ISO Update

R Rajeshkumar

Convener- ISO/IEC JTC1 SC17/WG3

Leader – SC17/WG3/TF5

Editor – Doc 9303 parts 9 and 12

Editor – VDS-NC, DTC, IDB, 39794-5 AP

Chief Executive – Auctorizium Pte Ltd

Technical Advisory Group

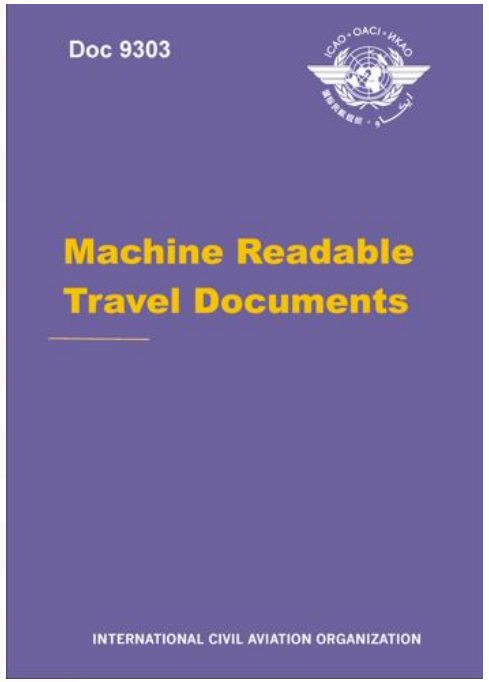
Implementation & **C**apacity **B**uilding **W**orking **G**roup

New **T**echnologies **W**orking **G**roup

Relationship governed by agreement between ICAO and ISO/IEC JTC1

ISO/IEC JTC1 SC17/WG3

Historical Facts:
Doc 9303 – MRTDs specifications



- First edition 1980;
- 1986 first meeting of TAG/MRP
- 1989 Liaison between ICAO and ISO for maintenance of Doc 9303
- 1990 The group was renamed to TAG/MRTD

What is ISO?

- A network of national standards institutes of 156 countries
- Non-government organization
- Central Secretariat in Geneva (CHE)
- Members:
  - Not delegations from national governments
  - Come from government institutions and the private sector .. *creating a consensus*

Initial Focus of ICAO and ISO

- Prior to 1990 ……..
- Each organization published its own Standard for a **Machine Readable Passport (MRP)**
-
- ICAO Published:
  - ICAO Doc 9303
- ISO Published:
  - ISO 7501-1

ICAO / ISO Partnership Formed

- ICAO / ISO agreed collaboration formula
- In 1989, Subcommittee 17 (SC17) of JTC1 of ISO agreed to the collaboration formula which had:
  - ICAO develop and agree specifications for MRTDs … supported by ISO participation
  - ISO endorse the ICAO specifications as the International Standard
- SC17/WG3 established – First meeting in Ottawa from Feb 26, 1990 – March 8, 1990

ICAO and ISO Partnership

- Over the past 36 years ……..
- ICAO and ISO have established and operated an effective partnership
- It has derived its effectiveness from:
  - the authority and leadership of ICAO;
  - the technical and standards setting competencies of ISO; and
  - the skills and dedication of the people contributing to both Organizations.

Working Relationship between ICAO and ISO

ICAO

ICAO Council

Air Transport Committee

TAG-TRIP

ICBWG

NTWG

ISO

JTC1

SC17

SC31 (2D Barcode)

SC37 (Biometric)

3166-MA (Country code)

WG3

WG4 (Contact chips)

WG8 (Contactless chips)

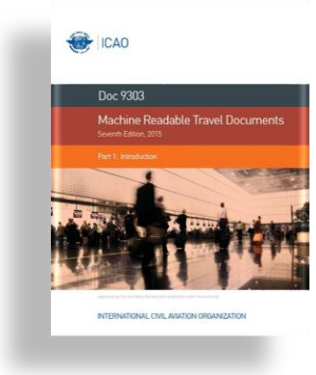
TF1

TF2

TF3

TF4

TF5



ICAO PKD

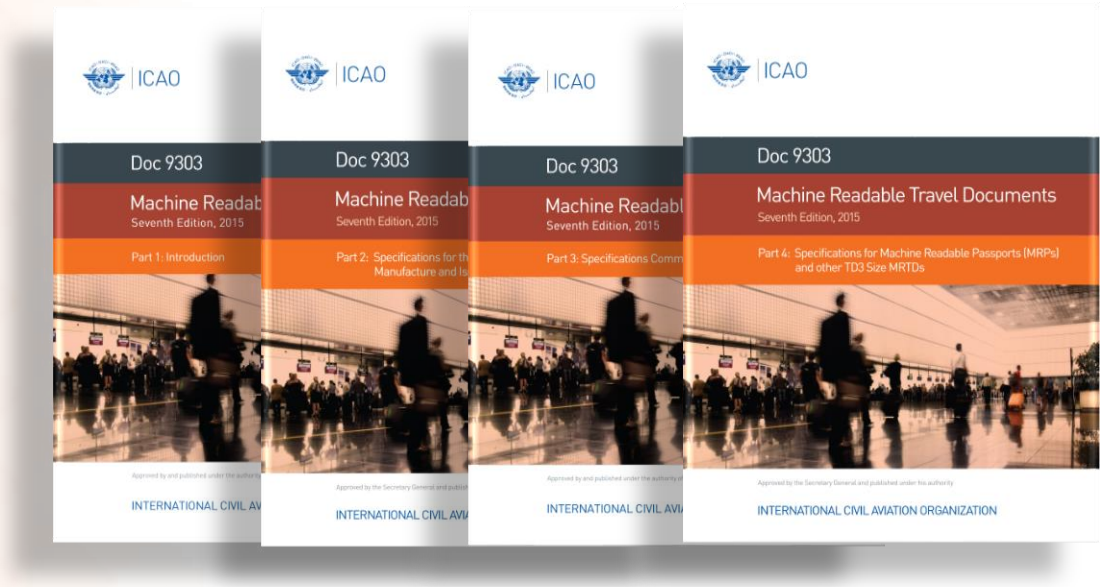
ICAO Doc 9303 / ISO-IEC 7501

eMRTD specifications

Doc 9303 – 8th edition

1. Introduction
2. Specifications for the Security of Design, Manufacture and Issuance of MRTDs
3. Specifications common to all Machine Readable Travel Documents
4. Specifications specific to TD3 size MRTDs, Machine Readable Passports
5. Specifications specific to TD1 size MRTDs, Machine Readable Official Travel Documents
6. Specifications specific to TD2 size MRTDs, Machine Readable Official Travel Documents
7. Machine Readable Visas
8. Emergency Travel Documents
9. The Deployment of Biometric Identification and Electronic Storage of Data in MRTDs
10. Logical Data Structure for storage of Biometrics and Other Data in Contactless Integrated Circuit (IC)
11. Security Mechanisms for MRTDs
12. Public Key Infrastructure for Machine Readable Travel Documents
13. Visible Digital Seal

How to use – Issuing MRTD



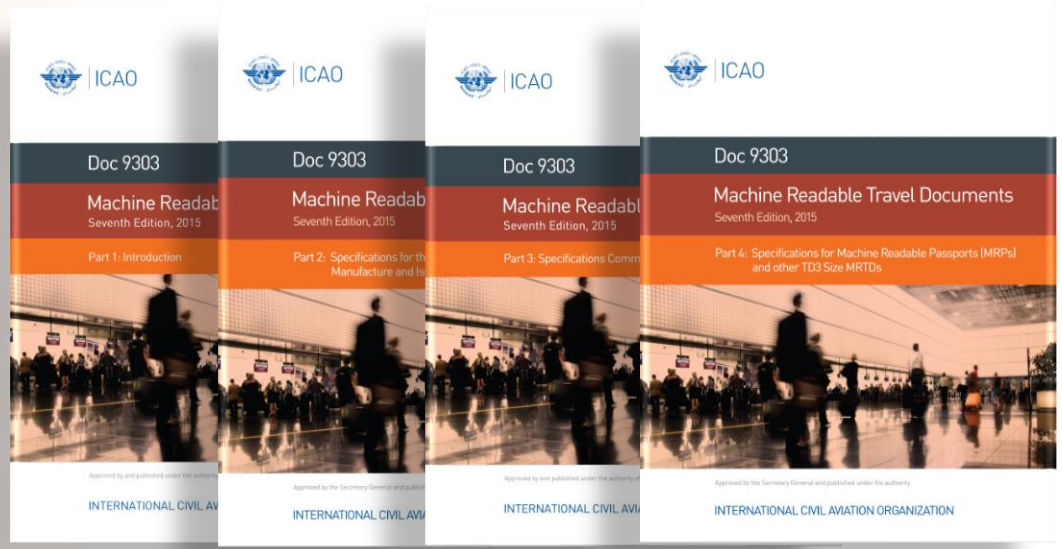
Part 1: Introduction

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

How to use – Issuing eMRTD

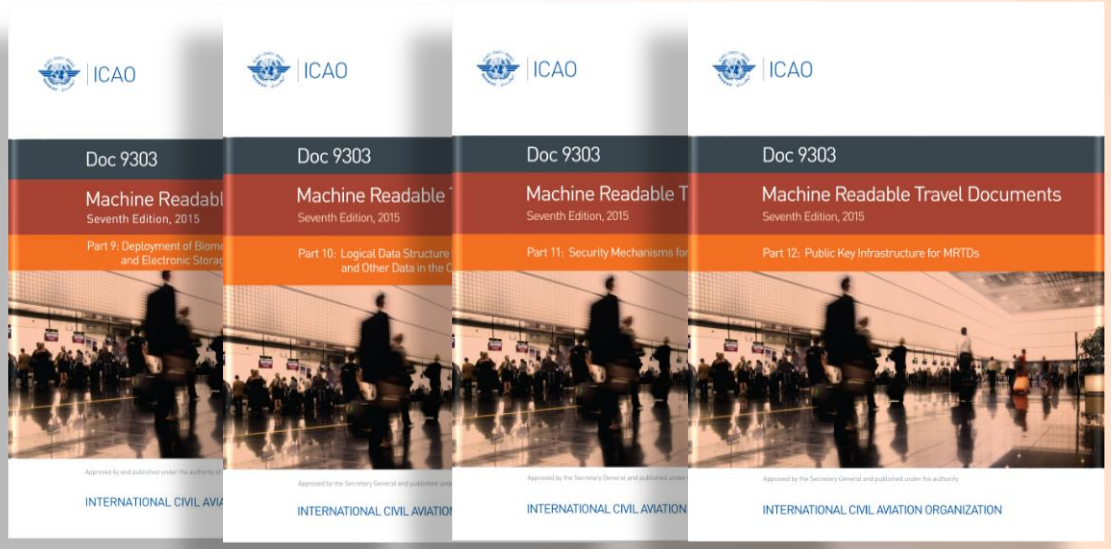


Part 1: Introduction

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



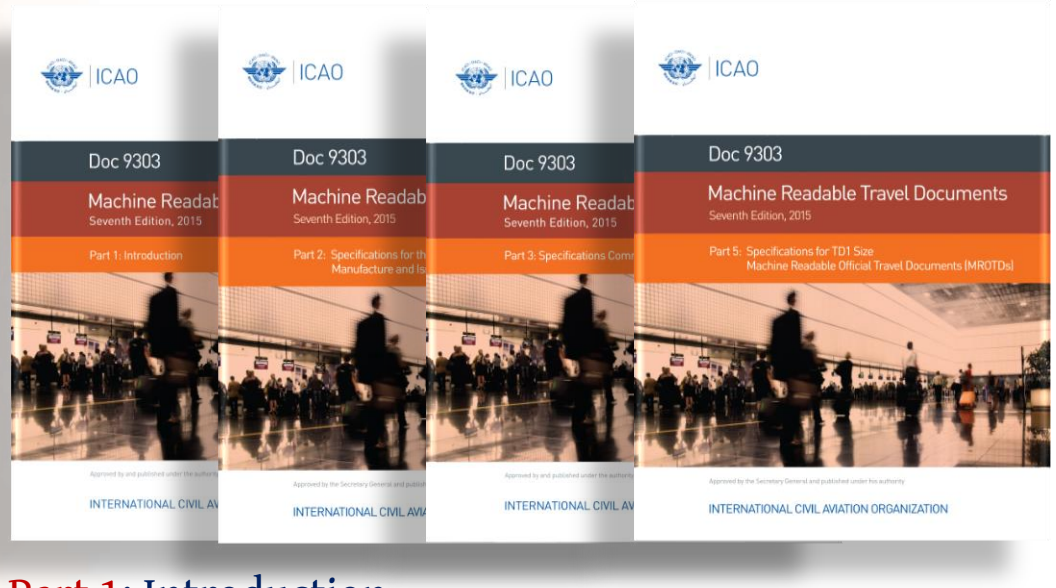
Part 9: The Deployment of Biometric Identification and Electronic Storage of Data in MRTDs

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

How to use – Issuing TD1 size card without chip



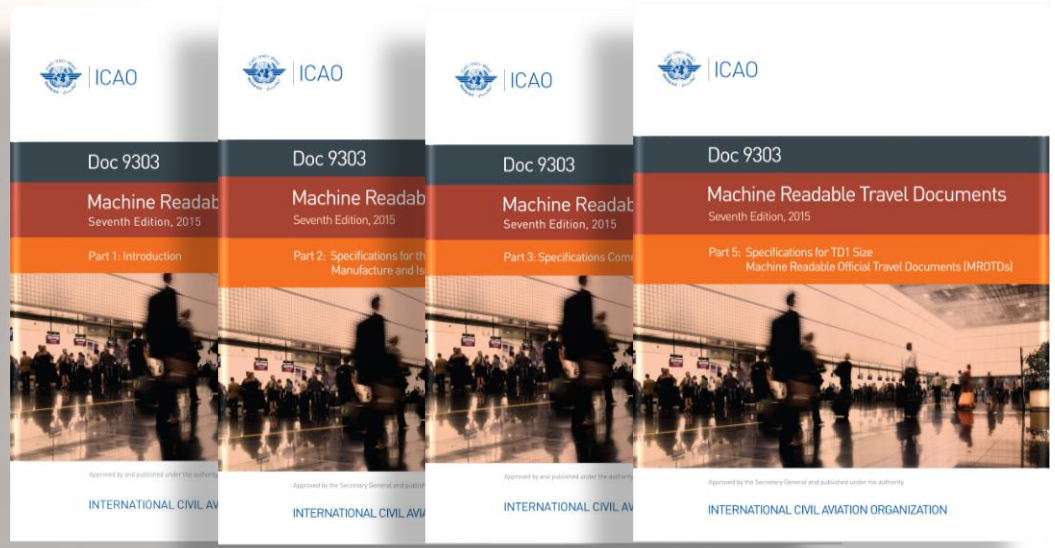
Part 1: Introduction

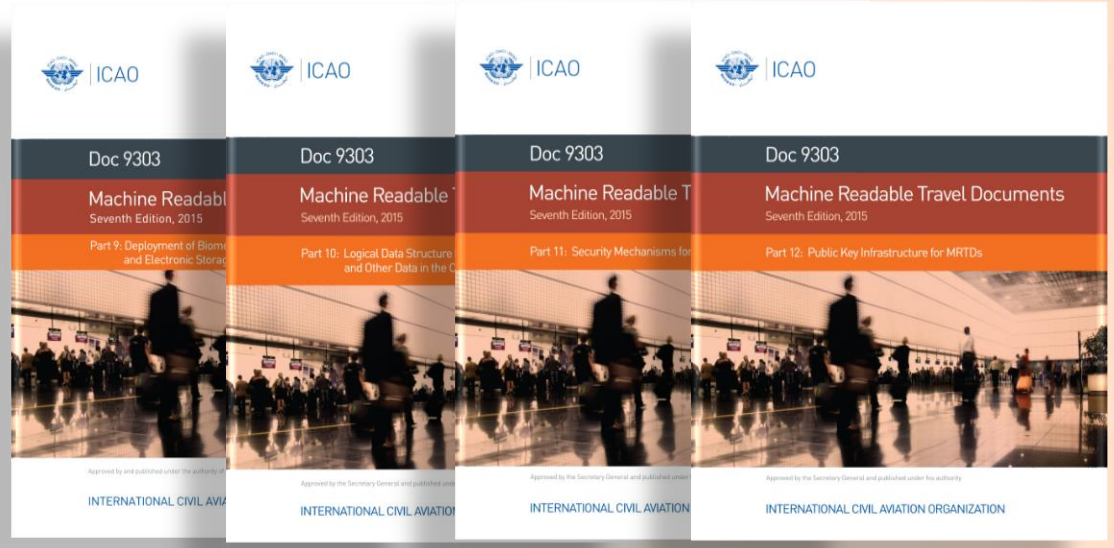
Part 2: Specifications for the Security of Design, Manufacture and Issuance of MRTDs

Part 3: Specifications common to all Machine Readable Travel Documents

Part 5: Specifications specific to TD1 size MRTDs, Machine Readable Official Travel Documents

How to use – Issuing TD1 size card with chip





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 5: Specifications specific to TD1 size MRTDs, Machine Readable Official Travel Documents

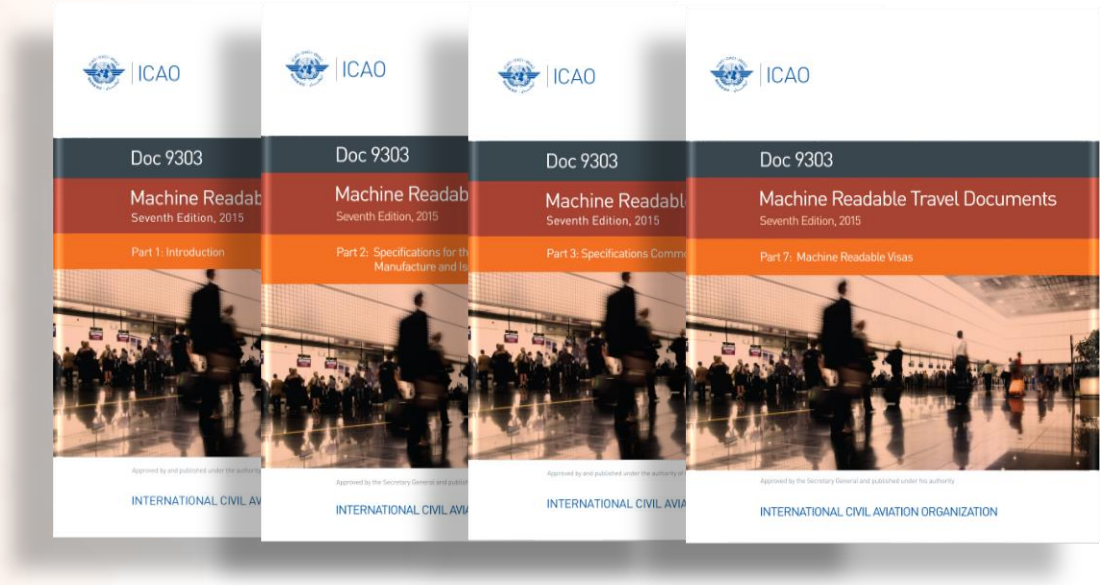
Part 9: The Deployment of Biometric Identification and Electronic Storage of Data in MRTDs

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

How to use – Issuing MRV



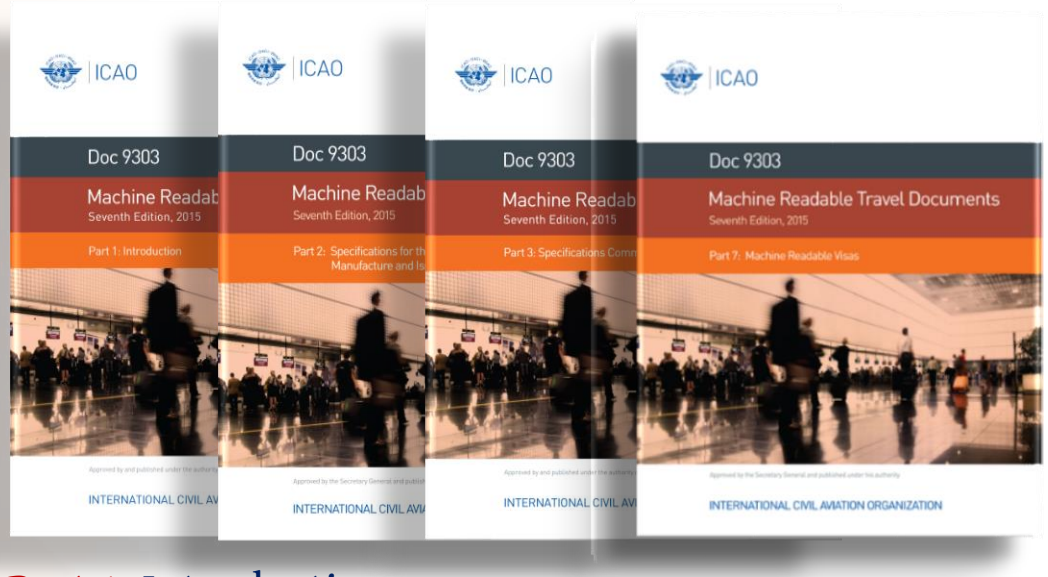
Part 1: Introduction

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

Part 3: Specifications common to all Machine Readable Travel Documents

Part 7: Machine Readable Visas

How to use – Issuing MRV with VDS

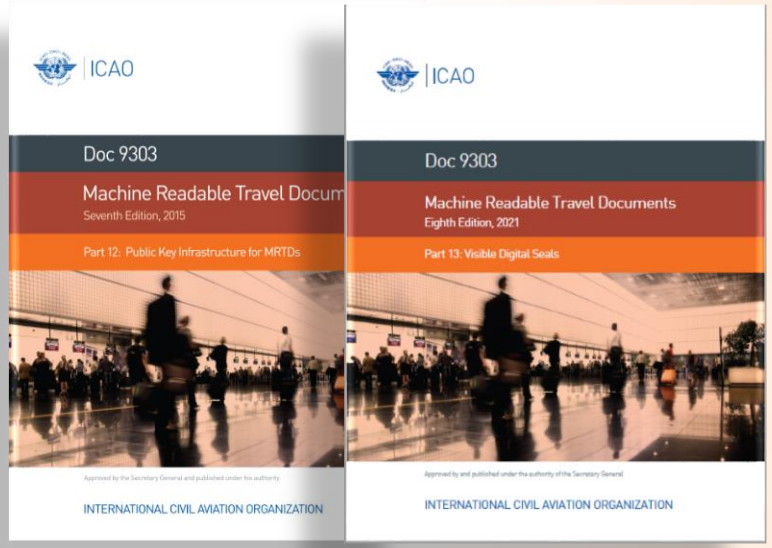


Part 1: Introduction

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

Part 3: Specifications common to all Machine Readable Travel Documents

Part 7: Machine Readable Visas



Part 12: Public Key Infrastructure for Machine Readable Travel Documents

Part 13: Visible Digital Seal

Structure of document

- Normative information – Mandatory

Any document claiming conformance to Doc 9303 MUST implement these specifications.

- Informative (Mostly in Appendices)

Either a guidance or could also refer to optional elements.

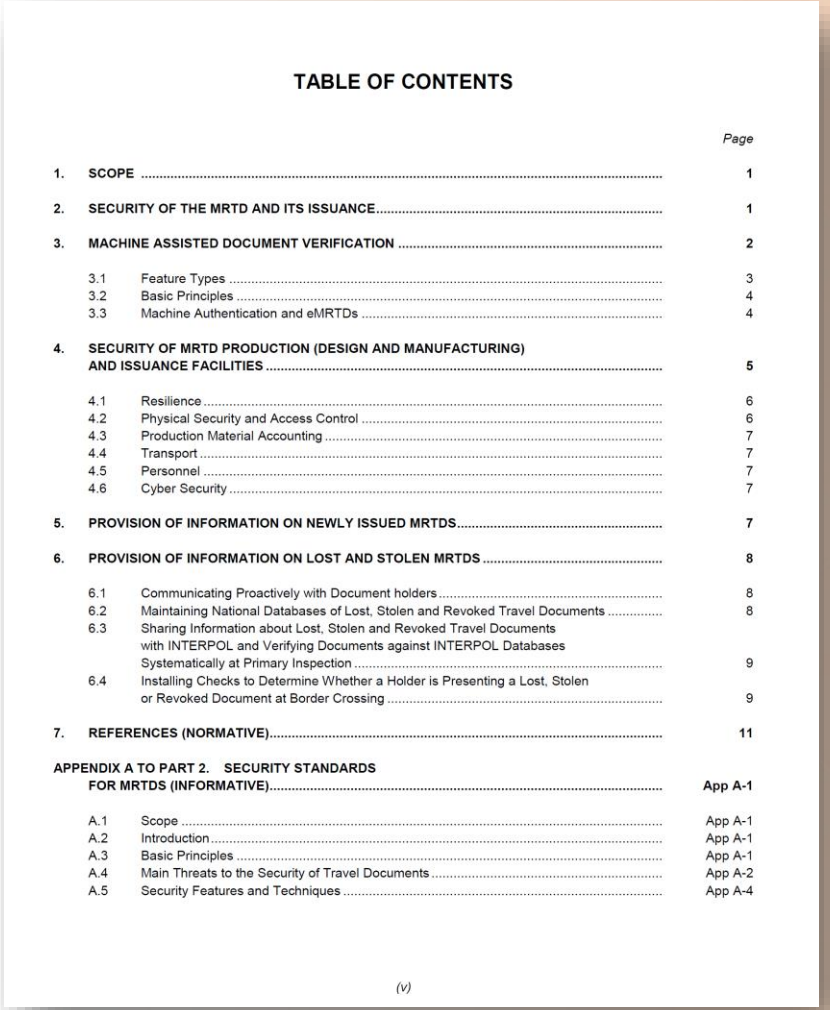


TABLE OF CONTENTS

(v)

Changes to Doc 9303

- Corrigenda – Correction of an error in the published document

- Amendment – A minor revision of the published document

Technical Reports

- New specifications developed after the publishing of a specific edition of Doc 9303
- Created by ISO, approved by NTWG and then endorsed by TAG.
- Once approved by NTWG and endorsed by TAG, it is published on ICAO website
- Considered to be part of the published version of Doc 9303 specifications

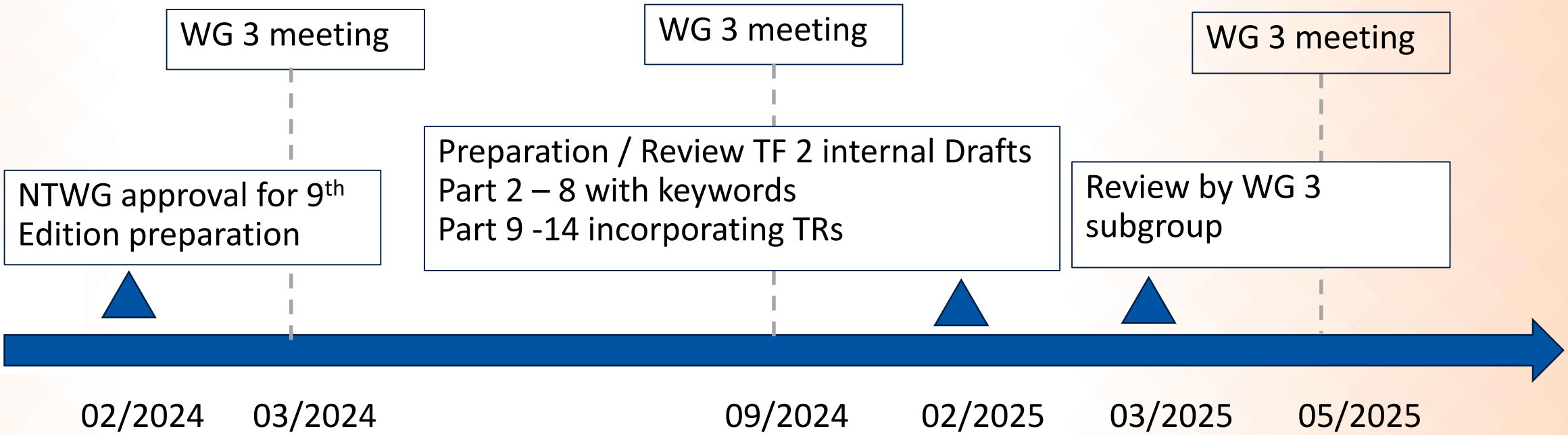
Next Edition of Doc 9303

- After a few technical reports are published, they are then incorporated directly into Doc 9303 to form the next edition.
- An editorial effort – No new specifications are introduced during this process
- On average, every 5 to 7 years – The technical reports are then retired in favour of the current edition of Doc 9303

Towards the 9th edition of Doc 9303

- Focus on editorial work
  - Incorporate published ICAO Technical Reports
  - Harmonize the terminology with the terms to be adopted in Annex 9 “Facilitation”
  - Express provisions in part 2 – 8 using the keywords SHALL, SHOULD, MAY etc.
  - Clarifications & correction of obvious errors / inconsistencies
  - Deprecate Doc 9303-6 for TD2 sized MROTDs

Doc 9303 9th Edition – Tentative Schedule



Targeting 2027 for new 9th edition

Technical Reports in progress

- eMRTD Bound DTC-VC Extended – add additional photo to the VC
- DTC-VC – Transmission Protocol
  - 2 existing protocol (OpenID4VP, ISO/IEC 23220-4 REST API) and 1 protocol under development (Browser API) are candidates
- DTC-PC Phase 2 – defining a Physical Component with alternate form factor (mobile phone)
  - Focus on security and certification of the device before defining the protocols

ISO/IEC 18745-1 revision – Physical Test Specifications

- Test for Hot Stamp on the cover to be investigated

Research on Post Quantum Cryptography

Cryptographic Protocol	Impact of a cryptographically relevant quantum computer on current protocol implementation.	Threat Severity
Passive Authentication	• Cryptographic protection of an electronic travel document would be entirely compromised. • Both the document issuing PKI (CSCA & Document/SealSigner) as well as the data stored by an eMRTD would be affected.	High
Chip/Active Authentication	• Protection against cloning or substitution of the eMRTD's chip would be no longer available.	Medium
PACE	• The inspection procedure of an eMRTD's chip would no longer be protected from sniffing and/or eavesdropping.	Medium
Terminal Authentication	• Protection of highly sensitive biometric data on a chip (fingerprints or iris) would no longer be available.	Medium
Secure Messaging	• None (if a sufficient key-length is used)	None

Status quo of Post-Quantum Cryptography

- First cryptographic primitives for digital signatures and key encapsulation are available
  - Stateful hash-based signature schemes: XMSS, LMS
  - NIST competition on Post-Quantum Encryption Standards released first 3 final standards: ML-KEM (CRYSTALS-Kyber), ML-DSA (CRYSTALS-Dilithium), SLH-DSA (Sphincs+)
- Primitives must be implemented into cryptographic protocols
  - Specifications for using PQC algorithms in X.509 certificates or CMS are still mostly in draft status
- Collaboration between SC17/WG3 and SC27/WG2 to take this forward – target is to have specifications by 2027

Doc 9303 cryptographic key length review

- Review all currently allowed cryptographic algorithms, domain parameters and key lengths in Doc 9303 (part 11, 12 and 13)
- Analyze the impact of further cryptographic primitives (e.g. SHA-3), key-lengths or domain parameters (e.g. finite fields > 2048 bits)
- Ad-hoc group prepared first draft
  - Only covers review of currently allowed algorithms
  - Idea: Map each algorithm & key length to a security strength
- Document is still under discussion
  - Challenge: Keep balance between raising security and technical feasibility
  - No recommendations for the time being

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

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 !!!!!!!!!!!
  - Will be looking at putting specifications into Doc 9303 for IS after the next NTWG meeting
- Detailed report will be out soon – will publish on ISO portal and ICAO teams – will be distributed to this group as well
- More interop events in future..

Thank You

R.Rajeshkumar@auctorizium.com
RRaj88@gmail.com