Regional Seminar on MRTDs and Traveller Identification Management
Tashkent, 8 to 10 April 2014

ICAO MRTD and eMRTD Standards and Specification:
Points to watch in implementing an ePassport

Gary McDonald
Senior Consultant
Identisec Canada
Introduction

• Historical overview
• Doc 9303
  – Current Structure
  – Future Structure
• ePassport
Historical Overview

- Standardization in the early 1980s
- Goal: Global Interoperability
- Consists of 3 Parts
  - Passports, Visas, Identity cards
- Technical Reports, Supplements
Part 1: Machine Readable Passports

Part 2: Machine Readable Visas
(3rd edition, 2005)

Part 3: Machine Readable Official Travel Documents
(3rd edition, 2008)
Doc 9303

- Part 1, Volume 1
- Passport Specification
  - Security Provisions
  - Visual Inspection Zone
  - Machine-Readable Zone
ePassport

• Part 1, Volume 2
• ePassport Specification
  – is at the discretion of the issuing state
• Biometric identification:
  – Facial recognition (mandatory)
  – Fingerprint (optional) or Iris scan (optional)
• Data to include: facial image, MRZ data plus any relevant info at the discretion of the State
ePassport Security

• Data in a chip is meant to be scanned and read
• Basic Access Control
  – Ensures information on the chip cannot be skimmed
• Public Key Infrastructure
  – Ensures information on the chip has not been altered
• PKI is implemented through the Public Key Directory (PKD) developed and provided by ICAO
• PKD:
  • PKD must be an integral part of every eMRP
Part 2 - Visas

- Format A Visa (MRV-A) fits in ID-3 travel document
  - Most common format, standard within the EU
- Format B Visa (MRV-B) is an ID-2 size
Part 3, Volume 1: ID Cards

- Two formats:
  - TD1 (ID1-sized card)
  - TD2 (ID2-sized card)
Part 3, Volume 2: eID Cards

• Identical approach to eMRTDs
  – Embedded contactless chip

• Must comply with Part 1, Volume 2 (ePassports)
Future Doc 9303

• Complete review is well advanced
• Reformatted into several volumes
• Easier to use
• Up to date

http://www.icao.int/Security/mrtd/Pages/default.aspx
ePassport

- Do I want an ePassport system?
- Do I need an ePassport system?
- Am I prepared to USE an ePassport system?
- Is the integrity of my current process consistent with and complementary to the technological advances of an ePassport program?
- “Make everything as simple as possible, but not simpler.” – Albert Einstein
Do You Want an ePassport System?

• Have you done a comprehensive risk identification and management analysis of your present system?
• Are you confident that your vulnerabilities will be identified and corrected to take advantage of the ePassport?
• Why is an ePassport useful to your country?
Do You Need an ePassport System?

• What will the “e” do that a traditional MRP will not?
• Are you prepared to take advantage of the extensive economies of scale (centralization) often accompanying ePassport implementation?
• Have you considered the impact on overseas issuance?
• Is your border management procedure and process equipped to deal with inspecting ePassports?
Are You Prepared to USE an ePassport System?

• Are your inspection processes ready to use the cryptographic keys in ePassport?
• Are you going to join the PKD prior to ePassport implementation; have you taken appropriate budgeting precautions?
• Have you prepared your traveling public for the changes that biometric capture and use will bring about?
Overall System Integrity: Is Yours Enough?

- Is the integrity of the current issuance and handling process consistent with and complementary to the technological advances of an ePassport program?
- Are evidence of identity procedures and safeguards as strong as the document that you issue that alleges identity?
- Have you effected changes to insure to respect personal privacy of biometric and other data?
- Have your human resource issues been thoroughly addressed?
- Do you comply with both the letter as well as the spirit of 9303?
- Have you examined overseas issuance considering inherent differences of culture, infrastructure, external pressures?
Measures of Integrity

- Human systems-zero tolerance
- Work atmosphere and environment
- Evidence of identification
- Spoiled document handling
- Blank document controls
- In-house auditing
- Penalties-legal/judicial system as well as administrative
Application and Entitlement Processes: Evidence of Identification

- Evidence that the claimed identity is valid, i.e., that the person was in fact born and, if so, that the owner of that identity is still alive.
- Evidence that the presenter links to the claimed identity – i.e., that the person claiming the identity is who they say they are and that they are the only claimant of the identity.
- Evidence that the presenter uses the claimed identity – i.e., that the claimant is operating under this identity within the community; Social Footprint
- Standards of performance and indices of variances-expectations and a framework so employees know the rules
- Breeder documents
- Online database linkages of a wide nature with real time access; civil registries, systems of birth, death, marriage, tax, real estate, and related commercial services
Thank You!

gary.mcdonald@identisec.com
+1 613 790-5800