



Machine Assisted Document Security Verification

Dr. Uwe Seidel
Germany

New Technologies Working Group (NTWG)

TAG/MRTD 20

**20th 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. This appendix was not updated during the last revision of Doc 9303.
- The world-wide introduction of e-passports facilitated the deployment of advanced flatbed MTRD 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 NTWG investigated the broadened use of machine assisted document security verification.
- During TAG-MRTD/19, the NTWG presented this topic as WP/10 including a detailed Discussion Paper.
- TAG-MRTD/19 approved on-going work on this issue aimed to develop a Technical Report for TAG-MRTD/20 which is now presented.



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 does not depend on the existence or the function of the 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 out-most 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.



Considerations

- MA features **are optional security elements** that may be included on the MRP at the discretion of the Issuing Authority.
- It will be necessary for each State to conduct a **risk assessment**: 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.
- MA technology 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.
- 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.**

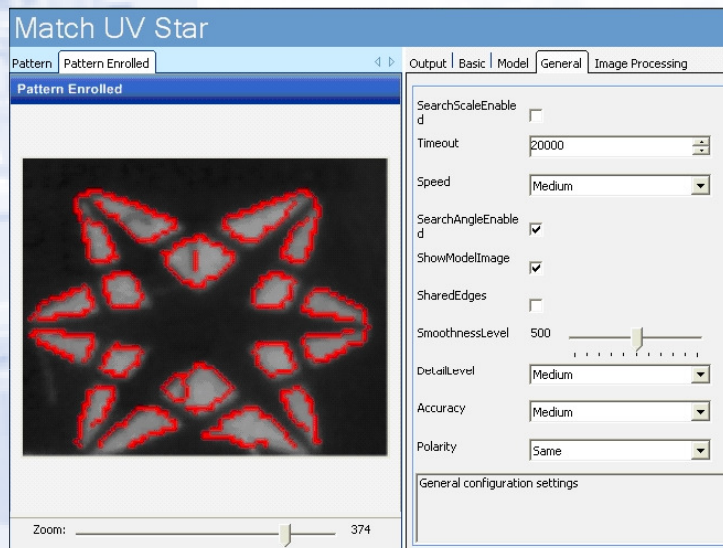


Considerations (criteria)

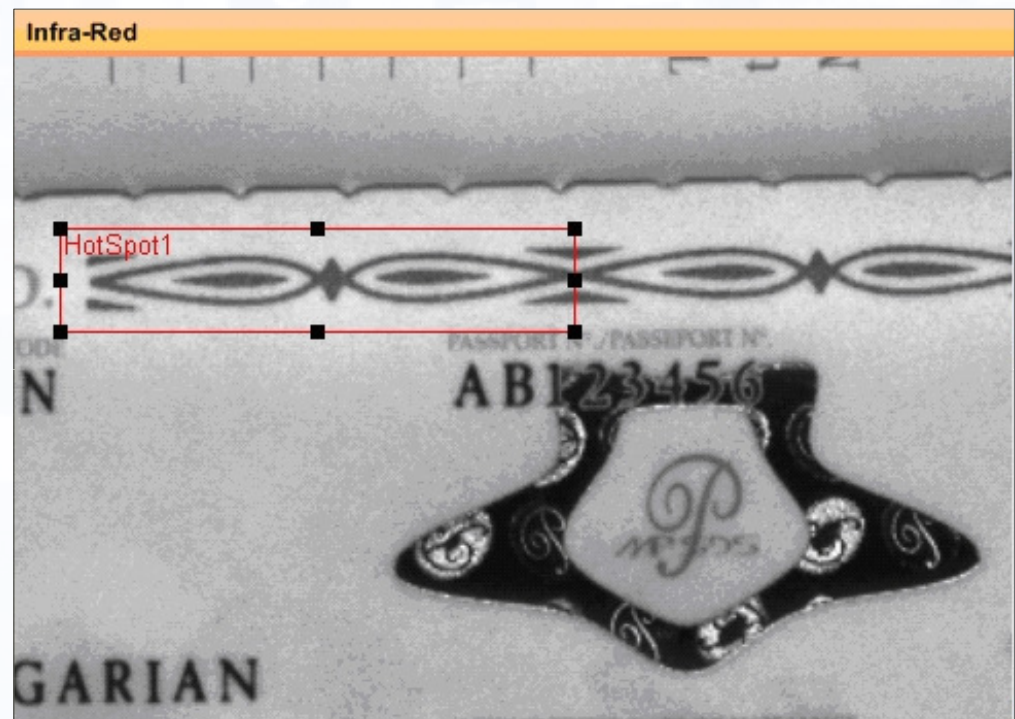
- Much like the ICAO selection process for the global interoperable biometric or the storage technology, criteria to recommend machine authentication features contain:
 - Security
 - Availability, but exclusiveness for security documents
 - Dual-use, i.e. additional purpose of the feature beyond machine authentication
 - Compatibility (for issuance and control processes, backward compatibility)
 - Interoperability
 - Cost (for feature & sensor)



Example: Pattern recognition using standard readers



Contrast outline definition [Avalon]



Pattern definition in IR spectral range [Avalon]




Example: Combined results

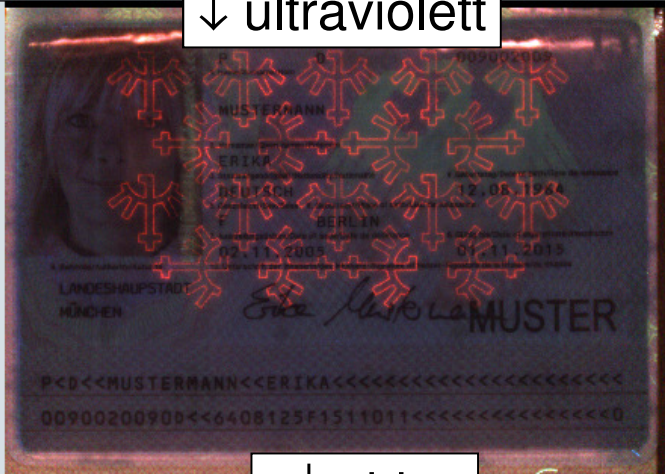
Federal Republic of Germany - Dokumententyp: P

Datei Einstellungen Hilfe

↓ infrared



↓ ultraviolet




↓ data page

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

Prüfung OK

↓ chip

Chip Daten	
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



Chip wurde erfolgreich ausgelesen.

Name	
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

Status: Prüfung OK

Verifier Status: Fehler / Info Vollbild

Auswertefortschritt:

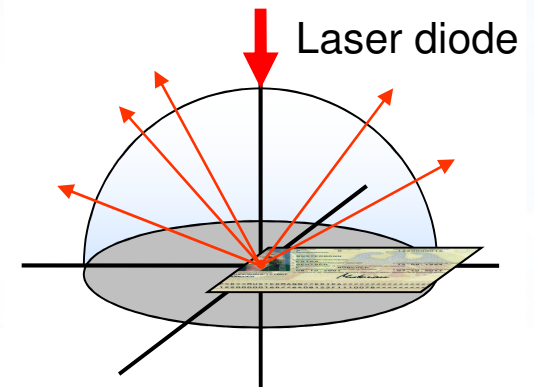
Vergleich >>

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

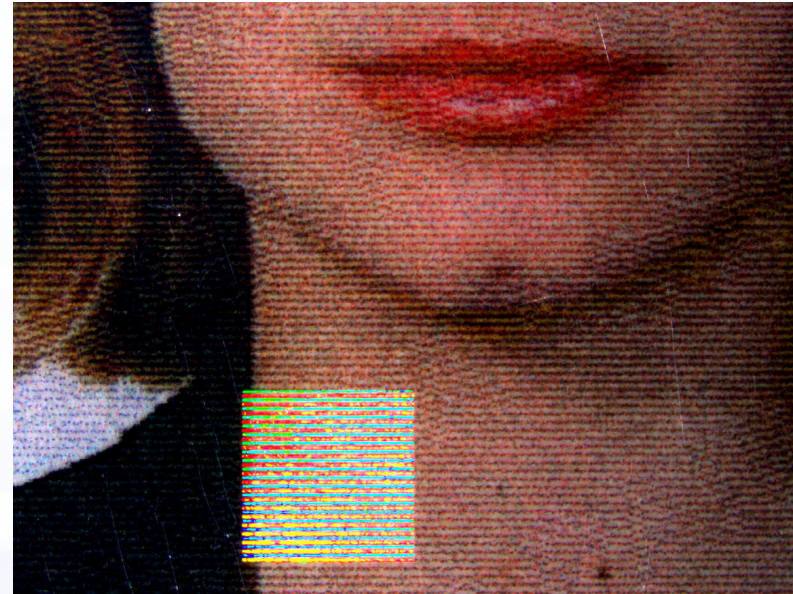
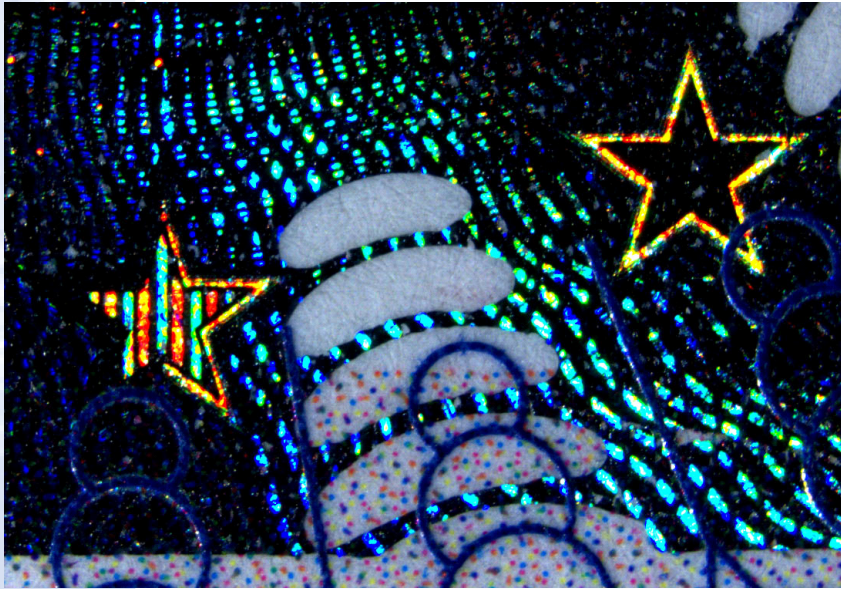


MA using advanced readers

- Advanced document readers may additionally 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
 - spectral analysis sensors)
- Usually, advanced reading capabilities are all based on national – bilateral – multilateral – proprietary agreements and require dedicated hardware.



Example: Advanced Readers



➤ **Diffraction Optically Variable Image Devices:**

- 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.

TR: “cookbook” for the use of MA

- The TR on MA identifies MA technologies for the security features recommended in Appendix E of Doc 9303.
- Example: 5.2.1 Background and text printing

Security Features	Sensor needed for MA				Advanced reader Special sensor	Pattern fix/variable	MA method
	Standard reader						
	VIS	UV	IR	RF			
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



TR: “cookbook” for the use of MA

➤ Example: 5.2.2. Inks

Security Features	Sensor needed for MA				Advanced reader Special sensor	Pattern fix/variable	MA method
	Standard reader		IR	RF			
	VIS	UV					
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



Technical Report: TOC based on Security Annex

1	Scope
2	Introduction
3	Feature Types and Basic Principles
3.1	Types of Machine Assisted Document Verification Features
3.2	Basic Principles
3.3	Machine authentication and eMRTDs
4	Document Readers and Systems for Machine Authentication
4.1	Standard Readers
4.2	Advanced Readers
4.3	Background Systems, PKI
5	Security features and their application for Machine Authentication
5.1	Substrate Materials
5.2	Security printing
5.3	Protection against copying
5.4	Personalization Techniques
5.5	Additional security measures for passport books
5.6	Additional security measures suited for machine authentication
6	Selection criteria for machine verifiable security features



Actions by the TAG

- The NTWG invites the TAG/MRTD
 - To **acknowledge** the work on machine authentication, documented in **the Technical Report on Machine Assisted Document Security Verification**.
 - To **approve the considerations** listed as guidelines for the use of machine authentication.
 - To approve the Technical Report on Machine Assisted Document Security Verification containing best practice recommendations for the use of machine authentication.
The content of this Technical Report shall be included as Informative Annex to Section III in Doc 9303.



➤ **Thank you for your attention.**

Dr. Uwe Seidel, Bundeskriminalamt, Germany

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

