ICAO

Doc 9303

Machine Readable Travel Documents

Seventh Edition, 2015

Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

ICAO

Doc 9303

Machine Readable Travel Documents

Seventh Edition, 2015

Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/security/mrtd

Doc 9303, *Machine Readable Travel Documents*
Part 2 — *Specifications for the Security of the Design, Manufacture and Issuance of MRTDs*
ISBN 978-92-9249-791-0

AMENDMENTS

Amendments are announced in the supplements to the *Products and Services Catalogue;* the Catalogue and its supplements are available on the ICAO website at www.icao.int. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by

TABLE OF CONTENTS

Page

1. SCOPE

The Seventh Edition of Doc 9303 represents a restructuring of the ICAO specifications for Machine Readable Travel Documents. Without incorporating substantial modifications to the specifications, in this new edition Doc 9303 has been reformatted into a set of specifications for Size 1 Machine Readable Official Travel Documents (TD1), Size 2 Machine Readable Official Travel Documents (TD2), and Size 3 Machine Readable Travel Documents (TD3), as well as visas. This set of specifications consists of various separate documents in which general (applicable to all MRTDs) as well as MRTD form factor specific specifications are grouped.

This Part provides mandatory and optional specifications for the precautions to be taken by travel document issuing authorities to ensure that their MRTDs, and their means of personalization and issuance to the rightful holders, are secure against fraudulent attack. Mandatory and optional specifications are also provided for the physical security to be provided at the premises where the MRTDs are produced, personalized and issued and for the vetting of personnel involved in these operations.

The worldwide increase in the number of people travelling and the expected continued growth, together with the growth in international crime, terrorism and illegal immigration have led to increasing concerns over the security of travel documents and calls for recommendations on what may be done to help improve their resistance to attack or misuse. Historically, Doc 9303 has not made recommendations on the specific security features to be incorporated in travel documents. Each issuing State has been free to incorporate such safeguards as it deemed appropriate to protect its nationally issued travel documents against counterfeiting, forgery and other forms of attack, as long as nothing was included which would adversely affect their OCR machine readability.

To meet the need of increased document security, ICAO's technical advisors decided it would be desirable to publish a set of "recommended minimum security standards" as a guideline for all States issuing machine readable travel documents. Thus,

- Appendix A to this Part describes security measures to be taken within the structure of the MRTD and of the premises in which it is produced;
- Appendix B describes optional means of achieving machine-assisted document verification;
- Appendix C describes the security measures to be taken to ensure the security of the personalization operations and of the documents in transit.

2. SECURITY OF THE MRTD AND ITS ISSUANCE

The MRTD, and its method of issuance, shall be designed to incorporate safeguards to protect the document against fraudulent attack during its validity period. Methods of fraudulent attack can be classified as follows:

- *Counterfeit* involves the creation of all or part of a document which resembles the genuine MRTD with the intention that it be used as if it were genuine. Counterfeits may be produced by attempting to duplicate or simulate the genuine method of manufacture and the materials used therein or by using copying techniques;
- *Fraudulent alteration, also known as forgery*, involves the alteration of a genuine document in an attempt to enable it to be used for travel by an unauthorized person or to an unauthorized destination. The biographical details of the genuine holder, particularly the portrait, form the prime target for such alteration; and

- *Impostors*. “Impostor” is defined as someone representing himself[1] to be some other person. Security features should be incorporated to facilitate the visual and/or automated detection of fraudulent use of the MRTD by an impostor.

There are established methods of providing security against the above types of fraudulent attack. These involve the use of materials which are not readily available, combined with highly specialized design systems and manufacturing processes requiring special equipment and expertise. Appendix A to this Part lists some of the techniques currently known to be available to provide security to an MRTD enabling an inspecting officer to detect a counterfeit or fraudulently altered document either visually or with the aid of simple equipment such as a magnifying glass or ultraviolet lamp.

All MRTDs that conform to Doc 9303 shall use the specified Basic Security Features listed in Table A-1 of Appendix A.

3. MACHINE ASSISTED DOCUMENT VERIFICATION

A travel document issuing authority may wish to incorporate into its MRTDs one or more security features which require the use of detection equipment to detect and verify their presence within the normal time for immigration clearance. This section provides advice on machine assisted authentication of security features incorporated in MRTDs made in accordance with the specifications set out in Doc 9303. Machine verifiable security features help confirm the authenticity of a genuine document made from genuine materials. Appendix B contains recommendations which cover machine authentication of the security features in the document itself (based on materials, on security printing and on copy protection techniques) as well as advice on reader technologies that apply to machine authentication of documents. Appendix A of this Part and the security standards recommended therein provide the basis for the considerations in this section, utilizing the security features recommended in the Appendix and expanding the capabilities of advanced readers already installed at the borders to accommodate electronic Machine Readable Travel Documents (eMRTDs) and their verification.

The worldwide success of ICAO’s electronic document initiative has led to the issuance of millions of eMRTDs as specified in Doc 9303. These advanced document concepts require the deployment of travel document readers equipped for reading contactless ICs at the points of document authentication, usually the points of entry at one country’s borders. Such advanced readers feature not only the contactless IC reading capability, but also the means for high resolution image acquisition in the visual, infrared and ultraviolet spectral range.

The aim of the recommendations in this chapter is to improve the security of machine readable travel documents worldwide by using machine assisted document authentication procedures completely in line with:

- the layout of machine readable travel documents as specified in Doc 9303 maintaining backward compatibility;

- the security features recommended in Appendix A of this Part; and

- making use of the technical capabilities of advanced readers installed worldwide to accommodate eMRTDs.

However, each State must conduct a risk assessment of the machine assisted document authentication features at its borders to identify their most beneficial aspects and minimize the risks. Doc 9303 does not specify any feature as a means of globally interoperable machine assisted document verification, as the use of a single feature worldwide would

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

make the feature highly vulnerable to fraudulent attack. Therefore, to minimize risk States should apply a variety of security features.

3.1 Feature Types

There are three main categories of machine-verifiable security features. These are described below along with examples of security features that are capable of machine verification.

3.1.1 Structure feature

A structure feature involves the incorporation of a measurable structure into or onto the MRTD data page. It is a security feature containing some form of verifiable information based on the physical construction of the feature. Examples include:

- the interference characteristic of a hologram or other optically variable device that can be uniquely identified by a suitable reader;
- retro-reflective images embedded within a security laminate; and
- controlled transmission of light through selective areas of the substrate.

3.1.2 Substance feature

A substance feature involves the incorporation into the MRTD of a material which would not normally be present and is not obviously present on visual inspection. The presence of the material may be detected by the presence and magnitude of a suitable property of the added substance. It involves the identification of a defined characteristic of a substance used in the construction of the feature. Examples include:

- the use of pigments, usually in inks, which respond in specific and unusual ways to specific wavelengths of light (which may include infrared or ultraviolet light) or have magnetic or electromagnetic properties; and
- the incorporation into a component of the data page of materials, e.g., fibres whose individual size or size distribution conform to a predetermined specification.

3.1.3 Data feature

The visible image of the MRTD data page may contain concealed information which may be detected by a suitable device built into the reader. The concealed information may be in the security printed data page but it is more usually incorporated into the personalization data especially the printed portrait.

Inserting the concealed information into the MRTD data page may involve the application of substance and/or structure features in a way which achieves several levels of security. The term steganography, in this context, describes a special class of data features typically taking the form of digital information which is concealed within an image, usually either the personalization portrait or the background security printing. The information may be decoded by a suitable device built into a full-page reader set to look for the feature in a specific location. The information might, for example, be the travel document number. The reader could then be programmed to compare the travel document number detected from

the feature with the travel document number appearing in the MRZ. Such a comparison involves no access to any data stored in the contactless IC of an eMRTD. Examples of this type of feature are:

- encoded data stored on the document in magnetic media such as special security threads; and
- designs incorporating the concealed data which only become detectable when viewed using a specific wavelength of light, optical filters, or a specific image processing software.

In more complex forms the amount of stored data can be significant, and this can be verified by electronic comparison with data stored in the contactless IC of the eMRTD.

3.2 Basic Principles

All three feature types, namely structure, substance and data, may be incorporated in travel documents and verified using suitably designed readers. Readers are now becoming available that can detect such features and use the responses to confirm the authenticity of the document. Appendix B concentrates on features that can be verified by detection equipment built into the MRTD reader, and used during the normal reading process.

Machine assisted document security verification uses automated inspection technology to assist in verifying the authenticity of a travel document. It should not be used in isolation to determine proof of authenticity, but when used in combination with visible document security features the technology provides the examiner with a powerful new tool to assist in verifying travel documents.

Machine assisted document security verification features are optional security elements that may be included on the MRTD at the discretion of the issuing authority.

The machine verifiable security features may vary in size from less than 1 mm (0.04 in) square up to the whole area of the document. Figure 1 provides guidance on the positions these features should occupy on a MRTD data page to facilitate interoperability. To maintain backward compatibility, it is recommended to deploy machine authentication features within the positions and areas indicated.

3.3 Machine Authentication and eMRTDS

The use of a fully compliant, contactless IC in an eMRTD offers excellent possibilities for machine authentication. However, machine authentication using the contactless IC fails if:

- the contactless IC is defective and fails to communicate; or
- there are no certificates available for checking the authenticity and integrity of the data on the contactless IC.

Therefore an alternative machine authentication is needed. This is especially relevant in automated border control (ABC) scenarios where the machine reader is used instead of a border official to read and validate the eMRTD. This alternative machine authentication establishes trust in the data used for decisions at the border.

A functioning contactless IC in an eMRTD can also aid machine authentication by storing the machine authentication features and its coordinates in the relevant Data Groups (DGs).

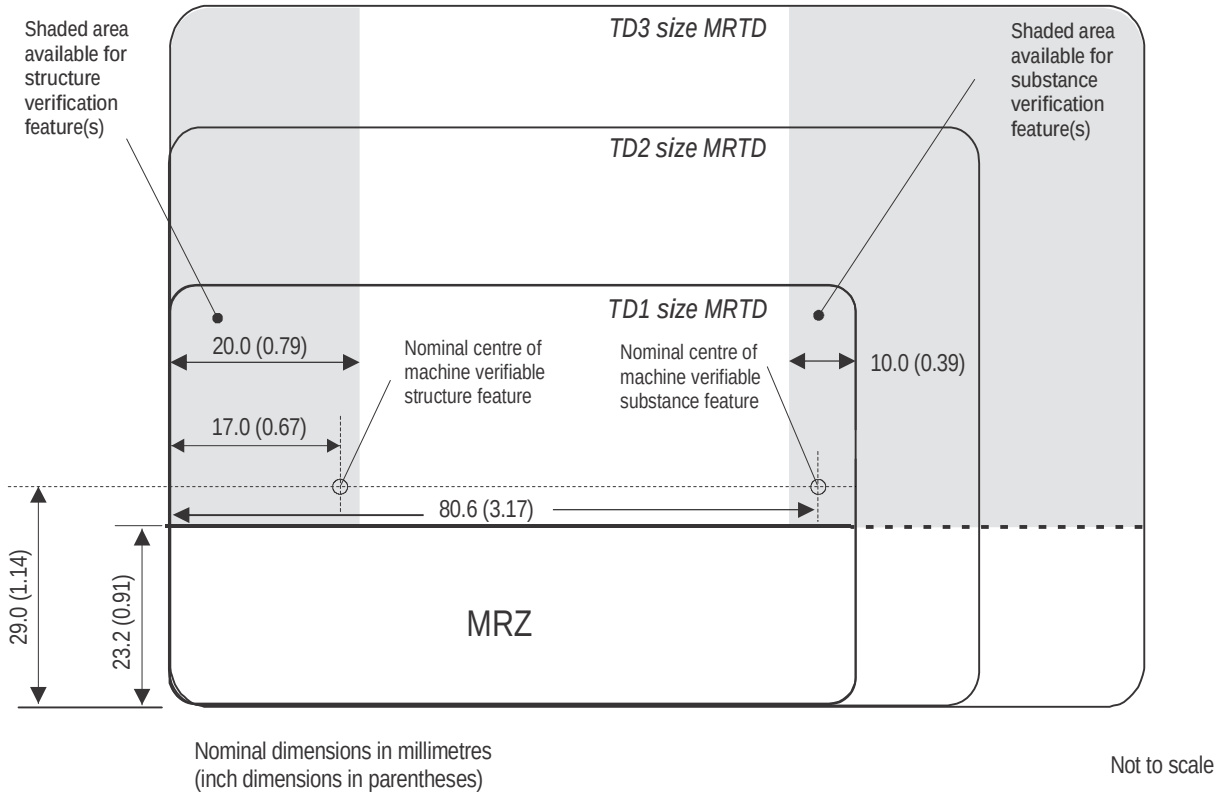

Figure 1. Three sizes of MRTD including the MRP (TD3 size) with recommended positions for machine assisted document verification features. The shaded area on the left is recommended for the incorporation of a structure feature and that on the right for the incorporation of a substance feature.

4. SECURITY OF MRTD PRODUCTION AND ISSUANCE FACILITIES

The State issuing the MRTD shall ensure that the premises in which the MRTD is printed, bound, personalized and issued are appropriately secure and that staff employed therein have an appropriate security clearance. Appropriate security shall also be provided for MRTDs in transit between facilities and from the facility to the MRTD's holder. Appendix C provides recommendations as to how these requirements can be met.

The following factors should be considered in the establishment of production and issuance facilities:

1) resilience;

2) physical security and access control;

3) production materials and MRTD accounting;

4) transport;

5) personnel; and

6) cyber security.

4.1 Resilience

States should take adequate steps to ensure that MRTD production can be maintained in the event of disaster situations such as flood, fire and equipment failure. Some considerations are:

- use of distributed production and issuing facilities;
- secondary production sites when production is centralized;
- emergency issuing facilities;
- rapid access to spare parts and support;
- second sourcing of all MRTD components.

States are recommended to consider possible failure modes in the design of production and issuance facilities, with the objective of eliminating common failures and single-points of failure.

4.2 Physical Security and Access Control

States should control access to production and issuance facilities. Control should be zoned and the requirements for access to each zone should be commensurate with value of the assets being protected.

Some examples of good practice for production facilities are:

- wire cages or solid walls to segregate production areas;
- strong rooms for storage of finished, un-personalized MRTDs and key security components for MRTD production;
- security pass-based access control between zones;
- video surveillance inside and outside the facility;
- perimeter security;
- full-time security personnel.

States should also consider the security that is in place at organizations providing MRTD components to the production facility because theft or sale of such components could make it easier to forge an MRTD.

Issuance facilities should separate back-office areas from public areas, with access control between the two. Staff should be afforded adequate protection, as determined by local circumstance.

4.3 Production Material Accounting

States should ensure that all material used in the production of MRTDs is accounted for and that MRTD production is reconciled with MRTD orders, so that it may be demonstrated that no MRTDs or MRTD components are missing.

Defective materials, MRTDs and MRTD components should be securely destroyed and accounted for.

Generally, reducing the number of issuance and production sites will make material accounting easier. However, this must be balanced against the need to provide resilience and acceptable customer service.

4.4 Transport

States are advised to use secure methods to transport MRTDs and MRTD components; cash-in-transit methods are normally adequate unless particularly high-value assets are being transported (e.g. holographic masters).

States should seek to minimize the amount of material transported in any one batch to reduce the effect of theft. In particular, States should not transport complete sets of printing plates in one operation.

4.5 Personnel

States should ensure that all personnel are subject to a security clearance process, which confirms their identity and suitability for employment in an environment where high-value assets are produced. Staff should be provided with credentials to enable them to identify themselves and to gain access to secure areas which they need to access in connection with their role.

4.6 Cyber Security

Production and issuance facilities are vulnerable to a variety of cyber attacks, such as:

1) viruses and other malware, both in conventional computing facilities and in production machinery;

2) denial-of-service attacks through online MRTD application channels and web services exposed by production and issuance systems;

3) compromise of issuing systems to enable attackers to issue passports or steal personal data or cryptographic assets (such as private keys for eMRTD production).

Countermeasures for these and related attacks are beyond the scope of this document. States should seek advice from their national technical authority.

5. PROVISION OF INFORMATION ON NEWLY ISSUED MRTDS

It is recommended that a State launching a new design of MRTD inform all other States of the details of the new MRTD including evident security features, preferably providing personalized specimens for use as a reference by the receiving State's department which is responsible for verifying the authenticity of such documents. The distribution of such specimens should be made to established contact points agreed by the receiving States.

6. PROVISION OF INFORMATION ON LOST AND STOLEN MRTDS

The exchange of information on lost, stolen or revoked travel documents is a key strategy to strengthen border control and mitigate the impacts of identity theft and immigration fraud. Accordingly, States should consider implementing the following operational procedures to offset the threats that work to undermine border management and national public safety:

1. communicating proactively with document holders;

2. maintaining national databases of lost, stolen and revoked travel documents;

3. sharing information about lost, stolen and revoked travel documents with INTERPOL and verifying documents against INTERPOL databases systematically at primary inspection;

4. installing checks to determine whether a holder is presenting a lost, stolen or revoked document at a border crossing.

6.1 Communicating Proactively with Document Holders

States should ensure that holders of travel documents are fully aware of their responsibilities regarding the use, safe-keeping and reporting procedures for lost or stolen travel documents. Guidelines for safe-keeping travel documents both at home and while travelling may assist in preventing the loss or theft of travel documents. At the time holders receive their documents, holders should be informed of the appropriate actions (including timely reporting) and channels for reporting lost or stolen documents. To assist in this process, States may consider providing travel document holders with multiple channels for securely reporting lost and stolen documents, including in person, telephone, physical mail and various ways of electronic communication including Internet.

States must also take appropriate measures to ensure that holders of travel documents are educated about the potential disruptions, inconveniences and added expenses that can arise when lost, stolen or revoked documents are presented at border control for the purposes of travel. This advice should highlight that once a travel document has been reported lost/stolen it is cancelled and can no longer be used and may be seized by authorities if an attempt is made to use it.

National legislation, or any suitable framework, should be in place to oblige holders of travel documents to report a lost or stolen travel document immediately. No new travel document should be issued until this report has been filed.

6.2 Maintaining National Databases of Lost, Stolen and Revoked Travel Documents

States that use national travel document databases to assist in the verification of the status of their nationally-issued travel documents should take measures to ensure that information is kept up to date. Reports about lost and stolen documents provided by the holders should be recorded into these systems in a timely fashion to ensure that risk assessments conducted using these systems are accurate. States may also wish to consider recording information about lost, stolen or revoked travel documents intercepts in these databases. In addition to updating these databases, States should ensure that border control and police authorities are able to access them easily.

6.3 Sharing Information about Lost, Stolen and Revoked Travel Documents with INTERPOL and Verifying Documents against INTERPOL Databases Systematically at Primary Inspection

States should participate in the global interchange of timely and accurate information concerning the status of travel documents to support in-country policing and border management, as well as efforts to mitigate the impacts of identity theft. Sharing information about lost, stolen and revoked travel documents serves to:

a) improve the integrity of border management;

b) assist in detecting identity theft or immigration fraud at the border, or in other situations where the document is presented as a form of identification;

c) improve the chances of identifying terrorist operatives travelling on false documents;

d) improve the chances of identifying criminal activity, including people smuggling;

e) aid in the recovery of national documents; and

f) limit the value and use of lost, stolen or revoked documents for illegal purposes.

INTERPOL's Automated Search Facility (ASF)/Stolen and Lost Travel Document Database (SLTD) provides States with a means to effectively and efficiently share information about lost, stolen and revoked travel documents in a timely fashion. States should share information about lost and stolen documents that have been issued, as well as blank documents that have been stolen from a production or issuance facility or in transit. Appendix D outlines the factors that must be considered prior to participating in the ASF/SLTD.

States should verify documents against INTERPOL databases systematically at primary inspection to ensure that only travellers holding valid travel documents are crossing border control checkpoints. Verifying the status of travel documents against these databases offers many of the same benefits afforded by sharing information about lost, stolen and revoked documents.

6.4 Installing Checks to Determine Whether a Holder is Presenting a Lost, Stolen or Revoked Document at Border Crossing

States must work within existing national laws and respect international agreements relating to the use of travel documents and border control when processing travellers at their borders. All travellers with reported travel documents (lost, stolen, revoked) shall be treated as if no illegal intention existed, until otherwise proven.

6.4.1 When a travel document gets a "hit" on INTERPOL's lost, stolen or revoked database

A traveller should not be refused entry or prevented exit solely based on the document appearing on the lost, stolen or revoked travel document database. There are many steps that States must take to support these actions. If a traveller is in possession of a travel document that has been recorded as lost, stolen, or revoked on the ASF/SLTD, States should, where possible, liaise with the issuing and reporting country to confirm that the document has been rightfully recorded as a lost, stolen or revoked travel document. States should also conduct an interview with the traveller to ascertain his true identity or nationality, and determine if he is the rightful bearer of the travel document.

If the document contains a chip, States should conduct biometric verifications to support their efforts to determine the true identity of the traveller. States should also make efforts to determine whether the data have been altered and whether the document is authentic.

6.4.2 Processing the rightful owner of the travel document through border control

In dealing with the rightful owners of travel documents, States should be cognizant that those identified as the rightful bearers of a travel document declared lost, stolen or revoked are not necessarily attempting to commit a criminal offense. Rather than focusing on penalizing these individuals, States should focus on identifying ways of removing these documents from circulation, while minimizing disruption to travel. Where permitted under national law, States may consider alternate methods of dealing with these travellers from ways of dealing with those that are intentionally attempting to illegally enter the country by committing identity fraud.

Travellers entering a foreign country on a document declared lost, stolen or revoked as a result of a data error	Border control in the receiving State should contact the issuing authority to confirm the data error. Once confirmed, States may process the document as a valid travel document, but should advise the traveller to contact the issuing authority upon return to his country. Travel document issuing authorities in the issuing State should take all the necessary steps to have this document removed from the lost, stolen and revoked database. States should also consider replacing the affected document at no cost to the holder.
Nationals attempting to leave their country on a document declared lost or stolen	Where exit controls exist, border control should advise these travellers that their documents are not valid for travel, and that they must obtain a valid travel document before embarking on their journey, as lost, stolen and revoked travel documents are considered to be invalid.
Nationals attempting to leave their country on a revoked document	Where exit controls exist, border control should consult with national law enforcement to determine what measures/laws may be invoked to prevent the traveller from leaving the country. If permitted, border management/police authorities should prevent travellers from leaving the State.
Nationals attempting to leave a country and return to their country on a document declared lost, stolen or revoked	Where exit controls are in place and the identity and nationality of the holder have been confirmed, border control may allow the traveller to proceed, but should advise him that the document presented is not valid and that he may be refused boarding by the carrier. When a traveller is re-entering his country of origin on a document declared lost, stolen or revoked, border control may, where permitted by national law and/or international agreement, seize or impound the document to return it to the issuer. If their documents have been seized or impounded, travellers should be advised to obtain new valid travel documents.
Nationals attempting to leave a foreign country and continue to a third country on a document declared lost, stolen or revoked	Where exit controls are in place, border control should advise the travellers that their travel documents are invalid, that they may be refused boarding by the carrier, and that they may face difficulties upon arrival at their next destination.

Travellers entering a foreign country on a document declared lost, stolen or revoked	Travellers who have been permitted to board should be advised by the receiving State to contact their consulate or embassy to obtain a valid travel document before attempting to continue on their journey. Travellers that have not been permitted to enter may be dealt with according to national law.

6.4.3 Processing a traveller after determining that he is not the rightful owner of a document declared lost, stolen or revoked

Once it is determined that a traveller is not the rightful bearer of a document, border/police authorities from the sending or receiving State should seek to determine how the traveller came into possession of the document, including whether there was collusion with the rightful owner, and should domestic law permit, working in cooperation with the issuing State, determine whether additional fraudulent documents have been issued in that identity. If it is determined that the traveller has presented a lost, stolen or revoked travel document, States should investigate the traveller, and where applicable apply criminal charges and/or removal from their State.

States should confiscate documents for the purposes of legal proceedings, including immigration and refugee processing, but should return these to the issuing State once they have served this purpose. Efforts should also be made to provide the issuer with as much information about the interception as possible, should domestic law permit.

States should also ensure that inadmissible persons are documented in accordance with the provisions of ICAO Annex 9 — *Facilitation* to the Convention on International Civil Aviation.

— — — — — — — —

APPENDIX A TO PART II — SECURITY STANDARDS FOR MRTDS (INFORMATIVE)

A.1 SCOPE

This Appendix provides advice on strengthening the security of machine readable travel documents made in accordance with the specifications set out in Doc 9303. The recommendations cover the security of the materials used in the document's construction, the security printing and copy protection techniques to be employed, and the processes used in the production of document blanks. Also addressed are the security considerations that apply to the personalization and the protection of the biographical data in the document. All travel document issuing authorities shall consider this Appendix.

A.2 INTRODUCTION

This Appendix identifies the security threats to which travel documents are frequently exposed and the counter-measures that may be employed to protect these documents and their associated personalization systems. The lists of security features and/or techniques offering protection against these threats have been subdivided into: 1) basic security features and/or techniques considered essential and; 2) additional features and/or techniques from which States are encouraged to select items which are recommended for providing an enhanced level of security.

This approach recognizes that a feature or technique that may be necessary to protect one State's documents may be superfluous or of minor importance to another State using different production systems. A targeted approach that allows States flexibility to choose from different document systems (paper-based documents, plastic cards, etc.) and a combination of security features and/or techniques most appropriate to their particular needs is therefore preferred to a "one size fits all" philosophy. However, to help ensure that a balanced set of security features and/or techniques is chosen, each State must conduct a risk assessment of its national travel documents to identify their most vulnerable aspects and select the additional features and/or techniques that best address these specific problems.

The aim of the recommendations in this Appendix is to improve the security of machine readable travel documents worldwide by establishing a baseline for issuing States. Nothing within these recommendations shall prevent or hinder States from implementing other, more advanced security features, at their discretion, to achieve a standard of security superior to the minimum recommended features and techniques set forth in this Appendix.

A summary table of typical security threats relating to travel documents and some of the security features and techniques that can help to protect against these threats is included.

A.3 BASIC PRINCIPLES

Production and storage of passport books and travel documents, including the personalization processes, should be undertaken in a secure, controlled environment with appropriate security measures in place to protect the premises against unauthorized access. If the personalization process is decentralized, or if personalization is carried out in a location geographically separated from where the travel document blanks are made, appropriate precautions should be taken when transporting the blank documents and any associated security materials to safeguard their security in transit and storage on arrival. When in transit, blank books or other travel documents should contain the unique document

number. In the case of passports the passport number should be on all pages other than the biographical data page where it can be printed during personalization.

There should be full accountability over all the security materials used in the production of good and spoiled travel documents and a full reconciliation at each stage of the production process with records maintained to account for all security material usage. The audit trail should be to a sufficient level of detail to account for every unit of security material used in the production and should be independently audited by persons who are not directly involved in the production. Records certified at a level of supervision to ensure accountability should be kept of the destruction of all security waste material and spoiled documents.

Materials used in the production of travel documents should be of controlled varieties, where applicable, and obtained only from reputable security materials suppliers. Materials whose use is restricted to high security applications should be used, and materials that are available to the public on the open market should be avoided.

Sole dependence upon the use of publicly available graphics design software packages for originating the security backgrounds should be avoided. These software packages may however be used in conjunction with specialist security design software.

Security features and/or techniques should be included in travel documents to protect against unauthorized reproduction, alteration and other forms of tampering, including the removal and substitution of pages in the passport book, especially the biographical data page. In addition to those features included to protect blank documents from counterfeiting and forgery, special attention must be given to protect the biographical data from removal or alteration. A travel document should include adequate security features and/or techniques to make evident any attempt to tamper with it.

The combination of security features, materials and techniques should be well chosen to ensure full compatibility and protection for the lifetime of the document.

Although this Appendix deals mainly with security features that help to protect travel documents from counterfeiting and fraudulent alteration, there is another class of security features (Level 3 features) comprised of covert (secret) features designed to be authenticated either by forensic examination or by specialist verification equipment. It is evident that knowledge of the precise substance and structure of such features should be restricted to very few people on a “need to know” basis. Among others, one purpose of these features is to enable authentication of documents where unequivocal proof of authenticity is a requirement (e.g., in a court of law). All travel documents should contain at least one covert security feature as a basic feature.

Important general standards and recommended practices for passport document validity period, one-person-one-passport principle, deadlines for issuance of Machine Readable Passports and withdrawal from circulation of non-MRPs and other guidance is found in ICAO Annex 9 — *Facilitation*.

There is no other acceptable means of data storage for global interoperability other than a contactless IC, specified by ICAO as the capacity expansion technology for use with MRTDs.

A.4 MAIN THREATS TO THE SECURITY OF TRAVEL DOCUMENTS

The following threats to document security, listed in no particular order of importance, are identified ways in which the document, its issuance and use may be fraudulently attacked:

- counterfeiting a complete travel document;
- photo substitution;

- deletion/alteration of data in the visual or machine readable zone of the MRP data page;
- construction of a fraudulent document, or parts thereof, using materials from legitimate documents;
- removal and substitution of entire page(s) or visas;
- deletion of entries on visa pages and the observations page;
- theft of genuine document blanks;
- impostors (assumed identity; altered appearance); and
- tampering with the contactless IC (where present) either physically or electronically.

Detection of security features can be at any or all of the following three levels of inspection:

- Level 1 – Cursory examination for rapid inspection at the point of usage (easily identifiable visual or tactile features);
- Level 2 – Examination by trained inspectors with simple equipment; and
- Level 3 – Inspection by forensic specialists.

To maintain document security and integrity, periodic reviews and any resulting revisions of document design should be conducted. This will enable new document security measures to be incorporated and to certify the document's ability to resist compromise and document fraud attempts regarding:

- photo substitution;
- delamination or other effects of deconstruction;
- reverse engineering of the contactless IC as well as other components;
- modification of any data element;
- erasure or modification of other information;
- duplication, reproduction or facsimile creation;
- effectiveness of security features at all three levels: cursory examination, trained examiners with simple equipment and inspection by forensic specialists; and
- confidence and ease of second level authentication.

To provide protection against these threats and others, a travel document requires a range of security features and techniques combined in an optimum way within the document. Although some features can offer protection against more than one type of threat, no single feature can offer protection against them all. Likewise, no security feature is 100 per cent effective in eliminating any one category of threat. The best protection is obtained from a balanced set of features and techniques providing multiple integrated layers of security in the document that combine to deter or defeat fraudulent attack.

A.5 SECURITY FEATURES AND TECHNIQUES

In the sections that follow, security features, techniques and other security measures are categorized according to the phases passed through during the production and personalization processes and the components of the travel document created thereby with regard to:

1) substrate materials;

2) security design and printing;

3) protection against copying, counterfeiting or fraudulent alteration; and

4) personalization techniques.

Issuing States are recommended to incorporate all of the basic features/measures and to select a number of additional features/measures from the list having first completed a full risk assessment of their travel documents. Unless otherwise indicated, the security features may be assumed to apply to all parts of a travel document including the cover and the binding of the booklet and to all the interior pages of a passport, comprising the biographical data page, end leaves and visa pages. Care must be taken to ensure that features do not interfere with the machine readability of the travel document.

A.5.1 Substrate Materials

A.5.1.1 Paper forming the pages of a travel document

Basic features:

- UV dull paper, or a substrate with a controlled response to UV, such that when illuminated by UV light it exhibits a fluorescence distinguishable in colour from the blue-white luminescence used in commonly available materials containing optical brighteners;
- watermark comprising two or more grey levels in the biographical data page and visa pages;
- appropriate chemical sensitizers in the paper, at least for the biographical data page (if compatible with the personalization technique); and
- paper with appropriate absorbency, roughness and weak surface tear.

Additional features:

- watermark in register with printed design;
- a different watermark on the data page to that used on the visa pages to prevent page substitution;
- a cylinder mould watermark;
- invisible fluorescent fibres;
- visible (fluorescent) fibres;

- security thread (embedded or window) containing additional security features such as micro print and fluorescence;
- a taggant designed for detection by special equipment; and
- a laser-perforated security feature.

A.5.1.2 Paper or other substrate in the form of a label used as the biographical data page of a travel document

Basic features:

- UV dull paper, or a substrate with a controlled response to UV, such that when illuminated by UV light it exhibits a fluorescence distinguishable in colour from the blue-white luminescence used in commonly available materials containing optical brighteners;
- appropriate chemical sensitizers in the paper (not normally possible in a plastic label substrate);
- invisible fluorescent fibres;
- visible (fluorescent) fibres; and
- a system of adhesives and/or other characteristics that prevents the label from being removed without causing clearly visible damage to the label and to any laminates or overlays used in conjunction with it.

Additional features:

- security thread (embedded or window) containing additional security features such as micro print and fluorescence;
- a watermark can be used in the paper of a data page in paper label form;
- a laser-perforated security feature; and
- die cut security pattern within the label to create tamper evidence.

A.5.1.3 Security aspects of paper forming the inside cover of a passport book

Paper used to form the inside cover of a passport book need not have a watermark. Although definitely not recommended, if an inside cover is used as a biographical data page (see A.5.5.1), alternative measures must be employed to achieve an equivalent level of security against all types of attack as provided by locating the data page on an inside page.

The paper forming the inside cover should contain appropriate chemical sensitizers when an inside cover is used as a biographical data page. The chemically sensitized paper should be compatible with the personalization technique and the adhesive used to adhere the end paper to the cover material of the passport.

A.5.1.4 Synthetic substrates

Where the substrate used for the biographical data page (or inserted label) of a passport book or MRTD card is formed entirely of plastic or a variation of plastic, it is not usually possible to incorporate many of the security components described in 5.1.1 through 5.1.3. In such cases additional security properties shall be included, including additional security printed features, enhanced personalization techniques and the use of optically variable features over and above the recommendations contained in 5.2 to 5.5.2. States should preferably ensure that the plastic substrate is manufactured under controlled conditions and contains distinctive properties, e.g. controlled fluorescence, to differentiate it from standard financial card substrates.

Basic features:

- construction of the data page should be resistant to physical splitting into layers;
- UV dull substrate with a controlled response to UV, such that when illuminated by UV light it exhibits a fluorescence distinguishable in colour from the blue-white luminescence used in commonly available materials containing optical brighteners;
- appropriate measures should be used to incorporate the data page securely and durably into the machine readable travel document; and
- optically variable feature.

Additional features:

- windowed or transparent feature;
- tactile feature; and
- laser-perforated feature.

A.5.2 Security Printing

A.5.2.1 Background and text printing

Basic features (see Glossary of Terms *in Doc 9303-1):*

- two-colour guilloche security background design pattern[1];
- rainbow printing;
- microprinted text; and

1. Where the guilloche pattern has been computer-generated, the image reproduced on the document must be such that no evidence of a pixel structure shall be detectable. Guilloches may be displayed as positive images, where the image lines appear printed with white spaces between them, or as negative images, where the image lines appear in white, with the spaces between them printed. A two-colour guilloche is a design that incorporates guilloche patterns created by superimposing two elements of the guilloche, reproduced in contrasting colours.

- security background of the biographical data page printed in a design that is different from that of the visa pages or other pages of the document.

Additional features:

- single or multi-colour intaglio printing comprising a “black-line white-line” design on one or more of the end leaves or visa pages;
- latent (intaglio) image;
- anti-scan pattern;
- duplex security pattern;
- relief (3D) design feature;
- front-to-back (see-through) register feature;
- deliberate error (e.g. spelling);
- every visa page printed with a different security background design;
- tactile feature; and
- unique font(s).

A.5.2.2 Inks

Basic features:

- UV fluorescent ink (visible or invisible) on the biographical data page and all visa pages; and
- reactive ink, where the substrate of the document pages or of a label is paper, at least for the biographical data page (if compatible with the personalization technique).

Additional features:

- ink with optically variable properties;
- metallic ink;
- penetrating numbering ink;
- metameric ink;
- infrared drop-out ink;
- infrared absorbent ink;
- phosphorescent ink;

- tagged ink; and
- invisible ink which fluoresces in different colours when exposed to different wave lengths.

A.5.2.3 Numbering

It is strongly recommended that the unique document number be used as the passport number.

Basic features:

- the passport number should appear on all sheets of the document and on the biographical data page of the document;
- the number in a document shall be either printed and/or perforated;
- the document number on a label shall be in a special style of figures or typeface and be printed with ink that fluoresces under ultraviolet light in addition to having a visible colour;
- the number on a data page of a passport made of synthetic substrate or on an MRTD card can be incorporated using the same technique as is used for applying the biographical data in the personalization process; and
- for MRTD cards, the number should appear on both sides.

Additional features:

- if perforated, it is preferable that laser perforation be used. Perforate numbering of the data page is optional but, if used, care should be taken not to interfere with the clarity of the portrait or VIZ and not obstruct the MRZ in any way. It is desirable to perforate the cover of the passport; and
- if printed, it should ideally be in a special style of figures or typeface and be printed with an ink that fluoresces under ultraviolet light in addition to having a visible colour.

A.5.2.4 Special security measures for use with non-laminated biographical data pages

The surface of the data page should be protected against soiling in normal use including regular machine reading of the MRZ, and against tampering.

If a page of a document is used for biographical data that is not protected by a laminate or an overlay as a protective coating (see 5.3.2, 5.4.3 and 5.4.4), additional protection shall be provided by the use of intaglio printing incorporating a latent image and microprinting and preferably utilizing a colour-shifting ink (e.g. ink with optically variable properties).

A.5.2.5 Special security measures for use with cards and biographical data pages made of plastic

Where a travel document is constructed entirely of plastic, optically variable security features shall be employed which give a changing appearance with angle of viewing. Such devices may take the form of latent images, lenticular features, colour-shifting ink, or diffractive optically variable image features.

A.5.3 Protection Against Copying

A.5.3.1 Need for anti-copy protection

The current state of development of generally available digital reproduction techniques and the resulting potential for fraud mean that high-grade security features in the form of optically variable features or other equivalent devices will be required as safeguards against copying and scanning. Emphasis should be placed on the security of the biographical data page of a passport book, travel card or visa, based on an independent, complex optically variable feature technology or other equivalent devices complementing other security techniques. Particular emphasis should be given to easily identifiable, visual or tactile features which are examined at Level 1 inspection.

Appropriate integration of optically variable feature components or other equivalent devices into the layered structure of the biographical data page should also protect the data from fraudulent alteration. The optically variable components and all associated security materials used to create the layered structure must also be protected against counterfeiting.

A.5.3.2 Anti-copy protection methods

Subject to the minimum recommendations described in 5.4.3 and 5.4.4 on the need for lamination, optically variable features should be used on the biographical data page of a passport book, travel card or visa as a *basic feature*.

When a biographical data page of a passport book, travel card or visa is protected by a laminate film or overlay, an optically variable feature (preferably based on diffractive structure with tamper-evident properties) should be integrated into the page. Such a feature should not affect the legibility of the entered data.

When the biographical data page is an encapsulated paper label, or a page in a passport, the biographical data must be suitably protected by a protective laminate or measures providing equivalent security in order to deter alteration and/or removal.

When the machine readable biographical data page of a passport book is made entirely of synthetic substrate, an optically variable feature should be incorporated. The inclusion of a diffractive optically variable feature is recommended to achieve an enhanced level of protection against reproduction.

Devices such as a windowed or transparent feature, a laser-perforated feature, and others considered to offer equivalent protection may be used in place of an optically variable feature.

When the travel document has no overlay or laminate protection, an optically variable feature (preferably based on diffractive structure) with intaglio overprinting or other printing technique shall be used.

A.5.4 Personalization Technique

A.5.4.1 Document personalization

This is the process by which the portrait, signature and/or other biographical data relating to the holder of the document are applied to the travel document. These data record the personalized details of the holder and are at the greatest risk of counterfeit or fraudulent alteration. One of the most frequent types of document fraud involves the removal of the portrait image from a stolen or illegally obtained travel document and its replacement with the portrait of a different person. Documents with stick-in portrait photographs are particularly susceptible to photo substitution. Therefore, stick-in photographs are NOT permitted in MRTDs.

A.5.4.2 Protection against alteration

To ensure that data are properly secured against attempts at forgery or fraudulent alteration it is very strongly recommended to integrate the biographical data, including the portrait, signature (if it is included on the biographical data page) and main issue data, into the basic material of the document. A variety of technologies are available for personalizing the document in this way, including the following, but not precluding the development of new technologies, which are listed in no particular order of importance:

- laser toner printing;
- thermal transfer printing;
- ink-jet printing;
- photographic processes; and
- laser engraving.

The same personalizing technologies may also be used to apply data to the observations page of the passport. Laser toner should not be used to personalize visas or other security documents that are not protected by a secure laminate.

Authorities should carry out testing of their personalization processes and techniques against malfeasance.

A.5.4.3 Choice of document system

The choice of a particular technology is a matter for individual issuing States and will depend upon a number of factors, such as the volume of travel documents to be produced, the construction of the document and whether it is to be personalized during the document or passport book making process or after the document or book has been assembled and whether a country issues passports centrally or from decentralized sites.

Whichever method is chosen, it is essential that precautions be taken to protect the personalized details against tampering. This is important because, even though eliminating the stick-in portrait reduces the risk of photo substitution, the unprotected biographical data remains vulnerable to alteration and needs to be protected by the application of a heat-sealed (or equivalent) laminate with frangible properties, or equivalent technology that provides evidence of tampering.

A.5.4.4 Protection against photo substitution and alteration of data on the biographical data page of a passport book

Basic features:

- personalizing the portrait and all biographical data by integration into the basic material;
- the security printed background (e.g. guilloche) shall merge within the portrait area;
- use of reactive ink and chemical sensitizers in the paper;
- a visible security device should overlap the portrait without obstructing the visibility of the portrait; an optically variable feature is recommended; and

- use of a heat-sealed (or equivalent) secure laminate, or the combination of an personalizing technology and substrate material that provide an equivalent resistance to substitution and/or counterfeit of the portrait and other biographical data.

Additional features:

- displayed signature of the holder may be scanned and incorporated into the printing;
- steganographic image incorporated in the document;
- additional portrait image(s) of holder;
- machine-verifiable features as detailed in Doc 9303, Parts 9 through 12.

A.5.5 Additional Security Measures for Passport Books

A.5.5.1 Position of the biographical data page

It is recommended that States place the data page on an inside page (the second or penultimate page). When the data page is situated on the inside cover of an MRP, the normal method of construction used in the manufacture of passport covers has facilitated fraudulent attacks on the data page, typically photo substitution or whole-page substitution. However, an issuing State may place the data page on a cover provided that it ensures that the construction of the cover used in its passport offers a similar level of security against all types of fraudulent attack to that offered by locating the data page on an inside page. Placing the biographical data page on the cover is, nevertheless, strongly NOT recommended.

A.5.5.2 Whole-page substitution

Issuing States' attention is drawn to the fact that with integrated biographical data pages replacing stick-in photographs in passports, some cases of whole-page substitution have been noted in which the entire biographical data page of the passport has been removed and substituted with a fraudulent one. Although whole-page substitution is generally more difficult to effect than photo substitution of a stick-in photo, it is nevertheless important that the following recommendations be adopted to help in combating this category of risk. As with all other categories of document fraud, it is better to employ a combination of security features to protect against whole-page substitution rather than rely on a single feature which, if compromised, could undermine the security of the whole travel document.

Basic features:

- the sewing technology that binds the pages into the book must be such that it must be difficult to remove a page without leaving clear evidence that it has happened;
- security background of the biographical data page printed in a design that is different from that of the visa pages;
- page numbers integrated into the security design of the visa pages; and
- serial number on every sheet, preferably perforated.

Additional features:

- multi-colour and/or specifically UV fluorescent sewing thread;
- programmable thread-sewing pattern;
- UV cured glue applied to the stitching;
- index or collation marks printed on the edge of every visa page;
- laser-perforated security features to the biographical data page; and
- biographical data printed on an inside page in addition to the data page.

Where self-adhesive labels are used, additional security requirements as described in A.5.1.2 and A.5.2.4 are advised including linking the label to the machine readable travel document by the travel document number.

A.5.6 Quality Control

Quality checks and controls at all stages of the production process and from one batch to the next are essential to maintain consistency in the finished travel document. This should include quality assurance (QA) checks on all materials used in the manufacture of the documents and the readability of the machine readable lines. The importance of consistency in the finished travel document is paramount because immigration inspectors and border control officers rely upon being able to recognize fake documents from variations in their appearance or characteristics. If there are variations in the quality, appearance or characteristics of a State's genuine travel documents, detection of counterfeit or forged documents is made more difficult.

A.5.7 Security Control of Production and Product

A major threat to the security of the MRP of an issuing State can come from the unauthorized removal from the production facility of genuine finished, but unpersonalized, MRPs or the components from which MRPs can be made.

A.5.7.1 Protection against theft and abuse of genuine document blanks or document components

Blank documents should be stored in locked and appropriately supervised premises. The following measures should be adopted:

Basic measures:

- good physical security of the premises with controlled access to delivery/shipment and production areas, and document storage facilities;
- full audit trail, with counting and reconciliation of all materials (used, unused, defective or spoiled) and certified records of same;
- all document blanks and other security-sensitive components serially numbered with full audit trail for every document from manufacture to dispatch, as applicable;

- where applicable, tracking and control numbers of other principal document components (e.g. rolls or sheets of laminates, optically variable feature devices);
- secure transport vehicles for movement of blank documents and other principal document components (if applicable);
- details of all lost and stolen travel document blanks to be rapidly circulated between governments and to border control authorities with details sent to the INTERPOL lost and stolen database;
- appropriate controls to be in place to protect the production procedures from internal fraud; and
- security vetting of staff.

Additional measures:

- CCTV coverage/recording of all production areas, where permitted; and
- centralized storage and personalization of blank documents in as few locations as possible.

Table A-1. Summary of security recommendations

Elements	*Basic features*	*Additional features*
Substrate materials (A.5.1)		
Paper substrates (A.5.1.1)	– controlled UV response – two-tone watermark – chemical sensitizers – appropriate absorbency and surface characteristics	– registered watermark – different watermark on the data page and visa page – cylinder mould watermark – invisible fluorescent fibres – visible (fluorescent) fibres – security thread – taggant – laser-perforated security feature
Paper or other substrate in the form of a label (A.5.1.2)	– controlled UV response – chemical sensitizers – invisible florescent fibres – visible (florescent) fibres – system of adhesives	– security thread – watermark – laser-perforated security feature – die cut security pattern
Synthetic substrates (A.5.1.4)	– construction resistant to splitting – optically dull material – secure incorporation of data page – optically variable features – see 5.2 – 5.5, as appropriate	– window or transparent feature – tactile feature – laser-perforated feature

Elements	*Basic features*	*Additional features*
Security printing (A.5.2)		
Background and text printing (A.5.2.1)	– two-colour guilloche background – rainbow printing – microprinted text – unique data page design	– intaglio printing – latent image – anti-scan pattern – duplex security pattern – relief design feature – front-to-back register feature – deliberate error – unique design on every page – tactile feature – unique font(s)
Inks (A.5.2.2)	– UV florescent ink – reactive ink	– ink with optically variable properties – metallic ink – penetrating numbering ink – metameric ink – infrared drop-out ink – infrared absorbent ink – phosphorescent ink – tagged ink – invisible ink
Numbering (A.5.2.3)	– numbering on all sheets – printed and/or perforated number – special typeface numbering for labels – identical technique for applying numbering and biographical data on synthetic substrates and cards	– laser-perforated document number – special typeface
Personalization technique (A.5.4)		
Protection against photo substitution and alteration (A.5.4.4)	– integrated biographical data – security background merged within portrait area – reactive inks and chemical sensitizers in paper – visible security device overlapping portrait area – heat-sealed secure laminate or equivalent	– displayed signature – steganographic image – additional portrait image(s) – biometric feature as per Part 9

Elements	*Basic features*	*Additional features*
Additional security measures for passport books (A.5.5)		
Page substitution (A.5.5.2)	– secure sewing technology – UV fluorescent sewing thread – unique data page design – page numbers integrated into security design – serial number on every sheet	– multi-colour sewing thread – programmable sewing pattern – UV cured glue to stitching – index marks on every page – laser-perforated security feature – biographical data on inside page
Security control of production and product (A.5.7)		
Protection against theft and abuse (A.5.7.1)	– good physical security – full audit trail – serial numbers on blank documents, as applicable – tracking and control numbers of components, as applicable – secure transport of blank documents – international information exchange on lost and stolen documents – internal fraud protection procedures – security vetting of staff	– CCTV in production areas – centralized storage and personalization

Note 1.— The list of additional features is not exhaustive, and issuing States and organizations are encouraged to adopt other security features not explicitly mentioned in this Appendix.

Note 2.— The descriptions in the table above are necessarily abbreviated from the main text. For ease of reference, the relevant sections of this Appendix are referenced by the paragraph numbers in parentheses in the "Elements" column of the above table.

Note 3.— Certain of the features are repeated one or more times in the table. This indicates that the particular feature protects against more than one type of threat. It is only necessary to include these features once within any particular document.

Note 4.— There are many other factors associated with passport security than are elaborated here. Appendices B and C provide additional guidance. Therefore, Appendices A, B and C need to be considered collectively to ensure document issuance integrity.

Note 5.— Any reference, direct or implied, to specific terms and/or technologies are solely intended to capture the terms and technologies in their generic form and do not have any association with specific vendors or technology providers.

— — — — — — — —

APPENDIX B TO PART II — MACHINE ASSISTED DOCUMENT SECURITY VERIFICATION (INFORMATIVE)

B.1 SCOPE

This Appendix contains recommendations which cover machine authentication of the security features in the document itself (based on materials, on security printing and on copy protection techniques) as well as advice on reader technologies that apply to machine authentication of documents.

B.2 DOCUMENT READERS AND SYSTEMS FOR MACHINE AUTHENTICATION

In order to verify traditional as well as innovative security features of MRTDs, it is important to have reading technology in place which accommodates the wide variety of travel documents in circulation. These readers have to be equipped with the appropriate sensors for the more common and advanced machine authentication features. This, of course, is a worldwide cost and infrastructure issue.

B.2.1 Standard Readers

Standard readers which are deployed at borders usually have the following hardware sensors:

- VIS, UV, IR illumination and high resolution image grabbing capabilities (minimum resolution 300 dpi) – this allows for reading the MRZ (preferably in the IR spectral range) and image processing of other features (in the VIS spectral range); and
- ISO 14443 compliant contactless IC readers (@ 13.56 MHz frequency).

Generally, standard readers are able to detect and verify the following security features:

- MRZ read and check digit verification;
- Contactless IC read and Passive Authentication (and, optionally, Active Authentication); and
- generic security checks (UV dull paper, IR readable MRZ, …).

Further “intelligence” of these readers solely depends on software, not on extra hardware sensors, and would therefore easily be deployed at the discretion of the receiving State without investing extra money for dedicated equipment. Software capabilities of readers may include:

- pattern recognition using databases (based on VIS, UV and IR images);
- read and authenticate digital watermarks (steganographic features) to check for authentic issuance;

- detect and read out (alphanumeric) displays and their future security features; and
- detect and read out LED-in-plastic based security features.

B.2.2 Advanced Readers

Additionally, advanced readers may have the following hardware sensors, suited to authenticate special security features:

- coaxial illumination for the verification of retro-reflective security overlays;
- laser diode or LED illumination for the verification of special structure features, e.g. for optically diffractive devices (DOVIDs);
- magnetic sensors for special substrate features, e.g. for the verification of magnetic fibres;
- spectral analysis or polarization detection devices; and
- transmission illumination of the MRP data page for the verification of registered watermarks, laser perforation, window-features and see-through registers – needs a special reader geometry to allow for the placement of the data page only (no cover behind) on the reader.

Usually, advanced reading capabilities are all based on national/bilateral/multilateral/proprietary agreements and require dedicated hardware.

B.2.3 Background Systems, Public Key Infrastructure (PKI)

To authenticate certain types of machine verifiable features, a background system or a PKI may be necessary. This could be the existing MRTD PKI (the ICAO PKD being the most prominent part) where States may exchange information on their security features within the logical data structure, secured by means of certificates.

B.3 SECURITY FEATURES AND THEIR APPLICATION FOR MACHINE AUTHENTICATION

The following paragraphs describe major security features and techniques as identified in Appendix A on Security Standards and explain how machine authentication could be deployed for these security mechanisms. Issuing Authorities which select security features from Appendix A may use the tables below to check which possibilities of machine authentication exist for such features.

B.3.1 Substrate Materials

B.3.1.1 Paper forming the pages of a travel document

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Basic features							
Controlled UV response		X					UV intensity
Two-tone watermark					Transmission	F	pattern matching
Chemical sensitizers							N/A
Appropriate absorbency and surface characteristics							N/A
Additional features							
Registered watermark					Transmission	F	pattern matching
Different watermark on the data page and visa page					Transmission	F	pattern matching*
Cylinder mould watermark					Transmission	F	pattern matching
Invisible fluorescent fibres		X	X			F/V	pattern matching
Visible (fluorescent) fibres	X	X				F/V	pattern matching
Security thread	X	X			Transmission, Magnetic	F	pattern matching
Taggant					Special	F/V	Depends on taggant
Laser-perforated security feature					Transmission	F/V	pattern matching

* User interaction required and not suitable for Automated Border Control systems

B.3.1.2 Paper or other substrate in the form of a label

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Basic features							
Controlled UV response		X					UV intensity
Chemical sensitizers							N/A
Invisible fluorescent fibres		X	X			F/V	pattern matching
Visible (fluorescent) fibres	X	X				F/V	pattern matching
System of adhesives							N/A
Additional features							
Security thread	X				Transmission, Magnetic	F	pattern matching
Watermark					Transmission	F	N/A
Laser-perforated security feature					Transmission	F/V	pattern matching
Die cut security pattern					Transmission	F	pattern matching

B.3.1.3 Synthetic substrates

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Basic features							
Construction resistant to splitting							N/A
Optically dull material		X					UV intensity
Secure incorporation of data page							N/A
Optically variable features							See 5.3

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
See 5.2 – 5.5, as appropriate							
Additional features							
Window or transparent feature					Transmission	F	pattern matching
Tactile feature					Retro-reflective	F/V	pattern matching
Laser-perforated feature					Transmission	F/V	pattern matching
Surface characteristics	X		X		Retro-reflective	F	pattern matching

B.3.2 Security Printing

B.3.2.1 Background and text printing

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Basic features							
Two-colour guilloche background	X	X	X			F	Pattern matching
Rainbow printing	X	X			High res camera	F	Pattern matching
Microprinted text	X	X	X		High res camera	F	Pattern matching
Unique data page design	X					F	Pattern matching
Additional features							
Intaglio printing	X	X	X			F	Pattern matching*
Latent image							N/A
Anti-scan pattern	X				High res camera	F	Pattern matching
Duplex security pattern					Transmission	F	Pattern matching*
Relief design feature					Retro-reflective	F	pattern matching

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Front-to-back register feature					Transmission	F	Pattern matching
Deliberate error	X	X	X			F	OCR, Pattern matching
Unique design on every page	X	X				F	Pattern matching[#]
Tactile feature					Retro-reflective	F	pattern matching
Unique font(s)	X	X	X				Pattern matching

* Impractical implementation for passport readers
[#] User interaction required and not suitable for Automated Border Control systems

B.3.2.2 Inks

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
UV florescent ink		X				F/V	Pattern matching
Reactive inks					Special		Depending on ink
Additional features							
Ink with optically variable properties	X				Variable illumination	F/V	Pattern matching
Metallic ink			X			F/V	Pattern matching
Penetrating numbering ink					Special	V	Pattern matching on both sides
Metameric inks	X	X	X			F	Optical filters and Pattern matching
Infrared dropout ink	X		X			F/V	Pattern matching
Infrared absorbent ink			X			F/V	Pattern matching
Phosphorescent ink		X	X			F/V	Pattern matching

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Tagged ink					Special	F	Pattern matching
Invisible ink		X	X			F	Pattern matching
Magnetic ink					Magnetic	F/V	Pattern matching
Anti-Stokes-Ink			X			F/V	Optical filters and pattern matching

B.3.2.3 Numbering

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Basic features							
Numbering on all sheets Printed and/or perforated number	X		X			F/V	OCR, Pattern matching
Special typeface numbering for labels	X		X			F/V	OCR, Pattern matching
Identical technique for applying numbering and biographical data on synthetic substrates and cards							N/A
Additional features							
Laser-perforated document number					Transmission	F/V	Pattern matching
Special typefonts	X					F/V	OCR, Pattern matching

B.3.3 Protection Against Copying

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
Optically variable features on the biographical data page	X				Variable illumination	F/V	Pattern matching
OVD with intaglio overprint if no laminate							N/A
Additional features							
Machine readable diffractive optically variable feature					Laser	F/V	decoding
Laser-perforated security feature					Transmission	F/V	Pattern matching
Anti-scan pattern	X				High res camera	F	Pattern matching

B.3.4 Personalization Techniques

B 3.4.1 Protection against photo substitution and alteration

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
Integrated biographical data							N/A
Security background merged within portrait area							N/A
Reactive inks and chemical sensitizers in paper							N/A
Visible security device overlapping portrait area	X				Variable illumination	F/V	Pattern matching
Heat-sealed secure laminate or equivalent	X					F/V	Pattern matching

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Additional features							
Displayed signature							N/A
Steganographic feature	X	X	X			F/V	Decoding
Additional portrait image(s)	X	X	X	X		V	Pattern matching
Biometric feature as per Part 9				X		V	RF reader

B 3.5 Additional Security Measures for Passport Books

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Basic features							
Secure sewing technology							N/A
UV fluorescent sewing thread		X				F	Pattern matching
Unique data page design	X					F	Pattern matching
Page numbers integrated into security design	X	X			High res camera		Pattern matching
Serial number on every sheet							N/A
Additional features							
Multi-colour sewing thread	X	X				F	Pattern matching
Programmable sewing pattern	X	X				F	Pattern matching
UV cured glue to stitching							N/A
Index marks on every page							N/A
Laser-perforated security feature					Transmission	F/V	Pattern matching
Biographical data on inside page							N/A

B 3.6 Additional Security Measures Suited for Machine Authentication

The following security features are suited for machine authentication but are not listed in Appendix A.

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Basic features							
MRZ read and check digit verification	X		X			F/V	Checksum calculation
Contactless IC read and Passive Authentication (+AA)				X			RF reader
Detect and read out LED-in-plastic based security features	X	X	X	X		F/V	Use R/F to power LED in plastic
Detect and read out (alphanumeric) displays and their future security features	X	X	X	X		F/V	Use R/F to power display in plastic
Detect and verify retro-reflective foil material	X				Coaxial lighting	F/V	Pattern matching
Barcodes	X	X	X			V	Decoding

B.4 SELECTION CRITERIA FOR MACHINE VERIFIABLE SECURITY FEATURES

If an issuing State considers incorporating security features for machine authentication in its MRTDs or a receiving State plans to deploy reader systems that are able to machine authenticate MRTDs, various criteria for the selection of these features have to be considered.

Much like the selection process for the global interoperable biometric or the storage technology, these criteria comprise:

- security – the most important criterion;
- availability, but exclusiveness for security documents (preferably more than one supplier available);
- dual-use, i.e. additional purpose of the feature beyond machine authentication, e.g. general anti-copy property or visual inspection;
- potential of the Machine Authentication feature to be personalized (i.e. individualized) with information from the passport to secure the personal data (e.g. the passport number, name) in order to avoid re-use of parts of genuine passports;
- compatibility to issuing processes for MRTDs;

- compatibility (to existing and standardized properties of MRTDs);
- compatibility to control process at the border and elsewhere (e.g. no obstruction of basic security features, no extra time needed);
- interoperability;
- sensor availability;
- cost (for feature and sensor);
- Intellectual Property (IP) issues, e.g., patents;
- primary inspection vs. secondary;
- time required to actually utilize the feature;
- potential difficulties associated with the book manufacturing and/or the personalization processes; and
- durability, i.e. according to the relevant ISO and ICAO specifications for MRTDs.

— — — — — — — —

APPENDIX C TO PART II — THE PREVENTION OF FRAUD ASSOCIATED WITH THE ISSUANCE PROCESS (INFORMATIVE)

C.1 SCOPE

This Appendix describes the fraud risks associated with the process of MRTD application and issuance. These risks are a consequence of the benefits that can accrue from the possession of an MRTD that can be used to confirm the identity and citizenship of the holder. The Appendix recommends precautions that an issuing State can take to prevent such fraud.

C.2 FRAUD AND ITS PREVENTION

Fraud perpetrated as part of the issuance process can be of several major types:

- theft of genuine blank MRTDs and completion to make them look valid;
- applying for the MRTD under a false identity using genuine evidence of nationality and/or identity stolen from another individual, or otherwise obtained improperly;
- applying for the MRTD under a false identity using manufactured false evidence of nationality and/or identity;
- using falsely declared or undeclared lost and/or stolen MRTDs that can be provided to people who might use them in look-alike fraud or with repetitive photo substitutions; and
- reliance on MRTD employees to manipulate the MRTD system to issue an MRTD outside the rules.

There are two additional categories in which the applicant applies under his own identity but with the intention to be complicit in the later fraudulent use of the MRTD by:

- altering a genuinely issued document to make it fit a bearer who is not the person to whom the MRTD was issued; and
- applying for an MRTD with the intention of giving or selling it to someone who resembles the true bearer.

C.3 RECOMMENDED MEASURES AGAINST FRAUD

To combat the above-mentioned threats, it is recommended that the MRTD-issuing authority of the State undertake the following measures, to the extent that adequate resources are available for their implementation.

A suitably qualified person should be appointed to be Head of Security directly responsible to the Chief Executive Officer of the issuing authority. The Head of Security should be responsible for ensuring that security procedures are laid down, observed and updated as necessary.

In each location where MRTDs are issued there should be a designated Security Manager. The Security Manager should be responsible for the implementation and updating of the security procedures and report directly to the Head of Security.

Vetting procedures should be established to ensure that all staff are recruited only after searches have verified their identity, ensured that they have no criminal record, and verified that their financial position is sound. Regular follow-up checks should also be made to detect staff whose changed circumstances mean they may succumb to temptations to engage in fraudulent activity.

All staff within the MRTD-issuing authority should be encouraged to adopt a positive attitude toward security matters. There should be a system of rewards for any staff member who reports incidents or identifies measures that prevent fraud.

Controls should be established that account for key components such as blank books and security laminates. Such items should each bear a unique serial number and should be kept locked in suitable secure storage. Only the required number should be issued at the start of each working day or shift. The counting of the items should be done and the figures agreed by two members of staff who should also record the unique numbers of the items. The person to whom they are issued must account for all items at the end of the shift in the form of either personalized documents or defective product. All items should be returned to the secure store at the end of the working period, again having been counted by two people and the unique numbers logged. The records should be kept at least for the life of the issued MRTDs.

Defective product or materials should be destroyed under controlled conditions and the unique numbers recorded.

The issuance process should be divided into discrete operations that are carried out in separate locations within the facility. The purpose is to ensure that no one person can carry out the whole issuance process without venturing into one or more areas that the person has no authorization to enter.

C.4 PROCEDURES TO COMBAT FRAUDULENT APPLICATIONS

The following procedures are recommended to prevent the issue of a genuine MRTD as a result of receipt of a fraudulent application.

The MRTD-issuing office should appoint an appropriate number of anti-fraud specialists (AFS) who have received a high level of training in the detection of all types of fraud used in MRTD applications. There should be at least one AFS present in each location in which MRTD applications and applicants are processed. An AFS should at all times be available to support those whose task it is to process applications (Authorizing Officers [AO]) and thus to provide assistance in dealing with any suspicious application. AFS personnel should regularly provide training to AOs to increase their awareness of potential fraud risks.

The MRTD-issuing authority should establish close liaisons with the issuers of breeder documents such as birth and marriage certificates and driving licences. Access to a database of death certificates assists in the prevention of fraud where an application for an MRTD is made in the name of a deceased person. The State should ensure that the departments holding records of births, marriages and deaths are reconciled and the data stored in a database, secure access to which should be available to the MRTD-issuing office. The aim is to facilitate rapid verification that submitted breeder documents are genuine and that an application is not being made, for example, in the name of a deceased person.

An applicant for an MRTD who has not held one previously should be required to present himself at an MRTD-issuing office with supporting breeder documentation for an interview with an AO and, where necessary, an AFS.

An interview may also be used to process applications for an MRTD to replace an expiring one. Alternatively, provided the MRTD-issuing office has an adequate database of personal information, including portraits, a replacement application may be processed by submission of the documentation, including a new portrait, by mail. In such cases it is desirable that the application and new portrait be endorsed by a responsible person. The return of the expiring MRTD with the new application should be required.

The MRTD-issuing office should initiate procedures that would prevent the fraudulent issue of more than one MRTD to an individual who may have attempted to assume more than one identity. Computer database checks of stored portraits using facial recognition and, where available, fingerprints can assist in this process.

Procedures in the MRTD-issuing office should prevent an applicant from selecting the AO who will serve him. Conversely the work flow should be such as to prevent any employee from selecting which applications he is to process.

The issuance of an MRTD to a young child should require the attendance at the issuing office of, preferably, both parents and of the child. This is to lower the risk of child smuggling or abduction of a child by one parent.

The replacement of an MRTD claimed to be lost or stolen should be made only after exhaustive checks including a personal interview with the applicant.

It is recommended that details, particularly document numbers, of lost or stolen MRTDs be provided to the database operated by INTERPOL. This database is available to all participating countries and can be used in the development of watch lists.

C.5 CONTROL OF ISSUING FACILITIES

A State should consider issuing all MRTDs from one or, at most, two centres. This reduces the number of places where blank documents and other secure components are stored. The control of such a central facility can be much tighter than is possible at each of many issuing centres. If central issuance is adopted, the provision of centres where applicants can attend interviews is required. Furthermore, since standard MRTDs cannot be issued instantly, a system should be established for the issue of emergency MRTDs.

— — — — — — — —

APPENDIX D TO PART 2 — ASF/SLTD KEY CONSIDERATIONS (INFORMATIVE)

Legislative requirements	Before States can begin uploading information to the INTERPOL ASF/SLTD, they must explore their legislation to determine whether they have the authority/mandate to provide international access to elements of citizens' travel document information. Should amendments to legislation be required, States should ensure that adequate coverage is provided for: 1. collection and storage of data; 2. privacy provisions (including security); 3. authorization for disseminating data to the international community; and 4. data life cycle and non-repudiation.
Data elements	A standard data set focusing on the document details rather than the holder of the document has been developed for the interchange of information pertaining to lost, stolen and revoked travel documents. States must meet the following required data fields when uploading to this database: 1. travel document identification number*; 2. type of document (passport or other); 3. issuing State's ICAO Code; 4. status of the document (i.e. stolen blank); and 5. country of theft (only mandatory for stolen blank travel documents). *Where the travel document has been personalized this should be the number contained in the MRZ; if dealing with a blank book, this number should be the serial number, if the numbers are not the same.
Information gathering	States should ensure that tools used to collect information about lost and stolen travel documents (i.e. telephone interviews, online forms) are comprehensive and conducive to securely gathering all the information required to complete the ASF/SLTD report.
Timely and accurate data provision	The strength of INTERPOL's ASF/SLTD rests on timely and accurate information. Accordingly, States should ensure that they have the systems and processes in place to share information in the most timely fashion to intercept attempts to use lost, stolen or revoked travel documents at border control. States should strive to share this information on a daily basis. Generally, once information is received that the travel document is no longer in the possession of the rightful holder or has been revoked, the issuing authority should officially record the information in its national database (if it runs and maintains one) and in the ASF/SLTD. States should also make ongoing efforts to ensure that data is accurate and reliable.

	Care must be taken to avoid input errors and to provide all the required document data, as accurate reporting is the responsibility of the issuing authority. Errors in reporting can be disruptive to travel and costly to both the traveller and issuing State. States must therefore take the necessary steps to ensure the accurate recording and reporting of lost, stolen and revoked travel documents. States should operate a round-the-clock response facility to promptly action requests for further information from INTERPOL on behalf of inquiring States.
Leveraging national databases on lost, stolen and revoked travel documents	States maintaining national databases on lost, stolen and revoked travel documents should consider using automated ways to transmit this information to INTERPOL to leverage their efforts.

— END —

ISBN 978-92-9249-791-0