International Civil Aviation Organization

WORKING PAPER

TAG/MRTD/20-WP/2
29/07/11
English Only

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

TWENTIETH MEETING

Montréal, 7 to 9 September 2011

Agenda Item 2: Activities of the NTWG
Agenda Item 2.2: Machine Assisted Document Security Verification

MACHINE ASSISTED DOCUMENT SECURITY VERIFICATION

(Presented by the NTWG)

1. INTRODUCTION

1.1 Part 1 of ICAO Doc 9303, Volume 1 (Sixth Edition), Informative Appendix 2 to Section III covers Machine Assisted Document Security Verification. This Appendix was not updated during the last revision of Doc 9303.

1.2 The world-wide introduction of e-Passports facilitated the deployment of advanced flatbed machine readable travel document readers which are not only able to read an e-Passport's Radio Frequency (RF) chip, but also capture high quality images in different wavelength regions.

1.3 The availability of flatbed MRTD readers now offers new possibilities for machine authentication of security features. The NTWG investigated a broadened use of machine assisted document security verification.

1.4 During TAG/MRTD/19, the NTWG presented this topic under WP/10 including a detailed Discussion Paper. The TAG/MRTD/19 approved on-going work on this issue aimed to develop a Technical Report for TAG/MRTD/20, provided in the appendix.

2. BACKGROUND

2.1 The current edition of Doc 9303 distinguishes three main categories of machine-verifiable security features. These are:

a) Structure feature: a security feature containing some form of verifiable information based on the physical construction of the feature.

b) Substance feature: a feature that involves the identification of a defined characteristic of a substance used in the construction of the feature.

c) Data feature: the visible image of an MRTD data page may contain concealed information which may be detected by a suitable device built into the reader. The concealed information may be in the security printed image but is more usually incorporated into the personalization data.

2.2 An RF chip in an eMRTD offers excellent possibilities for machine authentication, if used in a standard compliant way and therefore to its full potential. However, machine authentication does not depend on the existence or the function of an RF chip, especially in Automated Border Control (ABC) scenarios, where human examination of document security features is replaced by machine reading processes. The proof of authenticity of the documents itself is of utmost importance. Machine authentication may also provide added value for the machine assisted verification of security features in non e-Passports, once passport readers have been equipped accordingly.

2.3 On the other hand, machine authentication procedures can complement a (functioning) RF chip in an eMRTD where the chip can act as a reference basis. The feature or its details may also be stored in the respective data groups and/or co-ordinates to detect the feature may be given in the data group, thereby linking the physical security level of the document to the digital level.

3. CONSIDERATIONS

3.1 Machine assisted document security verification features are optional security elements that may be included on the Machine Readable Passports (MRP) at the discretion of the issuing authority.

3.2 Therefore, it is necessary for each State to conduct a risk assessment of machine assisted document authentication at its borders, to identify the most beneficial aspects and minimize the risk of concentrating on one selected feature or on the use of machines and software exclusively.

3.3 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.

3.4 All three types of features (structure, substance and data) may be incorporated in travel documents and verified by suitably designed readers. Future work on this issue will concentrate on features that can be verified by detection equipment built into an MRTD reader during the normal reading process without requiring additional time.

3.5 In order to verify traditional as well as innovative security features of MRTDs, document readers must be equipped with appropriate sensors for the more common and advanced machine assisted authentication features. Standard document readers deployed at borders usually have the following hardware sensors:

a) VIS, UV, IR illumination and high resolution image capture capabilities this allows for the MRZ reading and image processing (including pattern recognition) of security features;

b) ISO/IEC 14443 compliant contactless RF chip readers (at 13.56 MHz frequency); and

c) Advanced document readers may also have dedicated sensors to authenticate special security features (e.g. coaxial illumination for the verification of retro-reflective security overlays, laser diode illumination for the verification of DOVIDs, magnetic sensors and spectral analysis sensors). Usually, advanced reading capabilities are all based on national, bilateral, multilateral, proprietary agreements and require dedicated hardware.

3.6 Criteria to recommend machine authentication features need to be developed along the lines of the ICAO selection process for global interoperable biometric or storage technology. These shall contain:

a) Security;

b) Availability, but exclusiveness for security documents;

c) Dual-use, i.e. additional purpose of the feature beyond machine authentication;

d) Compatibility (for issuance and control processes, and backward compatibility);

e) Interoperability; and

f) Cost (for feature & sensor).

3.7 The attached Technical Report on Machine Assisted Document Security Verification identifies machine authentication technologies for the security features recommended Doc 9303 in Appendix E “Informative Appendix 1 to Section III Security Standards for Machine Readable Travel Documents”. The report aims to provide guidance on the expansion of the capabilities of document reading devices already installed at borders to accommodate electronic passports and their secure verification.

4. ACTION BY TAG/MRTD

4.1 The NTWG invites the TAG/MRTD to:

a. acknowledge the work on machine authentication, documented in the Technical Report on Machine Assisted Document Security Verification;

b. approve the considerations listed above as basic guidelines on the use of machine authentication; and

c. approve at Appendix A the Technical Report on Machine Assisted Document Security Verification containing best practice recommendations for the use of machine authentication which is intended to be included as an informative annex in Doc 9303, Section III.

— — — — — — — —

MACHINE READABLE TRAVEL DOCUMENTS

Technical Report

Machine Assisted Document Security Verification

Version – **1.0**
Date – 2011-07-26

Published by authority of the Secretary General

File:	Machine_Authentication_TR_v10
Author:	New Technology Working Group (NTWG), subgroup on Machine Authentication

Release Control

Release	Date	Description
0.1	2009-09-01	First outline of the content, by U. Seidel
0.2	2009-03-04	Editorial changes based on comments for the Discussion Paper of TAG19, incorporation of MA applications along security features of Appendix E
0.3	2011-06-03	Changes by T. Kinneging and U. Seidel
0.4	2011-07-21	Contains all Comments by T. Kinneging, P. Beer, M. Hirabayashi (incorporated by U. Seidel)
0.5	2011-07-21	Accepted changes and comments as long as they are not controversial.
0.6	2011-07-21	Resolution of comments (U. Seidel)
1.0	2011-07-26	Resolution of final comments (U. Seidel)

Editorial group		
Uwe Seidel	D	NTWG, sub-group leader
Barry Kefauver	USA	ISO WG3
Tom Kinneging	NLD	ISO WG3
David Westgate	GBR	NTWG
Mike Ellis	AUS	ISO WG3
Patrick Beer	CHE	NTWG
Antonio Villani	ITA	NTWG
Vladimir Prostov	RUS	NTWG
Mike Holly	USA	NTWG
Molly Hay	CAN	NTWG
Kenichi Kimura	JPN	NTWG
Ronald Belser	NLD	NTWG
Edmee Gosselink	NLD	NTWG
Andrea De Maria	ITA	NTWG
Masashi Hirabayashi	JPN	NTWG
Jan Verschuren	NLD	NTWG

Table of contents

1 Scope

This Technical Report provides advice on machine assisted authentication of security features incorporated in machine readable travel documents made in accordance with the specifications set out in Doc 9303, Part 1 (Machine Readable Passports), Part 2 (Machine Readable Visas) and Part 3 (Machine Readable Size 1 and Size 2 Official Travel Documents). The recommendations cover machine authentication of the security features in the document itself (based on materials, on security printing and on copy protection techniques) as well as advice on reader technologies that apply to machine authentication of documents.

This Technical Report indicates machine verifiable security features that help confirm the authenticity of a genuine document made from genuine materials. All travel document-issuing authorities shall consider this Technical Report which replaces Informative Appendix 2 to Section III "Machine –assisted document security verification" currently published in Doc 9303, Part 1, Volume 1, 6th edition, 2006.

2 Introduction

The worldwide success of ICAO's electronic document initiative – the e-passport – has led to the issuance of millions of electronically enabled machine readable travel documents (eMRTDs) as specified in Doc 9303, Part 1, Volume 2. These advanced document concepts require the deployment of radio frequency enabled travel document readers at the points of document authentication, usually the points of entry at one country's borders. Such advanced readers feature not only the chip reading capability, but also the means for high resolution image acquisition in the visual, infrared and ultraviolet spectral range.

On the other hand, Supplement to Doc 9303 contains the updated Appendix E "Informative Appendix 1 to Section III - Security Standards for Machine Readable Travel Documents". This Appendix identifies the security threats to which travel documents are frequently exposed and the countermeasures that may be employed to protect these documents. 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. Appendix E and the security standards recommended therein provide the basis for the considerations in this Technical Report on Machine Verification, utilizing the security features recommended in Appendix E and expanding the capabilities of advanced readers already installed at the borders to accommodate electronic passports and their verification.

The aim of the recommendations in this Technical Report is to improve the security of machine readable travel documents worldwide by using machine assisted document authentication procedures completely in line with 1) the layout of machine readable travel documents as specified in Doc 9303 maintaining backward compatibility, 2) the security features recommended in Appendix

E of Doc 9303 and 3) making use of the technical capabilities of advanced flatbed readers installed worldwide to accommodate eMRTDs.
However, it is necessary for each State to conduct a risk assessment of the machine assisted document authentication at its borders to identify their most beneficial aspects and minimize the risks. The reliance on a single feature to verify authenticity carries a high risk that the method will be compromised. States should be aware of this risk should they choose to use a machine assisted feature for their own purposes in their MRP.

3 Feature Types and Basic Principles

3.1 Types of Machine Assisted Document Verification Features

Doc 9303 distinguishes 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 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.
- Controlled transmission of light through selective areas of the substrate.

3.1.2 Substance feature

A substance feature 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 infra red or ultra violet light) or have magnetic or electromagnetic properties.
- The incorporation into a component of the data page of materials, e.g. fibres or planchettes whose individual size or size distribution conform to a predetermined specification

3.1.3 Data feature

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

Inserting the concealed information to the MRP data page may involve the application of substance and or structure features in a way which achieves several levels of security. The information may be decoded by a suitable device built into a full page reader set to look for the feature in a specific location. The information might, for example, be the passport number. The reader could then be programmed to compare the passport number detected from the feature with the passport number appearing in the MRZ. Such a comparison involves no access to any data stored on the optional microchip described in Volume 2 of Doc 9303 Part 1. Examples of this type of feature are:

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

3.2 Basic Principles

All three types of feature, structure, substance and data features may be incorporated in travel documents and verified with suitably designed readers. Readers are now becoming available that can detect such features and use the responses to confirm the authenticity of the document. This Appendix 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 MRP at the discretion of the Issuing Authority.

Figure 1 (already part of Doc 9303, Part 1 Volume 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 in Figure 1.

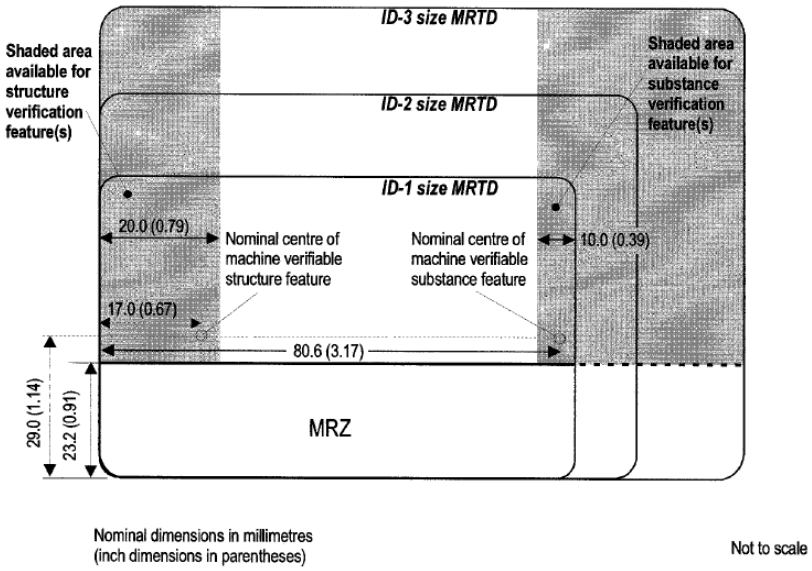

Figure 1: This diagram shows the three sizes of MRTD including the MRP (ID-3 size) with recommended positions for machine assisted document verification features. The shaded area on the left recommended for the incorporation of a structure feature and that on the right for the incorporation of a substance feature. Doc 9303, Part 1 Volume 1 Appendix 10 to Section IV

3.3 Machine authentication and eMRTDs

The RF chip in an eMRTD offers excellent possibilities for machine authentication on itself, if used standard compliant and therefore to its full potential. However, machine authentication using the RF chip fails if:

- there is no regular connection to the PKI infrastructure (e.g. in remote areas)
- there is no or a defect chip
- there are no certificates available (connectivity or distribution problems)

Therefore a trusted and secure back-up is needed. Especially in Automated Border Control (ABC) scenarios, there is no one looking at the document except the machine used to read the MRZ and the chip. As an analogy: *the liveness detection for biometric features of a person corresponds to machine authentication for documents*, to establish trust in the data used for decisions at the border.

Machine authentication also offers excellent possibilities to complement a (functioning) RF chip in eMRTDs where the chip can act as a reference basis: the MA feature could also be stored in the respective DG's and/or co-ordinates to detect the feature can be given in the DG.

4 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.

4.1 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)
- ISO 14443 compliant contactless RF chip readers (@ 13.56 MHz frequency)

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

- MRZ read & check digit verification
- chip read & Passive Authentication (and, optionally, Active Authentication)
- 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 & authenticate digital watermarks (steganographic features) to check for authentic issuance
- detect and read out (alphanumeric) displays and their future security features
- detect and read out LED-in-plastic based security features

4.2 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

- 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.

4.3 Background Systems, PKI

To authenticate certain types of MA 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.

5 Security features and their application for Machine Authentication

The following paragraphs describe major security features and techniques as identified in Appendix E on Security Standards and explain how Machine Authentication could be deployed for these security mechanisms. Issuing authorities which selected security features from Appendix E may use the tables below to check what possibilities of machine authentication are in existence for such features.

5.1 Substrate Materials

5.1.1 Paper forming the pages of a travel document

Security Features	Sensor needed for MA					Pattern fix/variable	MA 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 fibers		X	X			F/V	pattern matching

Visible (fluorescent) fibers	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

5.1.2 Paper or other substrate in the form of a label

Security Features	Sensor needed for MA					Pattern fix/variable	MA 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 fibers		X	X			F/V	pattern matching
Visible (fluorescent) fibers	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

5.1.3 Synthetic Substrates

Security Features	Sensor needed for MA					Pattern fix/variable	MA method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
Construction resistant to splitting							N/A
Optically dull material		X					UV intensity
Secure incorporation of data page							N/A
Optically variable features							See 5.3
See 5.2 – 5.5 as appropriate							
Additional features							
Window or transparent feature					Transmission	F	pattern matching
Tactile feature					Retro-reflective	F/V	pattern matching
Laser perforated feature					Transmission	F/V	pattern matching
Surface characteristics	X		X		Retro-reflective	F	pattern matching

5.2 Security printing

5.2.1 Background and text printing

Security Features	Sensor needed for MA					Pattern fix/variable	MA 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
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

5.2.2 Inks

Security Features	Sensor needed for MA					Pattern fix/variable	MA 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 ink			X			F/V	Pattern matching
Phosphorescent ink		X	X			F/V	Pattern matching
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

5.2.3 Numbering

Security Features	Sensor needed for MA					Pattern fix/variable	MA 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

5.3 Protection against copying

Security Features	Sensor needed for MA					Pattern fix/variable	MA 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

5.4 Personalization Techniques

5.4.1 Protection against photo substitution and alteration

Security Features	Sensor needed for MA					Pattern fix/variable	MA 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
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 Volume 2				X		V	RF reader

5.5 Additional security measures for passport books

Security Features	Sensor needed for MA					Pattern fix/variable	MA 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-color sewing thread	X	X				F	Pattern matching
Programmable sewing pattern	X	X				F	Pattern matching
UV cured glue to stitching							N/A
Index marks on every page							N/A
Laser perforated security feature					Transmission	F/V	Pattern matching
Biographical data on inside page							N/A

5.6 Additional security measures suited for machine authentication

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

Security Features	Sensor needed for MA					Pattern fix/variable	MA method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
MRZ read & check digit verification	X		X			F/V	Checksum calculation
Chip read & 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 (alpha-numeric) displays and their future security features	X	X	X	X		F/V	Use R/F to power display in plastic
Detect & verify retro-reflective foil material	X				Coaxial lighting	F/V	Pattern matching
Barcodes	X	X	X			V	Decoding

6 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 readers systems which 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; most important criteria
- 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 MA feature to be personalized (i.e. individualized) with information from the passport to secure the personal data (e.g. the passport number, name etc.) 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 etc.)
- Interoperability
- Sensor availability
- Cost (for feature & sensor)
- Intellectual Property (IP) issues, e.g. patents
- Primary inspection vs. secondary
- Time required to actually utilize the feature
- Difficulties associated with the book manufacturing and / or the personalization processes
- Durability, i.e. according to the relevant ISO and ICAO specifications for MRTDs