspection.
- Primary or Secondary inspection can include a three-way visual comparison of the MRTD holder, the printed portrait image on the Data Page of MRTD and the stored digital record read from the biometric storage medium in their MRTD (passport) or central database (visa)
- Ideal would be a gate/booth that captures those biometrics noted as in that holders passport ie booth capable of capturing all 3, but only actually captures based on read of the LDS eg if passport holder has face biometric only stored, face (image) is captured; if passport holder has fingerprint and face biometrics in their LDS, fingerprint and face is captured.
- Procedures need to be determined for how inspection officers would handle exceptions such as when the biometrics on the MRTD do not match the person at the border because the document is not working, the storage medium is damaged or not functioning properly, the verification software does not match the person successfully, the document has been physically tampered with, or the traveller is an imposter. Similarly inspection officers need to be aware of, and have procedures in place, with respect to liveness checking and detection of spoofing.
- States need to change the focus of border systems from merely processing entries and exits, to systems that confirm identities through automated systems; and thereby seek to also identify fraudulent identities and fraudulent travel documents.
- One-to-one verification systems (and one-to-few watch list checking systems) are the appropriate ones to implement at primary inspection. These could be supplemented by use of one-to-many systems at borders as appropriate.
- States need to be aware that land borders present unique challenges – many people cross the same land border regularly for commuting purposes and several people may cross in the same vehicle.
- Border Control systems can be complemented by the use of pre-entry systems including API (Advanced Passenger Information) which may also use verification systems as part of their processing.

Operationalization Considerations

When planning a biometrics-based system, States should have regard to a variety of considerations including:

- How to go about confirming identity at the time of issuance ?
- How to go about verifying identity at the time of inspection eg Airport-Gate type solutions?
- How to process secondary inspection (eg dealing with False Rejects) ?
- Impacts on time of processing
- At States own borders, for passports issued to their own citizens, whether to extract the biometric from the traveller's passport, or from a database containing the biometric template assigned to that traveller when their passport was issued (note some States are legislatively inhibited from storing biometric templates and in this case have no choice other than to use the image or template stored in the travel document).

Deployment Costs and Impacts

Deploying biometrics into MRTDs is a complex process and States need to be aware of the considerations and costs involved including:

- Review/upgrade of current systems to ensure they are conducting the necessary external verification checks to assist in verifying individuals identity including confirmation of the validity of breeder documents such as birth and citizenship certificates.
- Enrolment equipment, information technology infrastructure, software, communications, staff, facilities and training for that States biometric(s) of choice
- Review/upgrade of any existing enrolment systems (eg scanners) to ensure they meet minimum capture standards including image resolution
- Template encoding and 1:many matching software, handling of exceptions for the enrolment process
- Reading equipment, information technology infrastructure, software, communications, staff, facilities and training for the data storage technologys (IC chip), and biometrics (face / fingerprint / iris) that State chooses to verify at their borders
- Template encoding of the biometric presented at the border by the person, and 1:1 matching software with the biometric in the document (for passport holders) or in the database (for visa holders), handling of exceptions for the entry/exit process
- 1:many watch list matching in the enrolment process
- 1:many watch list matching in the border control process
- acquisition of the biometric storage medium (IC chip) for each MRTD
- equipment necessary to insert the biometric storage medium (IC chip) in the MRTD in a tamperproof manner, verify its integrity, personalise it as per LDS standards, and protect the data written to it
- systems integration with existing databases

6. Using the Logical Data Structure

Logical Data Structure Technical Report

The *Logical Data Structure Technical Report* specifies a single globally interoperable Logical Data Structure (LDS) for recorded identity details, including biometric data. It is a successor to the OCRB Machine Readable Zone on the Data Page, and complements this Machine Readable Zone. Its purpose is to facilitate confirmation of the presenter of an identification document or card as the rightful holder by machine-assisted means. The LDS is read electronically and designed to be flexible and expandable to suit State's emerging and future needs.

The LDS governs the recording of details when using any of the data storage technologies currently defined for identification documents and cards – which are:

- 2D barcodes – 2DB
- Magnetic stripe
- Integrated Circuit Chips – Contact IC
- Integrated Circuit Chips – Contactless IC
- Optical memory

LDS Data Update by Other States

Practical applications for the next version of the LDS specification include:

- Issuing State writing a second biometric into the LDS created by the Issuing State – eg updating a facial biometric as a result of plastic surgery
- Receiving State writing a second biometric into the LDS created by the Issuing State – eg adding verified live image of the passport holder as captured at the airport
- updating visa data

7. Enabling Global Interoperability

Image or Template ?

The crucial question with respect to selection of a data storage technology is “how much data has to be stored?”. The answer to this question drives States choice of data storage technology.

For global interoperability via use of biometrics, the question is “in what form is the biometric written by the Issuing State, such that it can be openly read by the Receiving State?”. In the case of the three endorsed biometrics the answers are becoming clear:

- **Face –**

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

- **Fingerprint –**

In terms of fingerprint biometrics, there are two classes of technology: minutiae based systems, and pattern based systems. Whilst standards have been developed within these classes to make most systems interoperable amongst their class, they are not interoperable between classes. It therefore is transpiring that 3 standards for fingerprint interoperability are emerging: storage of the image, storage of the minutiae rules and storage of the pattern rules.

- **Iris –**

Iris biometrics are complicated by the dearth of proven vendors. A defacto standard has therefore emerged based on the methodology of one recognized vendor. Other vendors may in future provide iris technology, but it is likely they will need the image of the iris as their starting point, rather than the template created by the current vendor.

Each of the above state-of-play situations with respect to face, fingerprint and iris biometrics all point to storage of the image as being the only reliable globally interoperable method for guaranteeing that a receiving State can process the data provided by the Issuing State against the image of the MRTD holder they capture at their border.

Recommendation:

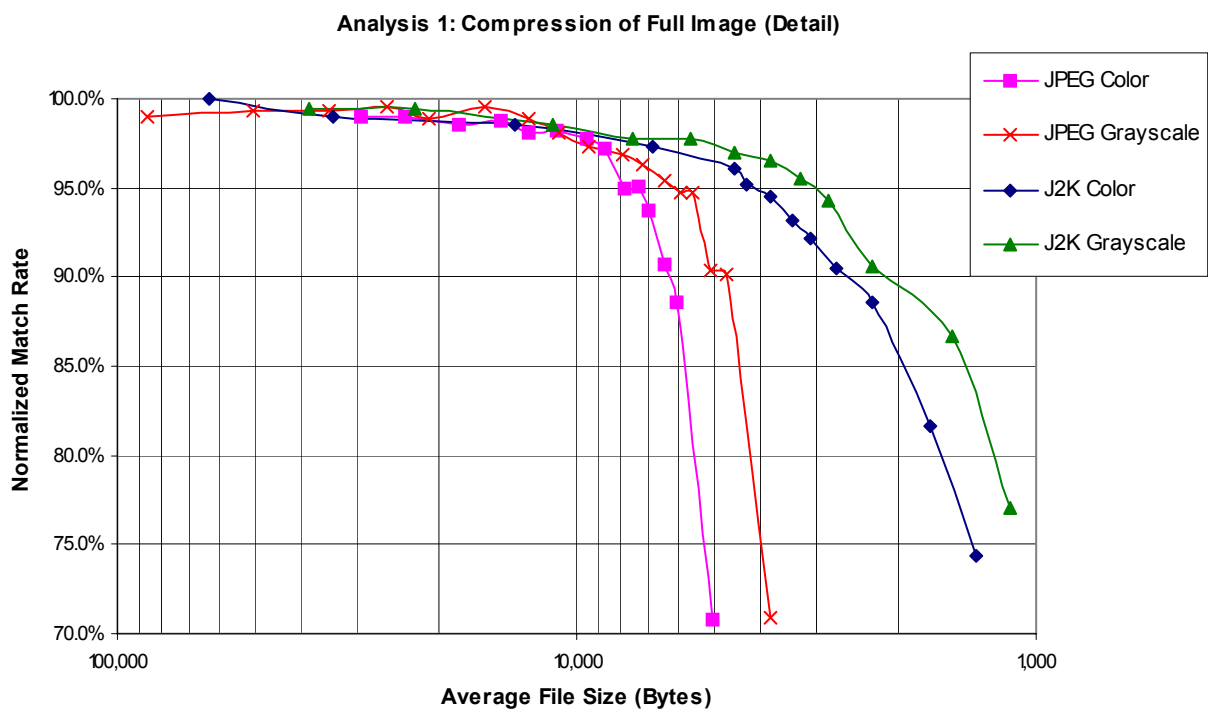
For each biometric type stored in the MRTD, storage of the image is mandatory, and storage of an associated template be optional at the discretion of the Issuing State.

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

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

For facial images, an ICAO-standard size photograph colour-scanned at 300dpi results in an image with approximately 90 pixels between the eyes and a size of approximately 112K (kilobytes) with very minimal compression.

The studies at Annex B and Annex C were undertaken using the same Australian Passport standard photograph images but using different vendor algorithms. The result obtained, using JPEG and JPEG2000 compression, shows the minimum optimal image size for an ICAO standard passport photo image is approximately 12K (kilobytes) of data. The studies show higher compression beyond this size results in less reliable facial recognition results.



Similar studies on fingerprint have shown the optimal image size is approximately 10K of data per finger.

Similar studies on iris have shown the optimal image size is approximately 30K of data per eye.

The degree to which the base image should be cropped is also a question. Whilst images can be cropped to save storage and show just the eye/nose/mouth features, the ability for a human to easily verify that image is of the same person in front of them, or appearing as the photograph in the data page of the passport, is diminished significantly.



For example, the image to the left provides a greater challenge in recognizing the person than the image to the right.



Recommendation:

Images stored in the LDS are to be either

- Not cropped ie identical to the image printed on the Data Page
- Be cropped from chin to crown, and edge-to-edge as a minimum as shown to the right



Storing optimally-compressed images ensures maximum flexibility and vendor independence for both current and future biometric matching requirements. States can then store in the MRTD one or more vendor-specific templates for their own use, and use by other States who use the same vendor systems.

Anything less than storage of images, would be a proprietary solution selecting one (or a select few) vendors solutions.

Additional biometrics can be added or updated seamlessly through the life of the MRTD eg a one-biometric system could easily be converted to a two-biometric fusion system or one-biometric additional templates could be added

Recommendation – storage of “optimally-compressed images” is mandatory

Minimum Data Items in the LDS that must be assigned values in a biometrics deployment of the LDS

The tables below show the types of qualifying information that needs to be included within specific Biometric Data Blocks within the LDS. These tables will be further defined and expanded upon in conjunction with the provisions of the *LDS Technical Report*.

Facial Recognition

DG 5	Photograph Image	Mandatory
DG 2	Facial Image Template	Optional
Biometric Data Block	Left Eye Co-ordinates	Mandatory
Biometric Data Block	Right Eye Co-ordinates	Mandatory
Biometric Data Block	Image Cropping Type {none or chin-to-crown}	Optional
Biometric Data Block	Compression Method {JPEG or JPEG2000}	Optional
Biometric Data Block	Expression Type {Neutral or Smile}	Optional
Biometric Data Block	Eye Alignment Type {Manual or Automatic}	Optional

Fingerprint

DG 5	Fingerprint Image	Mandatory
DG 2	Fingerprint Minutiae Template	Optional
Biometric Data Block	Fingerprint Pattern Template	Optional

Iris

DG 5	Iris Image	Mandatory
DG 2	Iris Image Template	Optional

8. Data Storage Technologies

Which Data Storage Technology is appropriate for a globally interoperable Biometrics Deployment ?

A standard data storage technology is necessary to enable States to conduct border deployment in a cohesive manner

- Non-proprietary (open) technology is required
- Flexibility is required
- Maintaining the integrity of the biometric data stored in the travel document and protection against destruction or tampering is required

Central to this question are the features of useability, data capacity and performance to achieve a high speed, high capacity and high security solution.

Useability –

Border Authorities have a strong desire for a contactless mode of operation - this is the data storage technology alternative most amenable to the passport booklet format, and the easiest for passport holders to manage – rather than swiping or sensing the electronic data it is simply retrieved via short-range antennae – the holder placing their MRTD on top of a designated reading device. High Density Magnetic Strip, Optical Memory and Contact IC chips all require direct contact of the technology with a reader. 2DB requires direct, or line-of-sight, contact of the technology with a reader. The only technology that requires neither direct or line-of-sight contact is **Contactless IC Chips**

Data Storage -

Transitional considerations aside, the minimum practicable data storage capacity needed for biometric verification given inclusion of facial images is approximately 12K (kilobytes) of data {ref Annexes B and C – Optimal Data Storage Sizes}. This need obviates the use of 2DB (typical capacity up to 2.2K, though some technologies up to 15.5K are available which have potential for deployment in localized travel document applications); and of High Density Magnetic Strip (typical capacity is up to 3,024 bytes gross; 2328 bytes net of overheads) The only technologies with sufficient capacity are **Contact IC chips, Contactless IC Chips and Optical Memory**.

Performance -

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

Overall in terms of the considerations of Useability, Data Storage and Performance, **Contactless IC Chip** is the only Data Storage Technology that meets all three considerations.

What Minimum Data Capacity should be Chosen ?

The New Orleans Resolution advises “Member States, in their initial deployment of MRTDs with biometrics identifiers, are encouraged to adopt Contactless IC media of sufficient capacity to facilitate on-board storage of additional MRTD data and biometric identifiers”.

The intent of this part of the Resolution, is that States adopt as high a capacity as they possibly can and which is operationally feasible and practicable, for the following reasons:

- **Future-proofing:** the data storage medium deployed in an MRTD must last for the life of that MRTD (typically 5 years up to, for some States, 10 years). Advances in data storage techniques, coupled with demand for new multi-purpose applications of smart-card technology in particular, has resulted in rapid advances in capacity being made (eg the vendors who were offering up to 8K (8 Kilobytes) per chip 1-2 years ago are now offering up to 64K), and these capacity rates will continue to increase. Also new memory technologies such as FLASH and FRAM have resulted in chips with capacity of 512K and 1024K (1MB) emerging as viable deployment options which will become increasingly more available.
- **Flexibility:** the LDS has been developed to allow for the storage of all types of biometrics including multiple types of biometrics ie face + finger + iris, and multiple instances of a particular biometric eg 10 fingers, 2 eyes, different face poses (if countries had an interest in such); as well as working towards the development of storage of visa and travel information in the LDS. States, therefore, who choose to do so will be able to add additional biometric data to MRTDs either at issue or subsequent to issue, and, in such cases the chip must provide available additional data capacity to enable this.

In terms of globally-interoperable storage of biometrics data in an LDS for identity verification at various States' borders, the **MRP must have a separate focus** from the MRV and Travel Card in the consideration of data storage capacities, as it has a more global purview and a longer validity period than the other MRTDs.

Minimum data capacity is a function of the type of data to be stored, and the usable data space remaining after overheads (such as chip operating systems) are deducted from the chip size. The section of this Technical Report entitled “*Enabling Global Interoperability – Image or Template*” along with the supporting Annexes, identifies optimally compressed image sizes for each biometric as face (~12K), fingerprint (~10K) and iris (~30K).

Given this calculated minimum data requirement of ~12K for an optimally compressed facial image + allowance of up to 5K for textual data and overheads including signing, the minimum data storage size of a chip in an MRP reaches **32K** (as chips size in powers of 2). **Ergo, the absolute minimum chip size for biometrics deployment in MRPs is 32K.**

But, the arithmetic is clear: the addition of just two fingerprint images to this data results in a required chip data storage size of **64K** ($12+5+10+10 > 32$). Add one iris, or a second updated instance, and the size becomes 128K.

Clearly, in view of futureproofing, the **goal has to be to implement as high a capacity as possible and practicable** to enable several additional data instances, and/or additional biometric images, to be added for update and/or biometric fusion purposes initially, or over the life, of the MRP.

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

Contactless IC Chip Recommendation

Recommendation:

- **Contactless IC Chip with as mandatory**
 - **On-board Operating System as per ISO/IEC Standard 7816-4**
 - **ISO 14443 Type A or Type B compliance**

- **Minimum data storage capacity to be as high as practicable**
 - in view of **future-proofing**, very high capacity is recommended
 - in view of **flexibility**, very high capacity is recommended
 - with fast read retrieval rates to ensure the chip can be practically used in a border situation

- **Minimum Set of Commands** as specified in the *Contactless IC Technical Report*, including as follows:
 - SELECT FILE by DF name (full name) to select the application
 - READ RECORD by short EF identifier with a specified record number or with a specified record identifier, to read data group
 - WRITE RECORD needed to load data group onto the chip

- Data stored in **LDS format** and with **encryption** and **signing** as per the *LDS Technical Report* and the *PKI Technical Report*

In considering chip deployment, States are advised to consider pricing as a factor of quantity of chips purchased, and to allow for the price of the chip, RF aerial, substrate, operating system and tamperproof insertion into the MRTD.

Data storage technologies other than Contactless IC Chip are to be used for non-globally-interoperable applications or transitional applications to Contactless IC chip ie

- by the Issuing State only for its own internal purposes, or
- by bilateral agreement as adjuncts to the Contactless IC chip

Contactless IC Chip Considerations

Refer to the *Contactless IC Technical Report* and the *LDS Technical Report*, in their current and subsequent versions, for more information on Contactless IC data storage technology, and detailed clarification of its applicable considerations.

Particular considerations to be addressed, are:

- Many vendors quote their chip sizes in Kilobits rather than Kilobytes. States should ensure that chip capacity is quoted in Kilobytes as the relevant data storage capacities are significantly different eg a 16K (kilobit) chip is in fact 2K (kilobytes) = 2048 bytes of information.
- a Contactless Chip can perform processing on board – tradeoffs in performance and flexibility between onboard processing or processing via software and downloading onto the chip need to be considered in designing the application.
- A Contactless IC Chip can provide a better security environment for the data – data written to the chip **must** be protected in terms of data integrity and data privacy (see the *LDS Technical Report* and the *PKI Technical Report*)
- Operations systems, memory management, cryptographic command sets and other overheads can all take up space on the chip. In deciding on chip size States need to determine, and verify, how much free usable memory will remain on the chip after these overheads are deducted. Planning the structure of the overhead items can enable additional space to be freed up eg the footprint of an operating system can potentially be reduced by exclusion of commands that will never be used by the Issuing State or any Receiving State.
- Contactless IC Chips with cryptographic co-processors on board can use challenge-response protocols to verify the chip has not been removed and placed in a different MTRD. Authenticating users before releasing data from the chip provides confidentiality for the information stored on the chip and it also makes skimming and producing duplicate chips more difficult
- Separate data in the LDS into different groups such as id verification, border control, issuer private data, and only release data appropriate to users authentication level
- Never update or destroy any information on the chip Just add new records at the end or in a different partition. The read application can be written to show only the most recent value or all values for a field.
- Use write-once memory to preserve integrity of data – but consider enabling ADD capability to enable future updates without overwriting existing data.
- What procedures to put in place as a Receiving State at the border if a Contactless IC chip fails to read (through inadvertent or malicious tampering)
- Deployment costs especially in less developed States which are only now coming to terms with MRTDs.
- Inspection – Data Page vs LDS – **recommendation** is reading the LDS will suffice thereby allowing potential for automated facilitation [but beware the potential of someone substituting/tampering one and not the other so States may choose to read both]. It is up to the Border Control Agency to determine which they wish to do.

- Durability of IC chip and Data Retention Period (lasting 10 years – States may consider moving to 5 year validity period for reasons such as technical flexibility and technology and security feature turnover)
- Proximity distance and data skimming considerations. **recommendation** = read distance range to be 0-10cm.
- Future-proofing issues – ensuring the chip laid down today can accommodate future LDS changes and future data additions
- Read standards – **recommendation** ISO 14443 Readers (type B) which also read Type A
- Security and Tamperproofing issues - **recommendation** encryption and digital signing be used to protect the data (see the *LDS Technical Report* and the *PKI Technical Report* for the detail of how this is to be achieved).

Where is the Contactless IC Chip placed in the passport ?

There are three apparent Location options for placement of the Contactless IC Chip in the passport booklet, each with their own advantages and disadvantages. Because the technology is contactless it should be immaterial to receiving Border Control Authorities which is used.

Above all the Contactless IC chip needs to be protected against physical tampering and casual damage including flexing and bending. The location of the chip is up to individual States to decide.

Suggested locations include:

- **Data page** – enables all data to be contiguous and technologies such as polycarbonate to be taken advantage of in embedding chips and antennae, but this must be balanced against the advantages of separating the Data Storage Technology from the data page (eg tamperers having to change two areas of the booklet rather than one)
- **Centre of Booklet** – advantage of providing a “sandwich” which protects the stitching and protects the Contactless IC from wear and tear as it is “wrapped” within the booklet pages
- **Between end paper and cover** – enables insertion of chips and antennae during assembly, but may have risks of interaction with gold blocking or embossing, or damage through covers being creased, or tampering via splitting cover from endpaper.

States also need to ensure the booklet manufacture process and the personalisation process do not introduce unexpected damage to the chip or to its antennae eg image-perforation security features puncturing the antennae; or heat lamination damaging the chip.

How is the Contactless IC Chip data protected in the passport ?

Equally importantly, the Contactless IC Chip needs to be protected against Logical Tampering. This means protection, encryption and authentication of the data. These concepts are explained in detail in the *PKI Technical Report* and the *LDS Technical Report*.

Data can be protected by various means including:

- Protection of data integrity by use of a cryptographic check sum (enabling detection of whether data has been changed while at the same time facilitating retrieval without any need for decrypting) – a recommended strategy if it is determined that LDS data such as the MRZ and facial images are not to be encrypted – see the *LDS Technical Report* for further clarification
- Protection of data integrity by use of digital watermarking, whereby secret digital bits are dispersively buried into an image without affecting its visual quality – States may choose to use such techniques for their own image verification purposes, but the techniques should not be regarded as globally interoperable because of their proprietary nature
- Protection of data privacy by using cryptographic methods of authentication and data encryption using secret keys (symmetric or asymmetric)
- Providing a public infrastructure for key generation and management ie PKI.

Use of PKI enables States to protect the confidentiality and integrity of the LDS data while severely controlling its availability for use. Using data encryption requires that a common key (the secret key for a symmetric algorithm, or the private key for a public key algorithm) be distributed to all locations where the template will be decrypted. Encryption can inherently provide an integrity check of the data as modification of the text would result in a corrupt decrypted template which would be evident by incorrect header information or incorrect checksums.

Authentication establishes the validity of the document and guards against forgeries or alteration. Public Key Infrastructure can be used to uniquely authenticate the source of the MRTD, to ensure that the electronic data therein has not been altered, and to protect the privacy of the data

Challenge Response protocols can be used to uniquely authenticate the MRTD, to ensure that the data storage technology therein has not been tampered with, and belongs to the MRTD it was originally inserted in.

The other key consideration is maintenance of audit trails. Data in the LDS should not be overwritten – it should be supplemented by retaining original data but appending more current data.

How to indicate in the document that there is a data storage technology in the MRTD ?

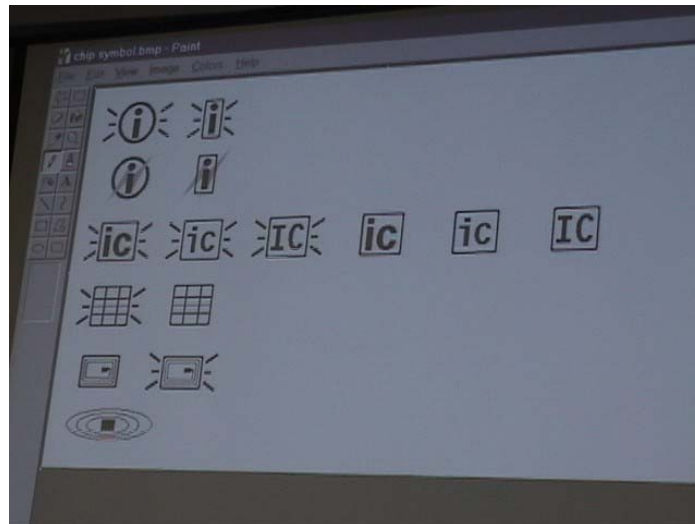
This is a crucial question – if the contactless IC chip is disguised cleverly enough in the passport, how does an inspector know it should or should not be there ?

Suggestions are:

The Visual Zone to have an icon printed on it – this is a very important technique to allow advertising to the traveler to indicate which border control lane they should queue in.

The Cover to have an icon printed on it is also a possibility.

Example icons are:



The Machine Readable Zone to have a standard indicator included in it - for example the letter immediately after the P indicating “Machine Readable Passport” could be denoted as B indicating “**Biometrically Enabled Passport**”.

Travel Document 10 Year Validity Considerations

Given the rapid technological advancements of today's world, States may wish to consider setting the maximum validity of their travel documents to 5 years.

States with 10 year maximum validity could consider phasing in a change to 5 years maximum validity for the following reasons:

- Chip technology is changing at a rapid rate and a shorter validity period enables more rapid takeup on new technology
- Most Chip applications assume a chip/smartcard validity of 2-3 years – how such technology will perform over 5-10 years is yet to be tested in real world applications as the technology typically has not been deployed with consumers for that length of time
- Biometrics technology is changing at a rapid rate, so a shorter validity period enables re-enrolment using more sophisticated technology
- Most countries wish/need to turnover their passport booklet design every 5 years to keep ahead of counterfeiters
- Security printing techniques are undergoing continual improvement, so it is desirable to turnover passport booklets more quickly
- Performance of biometrics can tend to decline over time (eg compare 10 year old photographs vs 5 year old photographs)
- Turnover of passport applicants on a more regular basis allows rechecking of their bona-fides against new available databases eg online breeder document verification may have become available since the applicant originally applied
- Child applications typically already have 5 years validity so such a change would bring adult validity in line with child validity

9. Visas

States may develop visas to include biometric technology, which can be used to verify the identity of persons applying for a visa, or entering the State pursuant to a visa. States are encouraged to undertake checks to confirm the identity of such persons, guard against multiple issue of visas to the same individual in different identities and ensuring that a person has not received a visa under a different name.

Non-citizens of a State enter the State through ports of entry in various ways and means (land, sea, air). From a travellers' perspective, entry and exit typically involve three distinct processes: pre-entry (from which they may be exempt), entry and exit.

The recommended pre-entry process is:

1. Establish a unique, biometric-based identity for a non-citizen seeking entry to the State
2. Use electronic databases and technology to support eligibility processing
3. Record the applicants data record into local (offshore) and central (onshore) database
4. Determine the applicant's eligibility to obtain an MRTD and that they have not previously applied in a different identity
5. If passed all eligibility/adjudication checks, issue the MRTD to the applicant

The outcome of these processes will result in a MRTD visa which is one of:

- Paper visa
- Electronic Visa with Advance Passenger Processing capability

Whether to put a Contactless IC Chip in a visa can be a moot point. Issuing States will typically set up a central database of visa data including the biometric captured at the time of enrolment. However, it is true States may wish to put a data storage technology in the visa as a backup should the central system be unavailable.

States should be aware of the risks (and develop appropriate mitigation) if putting a Contactless IC in a visa, including:

- Interference from the Contactless IC Chip in the host passport
- Interference from Contactless IC Chips in other visas
- Damage from Border Control Officers stamping visa pages

10. Other Interoperable Uses of Biometric-enabled MRTDs

Once a biometric identity verification solution has been implemented in an MRTD, organizations other than Receiving State border control authorities will find additional uses for it.

For example, passport holders may wish to use their passport as proof of identity when opening a bank account, and invite the bank to inspect them against their passport.

Such applications open up the questions of:

- Template Security
- Who owns it
- Ownership
- Protection
- Can a second application use it
- Need to bind primary data to the biometric template

And consequently

- How to segregate data for different applications ?
- How to segregate data, and provide requested services, with respect to privacy principles?

11. Security Requirements

- The biometrics information should be stored in a way to allow electronic authentication by the simplest possible means commensurate with the security requirement for travel documents. This will involve storing a digital certificate/public key on the document, as it would be impractical to manage worldwide certificate revocation lists
- Refer to the *PKI Technical Report* for an explanation of the algorithms for Digital Signatures and how to use them to protect the data in the LDS
- Biometrics information on a travel document will be captured and used by States, airlines and other authorities and it will become available for uses outside border control (eg banks)
- Ability to confirm authenticity of biometric details
- How to implement public keys for various countries
- Issuing State data vs receiving State ability to update some data such as visa details
- Ability to confirm integrity of biometric details
- Protection of “public verification data”
- Protection with respect to integrity, privacy
- Ability to determine if biometric, and specific type of biometric, is present without having to read the entire LDS
- Setting the security status, which allows access to protected functions, valuables, data, if verification result positive
- What to do if security is compromised by an individual travel document holder or, by a member State

12. Technical Reliability

- Biometric systems work by converting the captured image into a *biometric-identifier*, a more compact version of the image that captures just those key features and landmarks of the image that contribute to the distinctiveness of each person's face, eye or fingerprint. This biometric-identifier is then stored in a "token" they carry with them such as a travel document, and usually also in a home enrolment database.
- When a person needs to have their identity verified, another "live" image is taken and processed into a form that allows comparison with the biometric-identifier read from their travel document. In general, people will never present themselves (their biometric) in exactly the same way, and biometric systems need to allow some latitude in this matching process for the system to work.. However, too much latitude could allow impostors to masquerade as another person. The trade-off between rejecting people that fall outside the allowable bounds (*False Reject Rate*) and accepting impostors (*False Accept Rate*) can often be tuned, by varying threshold scores, to make the system easier to use or more secure depending on the application.
- Some people will find difficulty in using the system and the *Failure to Acquire* rate is a key factor in determining whether a particular biometric system can be used.

13. Interim/Transitional Strategies

Many States have recently made major overhauls in the way they personalize passports. Revision to incorporate biometrics is therefore a significant challenge.

Transitioning to support biometrics with an embedded chip is going to present many challenges to States – so it is imperative that NTWG recognize only one (1) data storage device and only one (1) encoding approach. States may wish to undertake complementary activities, but their **goal** must be to move to Contactless IC chip data storage technology.

There are three interim or transitional strategies that Receiving States have been considering prior to universal support of electronic storage of biometric data in LDS format on a Contactless IC chip. These strategies are:

- Use of the Data Page Portrait in lieu of a biometric
- Use of a 2D barcode in lieu of a Contactless IC chip
- Use of database sharing/lookup with the Issuing State.

It must however be remembered that any interim solution risks a danger of being not interim and not effective because:

- Passports that are reliant on the interim solution will be deploying it until they expire, which could be many years hence.
- Receiving States are now unlikely to build necessary infrastructure for interoperability other than via use of Contactless IC Chip.

Data Page Portrait

The Data Page Portrait **is not** an electronic biometric identifier and generally has many inhibitors against its use to create a facial biometric, such as:

- Risk that there has been photo substitution in the data page
- Quality of photograph as printed in the passport via low-quality or low-resolution lasers/inkjets. Some personalisation printing techniques produce inferior data page photo quality to that achieved with scanning of images from the original photograph, or a pasted photograph
- Security features on the passport Data Page may obscure or distort the facial features.

Moreover, the Data Page Portrait does not meet the *New Orleans Resolution* definition of the primary biometric for global interoperability purposes because it is not a “digitally-stored facial image”.

However, States can consider its use, mindful of the caveats:

- While they plan conversion
- During the period while a critical mass of MRPs with electronic encoded biometrics are being issued, to enable a degree of checking in legacy MRTDs which do not have the new data storage technology in them
- As a fallback or backup if the data storage technology device in an MRTD fails
- If they wish to attempt to biometrically verify a passport (or undertake a watch list check) from an Issuing State which does not have an electronic data storage technology in their MRTD.

14. Document 9303

Where might the above best go in Document 9303 ?

- There will be aspects to biometrics that will require changes to Parts 1, 2, 3 and the Common Specifications eg the sections in Part 1 that confirm identity using MRTDs.
- The Supporting Technical Reports all need to be incorporated:
 - The Biometrics Deployment Technical Report
 - The Logical Data Structure Technical Report
 - The PKI Technical Report
 - The Contactless IC Chip Technical Report

Recommendation:

NTWG continue its work on Biometrics Deployment and develop detailed specifications to facilitate the incorporate of biometrics into Document 9303.

15. Summary of Recommendations

- The Berlin and New Orleans Resolutions – ie if a State is putting biometrics in their travel documents, then incorporation of a facial image is mandatory and States may supplement this with fingerprint and/or iris digitally-stored images
- Storage of “optimally-compressed images” as per the standards specified in this Technical Report is mandatory
- Data Storage Technology for globally interoperable biometrics is to be
 - a contactless IC chip
 - with an Operating System as per ISO/IEC Standard 7816-4
 - with high speed of data retrieval eg 50K in < 5 seconds
 - with high data capacity
 - commands SELECT FILE, READ RECORD, and WRITE RECORD should all be supported to enable the most flexibility and selective/fast performance read rates by Receiving States
 - ISO 14443 Type A or Type B compliance (Borders should install Readers which can read A or B formats equally well)
 - read distance range to be 0-10cm (0-3 inches)
 - encrypted as per the *PKI Technical Report*
 - other data storage technologies to be used for local, bilateral or regional biometrics deployment only
- For Passports, positioning of the storage medium is to be one of
 - data page (contiguousness, but if separate then 2 places have to be changed.)
 - centre of booklet advantage of providing a “sandwich” to protect the stitching
 - between rear end paper and rear cover
- Images stored in the LDS be optimally compressed to a minimum storage size per image of :
 - 12K for Face
 - 10K for Fingerprint
 - 30K for Iris
- Images stored in the LDS be either:
 - Not cropped ie identical to the image printed on the Data Page
 - Be cropped to enclose from chin to crown, and face edge-to-edge as a minimum

- For each biometric type stored in the MRTD, storage of the image be mandatory, and storage of an associated template be optional at the discretion of the Issuing State
- Reading MRZ: At inspection it will be sufficient to read the MRZ from the LDS – it does not have to be also read from the Data Page as the two will be identical provided member States have adequately protected them against tampering. As an added security measure, States may choose to read the MRZ from both the Data Page and the LDS and compare them to detect fraud where one has been altered and not the other
- Durability of IC chip and Data Retention Period (lasting 10 years – States may consider moving to 5 year validity period for reasons such as technical flexibility, and technology and security feature turnover)
- Encryption and digital signing be used to protect the data integrity and data privacy (refer to the *LDS Technical Report* and the *PKI Technical Report* for detailed explanation)
- NTWG continue its work on Biometrics Deployment and develop detailed specifications to facilitate the incorporation of biometrics into Document 9303.

16. ANNEXES – [See these corresponding separate documents]

A - Guidelines for Taking Photographs to maximize Facial Recognition Results

{see separate attachment}

B - Facial Image Optimal Storage Size Study – 1

{see separate attachment}

C - Facial Image Optimal Storage Size Study – 2

{see separate attachment}

D - Facial Image Format for Interoperable Data Interchange

{see separate attachment}

E - Iris Image Format for Interoperable Data Interchange

{see separate attachment}

F - Fingerprint Image Format for Interoperable Data Interchange

{see separate attachment}

G - Fingerprint Minutiae Format for Interoperable Data Interchange

{see separate attachment}

H - Fingerprint Pattern Format for Interoperable Data Interchange

{see separate attachment}