



| ICAO

SECURITY & FACILITATION



# ICAO DOC 9303: COMPOSITION / AMENDMENTS / TECHNICAL REPORTS

Tom Kinneging  
Convener ISO/IEC JTC1  
SC17 WG3

Montréal, 2018-10-24





ICAO

SECURITY & FACILITATION



# ICAO Doc 9303 - Machine Readable Travel Documents

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
11. Security Protocols
12. Public Key Infrastructure for Machine Readable Travel Documents



| ICAO

SECURITY & FACILITATION



## Part 1 - Introduction

1. Foreword
2. Scope
3. General considerations
4. Definitions and Abbreviations
5. Guidance on the use of Doc 9303
6. References



ICAO

SECURITY & FACILITATION



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

1. Scope
  2. Security of the MRTD and its Issuance
  3. Machine Assisted Document Verification
  4. Security of MRTD Production and Issuance Facilities
  5. Provision of Information on Newly Issued MRTDs
  6. Provision of Information on Lost and Stolen MRTDs
- Appendix A – Security Standards for MRTDs
- Appendix B – Machine Assisted Document Security Verification
- Appendix C – The Prevention of Fraud Associated with the Issuance Process
- Appendix D – ASF/SLTD Key Considerations



ICAO

SECURITY & FACILITATION



## Part 3 - Specifications Common to all Machine Readable Travel Documents

1. Scope
  2. Physical Characteristics of MRTDs
  3. Visual Inspection Zone (VIZ)
  4. Machine Readable Zone (MRZ)
  5. Codes for Nationality, Place of Birth, Location of Issuing State/Authority and other Purposes
  6. Transliterations Recommended for Use by States
  7. Deviations
  8. References
- Appendix A – Examples of Check Digit Calculation
- Appendix B – Arabic Transliteration, Details and Examples



| ICAO

SECURITY & FACILITATION



## Part 3 - Amendments

- Editorial corrections
- Clarifications
- Three letter codes
  - EUE (European Union)
  - XBA (African Development Bank)
  - XEC (Economic Community of West African States)
  - XCE (Council of Europe)
  - XDC (Southern African Development Community)
- Representation of dates



## Part 4 - Specifications for Machine Readable Passports and other TD3 size MRTDs

1. Scope
2. Construction and Dimensions of the MRP and MRP Data Page
3. General Layout of the MRP Data Page
4. Contents of the MRP Data Page
5. References

Appendix A – Examples of a Personalized MRP Data Page

Appendix B – Construction of the Machine Readable Zone of the Passport Data Page



| ICAO

SECURITY & FACILITATION



## Part 4 - Amendments

- Revised figures (date formats)
- Added “After issuance no additional pages shall be added to the MRP”



## Part 5 - Specifications for TD1 size Machine Readable Official Travel Documents (MROTDs)

1. Scope
2. Dimensions of the TD1 size MROTD
3. General Layout of the TD1 size MROTD
4. Contents of a TD1 size MROTD
5. References

Appendix A – Examples of a Personalized TD1 size MROTD

Appendix B – Construction of the Machine Readable Zone of a TD1 size MROTD

Appendix C – Technical Specifications for a Machine Readable Crew Member Certificate (CMC)



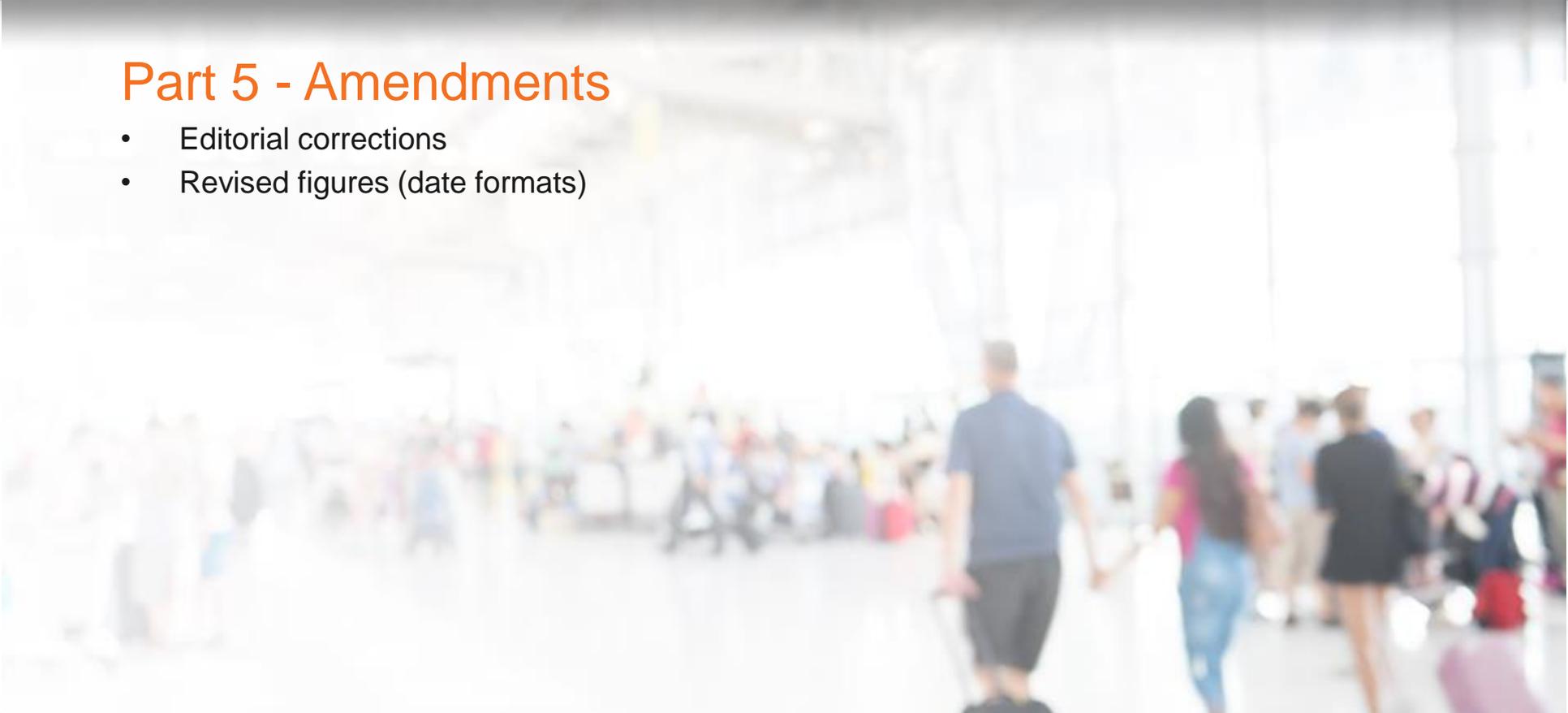
| ICAO

SECURITY & FACILITATION



## Part 5 - Amendments

- Editorial corrections
- Revised figures (date formats)





## Part 6 - Specifications for TD2 size Machine Readable Official Travel Documents (MROTDs)

1. Scope
2. Dimensions of the TD2 size MROTD
3. General Layout of the TD2 size MROTD
4. Contents of a TD2 size MROTD
5. References

Appendix A – Examples of a Personalized TD2 size MROTD

Appendix B – Construction of the Machine Readable Zone of a TD2 size MROTD



## Part 7 - Specifications for Machine Readable Visas

1. Scope
  2. Technical Specifications for Format-A Machine Readable Visas (MRV-A)
  3. General Layout of the MRV-A
  4. Detailed Layout of the MRV-A
  5. Technical Specifications for Format-B Machine Readable Visas (MRV-B)
  6. General Layout of the MRV-B
  7. Detailed Layout of the MRV-B
  8. Use of Optional barcodes on Machine Readable Visas
  9. References
- Appendix A – Examples of a Personalized MRVs
- Appendix B – Construction of the MRZ
- Appendix C – Positioning in Passport
- Appendix D – Materials and Production Methods



| ICAO

SECURITY & FACILITATION



## Part 8 - Guidance on Emergency Travel Documents (New)

1. Scope
2. Introduction
3. Background
4. Principles and Recommended Practices
5. Summary
6. References



## Part 9 - Deployment of Biometric Identification and Electronic Storage of Data in MRTDs

1. Scope
  2. eMRTD
  3. Biometric Identification
  4. The Selection of Biometrics Applicable to eMRTDs
  5. Storage of the Biometric and other Data in a Logical Format in a Contactless IC
  6. Test Methodologies for (e)MRTDs
  7. References
- Appendix A – Placement of the Contactless IC in an eMRP
- Appendix B – Process for Reading eMRTDs



| ICAO

SECURITY & FACILITATION



## Part 9 - Amendments

- Editorial corrections
- Added reference to ISO/IEC 14443 application profile
- Updated references to
  - ISO/IEC 18745-2,
  - ISO/IEC 10373-6,
  - ISO/IEC 14443 1-4
- Revised Appendix A



## Part 10 - Logical Data Structure (LDS) for Storage of Biometrics and other Data in the Contactless IC

1. Scope
  2. Requirements of the Logical Data Structure
  3. Application Profile for the Contactless IC
  4. File Structure Specifications
  5. Elementary Files
  6. Data Elements Forming Data Groups 1 through 16
  7. References
- Appendix A – Logical Data Structure Mapping Examples



| ICAO

SECURITY & FACILITATION



## Part 10 - Amendments

- Editorial corrections
- Inclusion of Document Signer Certificate in Security Object has become MANDATORY
- Added Appendix B (14443 application profile: The contactless IC in an eMRP)
- Added Appendix C (14443 application profile: Inspection Systems)



## Part 11 - Security Mechanisms for MRTDs

1. Scope
  2. Assumptions and Notations
  3. Securing Electronic Data
  4. Access to the Contactless IC
  5. Authentication of Data
  6. Authentication of the Contactless IC
  7. Additional Access Control Mechanisms
  8. Inspection System
  9. Common Specifications
  10. References
- Appendix A – Entropy of the MRZ-Derived Access Keys
  - Appendix B – Point Encoding for the ECDH-Integrated Mapping
  - Appendix C – Challenge Semantics
  - Appendix D – Worked Example: Basic Access Control
  - Appendix E – Worked Example: Passive Authentication
  - Appendix F – Worked Example: Active Authentication
  - Appendix G – Worked Example: PACE – Generic Mapping
  - Appendix H – Worked Example: PACE – Integrated Mapping



| ICAO

SECURITY & FACILITATION



## Part 11 - Amendments

- Editorial corrections
- Added Appendix I (PACE CA Mapping)





## Part 12 - Public Key Infrastructure for MRTDs

1. Scope
  2. Overview of the Public Key Infrastructure
  3. Roles and Responsibilities
  4. Key Management
  5. Distribution Mechanisms
  6. PKI Trust and Validation
  7. Certificate and CRL Profiles
  8. CSCA Master List Structure
  9. References
- Appendix A – Lifetimes
- Appendix B – Certificate and CRL Profile Reference Text
- Appendix C – Earlier Certificate Profiles
- Appendix D – RFC 5280 Validation Compatibility



| ICAO

SECURITY & FACILITATION



## Technical Reports & Guidance (TAG-TRIP 2)

- TR - Visible Digital Seals
- TR - Logical Data Structure 2
- TR - Portrait Quality
- TR - RF and Protocol Testing Part 3
- TR - RF and Protocol Testing Part 4
- TR - RF and Protocol Testing Part 5
- Guidance on CSCA Migration
- Best practice guidelines for Optical Machine Authentication
- Guidance on Evidence of Identity



| ICAO

SECURITY & FACILITATION



## 'Old' new specifications

- 2011 – LDS v1.8
  - LDS versioning in (signed) SOD
- 2014 – Supplemental Access Control
  - Password Authenticated Connection Establishment (PACE)
  - SAC = BAC + PACE
  - 01-01-2018 PACE-only passports



| ICAO

SECURITY & FACILITATION



<https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

Tom Kinneging

tom.kinneging@idemia.com