
ICAO
TRIP
2017
Passport
Passeport Pasaporte
护照 Паспорт جواز سفر
JAMAICA
KINGSTON
PORT-AU
Caribbean Sea
Cayman Trench
Desembarco del Granma
National Park

TRIP2017

Traveller Identification Programme

Regional Seminar Montego Bay

An overview of next generation ePassport technology

Logical Data Structure 2

Benoit Poletti

INCERT GIE director
Ministry of Economy of Luxembourg
ICAO NTWG member

ISO International Organization for Standardization

ICAO

Montego Bay, November 2017

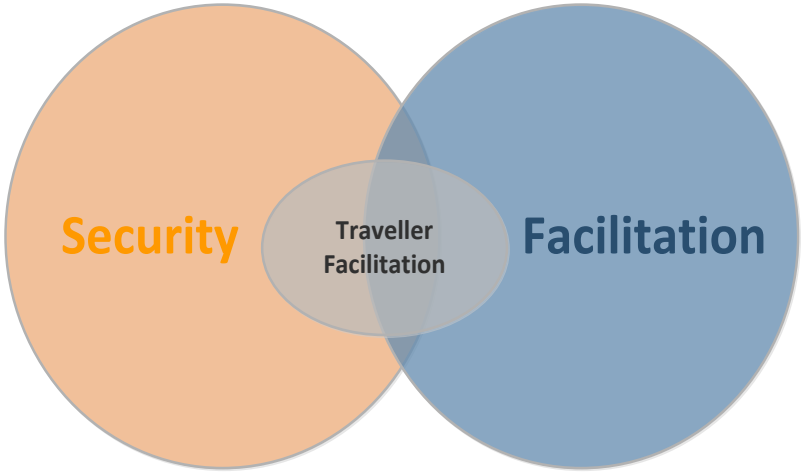
Presentation overview

- Overview of the Current ePassport
- Limits to Automation
- ePassport Developments
- Logical Data Structure 2 Overview, Applications and Advantages
- International specifications

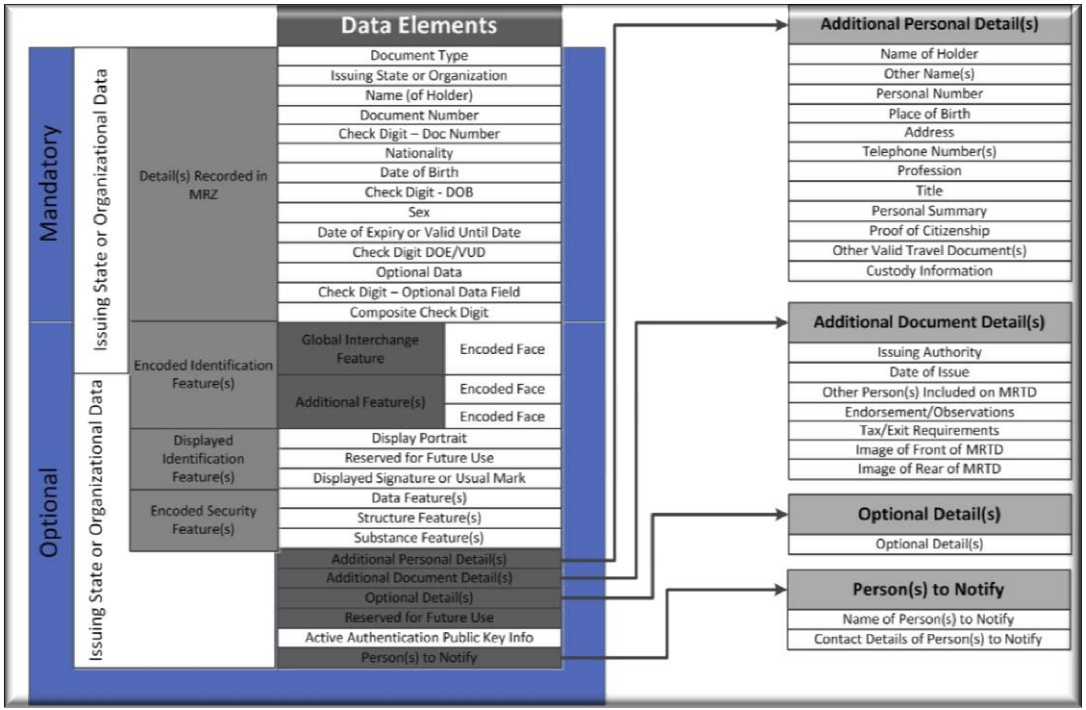
Overview of the current ePassport

- International technical specifications to support globally interoperable ePassport issuance are defined in ICAO Doc 9303.
    - ePassports contain a contactless integrated circuit (i.e. chip) that securely stores the holder's biometric and biographic data.

- The ePassport's capabilities provide States with possibilities to automate various border management processes.
    - With the use of the ICAO Public Key Directory (ICAO PKD), border management authorities can perform an authentication of a travel document and, in turn, rely on the data stored on the chip.



Overview of the current ePassport



Limits to automation

- The ability to automate passenger and border clearance processes is one of the primary advantages offered by the ePassport.

- ePassport's functions allow border control authorities to authenticate the document, which, in turn, allows them to rely on the information and facilitate the passage of low-risk travellers.

- Automation does have its limits, as border control authorities use other information in the ePassport (i.e. travel history, visas and observations) to make decisions on entry or passage.

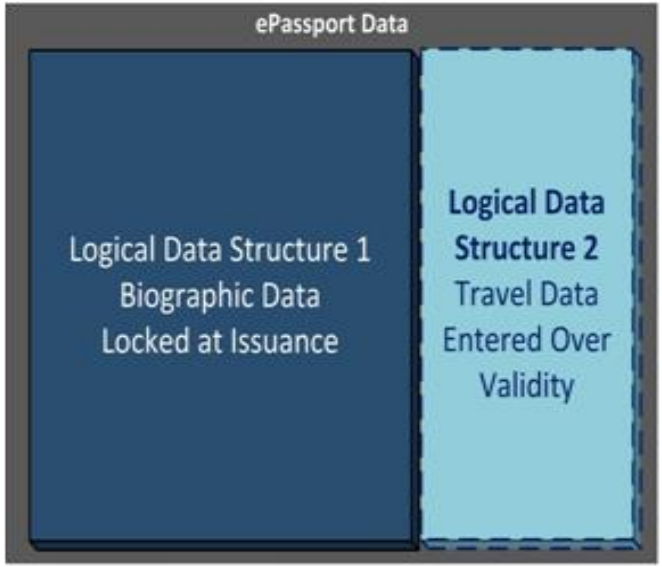
ePassport developments

- In response to interests to further secure and facilitate travel, ICAO's New Technologies Working Group (NTWG) has commissioned a sub-group to explore the policy and technical framework for the next generation of the ePassport.

- With direction from the ICAO NTWG, the sub-group explored changes to the ePassport that were:
  - backwards compatible and complementary to the current generation ePassport;
  - optional for all Member States; and
  - supportive to the broader TRIP Strategy.

Logical Data Structure 2 (LDS2)

- Logical Data Structure 2 (LDS2) is an optional and backwards compatible extension to the ePassport chip.
- LDS2 extends the use of the ePassport through the addition of applications to securely store visas, travel stamps, and additional biometrics, after the document has been issued.
- LDS2 applications operate independently alongside the LDS1 ePassport application.



Part 1 – LDS2 applications

Electronic Travel stamps

- Application will allow for electronic travel stamps (entry and exit) to be added to the document instantaneously.

- Checking the document will be easy!

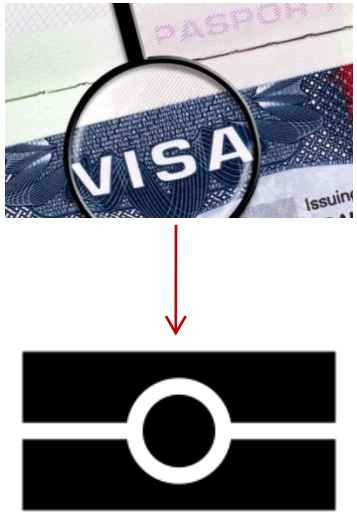
Drawbacks/Limitations

- Storage limitations
- Managing certificates

Part 1 – LDS2 applications

Electronic Visas

- Application will allow for electronic visas to be added to the document almost instantaneously, bolstering client service and reducing the costs associated with designing, shipping, and storing visas/travel stamps.
- Adding the visa directly to the document also reduces the need to rely on databases containing this information, which could facilitate transit travel, support third party validation, and mitigate the impacts of network outages or connection errors.



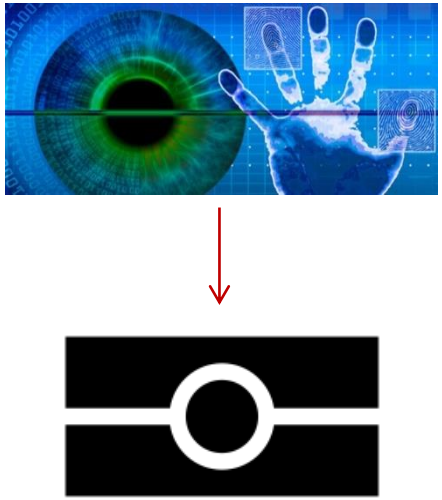
Drawbacks/Limitations

- Syncing with embassy and port of entry systems
- Managing certificates of expired and/or revoked visa entries
- Storage limitations

Part 1 – LDS2 applications

Additional Biometrics

- The ability to add secondary biometrics (iris and fingerprint) post-issuance provides States with more choices in national policy regarding secondary biometric storage and trusted traveller programs.
- In instances where the photo of the holder can no longer be used, States could add an updated photo of the holder, which could result in fewer replacement passports being issued, less unnecessary delays at border control, and more dependability on facial recognition.



Drawbacks/Limitations

- Exposure to greater privacy risks
- Privacy frameworks for data collection and storage
- Investments in additional biometric capture and verification

Potential advantages of LDS2 ePassports

- Extending the functions of the ePassport would create added opportunities to automate passenger and document processing at controlled points in travel.

- LDS2 ePassports will include the ‘missing’ information that is needed to systematically clear passengers using automated border clearance (ABC) technologies
    - Standard, reliable and protected travel data can be leveraged to perform an on-the-spot, systematic analysis of the risk that travellers present, and detect unusual travel patterns; disconnects between entry and exit stamps; and attempts to alter travel data.

- The possibility of being able to streamline various processes could improve the flow of passenger traffic, allow States to redirect attention to more high-value activities, and provide States with opportunities to make better use of investments in border clearance infrastructure.

Internal specifications

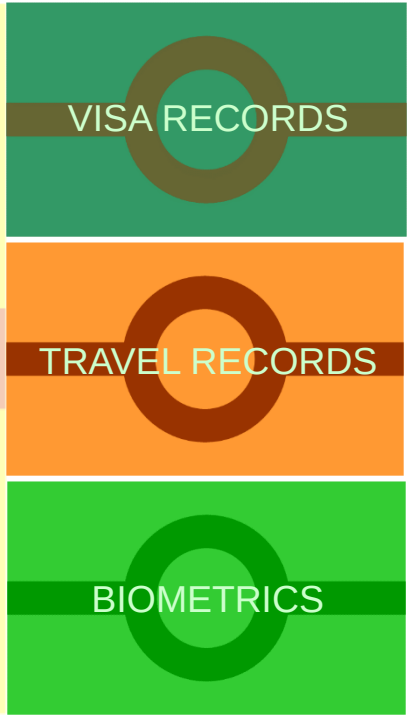
ICAO Doc 9303 - 7th edition

1. Introduction
2. Specifications for the Security of Design, Manufacture and Issuance of MRTDs
3. Specifications common to all Machine Readable Travel Documents
4. Specifications specific to TD3 size MRTDs, Machine Readable Passports
5. Specifications specific to TD1 size MRTDs, Machine Readable Official Travel Documents
6. Specifications specific to TD2 size MRTDs, Machine Readable Official Travel Documents
7. Machine Readable Visas
8. Emergency Travel Documents
9. The Deployment of Biometric Identification and Electronic Storage of Data in MRTDs
10. Logical Data Structure
11. Security Protocols
12. Public Key Infrastructure for Machine Readable Travel Documents

Logical Data Structure

LDS1

Data Group 01 - Machine Readable Zone
Data Group 02 - Encoded face
Data Group 03 - Encoded fingers
Data Group 04 - Encoded irises
Data Group 05 - Displayed portrait
Data Group 06 - Reserved for future use
Data Group 07 - Displayed signature or usual mark
Data Group 08 - Data features
Data Group 09 - Structure features
Data Group 10 - Substance features
Data Group 11 - Additional personal details
Data Group 12 - Additional document details
Data Group 13 - Optional details
Data Group 14 - Security options for secondary biometrics
Data Group 15 - Active Authentication public key info
Data Group 16 - Persons to notify



Part 3 - Logical Data Structure

LDS2 - Visa Records

Issuing State
Document Type
Place of issuance
Valid from - Valid until
Number of entries
Document number
Type/class/category
Additional information (endorsements: duration, limitations, and fees paid)
Name (full name)
Primary Identifier (surname)
Secondary Identifier (given name)
Passport number
Sex
Date of Birth
Nationality

Part 3 - Logical Data Structure

LDS2 - Travel Records

Type of stamp (entry, exit, other)
Visa approvals, refusals, and revocations as applicable
Destination State
Travel date
Inspection authority
Inspection location
Inspector reference
Authenticity token
Result of inspection
Mode of travel
Duration of stay
Conditions holder is required to observe whilst in issuing

Part 3 - Logical Data Structure

LDS2 - Additional Biometrics

Limited to Face, Finger, and Iris

Re-issuance of existing LDS1 biometrics possible (updated biometrics)

Additional data accompanying biometrics (f.i. to support frequent traveler programs)

Part 3 - Protocols

Data authenticity / integrity

- Passive Authentication

Copy / Clone protection

- Active Authentication
- Chip Authentication

Access Control / Communications encryption

- PACE

Read / Write authorization

- Terminal Authentication

Part 3 - Protocols

Authorization matrix

Description	Read	Write/Append	Update	Delete
Electronic Visas	1.	2.	n/a	n/a
Travel Records	1.	2.	n/a	n/a
Additional Biometrics	2.	2.	2.	2.

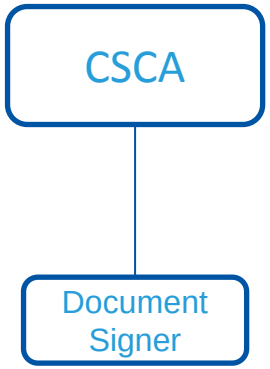
1. Default allow policy with selective denial.

2. Default denial with selective allow

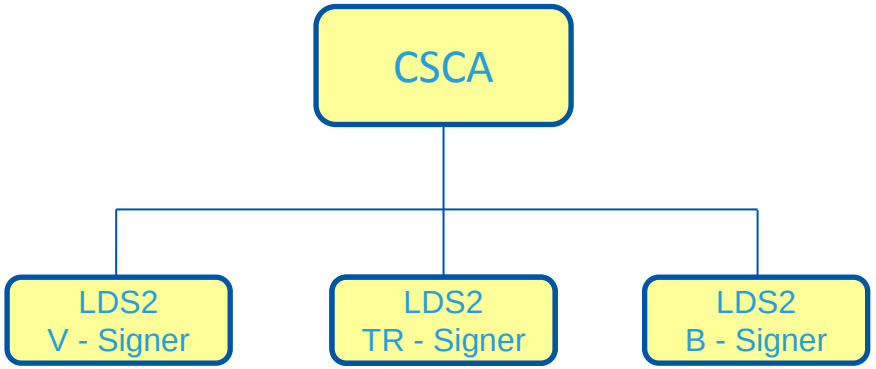
Public Key Infrastructure

Signature PKI

eMRTD issuing authority

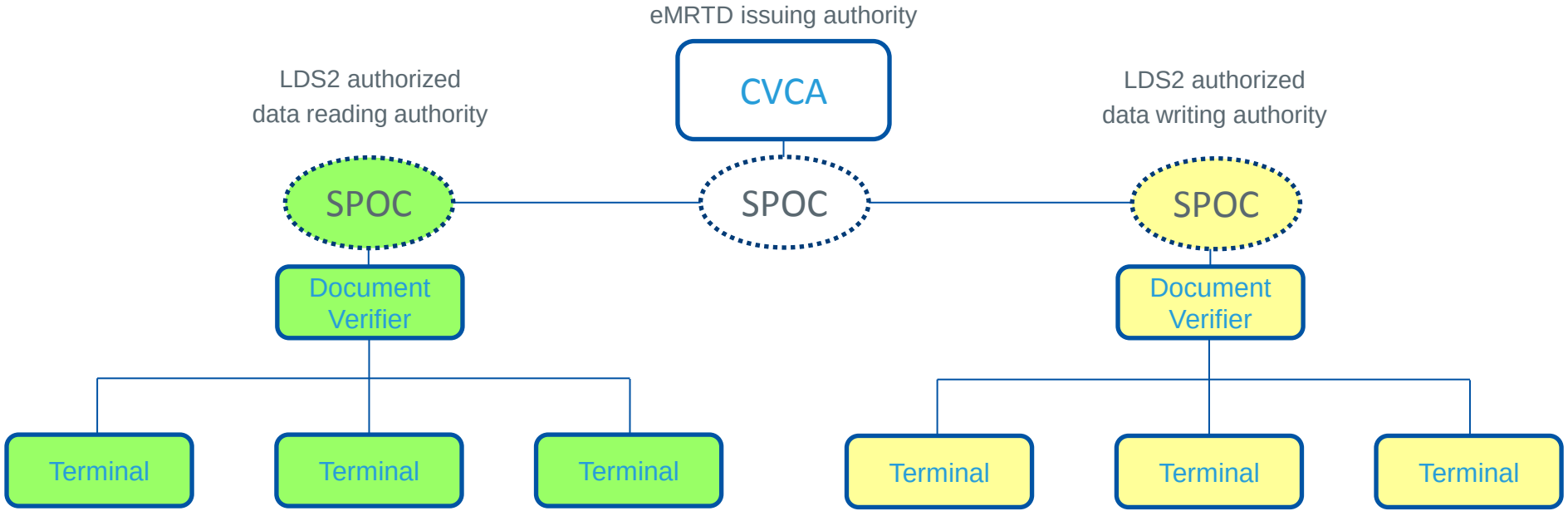


LDS2 authorized data writing authority



Public Key Infrastructure

Authorization PKI



Thank you

Benoit Poletti

INCERT GIE director
Ministry of Economy of Luxembourg
ICAO NTWG member

On behalf of

International Organization for Standardization

ICAO

Jasper Mutsaers

R&D Advisor, MoI, The Netherlands
Co-chair ICAO NTWG LDS2 Policy Sub-Group

Tom Kinneging

Senior advisor, OT-MORPHO
Convener ISO/IEC JTC1 SC17 WG3