International Civil Aviation Organization

WORKING PAPER

TAG-MRTD/19-WP/10
2/11/09
English Only

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

NINETEENTH MEETING

(Montréal, 7 to 9 December 2009)

Agenda Item 2: **Activities of the NTWG**
Agenda Item 2.10: **Machine Assisted Document Security Verification**

MACHINE ASSISTED DOCUMENT SECURITY VERIFICATION

(Presented by the New Technologies Working Group (NTWG))

1. INTRODUCTION

1.1 Part 1 of ICAO Doc 9303 Volume 1 (6th 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 ePassports facilitated the deployment of advanced flatbed MTRD readers which are not only able to read the ePassport's RF chip, but do 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 is about to investigate a broadened use of machine assisted document security verification. In the past, this work item was put aside for the activities on ePassports and biometrics.

1.4 The NTWG initially set out to discuss this topic within a Discussion Paper, attached as Appendix A, which shall then evolve into a Technical Report.

2. BACKGROUND

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

- *Structure features*: a structure feature is a security feature containing some form of verifiable information based on the physical construction of the feature.

- *Substance Features*: a substance feature involves the identification of a defined characteristic of a substance used in the construction of the feature.

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

2.2 The 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 the RF chip – it could provide a trusted backup if there is no connection to the PKI infrastructure or there is no or a defect chip; especially in Auto-mated 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 out-most importance. Machine authentication could also provide added value for the machine assisted verification of security features in non ePassports, once the passport readers are equipped accordingly.

2.3 On the other hand, machine authentication procedures can complement a (functioning) RF chip in the eMRTD where the chip can act as a reference basis: the feature or its details could also be stored in the respective data groups and/or co-ordinates to detect the feature can be given in the data group, therefore 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 MRP at the discretion of the Issuing Authority.

3.2 Therefore, it will be 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 minimizes the risk of either concentrating on one selected feature or concentrating 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 features) may be incorporated in travel documents and verified with suitably designed readers. Future work on this issue shall concentrate on features that can be verified by detection equipment built into the MRTD reader *during the normal reading process without adding extra time to it.*

3.5 Much like the ICAO selection process for the global interoperable biometric or the storage technology, criteria to recommend machine authentication features need to be developed. These shall contain:

- Security
- Availability, but exclusiveness for security documents
- Dual-use, i.e. additional purpose of the feature beyond machine authentication
- Compatibility (for issuance and control processes, backward compatibility)

- Interoperability
- Cost (for feature & sensor)
- Etc.

3.6 The most recent Supplement to Doc 9303 (Release 7, dated November 19, 2008) contains the updated Appendix E "Informative Appendix 1 to Section III - Security Standards for Machine Readable Travel Documents". Appendix E and the security standards recommended therein shall provide the basis for the future considerations 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.

4. ACTION BY THE TAG/MRTD

4.1 The NTWG invites the TAG/MRTD:

a) to acknowledge the work on machine authentication done so far, documented in the Discussion Paper, attached as Appendix A;

b) to approve the considerations listed above as guidelines for future work on machine authentication;

c) to approve on-going activities of the NTWG on the issue, aimed to develop a Technical Report for TAG-MRTD/20 containing best practise recommendations for the use of machine authentication. The content of this Technical Report shall later be included as Informative Annex to Section III in Doc 9303.

— — — — — — — —

APPENDIX A

MACHINE READABLE TRAVEL DOCUMENTS

Discussion Paper

Machine Assisted Document Security Verification

Version – 1.1
Date – 2009-10-30

Release Control

Release	Date	Description
0.1	2009-02-18	First draft, by U. Seidel
0.2	2009-02-24	Comments by U. Schneider
0.3	2009-02-27	Comments by E. Friedrich
0.4	2009-03-18	Comments by T. Kinneging and B. Kefauver
0.5	2009-06-10	Comments by NTWG (Brussels meeting) and Mr. Kimura, incorporated by U. Seidel, editorial changes by U. Seidel
0.6	2009-09-01	Comments on V0.5 by Mike Holly, Patrick Beer and Mike Ellis, incorporated by U. Seidel
1.0	2009-10-09	Incorporation of comments made by David Westgate, editorial changes leading to V1.0
1.1	2009-10-30	Minor editorial changes after NTWG meeting in Sydney, 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 Introduction

ICAO NTWG is about to investigate a broadened use of machine assisted document security verification. The topic 'Machine Authentication' has been around the ICAO NTWG community for a long time, but was put aside for the work on e-passports and biometrics.

Standardization is a necessity to make a certain technology or group of technologies globally interoperable. As an example, contactless chips were not interoperable by design, but ICAO & NTWG declared them as a worldwide standard and developed the rules for this standard. This standardization, hastened by political pressure eased the costs of spreading the necessary reader infrastructure. This could also be the case for machine-assisted document security verification or machine authentication (MA).

By initiating this work item, the NTWG is aware of the fact that countries just invested in new document readers to accommodate eMRTDs, but this should not prevent future oriented developments in the field of document security which might come into effect for the next generation of advanced document readers.

There were several questions asked and answered by the NTWG meeting in Brussels, March 2009:

1. Do we need machine authentication features beyond the tools available in the MRZ and through the RF chip in MRTDs?
2. Do we need to specify/standardize/recommend certain specific features, methods and processes?
3. Is it possible to standardize such MA feature(s) or provide guidance for their use without risking allowing malafides an easier path for abuse?
4. What are the specific Government policies that we would articulate in order to specify MA features?
5. What are the criteria to select promising MA features and appropriate sensors?
6. Will all issuing states need to adopt the feature(s) in order to meet the "standards"?
7. Even if full interoperability as defined by a standard is not achievable, do we recommend best practices for MA?

As an outcome of the Brussels NTWG meeting in March 2009, the sub-group was tasked to proceed and develop the current Discussion Paper, which will then evolve into a Technical Report.

2 What is currently in Doc 9303, Part 1 Vol. 1?

The following paragraphs partly repeat the *current section in Doc 9303, Part 1, Vol 1*. Several comments are included to highlight areas of future work and possible amendments of the standard.

INFORMATIVE APPENDIX 2 TO SECTION III

MACHINE-ASSISTED DOCUMENT SECURITY VERIFICATION

Note: ICAO Doc 9303 does not specify a machine assisted verification method that is globally interoperable. 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.

This note currently prevents the recommendation of one or more promising security features for MA by ICAO. A new guidance should highlight the pros and cons, but avoid such a general statement. **A future Technical Report shall recommend best practices for the deployment of MA features.**

1. Scope
1.1 This Annex indicates machine verifiable security features that a State may optionally use for its own purposes as an aid to the authentication of a travel document, i.e. that help confirm its authenticity as a genuine document made from genuine materials. Features based on the detection of the presence of a substance or of a particular structure at a particular place in the MRP are included, where the means of detection is built into the reader. Features which involve the accessing of data stored on a microchip are excluded as they are considered in Doc 9303 Part 1 Volume 2

The possibilities for MA which are offered by the RF chip and its data should be included in the Technical Report. Especially since there are promising new ideas which link the chip data content (LDS) with physical security features on the data page. The technical specifications for the data remain in Vol. 2.

2. Types of Machine Assisted Document Verification Features
2.1 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. This Appendix only describes features that can be verified by detection equipment built into the MRP reader during the normal reading process.

Very important point: A feature MUST be verified during the time period needed to check the document and with the equipment used to read & verify the (e)MRTD. It should not create additional processing time for the border control officer. Maybe the equipment has to be updated with special sensors, but a separate piece of hardware equipment is not an option.

2.1.1 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.*

2.1.2 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 whose individual size or size distribution conform to a predetermined* specification

2.1.3 Data feature: The visible image of the MRP data page may contain information which may be detected by a suitable device built into the reader. The information may be in the security printed image but it is more usually incorporated into the personalisation data especially the portrait. Inserting the 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 whole 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 data which only becomes detectable when viewed using a specific wavelength of light, optical filters, or a specific image processing software

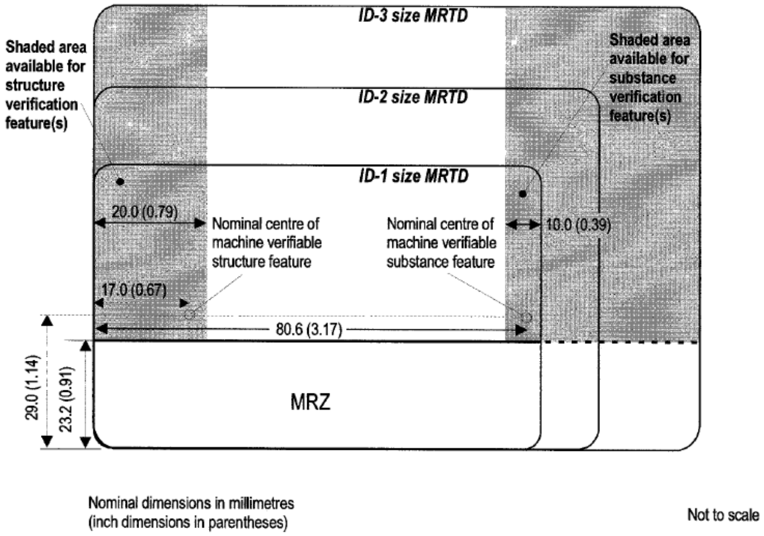
2.2 All three types of feature, structure, substance and data features may be incorporated in travel documents and verified with suitably designed readers. Readers are now becoming available that can detect such features and use the responses to confirm the authenticity of the document.

2.3 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)

2.4 Machine assisted document security verification features, are optional data elements that may be included on the MRP at the discretion of the Issuing Authority. Appendix 10 to Section IV of Doc 9303 Part 1 Volume 1 provides guidance on the positions these features should occupy to facilitate interoperability. However, at present there are no specifications for the functionality or performance of any of these features and hence their use is currently restricted to national and bilateral use.

See comment above. A future Technical Report should aim to develop exactly these specifications or best practice recommendations for machine authentication features which are missing today.

APPENDIX 10 to Section IV


ID-3 size MRTD
ID-2 size MRTD
ID-1 size MRTD
Shaded area available for structure verification feature(s)
Shaded area available for substance verification feature(s)
20.0 (0.79)
Nominal centre of machine verifiable structure feature
Nominal centre of machine verifiable substance feature
10.0 (0.39)
17.0 (0.67)
80.6 (3.17)
29.0 (1.14)
23.2 (0.91)
MRZ
Nominal dimensions in millimetres
(inch dimensions in parentheses)
Not to scale

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.

3 Do we need machine authentication?

The 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 the RF chip – it could provide a trusted backup if there is no connection to the PKI infrastructure or there is no or a defect 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 outmost importance.

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.

On the other hand, machine authentication procedures can complement a (functioning) RF chip in the eMRTD where the chip can act as a reference basis: the feature or its details could also be stored in the respective data groups and/or co-ordinates to detect the feature can be given in the data group, therefore linking the physical security level of the document to the digital level. This concept of course requires certain access rights to read the data groups containing that information.

4 Selection criteria for machine verifiable security features

If ICAO decides to recommend certain security features as especially suited for machine authentication on a global scale, 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

For the interoperability consideration of machine authentication security features, some differentiation between the features might be appropriate:

I. The production and the insertion of the feature into the MRTD is not proprietary and the verification can be done with standard, not vendor-specific equipment.
Examples:

- UV dullness of security paper and its detection with standard readers
- A digital seal using asymmetric cryptography as described in Annex 1
- IR readability of the MRZ

II. The production and the insertion of the feature into the MRTD is proprietary, but the verification can be done with standard, not vendor-specific equipment.
Examples:

- DOVID structure features – insertion into the holographic feature is vendor specific, the technology for the verification is not
- Analogue hidden images (e.g. IPI), which are verified by standard image analysis

III. Both, the production, the insertion of the feature into the MRTD and the verification equipment and procedures are proprietary. This case is certainly not recommended for MRTD issuing authorities. Examples:

- Digital watermarks as investigated in 2004/2005: vendor-specific encoding and decoding software was needed

5 Document readers for machine authentication

In order to verify the 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 security features, machine verifiable or not. This, of course, is a worldwide cost and infrastructure issue.

5.1 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)

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

- MRZ read & check digit verification
- chip read & Passive Authentication, 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. 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

5.2 Advanced Readers

Additionally, advanced readers may have the following hardware sensors:

- 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 and see-through registers – needs a special reader geometry to allow for the placement of the data page only (no covers!) on the reader

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

5.3 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) or an alternative, simpler scheme where States exchange information on their security features by means of certificates.

A private-public key system where each country has a private key for MA could work as follows: The public key is known and can be used to verify the digital signature included in the MA feature. The keys could be changed infrequently, perhaps with a new passport release (new design, series, etc) - these sort of changes have to be taken into account by readers that pattern match the data page and its visible security features to check the authenticity of the document. The public key could be broadcast by publications such as the ICAO MRTD Report and Keesing. It would be convenient to place the public key on the document but without the PKI certificate system this would invite forgers to fabricate their own private-public keys, so this would be inadvisable. Of course the key system could be compromised but it would be more difficult than forging a physical security feature such as a special ink or watermark. But more importantly the key system protects the personalized data which most of the physical security features do not.

Annex 1:
Security features for machine authentication

The following paragraphs describe certain security features and mechanisms which are, in principle, useable for machine authentication. The description will primarily focus on the ability to be used for MA, not on the technological details of the features.

Machine Readable Zone (MRZ)

The MRZ scheme with check digits offers simple and robust possibilities for machine authentication on a full page reader. The following checks can be performed:

- re-calculation of the check digits in the MRZ according to Doc 9303 checksum calculation, based on the MRZ content and comparison with the check digits found in the MRZ
- comparison of the data in the visual zone (VIZ) with those found in the MRZ
- comparison of the data in DG1 of the chip with those found in the MRZ (after successfully performing Passive Authentication, of course, to establish trust in the chip data)
- the existing MRZ technology can also be used to compare the MRZ in the IR spectral band and the according VIS image of the data page to prove the IR opacity of the MRZ as required by Doc 9303

It might also be worth considering improving the existing MRZ composition by a new and additional check digit that could be incorporated at the end of the first MRZ line (possibly using a different algorithm). This, of course, has to maintain backward compatibility to the existing scheme for the lower MRZ line.

RF chip

ICAO Doc 9303 Part 1 Vol. 2 specifies the mandatory Passive Authentication (PA) protocol and the best practice BAC. Together with the optional Active Authentication (AA) mechanism the RF chip can be used to:

- Verify the authenticity and integrity of the chip data (via PA)
- Verify the authenticity of the chip itself (via AA)
- Compare authentic chip data with data of the MRZ and/or VIZ
- Compare properties of data, structure or substance features stored in DG8, DG9 or DG10, respectively, to those found on (the data page of) the document.

Digital Watermarks

In the past, ICAO NTWG investigated the possibility of digital watermarks (steganographic features) in MRTDs. In 2005, the TAG/MRTD/16 concluded in WP/8 that

- *Since digital watermarks add highly to the security of the data page and is a key security feature to protect the photo against manipulation, digital watermarking must not be neglected in any considerations for future recommendations concerning ID and passport documents.*
- *The TAG/MRTD was invited to "support the continued market survey about technical cooperation between different suppliers with the target to decide, depending on the outcome, the eventual recommendation of steganographic techniques as globally interoperable security feature, if the interoperability can be technically guaranteed."*

In the meantime, new schemes and uses of digital watermarks have been developed and show potential for modern machine authentication. Used only as a security feature, the security of these devices has to be investigated thoroughly. On the other hand, digital watermarks comprise a novel and *relatively* secure method to establish trust in the authenticity of the personalization, which is of outmost importance for decentrally issued documents such as visa stickers and alike.

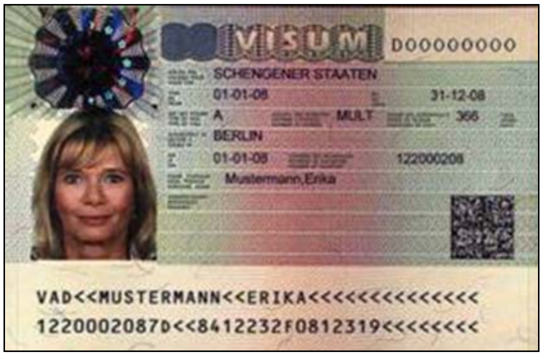
Digital Seals, a novel approach using asymmetric cryptography

New developments using asymmetric cryptography and making use of the e-passport PKI have evolved. This chapter briefly describes this new approach, which aimed at a solution which uses patent-free procedures and algorithms only[1].

The procedure consists of four major steps:

1. Digitize the facial image on the document → compress the image
   - create an image hash to get a short digital representation of the facial image
   - the hash function has to be robust against noise and distortion introduced by the print/scan-transformation
   - the hash function may be based on the principal component analysis of the facial image (much like some facial recognition algorithms)
2. Make the digital information secure → create a digital signature
   - A Signature is computed over the Hash of the facial image & the MRZ.
3. Code the signed digital information → 2D-barcode[2]
   - A 2D-Barcode is the preferred choice (especially in the absence of electronic storage media, error correction up to 25% possible, possible IR readability as the MRZ)
   - The coding consist of the signed hash of the facial image and the MRZ as well as some adjustment information for the facial image (to make up for print/scan-transformations)
4. Attach the coded information to the MRTD.

The certificate handling very much resembles the e-passport PKI design – document signer certificates may be stored in the barcode itself, or, in order to minimize barcode size, distributed via the PKD. For the verification, the e-passport PKI and mechanisms may be used to distribute Document Signer (DS)- and Country Signing Certificate Authority(CSCA)-certificates.



VISUM D000000000

SCHENGENER STAATEN

01-01-08 31-12-08

A MULT 366

BERLIN

01-01-08 122000208

Mustermann,Erika

VAD<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<

1220002087D<<8412232F0812319<<<<<<<<

Example of a MRV showing the digital seal
For enhanced security, the IR-readable barcode could partially cover the portrait
(Source: BSI)

[1] In 2008, the German BSI in collaboration with BKA, conducted a research project on this issue.

[2] The use of 2D barcode as interoperable storage media for MRTDs was excluded by ICAO in Doc 9303. The RF chip technology was chosen instead to store the interoperable biometric feature. However, the use of 2D barcode as an additional and specific security measure ('seal'), even on a bilateral or multilateral basis, is not prohibited by any ICAO

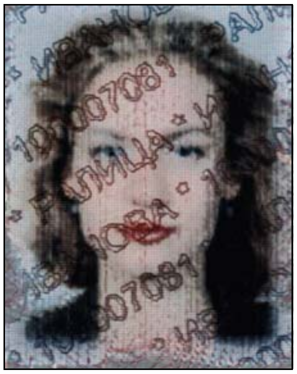
Alternatively, it might be possible that the idea of Digital Seals apply to physical characteristics of the MRP data page in addition to the facial image. In this case, such a technology might be called “Physically Unclonable Function” or “Artifact-Metrics”, identifying a product by physically random characteristics that are introduced during the manufacturing process and cannot be controlled, for example the distribution of fibers in a paper.

The process of extracting the information and incorporating it in the document is similar to the process described above.

Hidden Images

State-of-the-art document readers offer a wide range of image analysis technologies. They can be used to decrypt a hidden image, e.g. introduced in the background of the holder’s portrait. Even if the technology to introduce the hidden information into the image might be proprietary, certain types of (analogue) features can be detected by the reader’s camera and appropriate image analysis software, which is not dependent on the manufacturer of the feature.

On the other hand, if these features can be detected by manufacturer independent image analysis, their value at least as high security element is questionable. But again, this type of features provides a very useful tool to detect not authentic personalisation of decentrally issued documents.



Example of hidden image information, which was inserted using proprietary technology (in this case, an analogue feature).

The verification, however, took place by grabbing the image and subsequent image analysis without proprietary decoding software.

Structure Features

According to the current Doc 9303, Part 1, a *structure feature* is a security feature containing some form of verifiable information based on the physical construction of the feature.

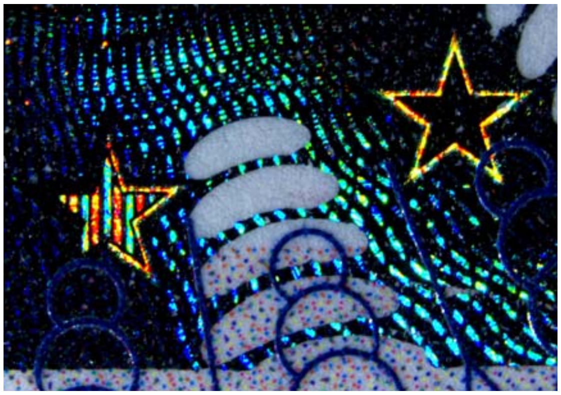
A widely used example is the interference characteristic of a hologram or other optically variable device that can be uniquely identified by a suitable reader. This class of structure features is especially suited for globally deployed machine authentication. ICAO Doc 9303 states in the *Informative Appendix 1 to Section III “Security Standards for Machine Readable Travel Documents”* in chapter 5.3.1 “*Anti-copy protection methods*” that *“…**optically variable features should be used on the biographical data page** of a passport book, travel card or visa **as a basic feature**.”*

specifications. On the other hand, the use of 2D barcode will require some space on already densely occupied data pages.

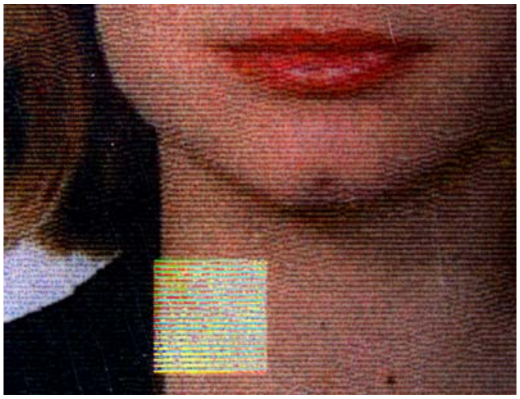
Today, literally every MRTD shows optically variable devices (OVD) on the data page, usually in the form of Diffractive Optically Variable Image Devices (DOVID), i.e. holograms, kinegrams or alike. Even if not all DOVIDs today use machine authentication features, their wide-spread use and the recommendation by ICAO make holographic and technologically related anti-copy-features a well suited technology to introduce machine authentication on a common technological basis but not necessarily by the same vendor. In 2005, approx. 15 countries used DOVID-based machine authentication features in more than 20 MRTDs. Additionally, all Schengen visa stickers are equipped with this technology.

DOVID based security features not only prevent counterfeits, but are also very helpful in the detection of altered documents because a manipulation of the laminate often results in their destruction. Additionally, DOVIDs combine visual authentication and machine authentication within the same security technology.

Generally, the principle of machine authentication of DOVIDs can be described as follows:
Diffractive microstructures are engineered to show a prescribed intensity distribution of the diffracted light which can be measured for authentication. Such machine-verifiable features can be designed to be verified through visual inspection or to a feature which holds hundreds of bits of information in a read-only diffractive optical memory. As all DOVIDs, these machine verifiable features are extremely resistant against counterfeiting.



Machine verifiable DOVID structure within the metallised kinegram® of a Schengen Visa sticker (left star in the image above, 6 o’clock star in the visa’s kinegram)



Machine verifiable DOVID structure within the transparent overlay of a Bulgarian passport (square region in the image above)

Another class of “macroscopic” structure features are latent images, multiple laser images (MLI), changeable laser images (CLI), Dynaprint® etc. although their suitability for MA is questionable.

Substrate Features

Substrate features may utilize spectral analysis, polarization and magnetic effects and may be present in inks, fibres, additives of substrate materials and in security overlays. Machine Authentication features can be built

into security features already specified in the "Informative Appendix 1 to Section III - Security Standards For Machine Readable Travel Documents" of Doc 9303, e.g.:
Features:

- UV inks (different wavelengths) fluorescing different visible colors; however, the availability of 365 nm UV inks may limit the security value of MA features based on this spectral range while the more exclusive 254 nm UV features can not be imaged through a normal glass plate of a full page reader
- Level of UV reflectance within a set parameter
- Inks with specific electrical properties (capacity, conductivity)
- IR inks fluorescing and/or transparent
- Polarized inks
- Polarized fibers
- Magnetic inks
- Tagged inks (additives)
- The use of a specific taggant within the substrate

Detection with:

- Camera (software)
- Cameras filters
- IR spectroscopy
- X-ray fluorescence detection
- Polarization detectors (needs special illumination)

Displays and Related Features

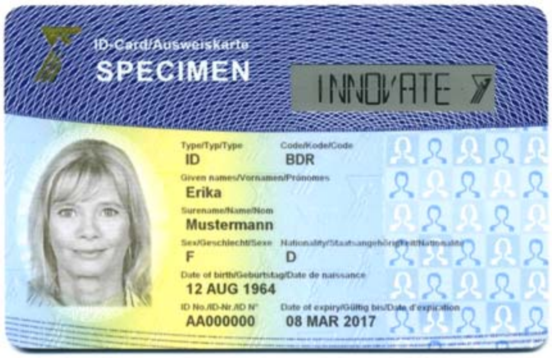
During the 2008 RFI, some innovative concepts were shown which have a high potential for machine authentication of documents. Concepts of displays or light emitting devices (LED), integrated in the polymer body of an eMRTD, were introduced.

A display or a LED on a document can be used as a multi-functional security feature. Both concepts could be used for an unique optical data transfer to verification systems.

The display concept is based on monochromic bistable display technology, also known as electronic ink or e-Paper. The bistability ensures the visibility of the display content without energy. The display works without an internal lifetime limiting battery. Instead, a standard contactless RFID smart card reader supplies energy for the operation of the display (i.e., for changing its information content).

Displays or LEDs can display passwords or special sequences of optical signals, even in other than the visual wavelength region. All those signals could be read by a normal full page reader, equipped with simple image grabbing capabilities. The existing infrastructure based on ISO 14443 can be utilized to power those devices and trigger an optical signal to be sent or the display to change its information content (which could origin from the well authenticated LDS data of the RF chip)
In the further future, it might be possible to use colour graphic displays in new generation documents. First prototypes with OLED displays have been made and tested. The display can show text data and also different pictures of the document owner, e.g. a 3D portrait.

Since a displays or LEDs are also visible to the naked eye, these features could also be used for a first line visual inspection as well.



An ID-1 card sample with an embedded display The bistability of the display ensures the visibility of the content without energy.
(Source: RFI 2008)

Annex 2:
Selected Security Features vs. Document Readers for machine authentication

The following table combines the considerations for **selected** machine authentication security features and the properties of readers & sensors.

		Sensor equipment needed for verification							
		available in standard readers				**special sensors neccessary**			
	Machine authentication process	VIS	UV	IR	RF reader	coaxial	laser/LED	magnetic	other
1	MRZ read & check digit verification	X		X					
2	chip read & Passive Authentication (+AA)				X				
3	generic security checks (UV dull paper, IR readable MRZ, …)		X	X					
4	Detect & verify retro-reflective foil material					X			
5	pattern recognition using databases (based on VIS, UV and IR images)	X	X	X					
6	read & authenticate digital seals (steganographic features)	X		X					
7	detect and read out LED-in-plastic based security features	X	X	X	X				
8	detect and read out (alphanumeric) displays and their future security features	X	X	X	X				
9	special structure features, e.g. for optically diffractive devices						X		
10	special substrate features, e.g. magnetic fibres, Anti-Stokes inks etc.							X	X
11	Special transmission features such as watermarks, see-through registers and laser perforation								X

Annex 3:
Security Features for Machine Authentication, based on Doc 9303 Security Annex

The table in this Annex combines **all** security features from Minimum Security Standard, Doc 9303 (SUPPLEMENT -- 9303 Release 7) and the properties of readers & sensors.

Security features		Sensor						fix/variable pattern	Verification
		VIS	VIS（ Transmission）	UV	IR	RF	Other（ Special）		
Paper forming the pages of a travel document									
BASIC	Controlled UV response								
	Two-tone watermark		available					F	pattern matching
	Chemical sensitisers								
	Appropriate absorbency and surface characteristics								
ADDITIONAL	Registered watermark		available					F	pattern matching
	Different watermark on the data page and visa page		available					F	pattern matching
	Cylinder mould watermark		available					F	pattern matching
	Invisible fluorescent fibres			available				F ／V	pattern matching
	Visible (fluorescent) fibres			available				F ／V	pattern matching
	Security thread	available	available				Magnetic	F	pattern matching
	Taggant						Special	F ／V	
	Laser perforated security feature		available					F ／V	pattern matching
Paper or other substrate in the form of a label									
BASIC	Controlled UV response			available				F ／V	pattern matching
	Chemical sensitisers								
	Invisible florescent fibres			available				F ／V	pattern matching
	Visible (florescent) fibres			available				F ／V	pattern matching
	System of adhesives								
ADDITIONAL	Security thread	available	available				Magnetic	F	pattern matching
	Watermark		available					F	pattern matching
	Laser perforated security feature		available					F ／V	pattern matching
	Die cut security pattern	available						F	pattern matching

Security features		Sensor						fix/variable pattern	Verification
		VIS	VIS（ Transmission）	UV	IR	RF	Other（ Special）		
Synthetic substrates									
BASIC	Construction resistant to splitting								
	Optically dull material	available						F	pattern matching
	Secure incorporation of data page								
	Optically variable features	available					laser	F/V	pattern matching
	See 5.2 – 5.5 as appropriate								
ADDITIONAL	Window or transparent feature	available	available					F	pattern matching
	Tactile feature								
	Laser perforated feature		available					F ／V	pattern matching
Security printing									
Background and text printing									
BASIC	Two-colour guilloche background								
	Rainbow printing								
	Microprinted text								
	Unique data page design								
ADDITIONAL	Intaglio printing								
	Latent image								
	Anti-scan pattern								
	Duplex security pattern								
	Relief design feature								
	Front-to-back register feature		available					F	pattern matching
	deliberate error								
	Unique design on every page								
	Tactile feature								
	Unique font(s)								

Security features		Sensor						fix/variable pattern	Verification
		VIS	VIS（ Transmission）	UV	IR	RF	Other（ Special）		
Synthetic substrates									
BASIC	Construction resistant to splitting								
	Optically dull material	available						F	pattern matching
Inks									
BASIC	UV florescent ink			available				F ／V	pattern matching
	Reactive inks								
ADDITIONAL	ink with optically variable properties	available						F ／V	pattern matching
	Metallic inks				available			F ／V	pattern matching
	Penetrating numbering ink								
	Metameric inks								
	Infrared dropout ink				available			F ／V	pattern matching
	Infrared ink								
	Phosphorescent ink			available				F ／V	pattern matching
	Tagged ink						Special	F	pattern matching
	Invisible ink			available				F	pattern matching
Numberring									
BASIC	Numbering on all sheets								
	Printed and/or perforated number	available			available		OCR	F ／V	OCR
	Special typeface numbering for labels	available			available		OCR	F ／V	OCR
	Identical technique for applying numbering and biographical data on synthetic substrates and cards								
ADDITIONAL	Laser perforated document number		available					F ／V	pattern matching
	Special typefonts	available			available		OCR	F ／V	OCR

Security features		Sensor						fix/variable pattern	Verification
		VIS	VIS（ Transmission）	UV	IR	RF	Other（ Special）		
Personalization technique									
Protection against photo substitution and alteration									
BASIC	Integrated biographical data								
	Security background merged within portrait area								
	Reactive inks and chemical sensitizers in paper								
	Visible security device overlapping portrait area	available					laser	F/V	decoding/pattern matching
	Heat-sealed secure laminate or equivalent	available					laser	F/V	decoding/pattern matching
ADDITIONAL	Displayed signature								
	Steganographic image	available	available	available	available			F ／V	decoding
	Additional portrait image(s)	available	available	available	available	available		F ／V	pattern matching
	Biometric feature as per Volume 2					available		F ／V	RF reader
Additional security measures for passport books									
Page substitution									
BASIC	Secure sewing technology								
	UV fluorescent sewing thread			available				F	pattern matching
	Unique data page design								
	Page numbers integrated into security design								
	Serial number on every sheet								
ADDITIONAL	Multi-colour sewing thread								
	Programmable sewing pattern								
	UV cured glue to stitching								
	Index marks on every page								
	Laser perforated security feature		available					F ／V	pattern matching
	Biographical data on inside page								

Security features		Sensor						fix/variable pattern	Verification
		VIS	VIS（Transmission）	UV	IR	RF	Other（Special）		
Security control of production and product									
Protection against theft and abuse									
BASIC	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								
ADDITIONAL	CCTV in production areas								
	Centralized storage and personalization								

— END —