The Challenges of Digital Passport Solutions

Louise Cole

Manager Passport Operations
Department of Internal Affairs
NEW ZEALAND

Strengthening Aviation Security through Improved Traveller Identification

Digital Travel Credentials

Next generation "virtual" credentials securely stored in mobile devices or cloud hosted and accessed via biometric authentication giving travelers the opportunity for document-free travel between participating countries.

Digital Passport Options

- Passports data, alongside biometric identifiers/LDS, shared between partner or participating countries as an extension or replacement to Interactive API (Advanced Passenger Information)

- LDS shared with destination country on check in or on booking by traveler as an extension or replacement of Interactive API

- Mobile device used as a container for Travel Credentials (iMRTD)

- Multi-tiered authentication

Why?

- Citizen driven demand for digital solutions
- Increased facilitation, both at border and for visa processing
- Increased security with a reduction in lost/stolen and reduction in ETD issuance
- Increased security with dependence on biometric matching

Issues & Risks

Cloud:

- Biometrics within the infrastructure
- System accessibility 24/7
- A companion to, or replacement of, the book?
- Privacy concerns

Mobile:

- Security of device and of app/container
- Risk of cloning
- Risk of stealing identity data
- Manipulation of Travel Credential
- Authentication

Questions to consider

- Is this a solution without a problem?
- What benefits would an iMRTD bring that an eMRTD doesn't already offer?
- What is the *actual* benefit to security and facilitation?
- Just because we *can* do something, does that mean we *should*?

Contact Details

Name: Louise Cole
Email: Louise.Cole@dia.govt.nz