



Machine Assisted Document Security Verification

Dr. Uwe Seidel
Germany

New Technologies Working Group (NTWG)

TAG/MRTD 19

19th Meeting of the Technical Advisory Group on Machine Readable Travel Documents

Editorial Group

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



Introduction

- Part 1 of ICAO Doc 9303 Volume 1 (6th Edition), Informative Appendix 2 to Section III covers Machine Assisted Document Security Verification.
- The world-wide introduction of e-passports facilitated the deployment of advanced flatbed MRTD readers which are not only able to read the e-passport's RF chip, but do also capture high quality images in different wavelength regions.
- 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.



Machine Authentication in Doc 9303

- Doc 9303 currently 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.



Reasons for Machine Authentication

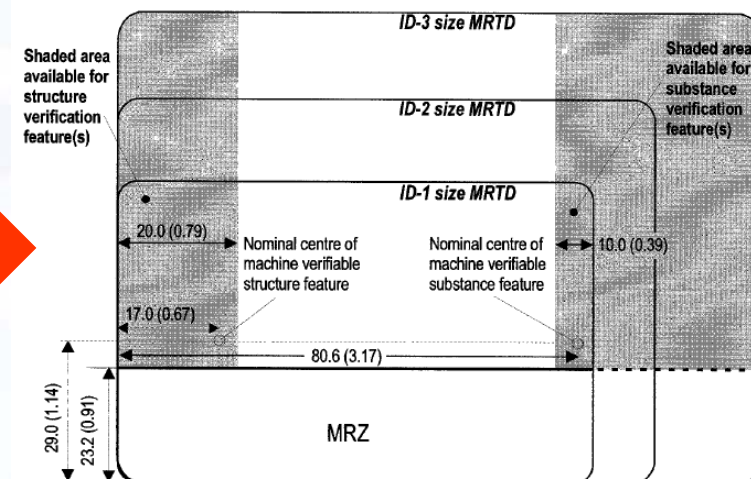
- The RF chip in an eMRTD itself offers excellent possibilities for machine authentication, if used in a standard compliant way and therefore to its full potential.
- Machine Authentication could provide a trusted backup if there is no connection to the PKI infrastructure or there is no or a defect chip; especially in cases, where human examination of document security features is replaced by machine reading processes, the proof of authenticity of the documents itself is of importance.
- Machine authentication could also provide added value for the machine assisted verification of security features in non e-passports, once the passport readers are equipped accordingly



Reasons for Machine Authentication

- MA 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.

DG 8	Data Features
DG 9	Structure Features
DG 10	Substance Features



Nominal dimensions in millimetres
(inch dimensions in parentheses)

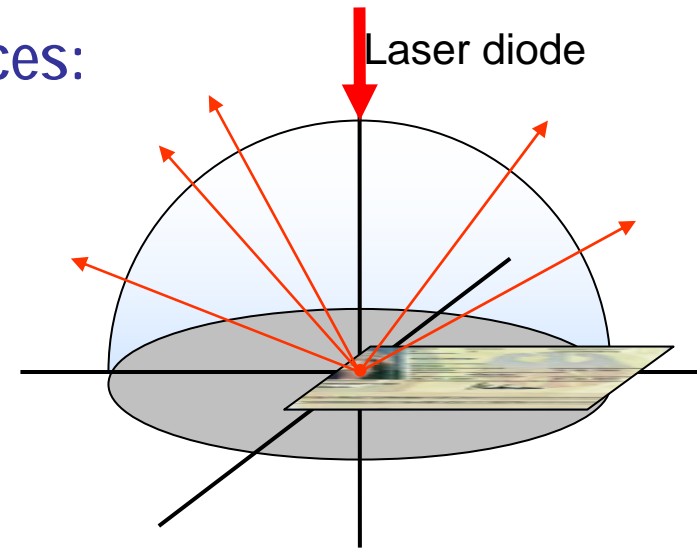
Not to scale



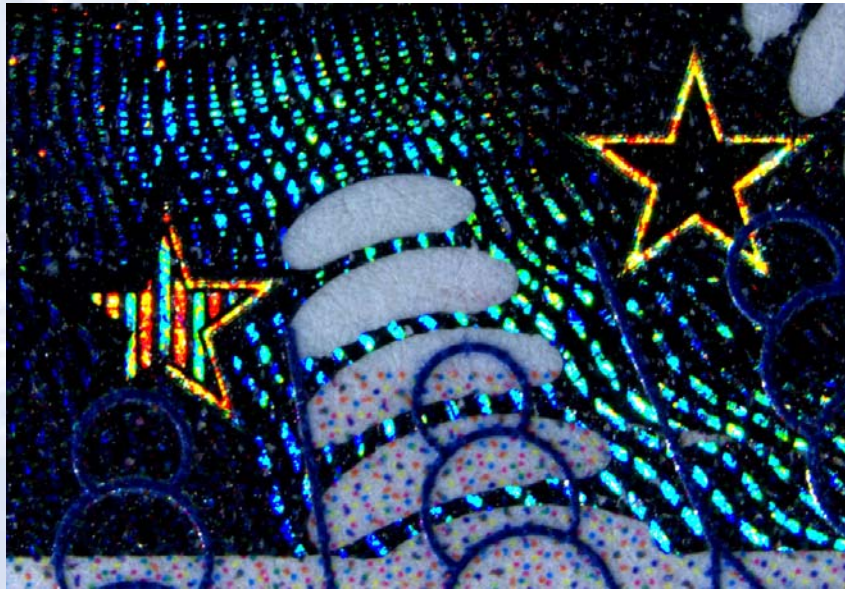
Example: Structure Feature

➤ Diffractive Optically Variable Image Devices:

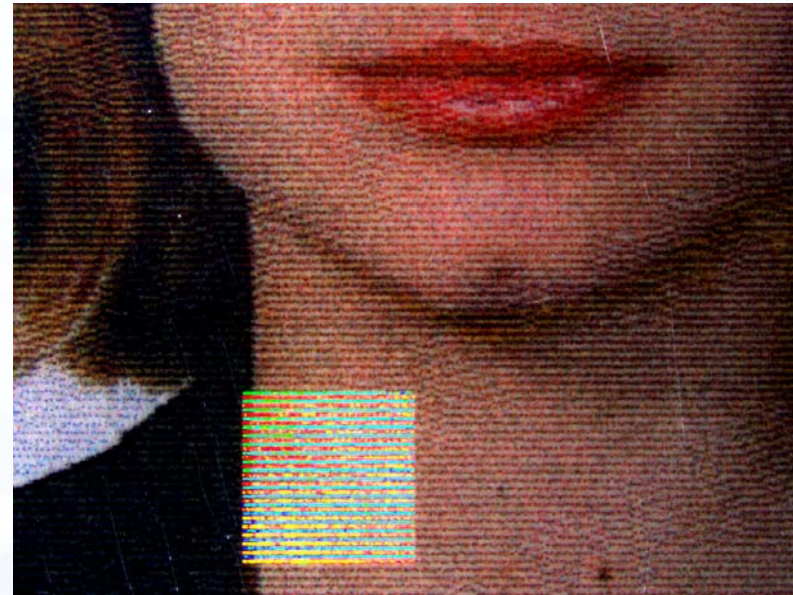
- Their wide-spread use and the recommendation by ICAO make holographic anti-copy-features a well suited technology to introduce MA on a common technological basis but not necessarily by the same vendor.
- In 2005, approx. 15 countries used DOVID-based MA features in more than 20 MRTDs. Additionally, all Schengen visa stickers are equipped with this technology.
- DOVIDs combine visual authentication and machine authentication within the same security technology.



Example: Structure Feature



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)



Example: Data Feature



Example of hidden image information.

Criteria

- 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)



Standard Readers (1/2)

- Hardware sensors used in standard readers:
 - 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)
- 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, ...)



Standard Readers (2/2)

- Further “intelligence” of these readers solely depends on software, not on extra hardware sensors:
 - 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



Standard Reader

Federal Republic of Germany - Dokumententyp: P

↓ infrared

↓ ultraviolett

↓ data page

↓ chip

Einzelergebnisse

- ✓ B-900-Test (IR)
- ✓ MLZ-Test
- ✓ Wertpapier-Test
- ✓ Laser-Test
- ✓ VIZ/MLZ-Vergleich
- ✓ Muster-Test
- ✓ Chip

Chip Daten

Prüfung OK

Chip wurde erfolgreich ausgelesen.

Name	MUSTERMANN
Vornamen	ERIKA
Nationalität	D
Geburtsdatum	12.08.1964
Geschlecht	F
Gültig bis	01.11.2015
Dokumenten-Nr.	009002009
Dokumententyp	P
Ausstell. Staat	D

Name	✓ MUSTERMANN
Vornamen	✓ ERIKA
Nationalität	✓ D
Geburtsdatum	✓ 12.08.1964
Geschlecht	✓ F
Gültig bis	✓ 01.11.2015
Dokumenten-Nr.	✓ 009002009
Dokumententyp	✓ P
Ausstell. Staat	✓ D

Verifier Status

Fehler / Info Vollbild

Auswertefortschritt:

Vergleich >>

Status: Prüfung OK

Start Verifier Status Federal Republic of Germ... DE 08:31



Advanced Readers

- Advanced readers require **extra 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



Considerations (1/2)

- Machine assisted document security verification features are **optional security elements** that may be included on the MRP at the **discretion of the Issuing Authority**.
- 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 only concentrating on one selected feature** and or only concentrating on the use of machines and software.



Considerations (2/2)

- 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.
- 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**.



Future TR: Draft TOC based on Security Annex

1	Scope.....	
2	Introduction.....	
3	Feature Types and Basic Principles.....	
3.1	Types of Machine Assisted Document Verification Features.....	
3.1.1	Structure Feature.....	
3.1.2	Substance feature.....	
3.1.3	Data feature.....	
3.2	Basic Principles.....	
4	Security features and their application for Machine Authentication.....	
4.1	Substrate Materials.....	
4.2	Security Printing.....	
4.3	Protection against copying.....	
4.4	Personalization Techniques.....	
4.5	Additional Security Measures for passport books.....	
5	Document Readers and Systems for Machine Authentication.....	
5.1	Standard Readers.....	
5.2	Advanced Readers.....	
5.3	Background Systems, PKI.....	
6	Selection criteria for machine verifiable security features.....	
7	Selected Security Features vs. Document Readers for Machine Authentication.....	
8	Security Features from Min. Security Standard Doc 9303 vs. Document Readers.....	
9	Contact.....	



Actions by the TAG

- The NTWG invites the TAG/MRTD
 - To acknowledge the work on machine authentication done so far, documented in the Discussion Paper No. XXX.
 - To approve the considerations listed above as guidelines for future work on machine authentication.
 - To approve on-going activities of the NTWG on the issue, aimed to develop a **Technical Report for TAG/MRTD-20** containing **best practice recommendations** for the use of machine authentication.



➤ Thank you for your attention.

Dr. Uwe Seidel, Bundeskriminalamt, Germany

E-Mail: Uwe.Seidel04@bka.bund.de

