Updates to Doc 9303

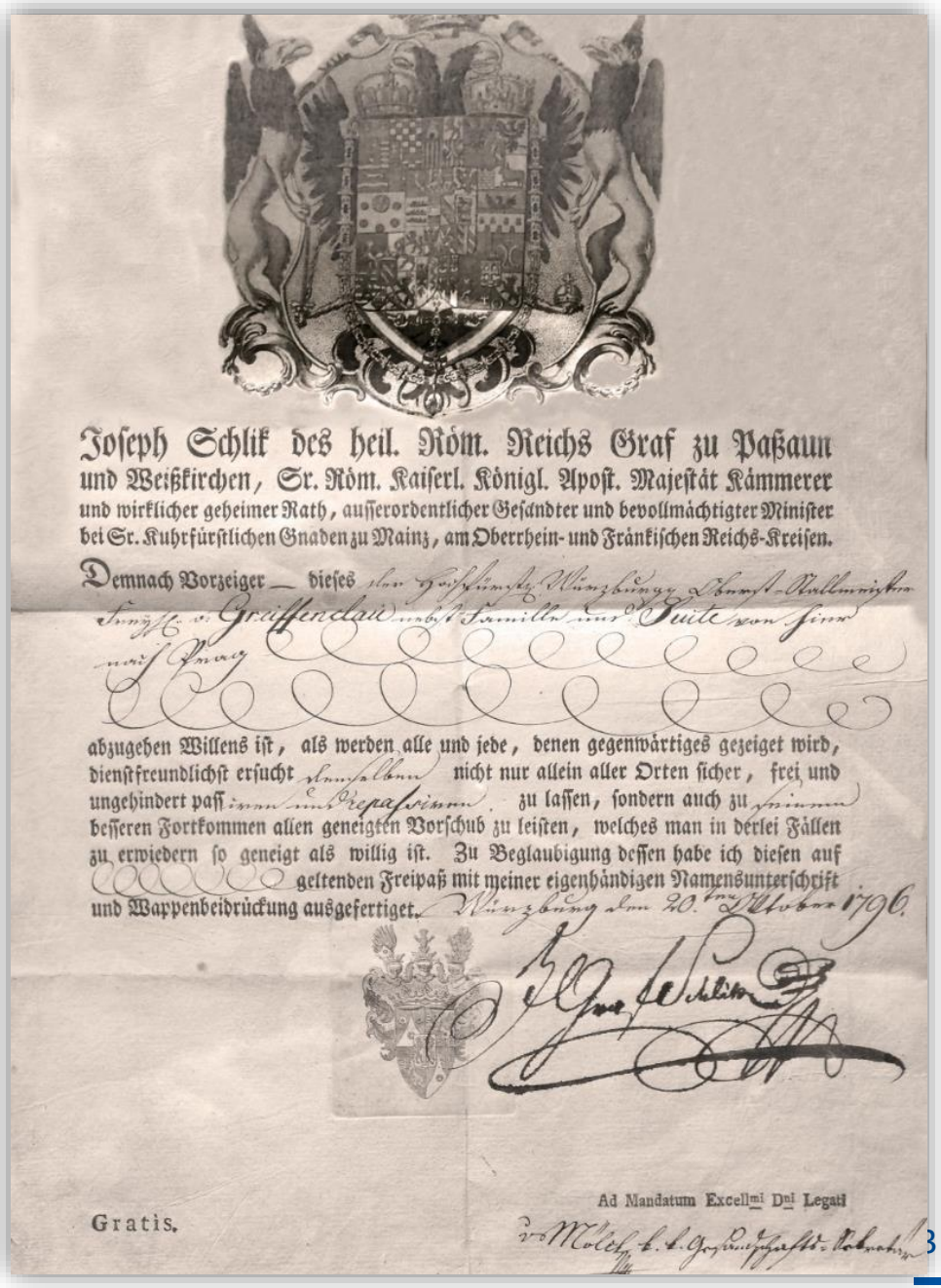
R Rajeshkumar

Convener – ISO/IEC JTC1 SC17/WG3

1. History

Passport 1796

- Limited document security features – good enough for it's time
- Binding to Holder – restricted to name – no biometrics
- No electronics
- Not globally interoperable



Joseph Schlik des heil. Röm. Reichs Graf zu Paßaun und Weißkirchen, Sr. Röm. Kaiserl. Königl. Apost. Majestät Kämmerer und wirklicher geheimer Rath, ausserordentlicher Gesandter und bevollmächtigter Minister bei Sr. Kuhrfürstlichen Gnaden zu Mainz, am Oberrhein- und Fränkischen Reichs-Kreisen.

Demnach Vorzeiger — dieses

Greiffendau

abzugehen Willens ist, als werden alle und jede, denen gegenwärtiges gezeiget wird, dienstfreundlichst ersucht nicht nur allein aller Orten sicher, frei und ungehindert pass zu lassen, sondern auch zu besseren Fortkommen allen geneigten Vorschub zu leisten, welches man in derlei Fällen zu erwiedern so geneigt als willig ist. Zu Beglaubigung dessen habe ich diesen auf geltenden Freipaß mit meiner eigenhändigen Namensunterschrift und Wappenbeidrückung ausgefertiget. Würzburg den 20. Oktober 1796.

Gratis.

Ad Mandatum Excellmi Dni Legati

Source: Dr. Uwe Seidel, Chair NTWG

Improvements – Physical Security Features

Substrate materials

- UV dull substrate, watermarks, sensitizers, fibers, threads …

Security design and printing

- Guilloche/rainbow printing, microprint, special inks, numbering …

Protection against copying and alteration

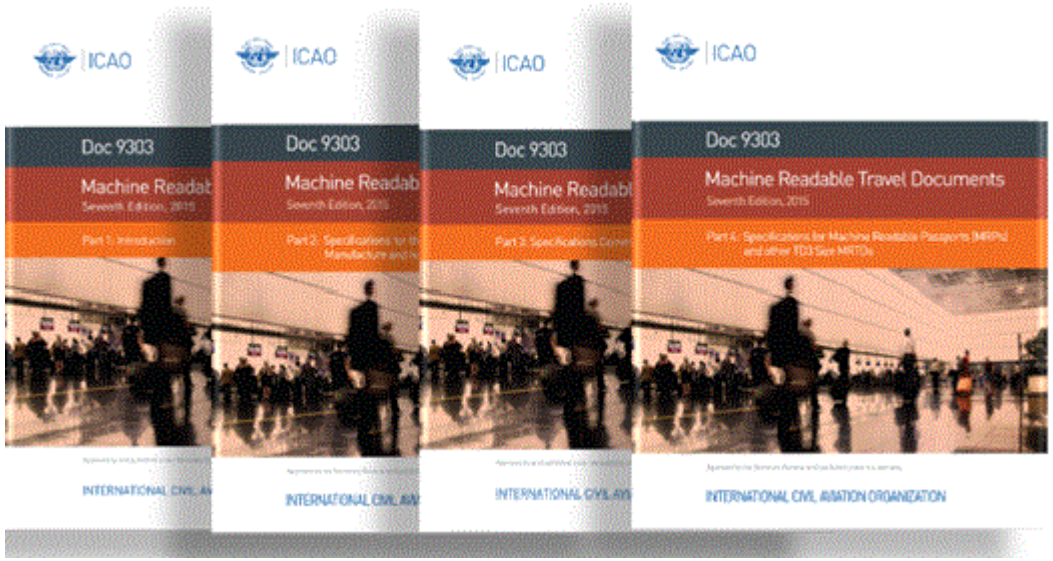
- Optically variable devices, multiple laser images, …

Personalization techniques

- Integration of personal data in the basis material of the document, e.g. by laser engraving

Source: Dr. Uwe Seidel, Chair NTWG

Improvements - ICAO MRTD



Part 1: Introduction

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

Part 3: Specifications common to all Machine Readable Travel Documents

Part 4: Specifications specific to TD3 size MRTDs, Machine Readable Passports

- Good Physical Security
- Binding to holder – Biographic and Biometric information
- No electronics
- Standardised data elements and fields – Global interoperability

Further Improvements – chip in passport

				DATA ELEMENTS
REQUIRED	ISSUING STATE OR ORGANIZATION DATA	Detail(s) Recorded in MRZ	DG1	Document Type
				Issuing State or organization
				Name (of Holder)
				Document Number
				Check Digit - Doc Number
				Nationality
				Date of Birth
				Check Digit - DOB
				Sex
				Data of Expiry or Valid Until Date
				Check Digit DOE/VUD
				Optional Data
				Check Digit - Optional Data Field
				Composite Check Digit
OPTIONAL	ISSUING STATE OR ORGANIZATION DATA	Encoded Identification Feature(s)	Global Interchange Feature	DG2 Encoded Face
			Additional Feature(s)	DG3 Encoded Finger(s)
				DG4 Encoded Eye(s)
		Displayed Identification Feature(s)	DG5	Displayed Portrait
			DG6	Reserved for Future Use
			DG7	Displayed Signature or Usual Mark
		Encoded Security Feature(s)	DG8	Data Feature(s)
			DG9	Structure Feature(s)
			DG10	Substance Feature(s)
			DG11	Additional Personal Detail(s)
			DG12	Additional Document Detail(s)
			DG13	Optional Detail(s)
			DG14	Security Options
			DG15	Active Authentication Public Key Info
			DG16	Person(s) to Notify

DataGroup 1

- Document Type
- Issuing State
- Name of Holder
- Document Number
- Nationality
- Date of Birth
- Check Digit DOB
- Sex
- Date of Expiry
- …

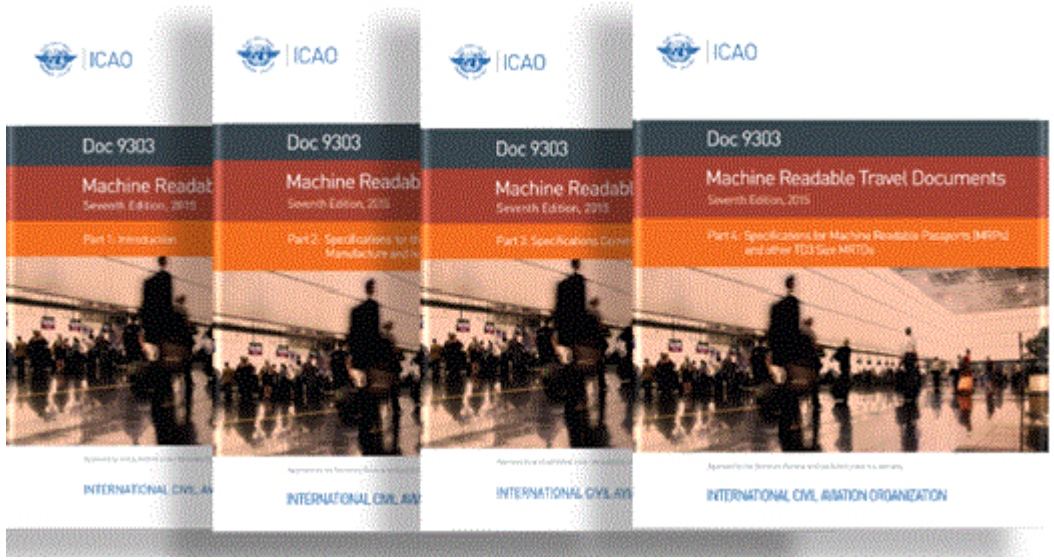
DataGroup 2

DataGroup 3

EU mandatory
- 2 Fingerprints

Source: Dr. Uwe Seidel, Chair NTWG

ICAO eMRTD



Part 1: Introduction

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

Part 3: Specifications common to all Machine Readable Travel Documents

Part 4: Specifications specific to TD3 size MRTDs, Machine Readable Passports

Part 9: The Deployment of Biometric Identification and Electronic Storage of Data in MRTDs

Part 10: Logical Data Structure for storage of Biometrics and Other Data in Contactless Integrated Circuit (IC)

Part 11: Security Mechanisms for MRTDs

Part 12: Public Key Infrastructure for Machine Readable Travel Documents

- Good Physical Security
- Binding to holder – Biographic and Biometric information
- Standardised data elements and fields – Global interoperability
- Electronic Security- eMRTD PKI, Clone detection

Further Improvement - Digital Travel Credentials (DTC)

LDS

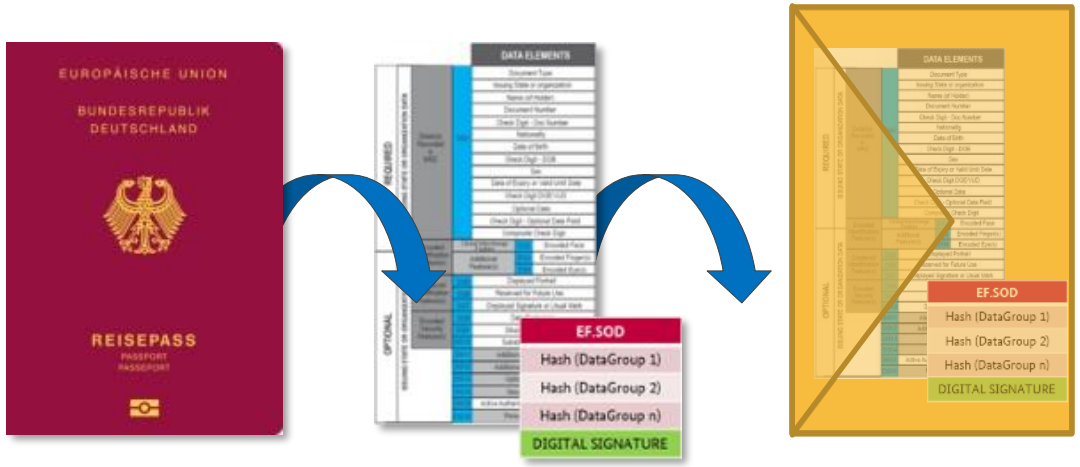
			DATA ELEMENTS
REQUIRED	ISSUING STATE OR ORGANIZATION DATA	Detail(s) Recorded in MRZ	DG1	Document Type
				Issuing State or organization
				Name (of Holder)
				Document Number
				Check Digit - Doc Number
				Nationality
				Date of Birth
				Check Digit - DOB
				Sex
				Data of Expiry or Valid Until Date
				Check Digit DOE/VUD
				Optional Data
				Check Digit - Optional Data Field
				Composite Check Digit
		Encoded Identification Feature(s)	Global Interchange Feature	DG2	Encoded Face
			Additional Feature(s)	DG3	Encoded Finger(s)
				DG4	Encoded Eye(s)
OPTIONAL	ISSUING STATE OR ORGANIZATION DATA	Displayed Identification Feature(s)	DG5	Displayed Portrait
			DG6	Reserved for Future Use
			DG7	Displayed Signature or Usual Mark
		Encoded Security Feature(s)	DG8	Data Feature(s)
			DG9	Structure Feature(s)
			DG10	Substance Feature(s)
			DG11	Additional Personal Detail(s)
			DG12	Additional Document Detail(s)
			DG13	Optional Detail(s)
			DG14	Security Options
			DG15	Active Authentication Public Key Info
			DG16	Person(s) to Notify

DataGroup 1	DataGroup 2
• Document Type • Issuing State • Name of Holder • Document Number • Nationality • Date of Birth • Check Digit DOB • Sex • Date of Expiry • …	

To proof integrity and authenticity of the data, the chip contains the Document Security Object

EF.SOD
Hash (DataGroup 1)
Hash (DataGroup 2)
Hash (DataGroup n)
DIGITAL SIGNATURE

Digital Travel Credentials



- No Physical Security
- Binding to holder – Biographic and Biometric information
- Standardised data elements and fields – Global interoperability
- Electronic Security- eMRTD PKI, Clone detection

The DTC will be covered in detail in Session 6

2. Current Landscape

Second Letter in Passport MRZ

- It is currently not possible to determine the type of passport from the MRZ
- This can cause issues at eGates as the visa requirements may differ depending on type of passport
- ICAO has specified the second letter and all issuers must switch to them by 2028

- National Passport – PP
- Emergency Passport – PE
- Single Sheet ETD - PU
- Diplomatic Passport – PD
- Official/Service Passport – PO
- Refugee Passport – PR
- Alien Passport – PT
- Stateless Passport – PS
- Laissez-passer type documents – PL

(UN, EU, Interpol, CARICOM, ECOWAS etc)

Issuance date in MRZ

- VIZ contains date of issue
- MRZ contains only date of expiry
- Knowing the date of issue allows a few possibilities:
  - Detecting the generation of passport for lookup of Physical Security feature template
  - Knowing date of issue can assist some verification workflows at border
- Completely optional

39794-5 Application Profile

- New encoding for DG2 agreed by NTWG and endorsed by TAG/TRIP
- Inspection Systems need to be ready by 2026 to handle the new encoding
- Issuers to switch to new encoding by 2030

ISO/IEC 39794-5 Application Profile

- SC37 has published 39794 in 2021
- NTWG agreed to transition from 19794 to 39794 for DG2, DG3 and DG4
- TF5 worked on Application Profile for Facial image
  - Applicable only to the first facial image stored in DG2
  - DG3 and DG4 encoding currently out of scope
  - Some metadata elements have additional restrictions
  - Gender (Sex) – Male, Female, Other – in line with Doc 9303
  - Image representation block – only 2D representation allowed
  - Image data formats – JPEG, JPEG2000 lossy and JPEG2000 lossless
  - 2D Face Image Kind – restricted to MRTD
  - 3D shape representation block – MUST NOT be used
  - ASN1 for 39794-1 and 39794-5 published to WG3 Github page

Interop tests

- Interoperability event for testing readiness of Issuers and Inspection Systems
- Sydney, October 2024
- Singapore, February 2025
- Silver dataset created and published to WG3 github site
- Additional test data created to simulate future extensions that might be defined by SC37
- Negative test cases – purposefully introduce encoding errors to test how Inspection Systems behave

Why negative tests?

- Encoding errors happen in ePassports
- Finland DTC pilot – defect analysis part of the pilot
- 13 defects detected in a one month trial

★In the attached table, the three columns are: Will fail PA, Can Fail PA, Will Not fail PA

★PA = Passive Authentication

	Will	Can	Will not
Wrong length encoding (security object of the document - SOD)		×	
Wrong criticality of certificate extensions (certificates)		×	
Country code in lower case (certificates)		×	
Wrong key usage (*document signer* certificate - DS)			×
Wrong encoding of eContentType (SOD)		×	
Wrong basicConstraint (DS certificate)			×
Wrong encoding of DocumentTypeList (certificate)		×	
Missing *authority key identifier* (DS certificate)	×		
Wrong Signer Identifier (SOD)	×		
Missing country code in issuer/subject *distinguished name* (certificates)	×		
Wrong encoding of key usage (*document signer* certificate - DS)		×	
Wrong Digest Algorithm (SOD)		×	
DH parameter encoding		×	

Participation

- Sydney
  - 13 eMRTD participants
  - 12 Inspection systems
- Singapore
  - 10 eMRTD participants
  - 10 Inspection Systems
  - 14 observers from governments and international organizations

ICAO TRIP 2025

ISO IEC SC

Test Method

Sydney

- 5 eMRTDs encoded as follows:
  - All mandatory elements
  - All elements
  - Some optional elements
  - Fictitious future extensions
- Reference implementation of an Inspection System that can handle both 19794 and 39794

Singapore

- 7 eMRTDs encoded as follows:
  - All mandatory elements
  - Some optional elements
  - Fictitious future extensions
  - Deliberate errors in encoding
- Reference implementation of an Inspection System that can handle both 19794 and 39794
- Emulator based test environment from two test labs

eMRTD specimens

Sydney

- Correctly encoded – 52%
- Wrongly encoded – 48%
- Re-use silver data set – 56%
- Correct encoding from scratch – 25%

Singapore

- Correctly encoded – 86%
- Wrongly encoded – 14%
- Re-use silver data set – 19%
- Correct encoding from scratch - 82%

Inspection system – positive tests

Sydney

- Read success – 79%
- With simulated extensions – 54%

Singapore

- Read success – 95%
- With simulated extensions – 95%

Inspection system – negative tests

Sydney

- Full success – 4%
- Displayed image without warning – 33%
- So, total success = 37%

Singapore

- Full success – 16%
- Displayed image without warning – 46%
- Total success = 62%

Summary

- Huge improvement in the ability of Inspection systems to handle 39794-5 AP with future extensions as well – 95%
- Serious issues with encoding errors
  - Doc 9303 does not have specifications for Inspection systems
  - BUT, there is a test specification for Inspection Systems
    - Requires IS to fail if there is an encoding error !!!!!!!!!!!
  - NTWG has endorsed creating specifications for Functional Requirements for Inspection Systems

3rd Interop test - Montreal

- November 6-7, 2025
- Participants – 19 States/Vendors
- Observers – 9 States/Organizations

Day 1 – Smoke test of passports and one on one debug sessions

Day 2 – Actual interop event

Doc 9303 9th edition

- Integration of Technical Reports into the 8th edition
- Removing ambiguity in Parts 3-8
- New part 14 on Biometrics
- Possible new Part 15 on Functional Requirements for Inspection Systems

3. Future Challenges

Post Quantum Cryptography

- ICAO compliant eMRTDs heavily rely on ‘classical’ public key cryptography (RSA, ECC algorithms), considered reliable and robust against ‘classical’ computational attacks
- A Quantum Computer will be able to break ‘classical’ cryptography; consequently, undermining the current security mechanisms
- Biggest Threat is to Passive Authentication
- Current work on “Quantum safe mechanisms for the Document Issuing PKI and Passive Authentication”- will include the migration strategy

Thank You

R.Rajeshkumar@auctorizium.com
RRaj88@gmail.com
www.linkedin.com/in/rraj88