



ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 2021

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



Approved by and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION



| ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 2021

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

Approved by and published under the authority of the Secretary General

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*

Order No.: 9303P2

ISBN 978-92-9265-319-4 (print version)

© ICAO 2021

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, without prior permission in writing from the International Civil Aviation Organization.

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

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

TABLE OF CONTENTS

	<i>Page</i>
1. SCOPE	1
2. SECURITY OF THE MRTD AND ITS ISSUANCE.....	1
3. MACHINE ASSISTED DOCUMENT VERIFICATION	2
3.1 Feature Types	3
3.2 Basic Principles	4
3.3 Machine Authentication and eMRTDs	4
4. SECURITY OF MRTD PRODUCTION (DESIGN AND MANUFACTURING) AND ISSUANCE FACILITIES	5
4.1 Resilience	6
4.2 Physical Security and Access Control	6
4.3 Production Material Accounting	7
4.4 Transport	7
4.5 Personnel	7
4.6 Cyber Security	7
5. PROVISION OF INFORMATION ON NEWLY ISSUED MRTDS.....	7
6. PROVISION OF INFORMATION ON LOST AND STOLEN MRTDS	8
6.1 Communicating Proactively with Document holders	8
6.2 Maintaining National Databases of Lost, Stolen and Revoked Travel Documents	8
6.3 Sharing Information about Lost, Stolen and Revoked Travel Documents with INTERPOL and Verifying Documents against INTERPOL Databases Systematically at Primary Inspection	9
6.4 Installing Checks to Determine Whether a Holder is Presenting a Lost, Stolen or Revoked Document at Border Crossing	9
7. REFERENCES (NORMATIVE).....	11
APPENDIX A TO PART 2. SECURITY STANDARDS FOR MRTDS (INFORMATIVE).....	App A-1
A.1 Scope	App A-1
A.2 Introduction	App A-1
A.3 Basic Principles	App A-1
A.4 Main Threats to the Security of Travel Documents	App A-2
A.5 Security Features and Techniques	App A-4

APPENDIX B TO PART 2. MACHINE ASSISTED DOCUMENT**SECURITY VERIFICATION (INFORMATIVE)..... App B-1**

B.1	Scope	App B-1
B.2	Document Readers and Systems for Machine Authentication	App B-1
B.3	Security Features and their Application for Machine Authentication	App B-2
B.4	Selection Criteria for Machine Verifiable Security Features	App B-11

APPENDIX C TO PART 2. OPTICAL MACHINE AUTHENTICATION (INFORMATIVE)..... App C-1

C.1	Introduction	App C-1
C.2	Definitions	App C-2
C.3	Catalogue of Generic Check Routines	App C-8
C.4	Recommendations for Machine Authentication of MRTDs	App C-14
C.5	Monitoring in Compliance with Data Protection	App C-48
C.6	Bibliography	App C-49

APPENDIX D TO PART 2. THE PREVENTION OF FRAUD ASSOCIATED**WITH THE ISSUANCE PROCESS (INFORMATIVE)..... App D-1**

D.1	Scope	App D-1
D.2	Fraud and its Prevention	App D-1
D.3	Recommended Measures against Fraud	App D-1
D.4	Procedures to Combat Fraudulent Applications	App D-2
D.5	Control of Issuing Facilities	App D-3

APPENDIX E TO PART 2. ASF/SLTD KEY CONSIDERATIONS (INFORMATIVE)..... App E-1

1. SCOPE

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 provides advice on strengthening the security of machine readable travel documents;
- Appendix B contains recommendations that cover machine authentication of the security features in the document;
- Appendix C describes the security measures to be taken to ensure the security of the personalization operations and of the documents in transit;
- Appendix D describes the fraud risks associated with the process of MRTD application and issuance.

2. SECURITY OF THE MRTD AND ITS ISSUANCE

Before the issuance of a travel document, the establishment of the holder and the entitlement to a travel document shall be carried out in line with the [ICAO EOI], ICAO TRIP Guide on Evidence of Identity, available at <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>.

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 that 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 oneself 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.
- *Spoofing.* Faking the sending address of a transmission to gain illegal entry into a secure system.

Note.— Impersonating, masquerading, piggybacking and mimicking are forms of spoofing.

- *Morphing.* Morphing is an image manipulation technique where two or more subjects’ faces are morphed or blended together to form a single face in a photograph.

There are established methods of providing security against the above types of fraudulent attack. These involve the use of materials that 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 in Appendix A.

3. MACHINE ASSISTED DOCUMENT VERIFICATION

In the field of machine assisted authentication of Machine Readable Travel Documents (MRTDs), considerable progress has been made over the last decade. Technical innovations made in the security design of MRTDs and in the development of authentication systems (readers, software, etc.) have allowed for machine-based document authentication to become an integral part of several control infrastructures and processes (e.g. border control).

However, new challenges arise for document experts, manufacturers and authorities involved in the field as technical improvements achieve higher security and efficiency in operational processes. Some of the main challenges are the lack of harmonization and standardization of the processes in place, and the lack of coordination between the main parties involved in those processes, both leading to system parts and components being developed independently without consideration for major implications resulting from their interaction. Furthermore, the complexity and diversity of the systems currently available on the market make it especially difficult to evaluate and/or compare them.

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. Appendix A of this Part and the security standards recommended therein provide the basis for the considerations in this section; Appendix B contains recommendations that cover machine verification of those security standards (based on materials, on security printing and on copy protection techniques) using the capability of document readers for high resolution image acquisition in the visual, infrared and ultraviolet spectral range. Finally, Appendix C provides a set of best practice recommendations for the main parties involved in the design, implementation and operation of the machine authentication systems and key components.

The aim of the recommendations in this section is to improve the security of machine readable travel documents worldwide by using machine assisted document verification 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 as recommended in Appendices B and C of this Part.

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 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 that 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 that 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 that 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 be, for example, 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 document reader is used instead of a border official to read and validate the eMRTD. As a reliable alternative, optical machine authentication establishes trust in the data used for decisions at the border.

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

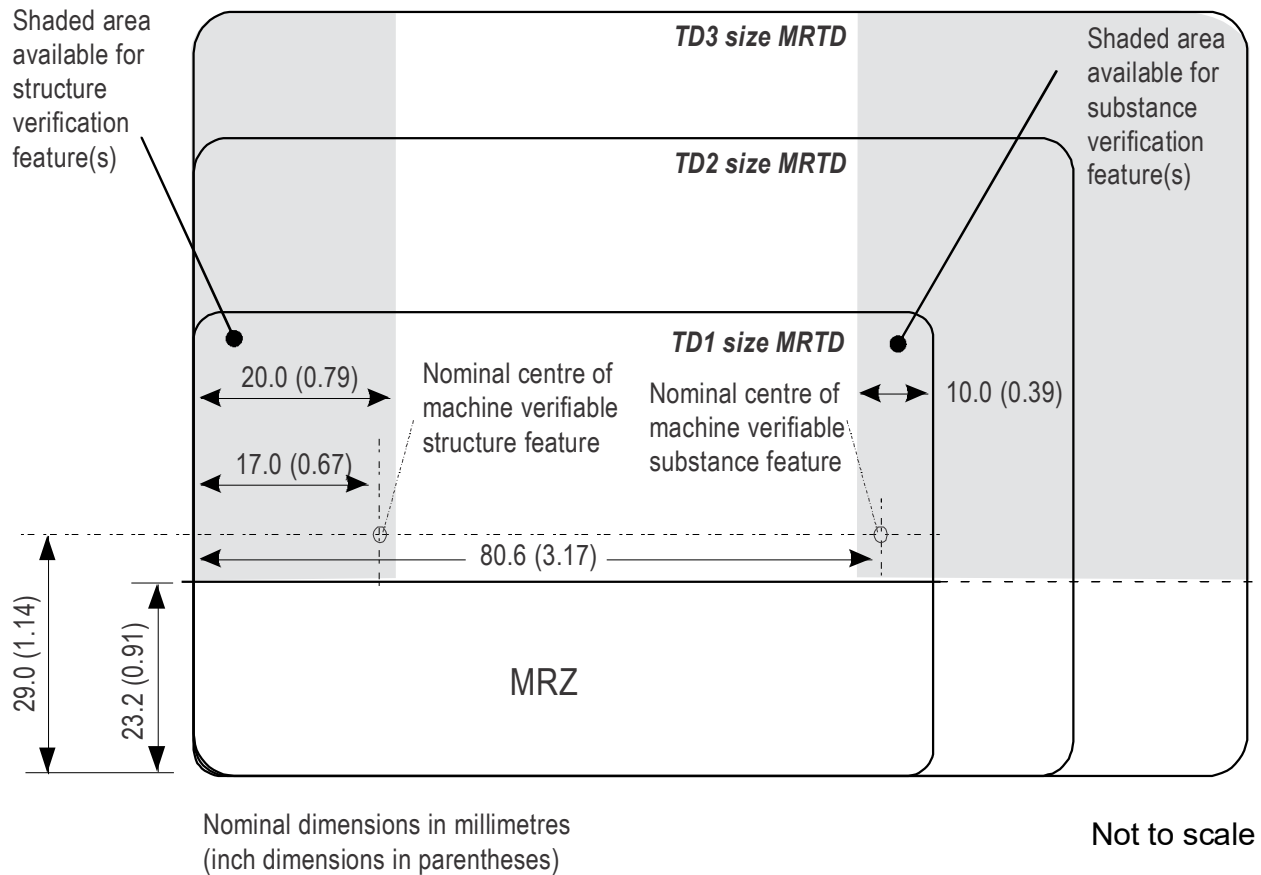


Figure 1. Three sizes of MRTD including the MRP (TD3 size) with recommended positions for machine assisted document verification features. The shaded area on the left is recommended for the incorporation of a structure feature and that on the right for the incorporation of a substance feature.

4. SECURITY OF MRTD PRODUCTION (DESIGN AND MANUFACTURING) 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 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 travellers to ascertain their true identity or nationality, and determine if they are the rightful bearers of the travel documents.

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.

<i>Travellers entering a foreign country on a document declared lost, stolen or revoked as a result of a data error</i>	<p>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 one's country.</p> <p>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.</p>
<i>Nationals attempting to leave their country on a document declared lost or stolen</i>	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.
<i>Nationals attempting to leave their country on a revoked document</i>	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.
<i>Nationals attempting to leave a country and return to their country on a document declared lost, stolen or revoked</i>	<p>Where exit controls are in place and the identity and nationality of the holder have been confirmed, border control may allow the travellers to proceed, but should advise them that the document presented is not valid and that they may be refused boarding by the carrier.</p> <p>When travellers are re-entering their 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.</p>
<i>Nationals attempting to leave a foreign country and continue to a third country on a document declared lost, stolen or revoked</i>	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 travellers after determining that they are 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.

7. REFERENCES (NORMATIVE)

Certain provisions of international Standards, referenced in this text, constitute provisions of Doc 9303. Where differences exist between the specifications contained in Doc 9303 and the referenced Standards, to accommodate specific construction requirements for machine readable travel documents, including machine readable visas, the specifications contained herein shall prevail.

Annex 9 to the Convention on International Civil Aviation (“Chicago Convention”), Annex 9 — *Facilitation*.

[ICAO EOI] ICAO TRIP Guide on Evidence of Identity, available at
<https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>.

— — — — —

APPENDIX A TO PART 2 — 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 A.5.1.1 through A.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 A.5.2 to A.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 Doc 9303-1, 4.2 — Terms and Definitions):

- two-colour guilloche security background design pattern¹;
- 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;
- metamerism 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 A.5.3.2, A.5.4.3 and A.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 are 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 A.5.4.3 and A.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

<i>Elements</i>	<i>Basic features</i>	<i>Additional features</i>
Substrate materials (A.5.1)		
Paper substrates (A.5.1.1)	<ul style="list-style-type: none"> – controlled UV response – two-tone watermark – chemical sensitizers – appropriate absorbency and surface characteristics 	<ul style="list-style-type: none"> – 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)	<ul style="list-style-type: none"> – controlled UV response – chemical sensitizers – invisible florescent fibres – visible (florescent) fibres – system of adhesives 	<ul style="list-style-type: none"> – security thread – watermark – laser-perforated security feature – die cut security pattern
Synthetic substrates (A.5.1.4)	<ul style="list-style-type: none"> – construction resistant to splitting – optically dull material – secure incorporation of data page – optically variable features – see A.5.2 – A.5.5, as appropriate 	<ul style="list-style-type: none"> – window or transparent feature – tactile feature – laser-perforated feature

<i>Elements</i>	<i>Basic features</i>	<i>Additional features</i>
Security printing (A.5.2)		
Background and text printing (A.5.2.1)	<ul style="list-style-type: none"> – two-colour guilloche background – rainbow printing – microprinted text – unique data page design 	<ul style="list-style-type: none"> – 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)	<ul style="list-style-type: none"> – UV florescent ink – reactive ink 	<ul style="list-style-type: none"> – 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)	<ul style="list-style-type: none"> – 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 	<ul style="list-style-type: none"> – laser-perforated document number – special typeface
Personalization technique (A.5.4)		
Protection against photo substitution and alteration (A.5.4.4)	<ul style="list-style-type: none"> – 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 	<ul style="list-style-type: none"> – 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)	<ul style="list-style-type: none"> – secure sewing technology – UV fluorescent sewing thread – unique data page design – page numbers integrated into security design – serial number on every sheet 	<ul style="list-style-type: none"> – 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)	<ul style="list-style-type: none"> – 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 	<ul style="list-style-type: none"> – 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 2 — 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 allow for 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 A.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 A.5.2 – A.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

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
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 2 — OPTICAL MACHINE AUTHENTICATION (INFORMATIVE)

C.1 INTRODUCTION

For the authentication of machine readable travel documents (MRTDs) as part of stationary border control, including ABC gates, the use of IT systems, which go beyond the pure extraction and checking of the documents' MRZ and automatically inspecting optical security features, increases. The major improvements in technologies used in the context of machine-based document authentication have contributed to the growth of the amount and diversity of the authentication systems. However, the significant increasing traveller volume still remains challenging for all actors involved in the design, production and deployment of authentication systems and MRTDs.

Authentication systems used to perform machine authentication of MRTDs include several components that are required to properly interact with each other. Furthermore, the security features of machine readable documents need to be designed and implemented in accordance with the capabilities of the authentication systems and the insight of experienced practitioners.

This Appendix provides a set of recommendations for the main parties involved in the design, implementation and operation of the affected systems and key components, whereby the main goals are:

- increase the awareness for the relevant security-related questions of machine authentication, involving the main stakeholders, e.g. security document producers, reading equipment manufacturers and government;
- propose a catalogue of generic check routines with consistent terminology; and
- define recommendations for security document designers, manufacturers of authentication systems, and operational levels.

This Appendix is meant to support practitioners in the design and development of authentication systems. It is however important to bear in mind that the authentication system should be used to facilitate adjudication for its operator¹, and should not be regarded as the sole decision maker, particularly with regard to the security features that cannot be checked by the machine and can only be verified by a human operator.

This Appendix only deals with the optical part of the authentication of MRTDs and the scope of the recommendations is limited to data acquired through full page readers, i.e. full size images of the document, as described in Appendix B of this Part. Furthermore, the guidelines do not distinguish between 1st, 2nd and 3rd level inspections, as full page readers can be used in each of those scenarios. Altogether, mobile devices are (so far) not taken into consideration due to their limited optical capabilities with respect to different light sources (neither UV nor IR) and therefore do not meet the proposed requirements.

1. Operator: A person who directly interacts with the authentication system (e.g. manual interaction with the document reader) in the context of a document check.

The basics and terminology required for a better understanding of optical machine authentication are introduced in section C.2. The issue of harmonization and standardization of check routines is addressed in section C.3, where a catalogue of generic check routines is defined. In section C.4 the focus is on elaborated recommendations for manufacturers of authentication systems, and section C.5 highlights several approaches and methodologies related to data processing in accordance with data protection policies.

C.1.1 Terminology

Although the recommendations and guidelines are non-binding for the parties directly affected, the terminology has been adopted and integrated into Part 1 of Doc 9303 in order to provide an unambiguous description of what should be observed in order to achieve the goals defined in this document.

The terminology should be regarded as a practical way to organize the recommendations and guidelines in order of importance, and should not be mistaken with a set of restrictive requirements similar to those used in classical standards (e.g. ISO). In order to provide the target group with clear, precise and unambiguous guidance as to what is and is not in line with best practices, the present terminology is being used.

C.1.2 Influence of the Electronic Check on the Authentication Process

Although focus is on the optical part of the authentication of MRTDs, the electronic part has to be taken into consideration. Based on the current state of technology, interaction between a chip (eMRTD) and an RF module (full page reader) during the authentication process is highly probable and can be expected. Some of the recommendations given in this document are best understood when keeping in mind that both optical and electronic checks (if applicable) are complementary processes converging to an overall result.

Two aspects of the interaction between electronic and optical checks are of particular interest: the comparison of optical and electronic data; and the implications behind the check for the presence of a chip if one is expected. For these two aspects, the influence of the electronic check cannot be disregarded and is highlighted in the corresponding recommendations.

C.2 DEFINITIONS

In the following section, consistent terminology is introduced for further use. The inspection process of MRTDs is described in general in section C.2.1 and in detail in section C.2.2. In section C.1.2 the influence of the electronic part of the authentication process is addressed.

C.2.1 Process of Identification and Verification of MRTDs

The authenticity verification of a travel document includes the verification of the document's optical security features. It is performed by an authentication system² which consists of the following components: a full page reader, authentication software³, an authentication database and optionally a reference database.

-
2. An authentication system describes the combination of a full page reader, authentication software, including an authentication database and optionally the expert reference database.
 3. The authentication software receives the live data set from the full page reader. It provides several authentication algorithms in order to apply the check routines to the live data set.

The full page reader creates full size images of the travel document to be verified under different light sources. This so-called *live data set* (full size images of the document)⁴ is transferred to the authentication software by the full page reader.

The authentication software usually identifies the so-called *document model* of the document using the Machine Readable Zone (MRZ) and/or additional information (e.g. document specific pattern, date of issue, specific optical features, etc.) as input. A document model covers those document series of a country/nation which have the same optical appearance.

In accordance with the technical guideline [BSI-TR-03135], a document model is defined by means of the country code (C), document type (T), a unique identification number (N) and the year value of first issuance (Y):

Document Model : = (C, T, N, Y)⁵

The country code C has to be filled in according to ICAO Doc 9303 specifications as a three-letter code.

The document type T is also specified by ICAO in Doc 9303.

The identification number N must be a unique chronological increasing integer number starting with 1 referencing the model – or generation – of the document.

The year Y refers to the year as a 4-digit integer value in which a document of that particular model was issued for the first time. If the year is unknown, this value shall be omitted.

For instance, the two British passport/document models from 2008 and 2010 in circulation have the following identifiers: (GBR, P, 1, 2008) and (GBR, P, 2, 2010).

There are various technical approaches for identifying the document model. MRZ acquisition is one of them (see section C.4.3.2). If the MRZ is used but not sufficient for the unambiguous determination of the document model, additional document parameters (e.g. patterns) have to be used to help narrow down the identification results; especially when dealing with several valid document models of the same country (e.g. British passport)⁶.

The authentication software sends the document model's identifier to the authentication database where the so-called *check routines* are stored. These check routines define which testing procedures have to be applied to the live data set of this particular travel document model. A specific set of check routines, the so-called *authentication data set*, is determined for each document model. After the receipt of the document model's identifier, the authentication database sends the corresponding data set to the authentication software. Further details on the setup of an authentication database is provided in section C.2.2. (See Figure C-1.)

-
4. Live data set: The visual, IR, and UV picture of the document under test to be verified with the reader system. These pictures are used for the document's inspection.
 5. This Appendix only focuses on the optical part of machine-based document authentication. This means that documents that are optically identical but differ when considering electronic features, are considered to belong to the same document model.
 6. Some countries, such as Australia, use a series Letter to distinguish different document models or series (e.g. N-series). Even though this method might be sufficient at a national level, it is not very efficient for international classification because of the lack of standardization. Therefore, this document follows the recommendations of [BSI-TR-03135], which are considered to be more suitable for international classification purposes.

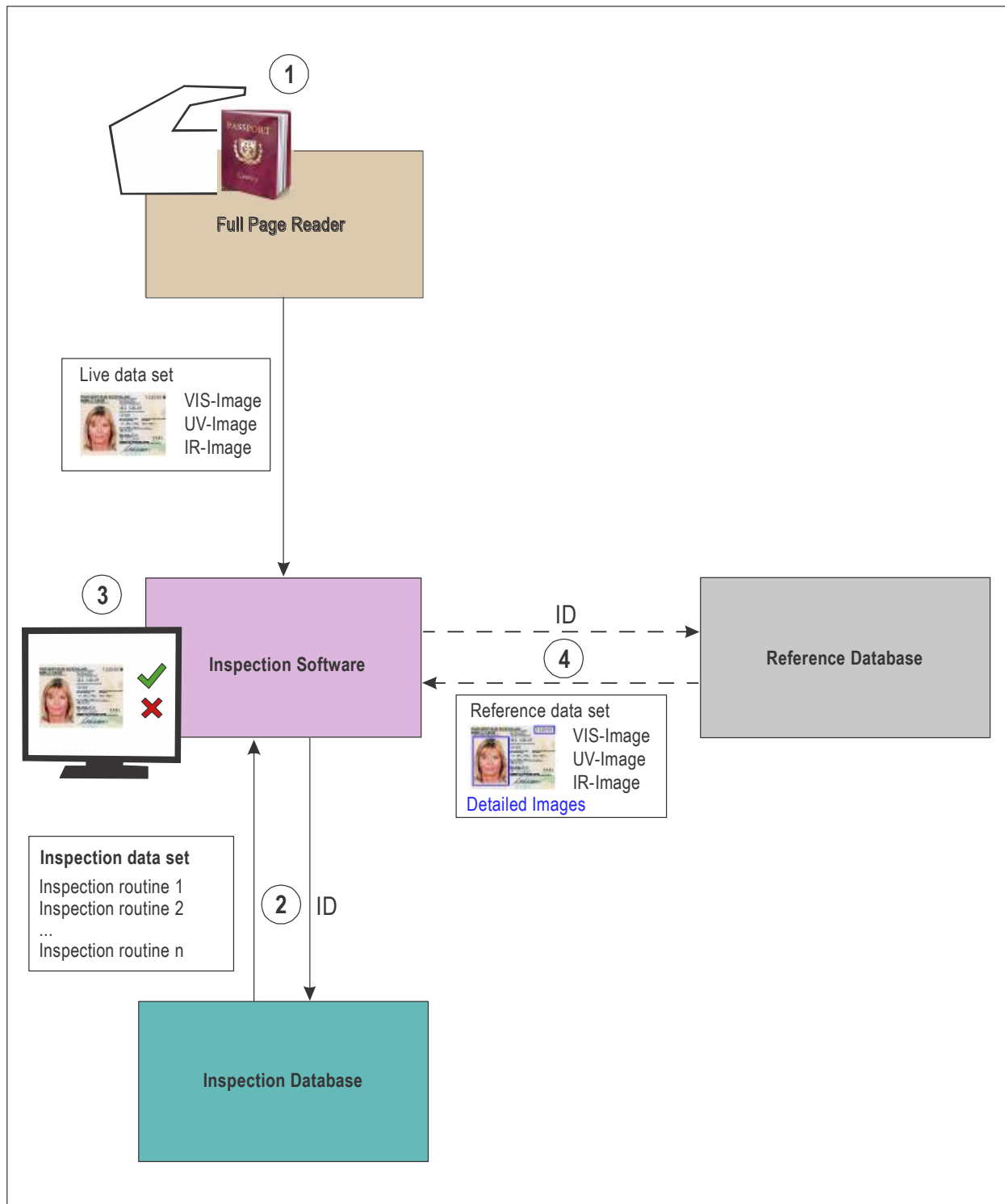


Figure C-1. Process of document identification and verification; the numbers denote the order of the involved process steps

The verification is then performed by the authentication software. The check routines are applied to the travel document's live data set. This examination usually leads to a Pass- or Fail-result. A Pass-result implies that the checked document does not present any abnormalities, whereby a Fail-result means the opposite. Depending on the application scenario, the interpretation of the result (pass or fail) is the responsibility of the human operator.

If a live data set cannot be assigned unambiguously to a particular document model, a subset of check routines may be performed (optionally). These check routines are specified independently of the document model.

In order to support the human operator in a manual verification, the authentication software can request the so-called *reference data set* from the reference database on the basis of the identified document model. The reference data set contains the visible light (white), IR and UV images of the document model; it can also include more detailed pictures of the document parts as well as further textual descriptions. However, this so-called reference database, also referred to as *expert database* in practice, is not a mandatory component of the actual authentication system. The process of document identification and verification is illustrated in Figure C-1.

C.2.2 Detailed Setup of an Authentication Database

In the authentication database a distinct set of check routines is stored for each document model. For instance, the check routines for the German document model from 2007 differ from the routines which have to be applied to the British document model from 2008.

A check routine of a set denotes a test specification for an optical security feature's property. For example, the check routine 1 in Figure C-2 checks whether the photo is absorbent in visible light. In this case, the photo is the optical feature, which is tested for the property of absorption under visible light (see light source 1 in check routine 1). The implementation of this check routine is carried out by an authentication algorithm provided by the authentication software (see authentication algorithm 1 in check routine 1). In this case, algorithm 1 is an authentication algorithm that checks the feature's brightness. In contrast, check routine x in Figure C-2 checks whether the ink is luminescent under UV light within the area of the photo by using the "pattern check" algorithm (check algorithm n of the authentication software in Figure C-2). This example shows clearly that an optical security feature can offer different properties under different light sources (see Figure C-3).

In terms of the EU regulation on minimum standards for security features and biometrics in passports and travel documents⁷, these check routines can be reasonably split into the three categories: material, printing technique and personalization.

7. Council Regulation (EC) No 2252/2004 of 13 December 2004.

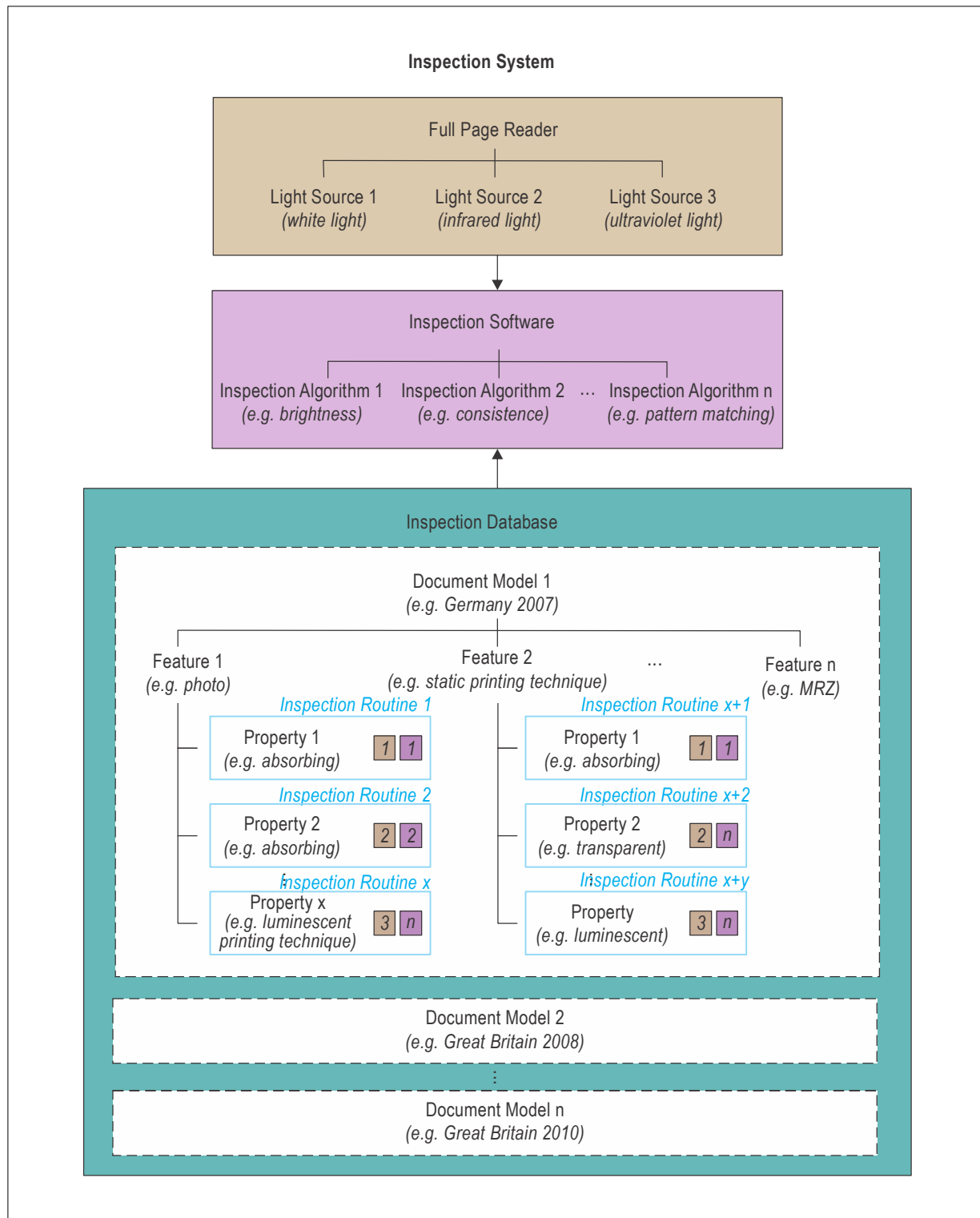


Figure C-2. Schematic diagram of the setup of an authentication system

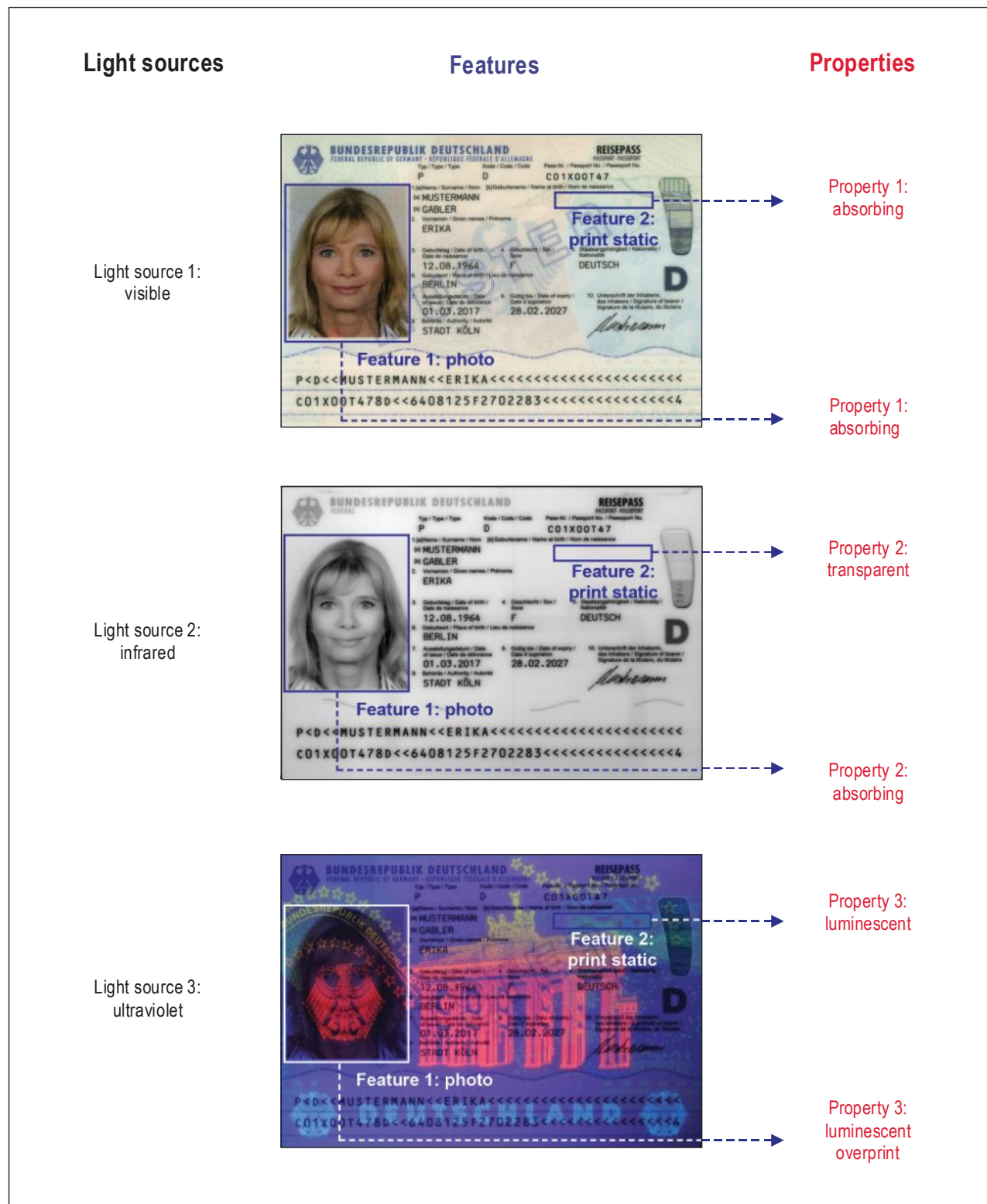


Figure C-3. Features and properties under different light sources using the German passport

C.3 CATALOGUE OF GENERIC CHECK ROUTINES

All developers of an authentication system define their own identifiers for the check routines. These check routines are distinct for each document model; however, the identifiers for these check routines are often not self-explanatory. Hence, the comparability of the applied check routines for the same document model for different authentication systems is, in general, non-existent.

In order to solve this problem, it is possible to define a catalogue of feasible check routines on the basis of the spectrally selective security features in travel documents. The content of this catalogue may be extended in future versions of this guideline preserving the proposed nomenclature. The corresponding so-called spectrally selective check routines record different reactions occurring on a document checked under visible (VI - visible light) or extra visible (UV - ultraviolet, IR - infrared) light. Based on the three records (VI, UV, IR), the absorbent, reflective or luminescent reactions of these features can be checked. Sequentially, these spectrally selective check routines are denoted by generic check routines as defined in the [BSI-TR-03135].

The application of this catalogue of generic check routines would greatly improve the above-mentioned situation and will allow for a better understanding of machine authentication mechanisms.

C.3.1 Description of Generic Check Routines

The unambiguous identifiers (defined below) of check routines have been defined for the optical machine authentication on the basis of the spectral reaction of security features in travel documents. They can be reasonably split into the following four categories defined in Appendix A:

- Check for material (substrate) properties: Reactions of the printing substrate are verified, e.g. brightness under UV light
- Check for printing technique properties: Features, which are printed onto/into the document irrespective of personalization, are tested, e.g. form printing
- Check for features that protect against copying: usually diffractive or holographic elements or laminates
- Check for issuing technique (personalization) properties: Personalized features are tested, e.g. the name of the document's holder

The optical appearance of the features of the category "copy protection" is very dependent on illumination geometry. Therefore, features of this category – which are well suited for human inspection – can be very problematic for machine authentication in general. For this reason, features of this category are not addressed by the proposed check routines.

The 48 generic check routines defined below consist of so-called *basic check routines (BR)* and *composite check routines (CR)*. Basic check routines are individual routines, which refer to one property (e.g. IR absorption) of a single feature. Composite check routines are defined as logical combinations of basic check routines. Consequently, a single feature can be tested for multiple properties such as IR absorption and transparency in visible light.

For the basic check routines, the following abbreviated definitions according to [BSI-TR-03135] are used:

Basic check routine := (XX, YY, ZZ)

XX specifies the light source for the image on which the check routine is performed:

- **IR** – Infrared light
- **UV** – Ultraviolet light
- **VI** – Visible (white) light

YY is an identifier for the optical property of the particular feature:

- **AB** – absorbent, property of ink
- **BR** – brightness, property of substrate (e.g. bright under exposure of UV light)
- **FR** – spatial frequency property of patterns (e.g. characteristics of patterns obtained after spatial frequency transformation, such as spatial Fourier transformation)
- **LU** – luminescent, property of patterns (e.g. visible under exposure of UV light)
- **TL** – translucent, property of ink shining through the substrate
- **TR** – transparent, property of ink (e.g. transparent under exposure of IR light)

ZZ is an identifier⁸ for the feature itself or the position in the document:

- **FI** – Fibres
- **FU** – Full (complete) data page
- **IS** – printed feature, which already exists on the substrate (ink static)
- **MR** – Machine Readable Zone (MRZ)
- **OM** – Overprinted MRZ
- **CA** – Card Access Number (short: CAN)
- **BC** – Barcode feature
- **PD** – Personalized, “dynamic” perforation
- **PS** – Perforation showing “static” content
- **PH** – Area of the photo

8. Within this nomenclature, document model-specific properties are denoted by “static” (such as UV overprint of a coat of arms), whereas document-specific (individual/personalized) properties are denoted by “dynamic” (such as UV overprint repeating the document number).

- **SP** – Area of the secondary photo
- **OP** – Overprinted photo
- **TH** – Security thread
- **VZ** – Visual inspection zone (VIZ)
- **WM** – Watermark
- **ID** – any other personalized, “dynamic” feature (ink dynamic), e.g. a secondary photograph
- **AF** – any additional feature that cannot be attributed to the items specified above

If a generic check routine consists of more than one single check routine, a sequential number has to be assigned to each single check routine.

The following generic check routines result from these short terms⁹:

Check of material properties: (12 BR + 1 CR)

- **(IR, AB, PS)** → (IR, absorbent, static perforation): Check whether the static perforation is visible under IR light.
- **(IR, AB, TH)** → (IR, absorbent, thread): Check whether the security thread is visible under IR light.
- **(IR, AB, WM)** → (IR, absorbent, watermark): Check whether the watermark is visible under IR light.
- **(UV, BR, FU)** → (UV, brightness, full): Check for the brightness of the full data page under UV light.
- **(UV, BR, MR)** → (UV, brightness, MRZ): Check for the brightness in the MRZ area under UV light.
- **(UV, BR, PH)** → (UV, brightness, photo): Check for the brightness in the photo area under UV light.
- **(UV, BR, VZ)** → (UV, brightness, VIZ): Check for the brightness in the Visual Inspection Zone (VIZ) under UV light.
- **(UV, LU, FI)** → (UV, luminescent, fibres): Check for the presence of fibres that are luminescent under UV light.
- **(UV, LU, PS)** → (UV, luminescent, static perforation): Check whether traces of a static perforation are luminescent under UV light.
- **(UV, LU, TH)** → (UV, luminescent, thread): Check for the presence of a security thread that is luminescent under UV light.
- **(VI, TR, TH)** → (VI, transparent, thread): Check whether the security thread is transparent under visible light.
- **(VI, AB, PS)** → (VI, absorbent, static perforation): Check whether a static perforation is visible under visible light.

9. Check routines based on the AF feature are not explicitly listed because they can be combined with each of the mentioned light sources and optical properties.

- **(IR, AB, TH) ° (VI, TR, TH) →** (IR, absorbent, thread) in combination with (VI, transparent, thread): Check whether a security thread, which is visible under IR light, is transparent under visible light.

Check of printing technique properties: (8 BR + 2 CR)

- **(IR, AB, IS) →** (IR, absorbent, static ink): Check whether the ink of the static print is absorbent under IR light.
- **(IR, TL, IS) →** (IR, translucent, static ink): Check whether the ink on the back of the data page (usually the title page) is translucent under IR light and can be detected on the IR image of the data page.
- **(IR, TR, IS) →** (IR, transparent, static ink): Check whether the ink of the static print is transparent under IR light.
- **(UV, LU, IS) →** (UV, luminescent, static ink): Check whether the ink of the static print is luminescent under UV light.
- **(UV, LU, OM) →** (UV, luminescent, overprinted MRZ): Check whether the ink of the static print is luminescent in the MRZ area under UV light.
- **(UV, LU, OP) →** (UV, luminescent, overprinted photo): Check whether the ink of the static print is luminescent in the area of the photo under UV light.
- **(VI, AB, IS) →** (VI, absorbent, static ink): Check whether the ink of the static print is absorbent under visible light.
- **(VI, TR, IS) →** (VI, transparent, static ink): Check whether the ink of the static print is transparent under visible light.
- **(IR, TR, IS) ° (IR, AB, IS) →** (IR, transparent, static ink) in combination with (IR, absorbent, static ink): Check whether parts of the static print are absorbent in IR light, whereas other parts of the same feature are transparent in IR light.
- **(IR, TR, IS) ° (VI, AB, IS) →** (IR, transparent, static ink) in combination with (VI, absorbent, static ink): Check whether the ink of the static print is both transparent under IR light and absorbent under visible light.

Check of personalization properties: (28 BR + 3 CR)

- **(IR, AB, ID) →** (IR, absorbent, dynamic ink): Check whether the ink of the dynamic print is absorbent under IR light.
- **(IR, AB, MR) →** (IR, absorbent, MRZ B900 check): Check whether the MRZ is visible under IR light.
- **(IR, AB, CA) →** (IR, absorbent, CAN): Check whether the CAN is visible under IR light.
- **(IR, AB, BC) →** (IR, absorbent, barcode): Check whether the barcode is visible under IR light.
- **(IR, AB, PD) →** (IR, absorbent, dynamic perforation): Check whether a dynamic perforation is visible under IR light.
- **(IR, AB, PH) →** (IR, absorbent, photo): Check whether the photo is visible under IR light.
- **(IR, FR, PH) →** (IR, frequency, photo): Check whether the pattern has the expected characteristics after spatial frequency transformation.
- **(IR, AB, SP) →** (IR, absorbent, secondary photo): Check whether the secondary photo is visible under IR light.
- **(IR, TR, SP) →** (IR, transparent, secondary photo): Check whether the secondary photo is transparent under IR light.

- **(IR, TR, ID) →** (IR, transparent, dynamic ink): Check whether the ink of the dynamic print is transparent under IR light.
- **(IR, TR, PH) →** (IR, transparent, photo): Check for the transparency of the photo under IR light.
- **(UV, FR, PH) →** (UV, frequency, photo): Check whether the pattern has the expected characteristics after spatial frequency transformation.
- **(UV, LU, SP) →** (UV, luminescent, secondary photo): Check whether the secondary photo is luminescent under UV light.
- **(UV, LU, BC) →** (UV, luminescent, barcode): Check whether the barcode is luminescent under UV light.
- **(UV, LU, ID) →** (UV, luminescent, dynamic ink): Check whether the ink of the dynamic print is luminescent under UV light.
- **(UV, LU, PD) →** (UV, luminescent, dynamic perforation): Check whether marks of a dynamic perforation are luminescent under UV light.
- **(VI, AB, ID) →** (VI, absorbent, dynamic ink): Check whether the ink of the dynamic print is visible under visible light.
- **(VI, AB, MR) →** (VI, absorbent, MRZ): Check whether the MRZ is visible under visible light.
- **(VI, AB, CA) →** (VI, absorbent, CAN): Check whether the CAN is visible under visible light.
- **(VI, AB, BC) →** (VI, absorbent, barcode): Check whether the barcode is visible under visible light.
- **(VI, TR, BC) →** (VI, transparent, barcode): Check whether the barcode is transparent under visible light.
- **(VI, AB, PD) →** (VI, absorbent, dynamic perforation): Check whether a dynamic perforation is visible under visible light.
- **(VI, AB, PH) →** (VI, absorbent, photo): Check whether the photo is visible under visible light.
- **(VI, AB, SP) →** (VI, absorbent, secondary photo): Check whether the secondary photo is visible under visible light.
- **(VI, TR, SP) →** (VI, transparent, secondary photo): Check whether the secondary photo is transparent under visible light.
- **(VI, FR, PH) →** (VI, frequency, photo): Check whether the pattern has the expected characteristics after spatial frequency transformation.
- **(VI, AB, SP) →** (VI, absorbent, secondary photo): Check whether the secondary photo is visible under visible light.
- **(VI, TR, ID) →** (VI, transparent, dynamic ink): Check whether the ink of the dynamic print is transparent under visible light.
- **(IR, TR, ID) (VI, AB, ID) →** (IR, transparent, dynamic ink) in combination with (VI, absorbent, dynamic ink): Check whether the ink of the dynamic print is transparent in IR light as well as absorbent under visible light.
- **(IR, TR, SP) ° (VI, AB, SP) →** (IR, transparent, secondary photo) in combination with (VI, absorbent, secondary photo): Check whether the secondary photo is transparent in IR light as well as absorbent under visible light.

- **(VI, TR, BC) ° (IR, AB, BC) →** (VI, transparent, barcode) in combination with (IR, absorbent, barcode): Check whether the barcode is transparent under visible light as well as absorbent under IR light.

The following composite check routine is defined jointly for the two inspection classes: printing and personalization:

- **(IR, TR, IS) ° (VI, AB, IS) ° (IR, AB, ID) →** (IR, transparent, static ink) in combination with (VI, absorbent, static ink) in combination with (IR, absorbent, dynamic ink): Check whether the ink of the static print is both absorbent under visible light and transparent in IR light. In addition, a dynamically printed feature is visible under IR light at the same position.

The check routines specified above are not of equal value related to their inspection significance. For instance, the result of the check routine (VI, AB, ID) is not meaningful per se. Though it gains in crucial importance for counterfeit detection when it is combined with the check routine (IR, TR, ID).

Counterfeit-specific properties or features should be incorporated by inverting the logic of check routines: e.g. a specific configuration of imitated security fibres should be checked for absence of this pattern (i.e. VI, TR, IS).

Table C-1 gives an overview of the classification of the generic check routine system. The three components of the routines' identifiers – feature, light source and property – are grouped in a matrix. The content of the rows, columns and cells describe a generic basic check routine. The assigned inspection classes are marked by the colours green (material), blue (printing technique) and yellow (personalization).

Table C-1. Matrix representation of the generic basic check routines.

Optical properties are abbreviated as follows: AB – absorbent, property of ink;

BR – brightness, property of substrate; FR – spatial frequency, property of patterns;

LU – luminescent, property of patterns; TL – translucent, property of ink shining through the substrate;

TR – transparent, property of ink inspection classes are marked by the colours: green (material), blue (printing technique) and yellow (personalization).

Feature		Light source		
		VI	UV	IR
Fibres	FI		LU	
Full data page	FU		BR	
Static printed feature	IS	{AB, TR}	LU	{AB, TR, TL}
MRZ	MR	AB	BR	AB
Overprinted MRZ	OM		LU	
CAN	CA	AB		AB
Barcode	BC	{AB, TR}	LU	AB
Personalized perforation (dynamic)	PD	AB	LU	AB
Perforation on the substrate (static)	PS	AB	LU	AB

Feature		Light source		
		VI	UV	IR
Photo	PH	{AB, FR}	{BR, FR}	{AB, FR, TR}
Secondary Photo	SP	{AB, TR}	LU	{AB, TR}
Overprinted photo	OP		LU	
Security thread	TH	TR	LU	AB
Visual inspection zone, VIZ	VZ		BR	
Watermark	WM			AB
Personalized dynamic feature	ID	{AB, TR}	LU	{AB, TR}
Additional feature	AF	{AB,BR,LU, TL,TR}	{AB,BR,LU, TL,TR}	{AB,BR,LU, TL,TR}

C.4 RECOMMENDATIONS FOR MACHINE AUTHENTICATION OF MRTDS

The following key components are involved in the process of automated machine authentication: the document, the full page reader and the authentication software (including the authentication database, see section C.2.2). However, these components are often designed/manufactured without consideration of their interdependencies, especially with respect to the security document design. In order to be able to perform an optimal machine authentication, it is crucial that these components flawlessly interact with each other.

In the following sections, recommendations are given for efficient and effective design for the document (see section C.4.1), for the full page reader (see section C.4.2), for the authentication software (see section C.4.3), for the authentication database (see section C.4.4) and for the reference database (see section C.4.5). In section C.4.6, the recommendations made in the former sections are mapped to exemplary usage scenarios in order to support operational managers¹⁰ in planning the operation of optical authentication systems.

When discussing recommendations for the different components, the differences in typically involved time scales should be respected when referring to changes to be made:

- Inspection system software: 1 to 12 months
- Inspection system hardware: 3 to 5 years
- Security Document: 10 to 20 years (resulting from a typical issuing period of 5 to 10 years, and a validity period of 5 to 10 years)

10. Operational manager: The organization responsible for the administration and the management of all processes related to the operation of the authentication infrastructure. The operational manager establishes and maintains communication channels with the vendors/manufacturers of the products used in the final authentication system.

C.4.1 Document Designers

To design a document with optical features as secure as possible, human inspection should not be the only goal of a document designer. The security features offered by the document should be applicable for machine authentication as well. In addition to the base design of MRTDs, according to ICAO Doc 9303, the following sections summarize suitable features for machine authentication. Additionally, the following sections will also summarize features that – even though they are of value for human inspection – may counteract machine authentication (see section C.4.1.2). These features are referred to as “potentially interfering” in the context of machine authentication. Document designers should not be deterred from including these features in a document and should consider including these features while keeping in mind their possible (negative) impact on the machine authentication process.

C.4.1.1 Suitable features for machine authentication

Recommendations concerning suitable features for machine authentication are listed below. These features have been selected because they are easy to detect on VI, IR and UV images, but at the same time these features increase the counterfeiting effort for the forger considerably.

- A.1 **Define unambiguous identification features:** It is a common practice among certain countries to bring out successive document models within a relative short period of time in order to improve the security properties of their MRTDs. The British passport models (GBR, P, 1, 2008) and (GBR, P, 2, 2010) are good examples of successive document models. It is therefore required, during the document design process, to define features, which enable unambiguous identification of the document model (e.g. barcode¹¹ with document model).
- A.2 **Define features under all three light sources:** While it is a standard feature of full page readers to capture images under these light sources, field experience has shown that it is quite challenging for counterfeiters to properly reproduce features that appear genuine under more than one of these light sources. The definition of optical security features under all three light sources (VI, IR and UV) is therefore required to significantly increase the effort required to produce counterfeits.
- A.3 **Define features in three categories:** Providing a balanced distribution of security features in the classes “material”, “printing technique” and “personalization” also increases the counterfeiting effort. Therefore, features must be defined in each class in compliance to ICAO Doc 9303.
- A.4 **Define features on both sides of ID cards:** ID-1 sized ID cards are allowed to be positioned on a full page reader with both sides. Hence, document designers shall design ID-1 sized ID cards with identification and verification features on both sides in order to allow identification and verification independent of the card side.
- A.5 **Define features reacting differently under different light sources:** Document features behaving differently under different light sources (see Figure C-4), help to reduce considerably the success probability of counterfeiters in producing proper counterfeits. For machine authentication, it is therefore required to use features that can be either checked for their presence and/or absence, depending on the corresponding light source (e.g. metameric inks, also called IR split in Figure C-4, checkable by routine (IR, TR, IS) (VI, AB, IS)).

11. This example using the barcode does not contradict the recommendations of Doc 9303, Parts 9 and 10, for electronic storage of biometric data.



The image displays two versions of a United Kingdom passport for Angela Zoe Croydon. The left version is the original passport, featuring a gold-colored design with a portrait of the holder, a coat of arms, and various security features. The right version is a duplicate of the same passport, but with a prominent red 'SPECIMEN' watermark overlaid across the center. The watermark is in a large, bold, sans-serif font. The passport details are as follows: Type/Type: P; Code/Code: GBR; Passport No./Passport No.: 925603778; Surname/Nom (1): UK SPECIMEN; Given names/Prénoms (2): ANGELA ZOE; Nationality/Nationalité (3): BRITISH CITIZEN; Date of birth/Date de naissance (4): 11 SEP /SEPT 88; Sex/Sexe (5): F; Place of birth/Lieu de naissance (6): CROYDON; Date of issue/Date de délivrance (7): 16 JUL /JUIL 10; Authority/Autorité (8): IPS; Date of expiry/Date d'expiration (9): 16 JUL /JUIL 20; Holder's signature/Signature du titulaire (10): A. Specimen. The passport number is 925603778. The watermark is a large, red, stylized 'SPECIMEN' text that is semi-transparent and covers the central part of the passport.

Figure C-5. Passport (GBR, P, 2, 2010): UV pattern with two colours¹²

12. Source: <http://edison.td.net/>

A.7

Define patterns with individual content, e.g. secondary facial image: It is recommended to define individual patterns that can both be checked for their property and compared with already existing dynamic content on the data page. For instance, a secondary facial image can be compared with the primary facial image, and these two representations can have the same or different spectral properties. The list of following patterns with secondary facial images is meant to illustrate this recommendation, but is neither complete nor is it meant to be an explicit recommendation for these specific features:

- a) Secondary facial image as smaller repetition of the facial image which is visible under visible light and transparent under IR light (checkable by (VI, AB, ID) ° (IR, TR, ID)).
- b) Optically variable ink (OVI) and diffractive optically variable image devices (DOVIDs) that are personalized, e.g. with laser engraving or laser ablation (see Figure C-6). The exemplary feature depicted in Figure C-6 shows different colours under different viewing angles in visible light (first and second picture) and a secondary facial image slightly visible under transmitted light (third picture). Under IR light, the secondary facial image can clearly be captured and compared to the facial image. The feature is checkable by the following composite check routine: (IR, AB, ID) ° (VI, AB, IS) ° (IR, TR, IS), which is a threefold combination.



Figure C-6. Passport (HUN, P, 1, 2006): Personalized OVI viewed under two different angles under transmitted light and under IR light

- c) Personalized laser engraving that reacts in an opposite (“negative”) manner (see Figure C-7). The exemplary feature depicted in Figure C-7 can be captured in visible light, where it shows a negative secondary facial image under two different angles.



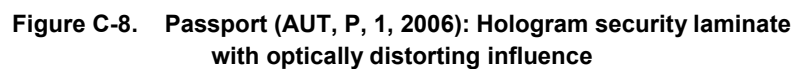
Figure C-7. Passport (LVA, P, 1, 2015): “Negative” personalization through laser engraving under different viewing angles in visible light

- A.8 **Define features that remain stable over the validity period of the MRTD:** Some features tend to wear out over time. Colours of UV patterns, for instance, may fade over the validity period of the MRTD. Overlay glues can make UV patterns considerably lose their sharpness over time, leading to possible inaccurate check results for the feature. It is therefore recommended to define features that remain as stable as possible over the validity period of the MRTD.
- A.9 **Define a utopian document holder for specimen documents:** In order to establish a standardized way to identify specimen documents, it is recommended to set the nationality of the document holder to “UTO” for sample documents.

C.4.1.2 Potentially interfering features for machine authentication

This section deals with features that can possibly interfere with machine authentication (within the context mentioned at the beginning of section C.4.1):

- **Overlapping features:** Overlapping features that are defined without considering their interdependency may negatively interact under the influence of a light source. The diffractive effects of a DOVID may interfere with the acquisition of the data page (see Figure C-8).



- **Features near the upper edge of the document:** Field experience has shown that optical features close to the document upper edge (e.g. in case of an involved booklet) can interfere with machine authentication and may lead to cutting of the captured area. A partial capture of that feature might lead to errors.
- **Features only visible in high resolution:** Based on the current state of technology, most of the current full page readers used in authentication systems support a maximal nominal resolution of 400 ppi providing real optical resolutions that are even below this value. Features that are only visible in high resolution of more than 400 ppi (e.g. microtext, Guilloches) remain undetectable for most of the full page readers currently available on the market (see Figure C-9). However, these features may be verifiable by full page readers in the near future having 600 ppi or more.



Figure C-9. Passport (D, P, 1, 2017): Comparison between a high-resolution image of the microtext (1000 ppi) and an image of the same microtext taken from a full page reader (nominal 400 ppi)

- **Features for which the appearance depends on individual handling:** Some features are potentially not suited for machine authentication because they can considerably change the appearance of the document, i.e. depending on how the page is placed on the document reader, the content of the live image is more or less different. In the following, two of such features are mentioned exemplarily:

- a) *Window feature:* Depending on how the data page and cover are placed on the document reader, it is possible to see the content of the cover through the window, the reader housing, the fingertip or the content of the window is empty (see Figure C-10) leading to incident light.

A single-sided window on ID-1 sized ID cards, i.e. a window feature that can be seen only from the front, is more suitable for machine authentication because the content of the window does not vary in the extent of Figure C-10 and does not obstruct the checking process on the back of the card.

- b) *Transparent full page overlay sheet:* These sheets can lead to different results depending on their presence (or absence) during the image capture process (see Figure C-11).

The difficulties related to the use of these features can be overcome by proper training of the operator (in the case of human-assisted document inspection) or user guidance (e.g. for automated border control).

- **Additional visa pages:** Passports that can be amended with additional visa page inserts can become too massive for ordinary full page reader geometries.

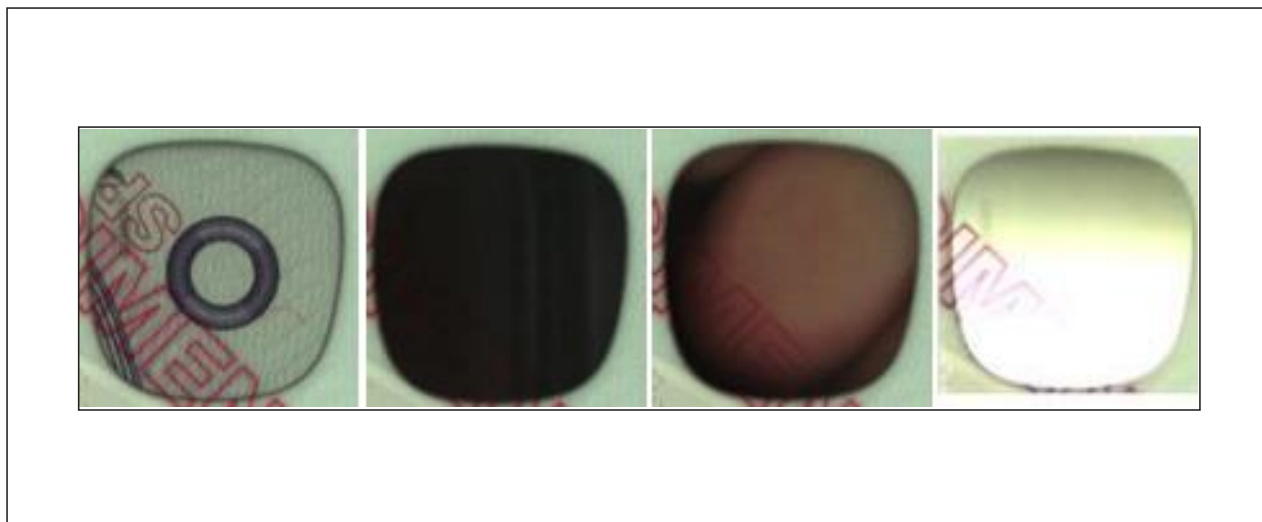


Figure C-10. Passport (SWE, P, 1, 2012): Window feature with variable content; from left to right: inner front cover; reader housing; fingertip; glare induced by incident light



Figure C-11. Passport (BEL, P, 1, 2008); left: plain data page; right: data page with an overlay of the transparent sheet for visual inspection

C.4.2 Manufacturer of Full Page Reader

The reliability of an authentication process not only depends on the set of functionalities provided by the full page reader used in the process; a practical and easy handling of the deployed full page reader also has a direct impact on the quality of the images delivered to the authentication software (see section C.4.3), and therefore automatically influences the overall result of the authentication process. The generic recommendations given in this section should be taken into consideration in the design process of full page readers:

B.1 **Assure proper wavelengths of light spectrum:** Image recording using proper wavelengths is a prerequisite for the appropriate analysis of optical features/properties. For example, a feature which is supposed to be transparent under IR light might become visible on an IR image if the capture is done with an inappropriate wavelength of the corresponding light spectrum. This might lead to faulty live data sets, and therefore to a wrong interpretation of the optical check results. Following wavelengths for the corresponding light spectrums are required for recording images of live data sets:

- VI: spectral range of 400 – 700 nm
- IR: a wavelength within the range of 850 – 950 nm¹³
- UV: 365 nm

Even though some passport readers support shorter UV wavelengths (e.g. 254 and 313 nm), this technology is still not widely spread and is not considered further in this document.

B.2 **Assure minimum resolution:** The quality of the live data sets delivered to the authentication software, measured in pixel per inch (short: ppi), has a direct impact on the accuracy of the authentication process. Field experience has shown that live data sets shall have a minimum resolution of 385 ppi [BSI-TR-03135], although many properties of security printing would profit from an acquisition resolution of 600 ppi or higher.

B.3 **Deliver standard image formats:** Live data sets shall be delivered in the most widely used/supported formats. As an example, the following formats can be used: BMP, JPG (including JPG2000) and PNG.

B.4 **Capture up to ID-3 size:** The full page reader should allow the verification of MRTDs of all sizes specified in Doc 9303. The capture area should therefore be suitable for documents up to ID-3 size. Although this document focuses on full page readers, one should keep in mind that there are application scenarios that do not require the verification of MRTDs of all sizes, but only require the full page reader to scan documents of a specific size (e.g. mobile devices).

B.5 **Assure capturing of all areas with the same quality:** The full page reader shall be able to capture the whole data page with constant image quality. This can, for example, be provided by a homogeneous illumination of the capture surface.

B.6 **Assure short response time and constant intensity:** The light source used for the capture shall have a short response time and shall provide constant light intensity because any deterioration of the light during the authentication process might lead to the generation of unsuitable live data sets.

13. This value was derived from the recommendations defined in Doc 9303, Part 3.

- B.7 **Assure constant image quality:** The light sources of full page readers of the same type might emit light differently due to production-related deviations. In addition, these light source conditions of a full page reader may change their intensity over time. The full page reader shall therefore implement functionalities that help to compensate for deviations, thus providing a constant image quality over time and regardless of the individual device being used. Two examples are given below in order to illustrate how this recommendation can be fulfilled:
- a) The manufacturer provides functionalities to perform colour management and additional calibration (e.g. by means of a calibration card) and customizes the settings of the full page reader (e.g. brightness, exposure time).
 - b) The manufacturer provides in-built sensors allowing for the automatic compensation of deviations.
- B.8 **Allow setting of UV light exposure by authentication software:** Different document models often require different UV light exposure in order to illuminate the document optimally. In this case, the UV light exposure information is stored in the authentication database. Therefore, the full page reader shall allow the setting of the UV light exposure via the authentication software through forwarding of UV settings stored in the authentication database (see section C.4.4.2, item D.8.).
- B.9 **Allow capturing of multiple UV images:** The full page reader should support multiple images captured with different exposure settings, e.g. for a combination of UV features showing a high contrast in luminescence (e.g. high dynamic range).
- B.10 **Allow glare-free images:** Reflections may appear on the captured image and often cover biographical data or security features of the data page. Therefore, the images delivered by the full page reader should contain as little glare as possible. This can be realized by capturing multiple visible (white) light images from different angles or by using diffused illumination.
- B.11 **Provide mechanism to press the document flat onto the capture area:** As stated previously, the user-friendliness of the full page reader directly influences the efficiency and the speed of the authentication process. The full page reader should therefore provide mechanisms to mechanically press the document flat onto the window in order to allow proper captures of the document pages.
- B.12 **Allow single-handed operation:** Additionally, single-handed operation of the reader should be possible and the reading process should be symmetric such that it can be operated by right- and left-handed users.
- B.13 **Provide interactive user guidance:** Interactive user guidance not only increases the comfort of users operating the document reader, it also helps to significantly reduce the duration of the whole authentication process. User guidance is crucial especially for ABC gates typically following a self-service approach: In contrast to stationary document control, the document authentication hardware is used by document holders themselves. Therefore, the document reader should be able to provide interactive user guidance. This can be realized by, for example, delivering a live-stream of the document placed on the capture surface indicating the progress of the image capture (e.g. scanner metaphor). In this way, the user gets direct feedback and can notice much faster if the document is placed correctly on the document reader.
- B.14 **Provide hardware with a high degree of robustness:** Depending on the deployment scenario, full page readers are subject to various external conditions (incorrect handling, humidity, etc.). Over time, these external conditions can more or less damage key components (e.g. scratches on the capture surface) of the full page reader, thus accelerating wear or even breakage of the device. It is therefore recommended to equip the full page reader with robust hardware components.

C.4.3 Manufacturer of Authentication Software

The following proposals are exemplarily based on the technical guideline [BSI-TR-03135] by the Federal Office for Information Security (BSI), as it currently provides the only public sector solution within this area. It is highly recommended to implement the authentication software in accordance with this guideline. The subsequent recommendations should be understood as an extension of [BSI-TR-03135].

Please consider the following technical recommendations for the authentication software:

- C.1 **Enable processing of pre-recorded images:** The authentication software shall also work without hardware and must be able to process pre-recorded images (minimum requirements for the images are given in section C.4.2, items B.1, B.2 and B.3). This functionality is especially important for automated evaluation processes. However, it is necessary to prevent the authentication software from processing pre-recorded images during productive operation, as this can be used as a potential attack vector. Therefore, the usage of the interface used to process pre-recorded images must be restricted to specific configurations (e.g. evaluation setup).
- C.2 **Enable processing of images from different hardware sources:** The software shall be able to process images taken from at least two different full page readers without degradation of verification results. The manufacturer of the authentication software shall therefore provide a specification describing the properties of the images delivered to the authentication software (colour space, contrast, etc.).
- C.3 **Abstract GUI (graphic user interface) from authentication software and hardware:** The optical authentication process of an MRTD is, most of the time, accompanied by the electronic check of the MRTD and a biometric verification with the document holder's face and maybe also the fingerprint. In addition, background checks, e.g. to the Schengen Information System (SIS), have to be performed. Therefore, it is recommended to use an abstraction layer between the GUI and the concrete software and hardware components needed for document, biometric and background checks. In this way, the GUI is independent from these components. Furthermore, the mentioned components can be easily switched without changing the GUI.

In the following sections, the recommendations for manufacturers of authentication software products are structured in accordance with the steps executed during the process of authentication. The document must be detected (see section C.4.3.1), identified (see section C.4.3.2) and subsequently verified (see section C.4.3.3). Furthermore, the whole process must be visualized (see section C.4.3.4) and documented by using appropriate logging mechanisms (see section C.4.3.5).

C.4.3.1 Document detection

For the detection of documents placed on the reader's surface, the following recommendations are given:

- C.4 **Detect document automatically and manually:** The authentication software shall provide mechanisms for automatic and manual triggering of document detection. Manual triggering is especially crucial if automatic document detection does not operate properly.
- C.5 **Compensate rotation and crop captured data page accordingly:** Image capturing is started automatically after the complete personal data page has been placed on the capture surface. The authentication software shall be able to compensate potential rotation and realign the image automatically. Additionally, the authentication shall crop the captured data page accordingly for further processing.

- C.6 **Detect document based on optical presence:** The presence of a document shall be detected only by using its optical properties. The detection process shall still be carried out optically even if an expected chip is absent or malfunctioning (see section C.1.3).

C.4.3.2 Identification

A prerequisite for document verification is the correct identification of the document model. For the identification of a live data-set, the following recommendations are given:

- C.7 **Identify the document model:** It is necessary to identify the document model, regardless of the methods applied, as long as the method applied guarantees a correct identification of the document model. The most common methods used for document model identification are MRZ (including pattern analysis) or pattern analysis only.
- C.8 **Allow fast identification via MRZ:** If the MRZ is used as primary input for document model identification, the authentication software should implement methods and routines allowing for a fast identification process. Two examples are given below in order to illustrate how this recommendation can be fulfilled:
- a) Begin with the capture of the IR image in order to extract the MRZ and derive the document model.
 - b) Because generating images in full resolution can be time-consuming, a fast IR image capture for an early MRZ analysis can be made with a lower resolution than the minimum recommended for the IR image used for identification purposes.
- C.9 **Provide fallback if MRZ is not readable under IR light:** An unambiguous identification of the document model should be possible by all means, as long as the document allows it. Even if the MRZ is not readable under IR light (not ICAO-compliant), the document has to be identified correctly. The software manufacturer therefore must support fallback solutions like performing OCR in the VI image for MRZ analysis if the MRZ is not printed using IR absorbent ink.
- C.10 **Provide an unambiguous document model:** The software manufacturer must provide an unambiguous link to the document model in order to allow access to the authentication data set of this document model in the authentication database.
- C.11 **Enable partial identification:** The authentication software should enable partial identification to be configured in order to considerably reduce false identification and non-identification rates. Nevertheless, the assessment of partial identification requires human interaction and specific knowledge on MRTDs to select the correct document model manually and therefore does not suit every scenario, e.g. ABC gates.
- C.12 **Enable manual identification:** The system should allow for a completely manual choice of the document model – instead of the automatic process and/or by overruling the machine's choice – for cases in which the system's automatic identification process fails. Furthermore, the system should only allow for manual identification if partial identification cannot be performed. Manual identification requires human interaction, specific knowledge on MRTDs and therefore does not suit every scenario (e.g. is not practical for ABC).
- C.13 **Identify ID cards on both sides:** ID-1 sized documents are special in the sense that the MRZ is not on the personal data page (showing the facial image). However, ID-1 sized ID cards are allowed to be positioned on a full page reader with both sides. Therefore, ID-1 sized documents should be identifiable on either side of the document (see recommendation A.4 in section C.4.1.1).

- C.14 **Identify specimen documents:** The authentication software should also identify sample or specimen documents as such and inform the operator accordingly, without interrupting the authentication process (see recommendation A.9 in section C.4.1.1).

Recommendations for the visualization of the identification procedure in the graphic user interface can be found in section C.4.3.4.

C.4.3.3 Verification

Recommendations for verifying documents are given below:

- C.15 **Perform a minimum number of spectrally selective checks:** Spectrally selective check routines must be performed in order to check the absorbent, reflective or luminescent reactions of the live data set. Even if a document could not be identified, following mandatory checks must be performed:
- a) (IR, AB, MR): this check routine, also known as B900 test, can be performed without the selection of a document model; and
 - b) (UV, BR, FU): with certain restrictions on accuracy, this check routine can also be performed on non-identified live data- sets.
- If the document model is identified, the following spectrally selective checks, complementary to the above-mentioned (i.e. checking the optically opposite property), shall be performed additionally:
- c) (IR, TR, ZZ): at least one check that investigates the complementary property “transparent under IR light” compared to (IR, AB, MR) shall be performed; and
 - d) (UV, LU, ZZ): at least one check that investigates the complementary property “luminescent under UV light” compared to (UV, BR, FU) shall be performed.
- C.16 **Perform MRZ consistency check:** Besides the minimum number of spectrally selective checks, plausibility checks (e.g. errors in MRZ, ICAO 3-letter code) must be performed with all documents in order to guarantee minimal security, including in the case of non-identification.
- C.17 **Perform checks in all categories:** The authentication software shall perform check routines in all three categories (material, printing technique and issuing technique) and cover all three light source images (see recommendation A.3 for document designers in section C.4.1.1).
- C.18 **Verify chip presence:** If the existence of an RF chip is expected for a particular document model, which is not working or seems not existent, this must clearly raise a warning in addition to the optical results (see section C.1.3).
- C.19 **Check dynamic patterns:** It is recommended to provide algorithms that compare individual dynamic patterns (e.g. photo, signature). For instance, the facial image could be compared with a secondary facial image located on the data page (see Figure C-12 and recommendation A.7 for document designer in section C.4.1.1).



Figure C-12. Passport (EST, P, 1, 2013): Verify the facial image in the visible light image against the one printed with UV luminescent ink

C.20 **Combine check routines if necessary:** Some features can be checked by different check routines. For example, features behaving differently under different light sources serve as input for separate check routines (see recommendation A.5 for document designers in section C.4.1.1). It is therefore recommended to combine the results of such check routines logically or to combine the check scores by a decision function. For instance, a composite check routine could still output a pass-decision, even if the score of one basic check routine is slightly below its threshold.

C.21 **Perform redundant check routines on multiple positions:** For features that appear more than once on the document, the corresponding check routine should be also performed on multiple positions on the live data set. For example, for the document model (D, P, 1, 2007) in Figure C-13, the UV eagle-pattern can be checked on multiple positions. A check routine performed on multiple positions is called a redundant check routine.

In addition to multiple appearances of a feature, some features are statistically more subject to falsification than others. In many cases, counterfeiters, for example, change the date of expiry or substitute the facial image. It is therefore recommended to perform check routines, which are able to detect attacks on these “sensitive” features, redundantly.

C.22 **Perform redundant check routines on multiple UV colours:** Execution of redundant check routines is also recommended for UV features, which appear in multiple colours on the document (see recommendation A.6 and Figure C-5 for document designers in section C.4.1.1).

C.23 **Link and check both pages of an ID card:** A second page scan shall be linked automatically to the previous scan if both are from the same ID document. In addition, it is recommended to verify both sides of ID-1 sized documents in order to get an overall verification result for both sides, and maximize the number of optical features used for the authentication of the document (see recommendation A.4 for document designers in section C.4.1.1).

C.24 **Allow multiple pages cross checking of personal data:** Personal data of the document’s holder should be identical, regardless of the page on which they appear. For instance, personal data on the data page of a passport are supposed to be identical to personal data on a potentially existing visa. It is therefore recommended to perform multiple sides cross checks if, for example, personalized contents are expected to be identical/redundant.



Figure C-13. Redundant pattern verification

- C.25 **Perform check routines dependent on significance:** It is not always necessary or meaningful to perform a whole set of check routines just because it is technically possible to apply them on the live data set. A more efficient approach would be to assess the relevance of the checks in correlation with the verification process. Some check routines are more susceptible to deliver helpful results than others, and deliver information leading to a more accurate analysis of the verification results. Therefore:
- a) the checks should be conducted by order of their relevance/significance and the results immediately shown in the graphical user interface (see Visualization in section C.4.3.4); and
 - b) the results of the checks should be combinable by decision functions different from only performing a simple logical AND-combination (i.e. using weighted check results). Decision functions have to be logged in the XML catalogue (see recommendation C.46 for Logging in section C.4.3.5).
- C.26 **Consider feature deviation:** Security features may change over time because of wear and tear of the MRTD, e.g. some UV colours may degrade. However, these features have to be checked with constant reliability during the MRTD validity period. Therefore, tolerances of check routines should be considered.

- C.27 **Detect generic attacks:** In addition to the pure verification of document feature properties, the authentication software should provide tools for the detection of traces of generic attacks, such as “paper damage”, “cut marks”, “photo substitution” or “lamine wrinkles” if the illumination conditions allow for it. The scheme for generic check routines can also be applied to checks detecting forgeries.

Recommendations for the visualization of the verification procedure in the graphic user interface can be found in the next section.

C.4.3.4 Visualization

Visualization of the authentication results is the process by which the user of the authentication system is provided with visual feedback and information about the results of the authentication process. The visualization should be realized in the form of a graphic user interface (short: GUI).

The GUI for the visualization of optical check results should provide the user only with the most relevant information in order to be able to determine irregularities at first sight. This information is divided below into the so-called “process summary area” (see C.29), the so-called “optical overview area” (see C.30) and more detailed information in the so-called “optical details area” (see C.35).

Recommendations for choosing eligible information and displaying it in a compact and minimalistic way are made in the following:

- C.28 **Display all document checks in one GUI:** The GUI may be an integral part of the delivered authentication software or be delivered and operated in a separate abstraction layer. Independent from this, it is recommended to display all types of performed checks (electronic, biometric, optical and background) in one GUI. This considerably reduces the effort of the system’s operator and facilitates the assessment of the check results due to a better overview of the process. Furthermore, special focus should be placed on occurring anomalies or irregularities (see recommendations C.41 to C.45).
- C.29 **Always show process summary area:** This area should show the overall result of the optical authentication and must be displayed to the user on the start page (see Figure C-14 for exemplary stationary border control GUI). This area should always be visible to the user, independent of further selected details on specific verification results. The process summary area should show one overall result of the optical authentication with a traffic light symbol. Furthermore, the area should display a cropped facial image of the data page next to the facial image stored on the chip, if present.
- C.30 **Display optical overview area on start page:** This area shows an overview of the optical check routines and should be displayed to the operator on the start page.
- a) This area should contain the following information (see Figure C-14):
- The VI (visible light) image of the document per default. The operator staff should be able to change the default image to IR or UV, depending on the specific requirements.
 - The personal data of the document holder contained in the MRZ: last name, first name, date of birth, sex, nationality and optional data.
 - The document data: document type, document number, issuing State or organization, date of expiry and optional data.



- The extracted MRZ to allow comparison of the extracted MRZ with the MRZ printed on the document.
 - A button to allow the manual triggering of the document reading process.
 - A cropped facial image of the data page next to the facial image stored on the chip, if present, (see section C.1.3) to allow easy detection of photo substitution.
- b) It is also recommended to display the following information in the optical overview area:
- The age of the document holder as well as the remaining validity period. This information can be recognized easier and faster by the operator than the dates contained in the MRZ.

- C.31 **Select more details via one click:** From the optical overview area, the operator should click only once to obtain access to an additional page containing more details of the optical verification: the *optical details area* (see C.35). For instance, in the exemplary GUI in Figure C-14, more details can be retrieved by clicking on the area “Document data”.
- C.32 **Show results with traffic lights:** As specified in [BSI-TR-03135], the results of the optical check processes should be displayed using a traffic light system (e.g. red/green/yellow/grey lights). In addition to the colour, the traffic lights should contain unambiguous symbols indicating the verification results (e.g. check, cross). This is especially important for users with red-green colour blindness. Furthermore, the representation scheme should be the same for all areas of the GUI (e.g. negative results are all displayed with the same symbol and colour).
- C.33 **Provide result mapping according to [BSI-TR-03135]:** The traffic light system should provide a consistent mapping to the following verification results: **successful**, **failed**, **undetermined** and **not supported/not performed** defined in [BSI-TR-03135]. Table C-2 gives an overview of the mapping used in this document. This mapping is based on [BSI-TR-03135] and should be used for practical implementations of the GUI.

Table C-2. Traffic light system mapping

<i>Verification result</i>	<i>Traffic light colour</i>
Successful	green
Failed	red
Undetermined	yellow
Not supported/not performed	grey
Aborted	black

- C.34 **Provide minimalistic result mapping:** Alternatively, a minimalistic mapping consisting only of the colours green and red may be used for the traffic light system. As displayed in Table C-3, the colour green can be used to display a positive verification result, whereby the colour red can be used to display any other verification result.

Table C-3. Minimalistic traffic light system mapping

<i>Verification result</i>	<i>Traffic light colour</i>
Successful	green
Failed	red
Undetermined	
Not supported/not performed	grey
Aborted	

A further reduction of the mapping would be to display the last four verifications in Table C-3 results with red.

C.35 Display details in a dedicated *optical details area*: The details view is only available when expanding the area and contains detailed information about the different processes and results of the optical authentication. It is meant to provide the user with the information needed to perform further analysis, if required.

a) The optical details area should contain the following information (see the example in Figure C-15):

- The VI, the IR and the UV image of the document. The three images should be presented next to each other.
- The proprietary document model identifier of the manufacturer of the authentication software, if the document model identifier proposed in section C.2.1 cannot be displayed in generic form.
- A list of selected check routines, showing their results via traffic lights: In the context of border control, the border control guard should only be confronted with the most important verification information in a human readable form. Therefore, the results of the generic check routines are summarized in three categories, described by easy and understandable terms, as follows:
 - MRZ IR readability: The corresponding traffic light shows the result of the generic check routine (IR, AB, MR).
 - UV brightness: The corresponding traffic light shows the combined result of the generic check routines (UV, BR, FU), (UV, BR, VZ), (UV, BR, PH) and (UV, BR, MR).
 - Pattern check: The corresponding traffic light shows the combined result of the remaining generic check routines that have been performed for this document (see section C.3).
- In addition, the results of the following mandatory checks according to [BSI-TR-03135] should be visualized using traffic lights:
 - MRZ consistency
 - Date of expiry



Figure C-15. Exemplary view for the optical details area

- The extracted MRZ.
 - During the authentication process, the data elements extracted from the optically read MRZ are compared with the MRZ elements stored on the chip (if available). The data elements of the optical MRZ should be displayed with the result(s) of this comparison. The result(s) should be displayed with the same traffic light system used throughout the GUI.
- b) It is also recommended to display the following information in the optical details area:
- The identified document model in human readable form, e.g. D 2007. Using the standard document model identifier of [BSI-TR-03135] could probably cause more confusion than clarity among the users of the GUI. The representation of the document model identifier in the GUI should therefore be specified on the basis of common agreement with the operator of the authentication system.
 - Both the data elements extracted from the optically read MRZ and those extracted from the chip should be displayed next to each other (see section C.1.3).

- C.36 **Guide users during document reading:** During the reading process, a hint should be given to the user not to remove the document before the reading process is complete (see recommendation B.13 in section C.4.2). For example, this hint can be realized as a process indicator displayed during the reading process. This hint can be placed upon the process summary area.
- C.37 **Display information from central databases:** If the authentication process requires queries to a background database system, the optical details page may show the information retrieved from this system if it is correlated to optical authentication, e.g. the facial image retrieved from the central visa information system (C-VIS).
- C.38 **Provide homogenous layout for MRTDs:** The layout of the GUI should be the same for all types of machine readable documents (e.g. passports, national ID cards, resident permits, etc.). For instance, the optical authentication information obtained from both sides of an ID-1 card should be displayed analogous to the visualization of the passport verification (one process summary area, one optical overview area and one optical details area).
- C.39 **Guide operators through multi-page verification:** The verification of both sides of an ID-1 sized document demands interactive guidance for the user. For a card put on the capture surface, the user should get a hint that the presentation of the second page could be the next step.
- C.40 **Allow comparison of passport and visa/electronic residence permit (eRP) content:**
- a) *Guide operators through multi-page verification:* During the verification of a passport, the user should be warned that the passport holder requires a visa/eRP in order to cross the border. This can, for example, be realized with a prompt on the overview page. This prompt should be an indication for the user that the presentation of the visa/eRP to the full page reader is a possible next step.
 - b) *Keep passport information available:* During optical visa/eRP authentication, the overview and details areas showing the passport authentication results must still be available, in order to be able to switch to over to these details, if desired.
 - c) *Allow comparison in process summary area:* Besides the optically captured facial image from the data page, the facial image on the visa/eRP should be displayed (see example in Figure C-16). In addition, the chip image of the passport holder (if available, see section C.1.3) and the image retrieved from a visa information query system (e.g. the European VIS) or from the eRP chip, should be displayed (see C.37).
 - d) *Allow comparison in visa optical details area:* During the authentication process, the data elements Last Name, First Name, Date of birth, Sex and Nationality extracted from the optical MRZ of the visa are compared with these MRZ elements on the data page of the passport and/or the chip (see section C.1.3). The data elements of the visa MRZ should be displayed with the result(s) of this comparison. The result(s) should be displayed with the same traffic light system used in the rest of the GUI. The age of the document holder as well as the remaining validity period of the visa should also be displayed in this area, because this information can be recognized easier and faster by the operator than the dates contained in the MRZ.

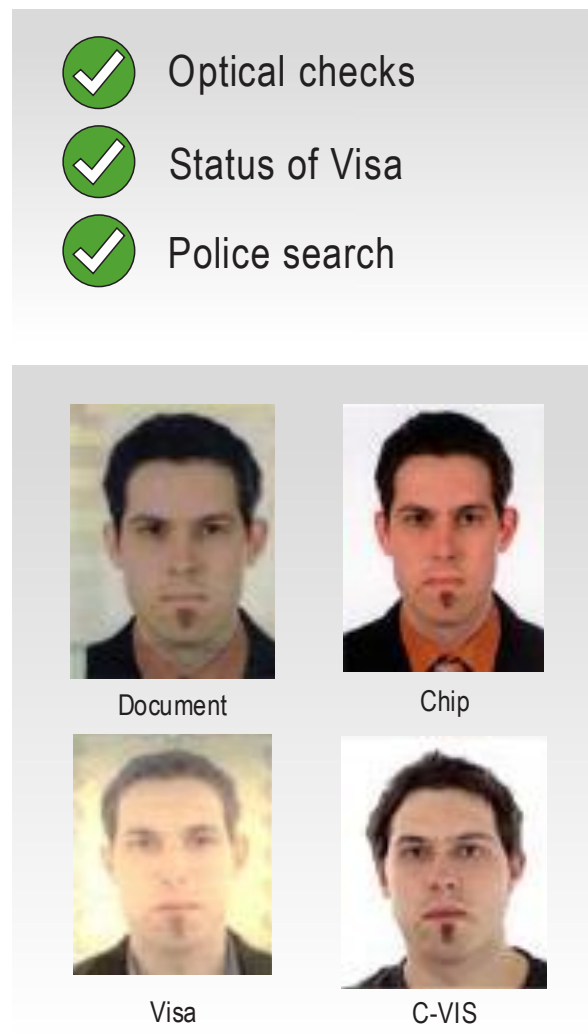
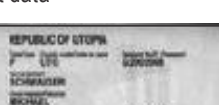
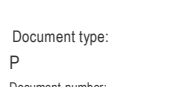



Figure C-16. Exemplary view for the comparison of passport and visa

Recommendations for displaying errors are given below:

- C.41 **Highlight only irregularities:** It is required to make use of colour highlighting only to signalize irregularities in the authentication process (e.g. example for check failure in Figure C-14). This approach considerably helps the user in recognizing the most relevant information delivered by the GUI at first sight.
- C.42 **Display errors in process summary area:** If a document is not authentic, the traffic light for the optical authentication must show a negative overall result. If the document model could not be identified, the traffic light for the overall optical authentication result should show a warning.
- C.43 **Display errors in optical overview area:** If errors occur because of optical irregularities, they should be displayed in the following way:

- a) *Irregularity of spectrally selective property:* If an error occurs because of a spectrally selective check routine, the image in the corresponding light spectrum should be displayed in the optical document data area instead of the standard VI image (e.g. if (UV, BR, FU) fails, the UV image should be displayed). In addition, the optical overview area should be surrounded by a red frame.
- b) *MRZ not consistent:* If an error occurs because of the MRZ consistency check, the corresponding part of the extracted MRZ, including the check sum, should be highlighted in red. In addition, the corresponding inconsistent personal data and the area containing the personal data should be highlighted in red (e.g. see Figure C-17). The operator should be able to manually correct the MRZ and trigger another reading process manually via a button.

Document data	Personal data
 <p>Document type: P</p> <p>Document number: G20002068</p> <p>Country code: UTO</p> <p>Date of expiry: 17.11.19</p> <p>valid for 1250 days</p> <p>Optional data: 1122334455</p>	<div style="display: flex; justify-content: space-around;">   </div> <p>Last name: SCHWAIGER</p> <p>First name(s): MICHAEL</p> <p>Date of birth: 04.02.85 ⚠️</p> <p>Sex: M</p> <p>Nationality: AUT / Austria</p>
<p>IR image of the data page</p>	<p>Document Chip</p>


Machine readable zone (MRZ)	Document check results
<pre>P<UTOSCHWAIGER<<MICHAEL<-----
G20020D68<OAUT6502040>X19111721122334455<<<84</pre> <div style="text-align: center;">  Read document again </div>	<p>Document (opt.) ⚠️ MRZ Error!</p> <p>Chip (electr.) ⚠️ Chip access not possible!</p>

Figure C-17. Exemplary view for error visualization: MRZ consistency

- c) *Document expired*: If the document is expired, the date of expiry should be highlighted in red.
- d) *Chip not detected*: If an electronic chip is expected in the identified document model, but it cannot be detected (see section C.1.3), a warning should be displayed. The warning symbol should clearly be distinguishable from the traffic light symbols used to display the check results (e.g. yellow triangular warning sign).

C.44

Display errors in optical details area: If errors occur because of optical irregularities, they should be displayed in the following way:

- a) *Document not identified*: If the document model could not be identified, a warning symbol should be displayed as result of the document model identification. The warning symbol should be clearly distinguishable from the traffic light symbols used to display the check results (e.g. yellow triangular warning sign, see Figure C-18). A warning text should be displayed next to the warning symbol, e.g. "Document model could not be identified".

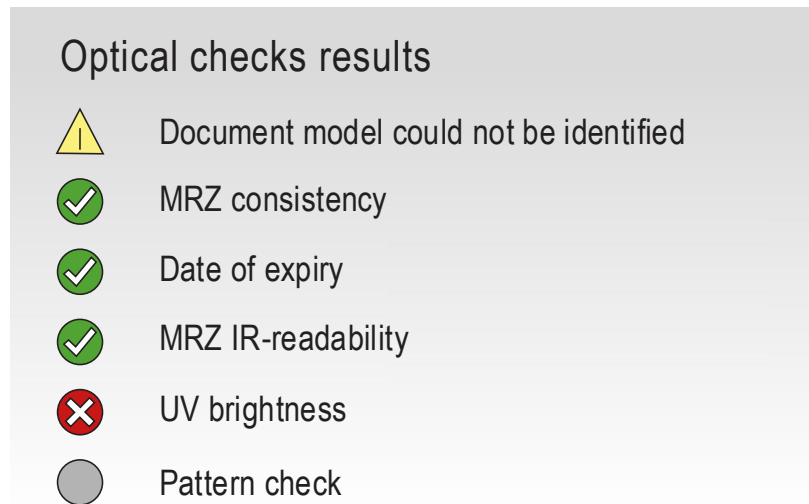


Figure C-18. Exemplary for view error visualization: Document model and negative verification check


- b) *Negative verification check:* For every verification check displayed in the details page (see Figure C-18), a negative check result should lead to a red traffic light. The respective features of the failed spectrally selective check should be highlighted on the corresponding image, e.g. by showing a red rectangle surrounding the searching area of the feature (e.g. the MRZ of the IR image due to a negative MRZ IR readability).
- c) *Inconsistent chip information:* For every MRZ data that is not the same for the optical data page and the chip (see section C.1.3), the inconsistent pair of information should be displayed in red (with a warning symbol, see Figure C-19).
- d) *Inconsistent overall check digit:* Errors related to the overall check digit (see Doc 9303, Part 3, Chapter 4 ("MRZ")) could be an indication for a manipulation of the check digits, e.g. insertion of incorrect check digits in the MRZ in order to prevent the execution of access control mechanisms (e.g. Basic Access Control (BAC)). For every failed check on the optical MRZ, the captured check digit of the corresponding MRZ element should be displayed next to the expected check digit.

Personal data
MRZ DG1

Last name:
SCHWAIGER SCHWAIGER

First name:
MICHAEL MICHAEL

Date of birth:
05.02.85 05.02.85

Sex:
 F M

Nationality:
AUT AUT

Document type:
P P

Document number:
G2002068 G2002068

Country code:
UTO UTO

Date of expiry:
17.11.19 17.11.19

Optional data:
1122334455 1122334455

Figure C-19. Exemplary view for error visualization: MRZ data

C.45

Display errors of passport and visa/eRP comparison: If at least one of the comparable MRZ data is not the same for the passport and the visa/eRP, this inconsistency should be displayed in the following way:

- a) *Visa/eRP overview area:* The comparable MRZ data (Last Name, First Name, Date of Birth, Sex, and Nationality) of the passport must be displayed in the visa/eRP overview page next to the MRZ data of the visa/eRP. Every inconsistent pair of information should be displayed in red with a warning symbol (see example in Figure C-20).



 Personal data	Passport data
	
Last name: LIN	Last name: SCHWAIGER
First name(s): VALERY	First name(s): MICHAEL
Date of birth: 30.04.73	Date of birth: 05.02.85
Sex: M	Sex: M
Nationality: CHN / China	Nationality: D / Germany
Visa	

Figure C-20. Exemplary view for the comparison of the visa and the passport data

- b) *Visa/eRP details area*: For every MRZ data which is not the same for the visa/eRP and the passport, the inconsistent pair of information should be displayed in red (with a warning symbol).

C.4.3.5 Logging

For the logging of the optical machine authentication process, the following recommendations are applicable:

C.46 **Log XMLs according to [BSI-TR-03135]**: Logging must be realized according to the XML schemes defined in [BSI-TR-03135] which also contain, besides the detailed optical results, the results of the electronic and combined (optical and electronic) verification of a document. For instance, this allows:

- Logging the generic check routine identifier of a proprietary check routine (see section C.3).
- Putting check routines in silent mode, i.e. the routine is executed and its results are logged, but the check result is not taken into account in the overall result of the authentication process. This is of particular importance if new check routines, algorithms or thresholds are evaluated.

Further information on the spectrally selective checks might be required by the operator for evaluation purposes and to update the underlying database to guarantee consistent and high quality authentication results over time. This information is the same for all documents of a specific document model; for example the decision function, textual explanations on the check routines, and the image section from the reference database. Therefore, the manufacturer must supply this XML catalogue in machine readable form according to the defined XML scheme in [BSI-TR-03135], which summarizes all necessary information on the spectrally selective verification checks. Due to the format, the catalogue can be integrated into the evaluation of the results.

- C.47 **Allow logging of optional image data:** The XML schemes defined in [BSI-TR-03135] allow, but not directly regulate, the storage of the processed live data set as well as cropped images displaying the search area of check routines. The authentication software must be able to store the mentioned image data in the XML data structure. Recommendations for the operational manager for storing image data in compliance with the prevailing data protection regulations are made in section C.5.
- C.48 **Provide anonymization capabilities:** The software should provide capabilities to anonymize the live data set directly after the authentication, in order to be allowed to permanently store the images for further inspection. Please refer to section C.5.1 for recommendations for anonymization.

C.4.4 Manufacturer of the Authentication Database

As described in sections C.2.1 and C.2.2, the authentication database contains distinct sets of check routines for different document models. It directly interacts with the authentication software to which it delivers the set of check routines corresponding to the identified document model. Because of new established document models and permanently arising counterfeits, a well-maintained, flexible authentication database is crucial. In the following sections, the recommendations for the database are summarized concerning the updating process (see section C.4.4.1) and the configurability of the database (see section C.4.4.2).

C.4.4.1 Update

The following recommendations are given for manufacturers of authentication databases regarding the update process:

- D.1 **Exchange information about new document models or counterfeits:** The manufacturer of the authentication database shall establish a dedicated communication channel with the operational manager for secure transfer of data- sets of information on new document models that should be inserted in the database. The manufacturer shall exchange information about new document models with the operational manager by using one of the following methods:
- a) *Exchange via original sample:* In this case, an original sample of the new document model or the counterfeit must be provided for definition and upload of the corresponding set of check routines in the database. The established communication channel and associated processes must take into account national legislation on data protection (see section C.5).
 - b) *Exchange via capture software:* In this case, capture software has to be provided to the operational manager in order to generate a suitable live data set of new document models or counterfeits. This data set must at least contain one VI, UV and IR image. Ideally, several images of one light spectrum should be generated by this capture software (analogous to high dynamic range photography). The data set is transferred to the manufacturer for definition of a corresponding set of check routines to be included in the next edition of the database. The manufacturer must recommend a list of suitable capture devices for this purpose.
- D.2 **Update database regularly:** The authentication database shall enable regularly scheduled updates (minimum every 3 months). The authentication database shall also enable ad hoc updates on special (urgent) request:
- a) if the manufacturer obtained new information about genuine documents or counterfeits and updated the document database based on this information in cooperation with the operational manager (see D.1 a), or

- b) if the operator generated a live data set with the capture software (genuine document or counterfeit) and sent it to the manufacturer (see D.1 b).
- D.3 **Provide incremental updates:** By default, the manufacturer of the authentication database must supply the operator with full version updates. Incremental updates should also be distributed in order to save time and bandwidth.
- D.4 **Provide sufficient documentation on changes:** At update delivery, the manufacturer of the authentication database must provide sufficient documentation about the changes made in the database.

C.4.4.2 Database content and configurability

In this section, a list of recommendations for manufacturers of authentication databases regarding the content and configurability of the database are given:

- D.5 **Provide reduced content:** The authentication database should be available with different scope and therefore customizable for different scenarios. For instance, commercial scenarios are limited in scope and the type of checked documents is generally very specific (e.g. document authentication at car rental companies). It is therefore recommended to provide authentication databases that specifically address the needs of commercial scenarios via reduced complexity. By providing a database with reduced contents, the manufacturer ensures that it remains cost efficient and easy to integrate into different setups.
- D.6 **Allocate checks with significance levels:** Checks should be allocated with a significance level to allow the authentication software to perform the checks in order of significance (see recommendation C.25 a) for manufacturers of authentication software referred to in section C.4.3).
- D.7 **Provide different operational modes:** Different usage scenarios require different levels of security concerning the acceptance or rejection of a document. Stationary border control, for instance, relies on high security, whereas commercial scenarios focus more, in general, on high convenience for the document's holder. Therefore, the authentication database should provide at minimum two different operational modes for high security and for high convenience.
- D.8 **Provide document model specific UV light exposure information:** As mentioned in section C.4.2, different document models often require different UV light exposure. For example, certain document models require a longer UV illumination in order to properly check specific features under UV light. Therefore, the authentication database should contain information about the UV exposure settings required for corresponding document models, so that the authentication software can automatically configure the full page reader accordingly (see section C.4.2, item B.8).
- D.9 **Support server-based setup:** It is recommended to supply an authentication database that can also be operated in a server-based setup. In this case, different authentication software would be able to access a single authentication database. Additionally, two or more authentication databases could be operated as a cluster being accessible for several authentication software products.

C.4.5 Manufacturer of the Reference Database

Even though the reference database is not directly a part of the authentication system (see section C.2.1), it can be used as a complementary source of information if the authenticity of a document cannot be clearly determined on the basis of the machine authentication. In this case, the reference database is able to support the operator with detailed information on the corresponding document model, e.g. with high quality images of features, textual explanations and information on

common counterfeits (aimed for 2nd-line/back-office inspection). An example of a reference database provided by the European Union is the so-called FADO system (False and Authentic Documents Online). The publicly available counterpart of the FADO is the so-called PRADO¹⁴ (Public Register of Authentic Documents Online).

In case of its usage, there are some practical implications that need to be considered by the manufacturer of the reference database. This section addresses these implications in the form of recommendations:

- E.1 **Provide automatic output:** The reference database shall receive and process an unambiguous link to a document model as input from the identification process. It should also provide a reference data set corresponding to the link as output.
- E.2 **Allow manual selection of data set:** In addition to the automatic selection of a reference data set, an operator shall also be able to manually search for and choose a specific data set via a GUI.
- E.3 **Provide extensive information on authentic documents:** The reference database shall contain information on authentic documents and may be accompanied by linked descriptions of typical forgeries. Specific properties of the reference document models shall be described in detail and every content shall have a textual description.

In this context, it is worth mentioning that a database such as EDISON-TD can also be taken into consideration. In order to increase the usage of commercial databases, the mechanisms described in recommendation D.1 can be used.

C.4.6 Operational Manager

The so-called *operational manager* is the organization responsible for the administration and the management of all processes related to the operation of the authentication infrastructure. Operators are members of the operational manager's staff who directly interacts with the authentication system.

The concrete realization of the planned operation depends on the inspection scenario. Exemplary scenarios are:

- **Stationary border control** (in short SBC): In this case, governmental authorities for stationary border control assume the role of the operational manager (e.g. border police). Usually for this setup, operators are very familiar with optical document verification. The inspection scope is immense due to the high number and diversity of the checked documents. Furthermore, the system requires extensive interaction and assessment of the operators who directly interact with both the system and the document's holder.
- **Automated border control via ABC gates** (in short ABC): For this scenario, governmental authorities for ABC gates also assume the role of the operational manager, which often more focus on fast document authentication than on extensive document authentication. The operators in this case are also well-trained border guards and usually supervise a set of ABC gates respecting minimalistic visualization. In contrast to stationary border control, the system is used by travellers and therefore needs extensive user guidance, which is out of the scope of this manual.
- **Document authentication for commercial purposes** (in short CP): In this case, commercial entities assume the role of the operational manager (e.g. in banks). Contrary to the previous mentioned scenarios, the operators are usually not familiar with optical document verification and the inspection scope is generally smaller than for border control.

14. <http://prado.consilium.europa.eu/en/homeindex.html>.

The capabilities of the components acquired must be in line with the needs of the operational manager and the requirements of the deployment scenario. In this section, the recommendations for the manufacturers of full page readers (see section C.4.2), of authentication software (see section C.4.3), of authentication databases (see section C.4.4) and of reference databases (see section C.4.5) are mapped to the usage scenarios. Recommendations for monitoring in compliance with data protection regulations are made in section C.5.

For each scenario, the following Table C-4 summarizes the reasonable usage of the recommendations for the manufacturer of full page readers.

Table C-4. Recommendations for full page readers classified by inspection scenarios

<i>Manufacturer of full page readers</i>				
<i>No.</i>	<i>Short description</i>	<i>Usage scenario</i>		
		<i>SBC</i>	<i>ABC</i>	<i>CP</i>
B.1	Assure proper wavelengths of light spectrum	X	X	X
B.2	Assure minimum resolution	X	X	X
B.3	Deliver standard image formats	X	X	X
B.4	Capture up to ID-3 size	X	X	X
B.5	Assure capturing of all areas with the same quality	X	X	X
B.6	Assure short response time and constant intensity	X	X	X
B.7	Assure constant image quality	X	X	
B.8	Allow setting of UV light exposure by authentication software	X	X	
B.9	Allow capturing of multiple UV images	X		
B.10	Allow glare-free images	X	X	
B.11	Provide mechanism to press the document flat onto the capture area	X	X	X
B.12	Allow single-handed operation	X	X	X
B.13	Provide interactive user guidance		X	X ¹⁵
B.14	Provide hardware with a high degree of robustness	X	X	X

15. The way user guidance is understood depends highly on the commercial use case.

For each scenario, the following Table C-5 summarizes the reasonable usage of the recommendations for the manufacturer of authentication software products.

Table C-5. Recommendations for authentication software classified by inspection scenarios

<i>Manufacturer of authentication software</i>				
<i>No.</i>	<i>Short description</i>	<i>Usage scenario</i>		
		<i>SBC</i>	<i>ABC</i>	<i>CP</i>
C.1	Enable processing of pre-recorded images ¹⁶	X		
C.2	Enable processing of images from different hardware sources	X	X	X
C.3	Abstract GUI (graphic user interface) from authentication software and hardware	X	X	X
Document detection				
C.4	Detect document automatically and manually	X	X ¹⁷	
C.5	Compensate rotation and crop captured data page accordingly	X	X	X
C.6	Detect document based on optical presence	X	X	X
Identification				
C.7	Identify the document model	X	X	X
C.8	Allow fast identification via MRZ	X	X	X
C.9	Provide fallback if MRZ is not readable under IR light	X	X	X
C.10	Provide an unambiguous document model	X		
C.11	Enable partial identification	X		
C.12	Enable manual identification	X		
C.13	Identify ID cards on both sides	X	X	X
C.14	Identify specimen documents	X	X	X
Verification				
C.15	Perform a minimum number of spectrally selective checks	X	X	X

16. This recommendation is important for evaluation of authentication software products.

17. Manual document detection is not applicable in the automated border control scenario.

Manufacturer of authentication software				
No.	Short description	Usage scenario		
		SBC	ABC	CP
C.16	Perform MRZ consistency check	X	X	X
C.17	Perform checks in all categories	X	X	X
C.18	Verify chip presence	X	X	X
C.19	Check dynamic patterns	X	X	X
C.20	Combine check routines if necessary	X	X	X
C.21	Perform redundant check routines on multiple positions	X		X
C.22	Perform redundant check routines on multiple UV colours	X		
C.23	Link and check both pages of an ID card	X	X	X
C.24	Allow multiple pages cross checking of personal data	X	X	X
C.25	Perform check routines dependent on significance	X	X	X
C.26	Consider feature deviation	X	X	X
C.27	Detect generic attacks	X	X	X
Visualization				
C.28	Display all document checks in one GUI	X	X	X
C.29	Always show <i>process summary area</i>	X	X	X
C.30	Display <i>optical overview area</i> on start page	X		
C.31	Select more details via one click	X	X	
C.32	Show results with traffic lights	X	X	X
C.33	Provide result mapping according to [BSI-TR-03135]	X	X	X
C.34	Provide minimalistic result mapping	X	X	X
C.35	Display details in a dedicated <i>optical details area</i>	X		
C.36	Guide users during document reading	X	X	X
C.37	Display information from central databases	X		

Manufacturer of authentication software				
No.	Short description	Usage scenario		
		SBC	ABC	CP
C.38	Provide homogenous layout for MRTDs	X		X
C.39	Guide operators through multi-page verification	X		
C.40	Allow comparison of passport and visa/electronic residence permit (eRP) content	X		
C.41	Highlight only irregularities	X	X	X
C.42	Display errors in process summary area	X	X	X
C.43	Display errors in optical overview area	X		
C.44	Display errors in optical details area	X		
C.45	Display errors of passport and visa/eRP comparison	X		
Logging				
C.46	Log XMLs according to [BSI-TR-03135]]	X	X	X
C.47	Allow logging of optional image data	X	X	X
C.48	Provide anonymization capabilities	X	X	X

For each scenario, the following Table C-6 summarizes the reasonable usage of the recommendations for the manufacturer of authentication databases.

Table C-6. Recommendations for authentication databases classified by inspection scenarios

<i>Manufacturer of authentication database</i>				
<i>No.</i>	<i>Short description</i>	<i>Usage scenario</i>		
		<i>SBC</i>	<i>ABC</i>	<i>CP</i>
D.1	Exchange information about new document models or counterfeits	X	X	
D.2	Update database regularly	X	X	X
D.3	Provide incremental updates	X	X	X
D.4	Provide sufficient documentation on changes	X	X	X
D.5	Provide reduced content			X
D.6	Allocate checks with significance levels	X	X	X
D.7	Provide different operational modes	X	X	X
D.8	Provide document model specific UV light exposure information	X	X	X
D.9	Support server-based setup	X	X	X

For each scenario, the following Table C-7 summarizes the reasonable usage of the recommendations for the manufacturer of reference databases.

Table C-7. Recommendations for reference databases classified by inspection scenarios

<i>Manufacturer of reference database</i>				
<i>No.</i>	<i>Short description</i>	<i>Usage scenario</i>		
		<i>SBC</i>	<i>ABC</i>	<i>CP</i>
E.1	Provide automatic output	X		
E.2	Allow manual selection of data set	X		X ¹⁸
E.3	Provide extensive information on authentic documents	X		X ¹⁸

C.5 MONITORING IN COMPLIANCE WITH DATA PROTECTION

An optical authentication process may lead to an unexpected result due to one of the following reasons:

- A counterfeit has been detected.
- A counterfeit has been classified as authentic.
- An authentic document has been classified as counterfeit.
- A handling error of the full page reader occurred, e.g. the document has been removed from the reader during authentication.
- The document model could not been identified.

In these cases, it is crucial for the operational manager to be able to analyse the reason for the wrong decision. Thus, the information gained in the authentication procedure — possibly including personal information — has to be logged and analysed. This directly raises data protection issues because personal data is not allowed to be stored, even encrypted, without the consent of the document's holder or a determined reason. The following recommendations can be made for the operational manager:

- F.1 **Log authentication reporting:** Reporting information of the authentication procedure without personal data (e.g. identified document model, authentication results, check routine results, etc.) must be logged according to [BSI-TR-03135]. The live data set, the MRZ and the VIZ are therefore excluded from logging. Such reporting information is not time critical and can be used for statistical analyses.

18. Considering CP, it is important to adjust the level of knowledge, depending on the use case.

- F.2 **Set up feedback loop to manufacturer:** Regular feedback from the operation can be used to optimize the authentication software. Therefore, the reporting information clarified in F.1 should be forwarded to the manufacturer of the authentication software regularly.
- F.3 **Store unaltered live data set if eligible:** Analysis of errors can be done best on the same live data set that has been provided for authentication. It is therefore recommended to store unaltered live data sets in the XML scheme defined by [BSI-TR-03135], if this can be done with consent to data privacy concerns. The following logging possibilities including images exist:
- a) *Store live data set with consent of document holder:* If the scenario allows for it, the live data set used for authentication can be stored, if the consent of the document holder has been collected first in written form. This way is only conceivable for scenarios allowing a communication with the document holder, such as pilots, and not for permanent operation. Furthermore, the live data sets have to be deleted irretrievably after a contractually defined time period.
 - b) *Store live data set in case of error:* Personal data is allowed to be stored for a contractually defined time period, if a determined reason for the storage exists, e.g. if an error occurred during authentication. If the scenario allows, this time period can be used for error analysis on the unaltered live data set, which has to be deleted irretrievably afterwards.
 - c) *Log privacy friendly regions:* To avoid data privacy concerns and at the same time preserve rough analysis possibilities, only “privacy-friendly” cropped images displaying the search area of check routines can be logged. These regions of interest must not contain the whole facial image, the MRZ or the VIZ and can be stored for all authentication processes with no time restriction in the XML scheme defined by [BSI-TR-03135].
- F.4 **Anonymize images if eligible:** Another proposition to avoid data privacy concerns, but still store the complete live data set with no time restriction, is to anonymize the personal data on the live data set. Via this method, the areas containing personal data are difficult to analyse, whereas non-personal-related parts of the document remain fully analysable.

Note.— To clarify data privacy concerns: The data privacy concerns mentioned in recommendations F.1 to F.4 must be clarified by the operational manager, e.g. via a data privacy concept. Recommendations for storing the live data set made in F.3 and F.4 can be combined, e.g. store privacy-friendly regions.

C.6 BIBLIOGRAPHY

- [BSI-TR-03135] BSI, Machine Authentication for Public Sector Applications, TR-03135, 2017.
url: <https://www.bsi.bund.de/tr03135/>
- [FRONTEX-ABC] FRONTEX: Best Practice Technical Guidelines for Automated Border Control (ABC) Systems, 2012

— — — — —

APPENDIX D TO PART 2 — THE PREVENTION OF FRAUD ASSOCIATED WITH THE ISSUANCE PROCESS (INFORMATIVE)

D.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.

D.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 applicants apply under their 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.

D.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.

D.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. Applicants for an MRTD who have not held one previously should be required to present themselves 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 employees from selecting which applications they are 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.

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

Legislative requirements	<p>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:</p> <ol style="list-style-type: none"> 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	<p>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:</p> <ol style="list-style-type: none"> 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). <p>*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.</p>
Information gathering	<p>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.</p>
Timely and accurate data provision	<p>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.</p>

	<p>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.</p> <p>States should operate a round-the-clock response facility to promptly action requests for further information from INTERPOL on behalf of inquiring States.</p>
Leveraging national databases on lost, stolen and revoked travel documents	<p>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.</p>

— END —

ISBN 978-92-9265-319-4



9

789292

653194