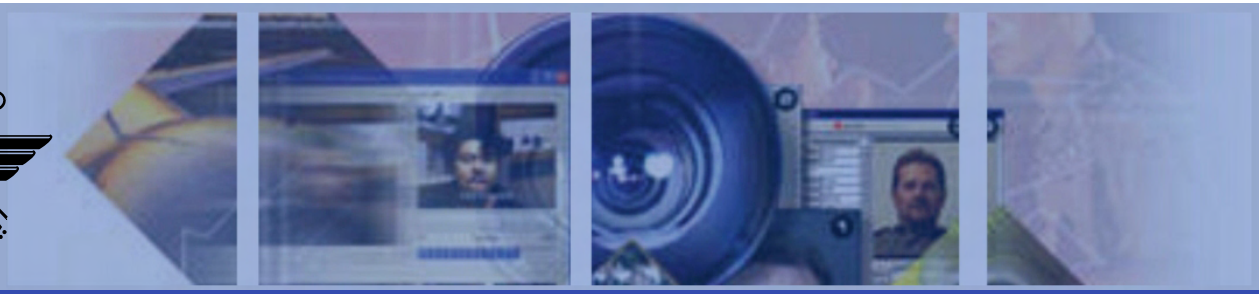

2nd Symposium on ICAO-Standard MRTDs, Biometrics and Security

Implementing Standard Biometric ePassports

Gary K McDonald
Chair, ICAO
New Technologies WG

MRTD Symposium
ICAO Headquarters, Montréal
6 – 7 September 2006

Overview

- Vision, Goals and Objectives
- Considerations
- Interoperability
- e-Passport Specifications
- Identity Management

Vision, Goals and Objectives

- Goals
  - Improve document security
  - Improve facilitation
  - Use of biometrics
    - Create a link between the document and the bearer
  - Global interoperability

Interoperability

- Four Pillars of Interoperability
  - Common Data Structure
  - Common Biometrics
  - Common Data Storage
  - Common Security (Encryption/PKI)

Common Data Structures

- Type of data
- Order of appearance
- Only basic bio-data is mandatory

Biometrics

- Reviewed a variety of biometric approaches
- Facial recognition selected as the biometric for global interoperability
  - Iris and Fingerprint as optional second biometrics

Common Data Storage

- Contactless IC Chip
  - ISO 14443 standard
- 32K technical minimum
  - 64K is viewed as a ‘best practice’
- Location not specified

Common Security

- Public Key Infrastructure
  - Digitally sign data
- Sharing of Public Keys
  - ICAO to host a Public Key Directory (PKD)

E-Passports

- Standard passport booklet with:
  - Embedded contactless chip
  - Personal bio-data and photo
  - All stored and secured in accordance with ICAO specifications
- MRZ required
  - Basic Access Control recommended

Identity Management

- Essential to correctly identify applicants for passports

- Consequences of misidentification