Regional Seminar on MRTDs, Biometrics and Identification Management Sint Maarten, 9-11 July 2013



ICAO MRTD and eMRTD Standards and Specifications

Tom Kinneging Senior expert standardization, Morpho, Netherlands
Convenor ISO/IEC JTC1 SC17 WG3

The Doc 9303 standard

- Part 1 Machine Readable Passports, Sixth edition 2006
 - o Volume 1 Passports with Machine Readable data stored in OCR format
 - o 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
 - o Volume 1 MRtds with Machine Readable data stored in OCR format
 - o Volume 2 Electronically enabled MRtds with Biometric Identification Capability
- Supplement to Doc 9303, Release 12 2013
- Technical Reports

http://www.icao.int/security/mrtd/pages/default.aspx

Doc 9303 revision

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

Clean-up Supplement

- Supplement Release 12 2013
- 155 issues
 - Clarifications
 - o Interpretations
 - o Fixes
- Doc 9303 readability
- Incorporate Supplement issues into Doc 9303

- TR MRTDs: History, Interoperability and Implementation
- TR CSCA Countersigning and Master List issuance
- TR LDS and PKI Maintenance
- TR Supplemental Access Control for MRTDs
- TR Machine reading options for td1 size MRTDs
- TR Machine Assisted Document Security Verification
- TR Transliteration of Arabic Script in MRTDs

- TR MRTDs: History, Interoperability and Implementation
 - o Version 1.4 March 2007
- Summary of ICAO key decisions
 - Policies
 - Procedures
 - o Technology
- Guide in using specifications
 - o Doc 9303
 - o Supplement
 - o Technical reports
- Concepts
 - o Global interoperability
 - o Uniformity
 - o Technical reliability
 - o Practicality
 - Quality

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

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

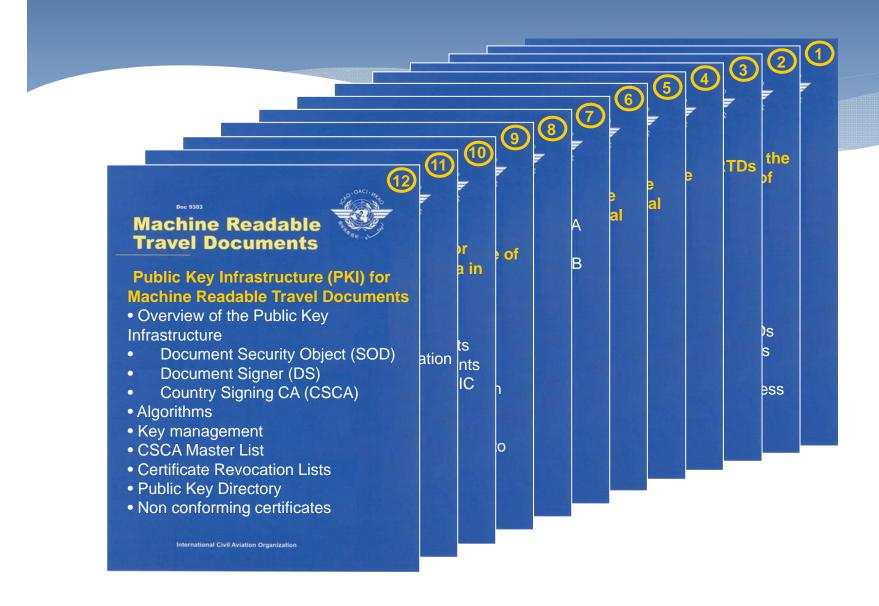
- TR Supplemental Access Control for MRTDs
 - o Version 1.01 November 2010
- Basic Access Control recommended feature
 - o Anti skimming (access control)
 - o Anti eavesdropping (session encryption)
 - o Strength limited by design
 - o 5 & 10 years passport validity periods
- Supplemental to Basic Access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

- TR Machine reading options for td1 size MRTDs
 - o Version 1.0, April 2011
- Machine reading issue
 - MRZ on rear side
 - o 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
 - o One-line MRZ
 - o (2D) barcode
 - o Further study
- Chip enabled
 - o Chip access
 - o CAN position specified

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

- TR Transliteration of Arabic Script in MRTDs
 - o Version 2.9, July 2012
- \/|Z
 - o Doc 9303 mandates provision of Latin character equivalent
 - o Transcription
 - Transliteration
- MRZ
 - MRZ character set
 - o Unambiguous database searches
 - o Reversible

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



Machine Readable Machine Readable Travel Documents Travel Documents ePassport book The deployment of biometric Introduction identification & electronic storage of data in MRTDs **Machine Readable Machine Readable Machine Readable Travel Documents Travel Documents Travel Documents** etrics solution Specifications for the security of the Specifications common to all MRTDs Specifications specific to ID3 size olutions design, manufacture & issuance of Illustrative guidelines for portraits MRTDs - Machine Readable MRTDs Three letter codes **Passports** olicable to • Security of the MRTD & Transliterations Construction & dimensions MRP data page use of zones **Machine Readable Machine Readable Machine Readable** pection Zone **Travel Documents Travel Documents Travel Documents** Readable Zone data elements A Logical Data Structure (LDS) for Protocols Public Key Infrastructure (PKI) for agrams storage of biometrics & other data in · Basic Access Control Machine Readable Travel Documents • PACE V2 the contactless IC Overview of the Public Key Process for reading eMRTDs Passive Authentication Infrastructure • Requirements of the LDS · Active Authentication Document Security Object (SOD) · Mandatory & optional data elements eMRTD production and personalization Document Signer (DS) eMRTD inspection Ordering & grouping of data elements Country Signing CA (CSCA) · Mapping principles for contactless IC Worked examples Algorithms Data Group specifications · Key management · Worked examples CSCA Master List Certificate Revocation Lists · Public Key Directory · Non conforming certificates

Machine Readable Machine Readable Travel Documents Travel Documents Non-chip td1 card The deployment of biometric Introduction identification & electronic storage of data in MRTDs **Machine Readable Machine Readable Machine Readable Travel Documents** Tr **Travel Documents Travel Documents** Specifications for the security of the Specifications common to all MRTDs Specifications specific to td1 size design, manufacture & issuance of MRTDs - Machine Readable Official Illustrative guidelines for portraits MRTDs Three letter codes Pas **Travel Documents** • Security of the MRTD & Transliterations Dimensions of the td1 size MRTD General layout · Content & use of zones Visual Inspection Zone **Machine Readable Machine Readable Machine Readable** · Machine Readable Zone **Travel Documents Travel Documents Travel Documents** Passport card Sequence of data elements A Logical Data Structure (LDS) for Protocols Public Key Infrastructure (P Schematic diagrams storage of biometrics & other data in · Basic Access Control Machine Readable Travel Do • PACE V2 the contactless IC Overview of the Public Key Crew Member Certificates (CMC) Process for reading eMRTDs Passive Authentication Infrastructure • Requirements of the LDS · Active Authentication Document Security Object · Mandatory & optional data elements eMRTD production and personalization Document Signer (DS) eMRTD inspection Ordering & grouping of data elements Country Signing CA (CSCAT · Mapping principles for contactless IC Worked examples Algorithms Data Group specifications Key management CSCA Master List · Worked examples Certificate Revocation Lists · Public Key Directory Non conforming certificates

Doc 9303 revision project

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

THANK YOU



Tom KINNEGING

Senior Expert Standardization
Business Unit ID Documents

tom.kinneging@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