



INTERNATIONAL CIVIL AVIATION ORGANIZATION



CASA DA MOEDA
DO BRASIL



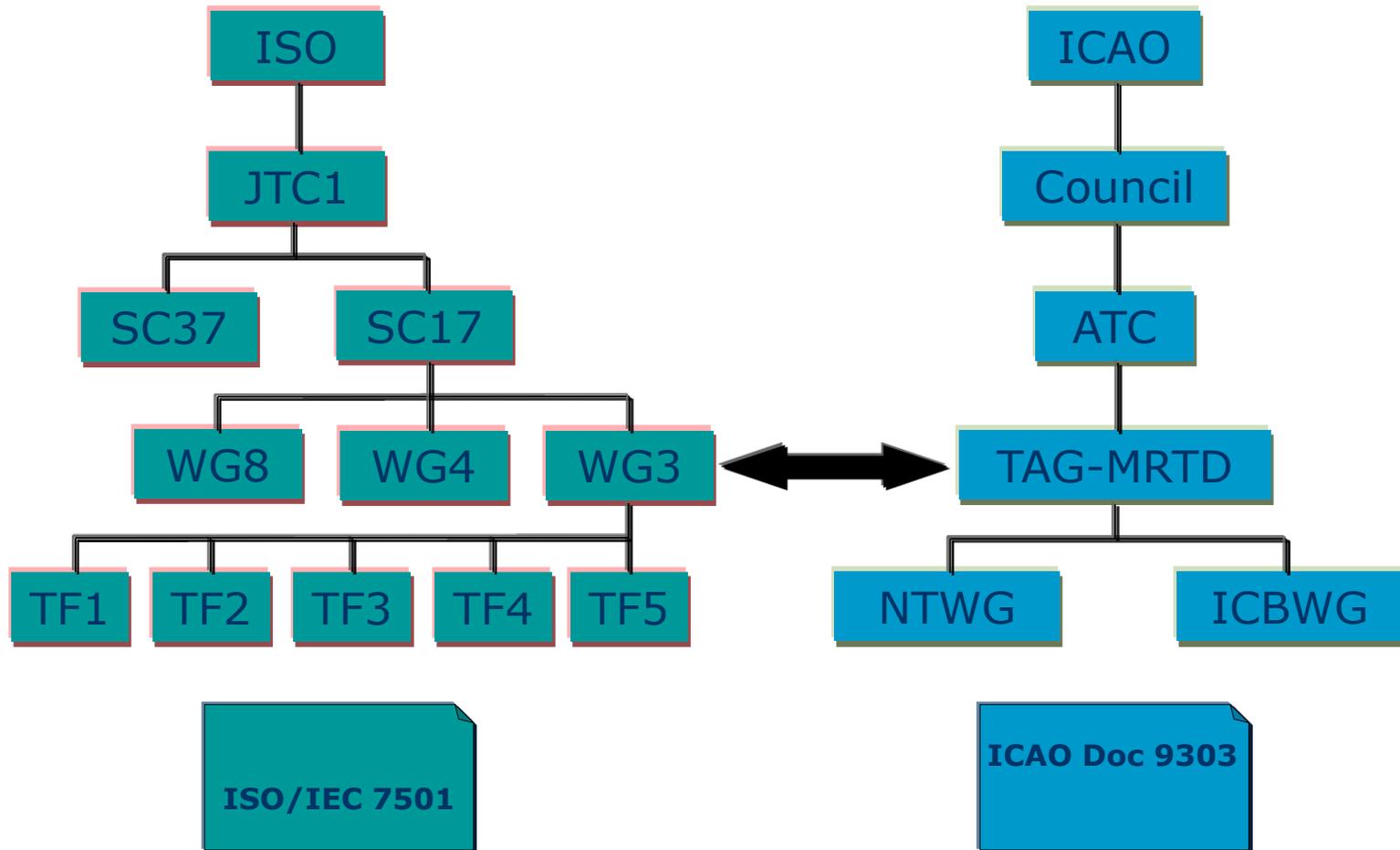
New Doc 9303 developments and latest Technical Reports

Tom Kinneging

Senior expert standardization, Morpho, Netherlands

Convenor ISO/IEC JTC1 SC17 WG3

ICAO-ISO collaboration



The 9303 standard

- ▶ Part 1 – Machine Readable Passports, Sixth edition – 2006
 - Volume 1 – Passports with Machine Readable data stored in OCR format
 - Volume 2 – Electronically enabled Passports with Biometric Identification Capability
- ▶ Part 2 – Machine Readable Visas, Third edition – 2005
- ▶ Part 3 – Machine Readable Official Travel Documents, Third edition – 2008
 - Volume 1 – MRtds with Machine Readable data stored in OCR format
 - Volume 2 – Electronically enabled MRtds with Biometric Identification Capability
- ▶ Supplement to Doc 9303, Release 11 – 2011
- ▶ Technical Reports

Doc 9303 revision

- ▶ Three activities
 - Clean up Supplement
 - Incorporate Technical Reports
 - Re-structure Doc 9303

Clean-up Supplement

- ▶ Supplement Release 11 – 2011
 - ▶ 146 issues
 - Clarifications
 - Interpretations
 - Fixes
 - ▶ Doc 9303 readability
 - ▶ Incorporate Supplement issues into Doc 9303
- 

Incorporate Technical Reports

- ▶ TR – CSCA Countersigning and Master List issuance
 - ▶ TR – Supplemental Access Control for MRTDs
 - ▶ TR – LDS and PKI Maintenance
 - ▶ TR – Machine Assisted Document Security Verification
 - ▶ TR – Machine reading options for td1 size MRTDs
- 

Incorporate Technical Reports

- ▶ TR – CSCA Countersigning and Master List issuance
 - Version 1.0 – June 23, 2009
- ▶ Bilateral exchange of CSCA certificates
 - Lack of specified mechanisms
 - Inefficiency
- ▶ CSCA certificate distribution/publication mechanism
 - Electronically
 - Publication of signed list of received & validated certificates
 - PKD

Incorporate Technical Reports

- ▶ TR – Supplemental Access Control for MRTDs
 - Version 1.01 – November 11, 2010
- ▶ Basic Access Control recommended feature
 - Anti skimming (access control)
 - Anti eavesdropping (session encryption)
 - Strength limited by design
 - 5 & 10 years passport validity periods
- ▶ Supplemental to Basic Access Control
 - PACE V2 (Password Authenticated Connection Establishment)
 - Strength of session keys independent of password
 - Password: Document Number, Date-of-Birth, Date-of-Expiry
 - Password: Card Access Number

Incorporate Technical Reports

- ▶ TR – LDS and PKI Maintenance
 - Version 1.0, endorsed September 2011
- ▶ Evaluation of the standard
 - Accuracy
 - Security
 - Especially cryptographic security features and PKI
- ▶ Updated specifications
 - LDS version number electronically signed
 - Updated certificate profiles
 - Access Control
 - Active Authentication with Elliptic Curve Cryptography

Incorporate Technical Reports

- ▶ TR – Machine Assisted Document Security Verification
 - Version 1.0, endorsed September 2011
 - ▶ Updates/Replaces Doc 9303 Informative Appendix
 - Machine-assisted document security verification
 - ▶ Machine authentication of document security features
 - Materials
 - Security printing
 - Copy protection techniques
 - ▶ Advice on reader technologies
- 

Incorporate Technical Reports

- ▶ TR – Machine reading options for td1 size MRTDs
 - Version 1.0, endorsed September 2011
- ▶ Machine reading issue
 - MRZ on rear side
 - Biographical profile (including photograph) on front side
 - Document related features on front side
 - Card turning
- ▶ Study on options for one-side reading
- ▶ Non-chip enabled
 - One-line MRZ
 - (2D) barcode
 - Further study
- ▶ Chip enabled
 - Chip access
 - CAN position specified

Re-structure Doc 9303

- ▶ Different publication dates for different parts
- ▶ Until 2009 paper based
 - Separate (complete) standards for part 1, 2 and 3
 - Duplicate, mainly general, information
 - Volumes 2 of part 1 and 3 almost identical
- ▶ Since 2009 electronic (pdf) format
 - Maintenance
 - Readability
 - Efficiency
- ▶ Restructuring
 - Specifications appear only once
 - Grouping of general as well as form factor specific specifications
 - Set of (pdf) files
 - User composes relevant subset

Re-structure Doc 9303



Re-structure Doc 9303

▶ ePassport book

The image displays 12 covers of the 'Machine Readable Travel Documents' (Doc 9303) series, each with a numbered circle in the top right corner. The covers are arranged in a grid-like fashion, with some overlapping. The covers are blue with white and yellow text. Each cover features the ICAO logo and the title 'Machine Readable Travel Documents'.

- 1** Introduction
 - Amendments
 - Foreword
- 2** Specifications for the security of the design, manufacture & issuance of MRTDs
 - Security of the MRTD &
- 3** Specifications common to all MRTDs
 - Illustrative guidelines for portraits
 - Three letter codes
 - Transliterations
- 4** Specifications specific to ID3 size MRTDs - Machine Readable Passports
 - Construction & dimensions
- 5** The deployment of biometric identification & electronic storage of data in MRTDs
- 6** Specifications for the security of the design, manufacture & issuance of MRTDs
- 7** Specifications for the security of the design, manufacture & issuance of MRTDs
- 8** Specifications for the security of the design, manufacture & issuance of MRTDs
- 9** The deployment of biometric identification & electronic storage of data in MRTDs
- 10** A Logical Data Structure (LDS) for storage of biometrics & other data in the contactless IC
 - Process for reading eMRTDs
 - Requirements of the LDS
 - Mandatory & optional data elements
 - Ordering & grouping of data elements
 - Mapping principles for contactless IC
 - Data Group specifications
 - Worked examples
- 11** Protocols
 - Basic Access Control
 - PACE V2
 - Passive Authentication
 - Active Authentication
 - eMRTD production and personalization
 - eMRTD inspection
 - Worked examples
- 12** Public Key Infrastructure (PKI) for Machine Readable Travel Documents
 - Overview of the Public Key Infrastructure
 - Document Security Object (SOD)
 - Document Signer (DS)
 - Country Signing CA (CSCA)
 - Algorithms
 - Key management
 - CSCA Master List
 - Certificate Revocation Lists
 - Public Key Directory
 - Non conforming certificates

Re-structure Doc 9303

▶ Non-chip td1 card



Doc 9303 revision project

- ▶ Three activities – Three phases
 - Phase 1 – Re-structuring
 - Phase 2 – Supplement incorporation
 - Phase 3 – Technical Reports incorporation
- ▶ Timeline
 - New structure design – Q4 2011
 - Re-structuring finalized – Q3 2012
 - Supplement issues incorporated – Q4 2012
 - Technical Reports incorporated – Q2 2013
 - Ready for translation / publication – Q3 2013

Thank you for your attention



Tom KINNEGING
Senior Expert Standardization
Product Line ID Documents

tom.kinninging@morpho.com
M +31 65 12 13 702
T +31 23 79 95 218

Morpho B.V.
P.O. Box 5300, 2000 GH Haarlem, The Netherlands
www.morpho.com