The ePassport: What’s Next?

Justin Ikura

LDS2 Policy Sub-Group Co-chair

Tom Kinneging

Convenor of ISO/IEC JTC1 SC17 WG3
International Organization for Standardization (ISO)

Strengthening Aviation Security through Improved Traveller Identification

Presentation Overview

Part 1

- ICAO Traveller Identification Program (TRIP)
- Overview of the current ePassport
- Developments to technology

Part 2

- International specifications

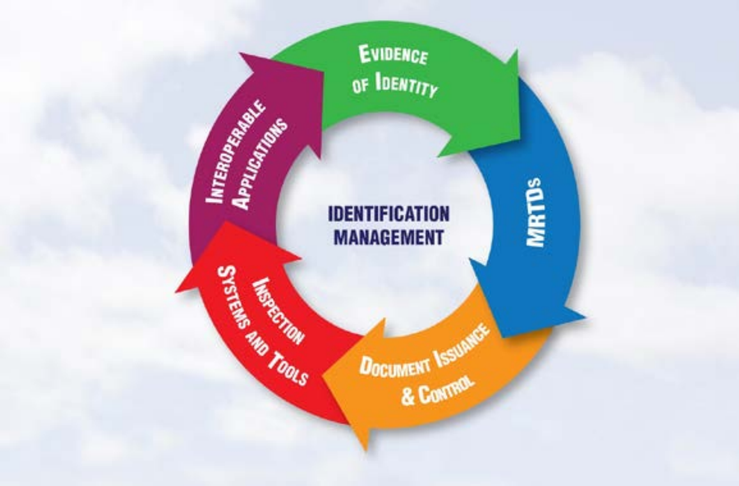
Part 3

- Technical demonstration

Part 1: ICAO TRIP

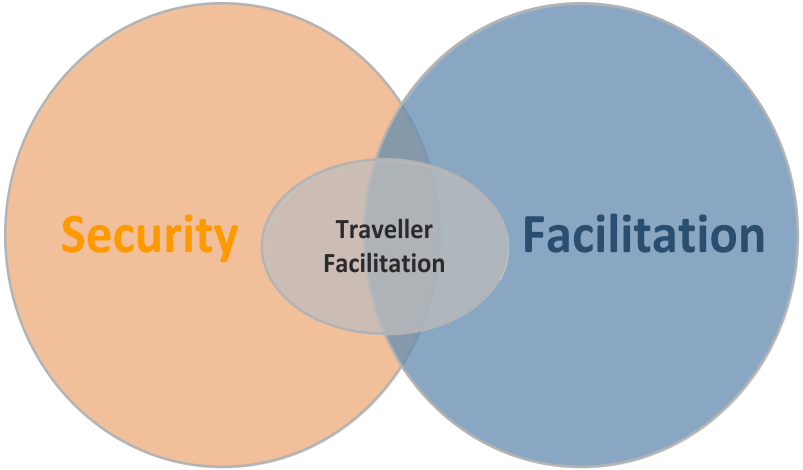
- The ICAO Traveller Identification Program (TRIP) promotes the efficient, timely and reliable confirmation of traveler identities.

- ePassport technology contributes to improving traveller facilitation by providing authorities with a secure, fixed and verifiable identity that can be leveraged in the travel continuum.
  - The digital inclusion of the holder’s biometric and biographic data can be leveraged in automated schemes at the border.
  - The use of a public key infrastructure to protect this data assists in preventing fraud and/or manipulation.

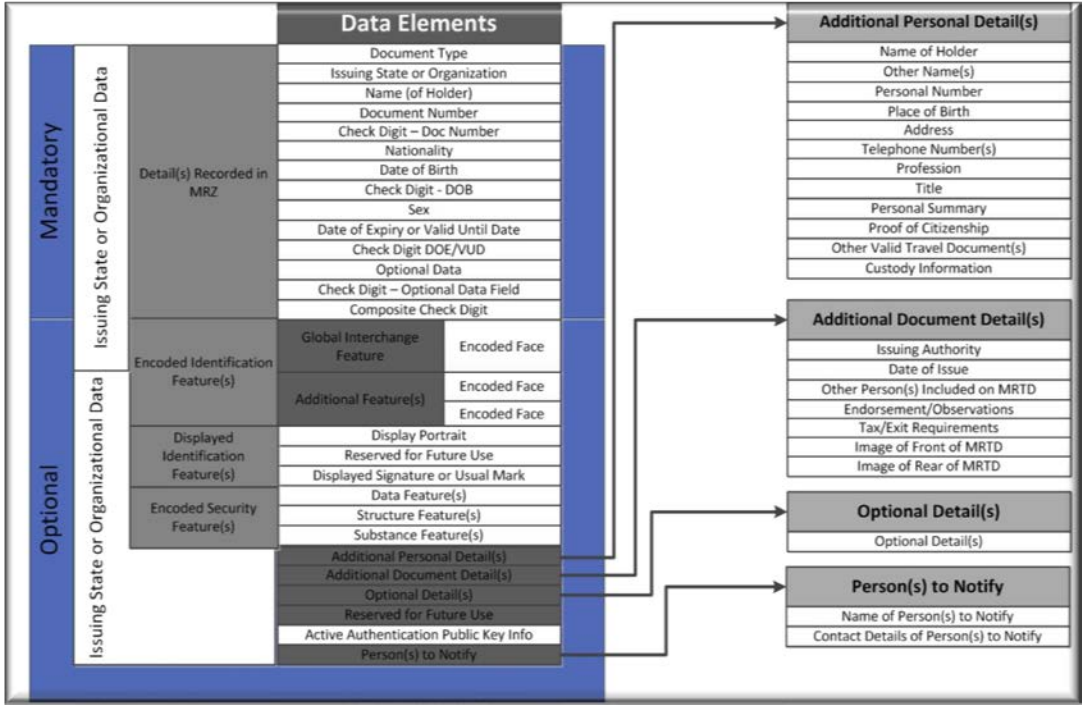

Evidence of Identity
MRTDs
Document Issuance & Control
Inspection Systems and Tools
Interoperable Applications
Identification Management

Part 1: ePassport Current State

- International technical specifications to support global and interoperable ePassport issuance are defined in ICAO Doc 9303.
  - ePassports contain a contactless integrated circuit (i.e. chip) that allows the document to securely store 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.
- 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.



Part 1: ePassport Current State



Mandatory
Optional
Issuing State or Organizational Data
Issuing State or Organizational Data

Data Elements

Detail(s) Recorded in MRZ
- Document Type
- Issuing State or Organization
- Name (of Holder)
- Document Number
- Check Digit – Doc Number
- Nationality
- Date of Birth
- Check Digit - DOB
- Sex
- Date of Expiry or Valid Until Date
- Check Digit DOE/VUD
- Optional Data
- Check Digit – Optional Data Field
- Composite Check Digit

Encoded Identification Feature(s)
- Global Interchange Feature: Encoded Face
- Additional Feature(s): Encoded Face; Encoded Face

Displayed Identification Feature(s)
- Display Portrait
- Reserved for Future Use
- Displayed Signature or Usual Mark

Encoded Security Feature(s)
- Data Feature(s)
- Structure Feature(s)
- Substance Feature(s)

- Additional Personal Detail(s)
- Additional Document Detail(s)
- Optional Detail(s)
- Reserved for Future Use
- Active Authentication Public Key Info
- Person(s) to Notify

Additional Personal Detail(s)
- Name of Holder
- Other Name(s)
- Personal Number
- Place of Birth
- Address
- Telephone Number(s)
- Profession
- Title
- Personal Summary
- Proof of Citizenship
- Other Valid Travel Document(s)
- Custody Information

Additional Document Detail(s)
- Issuing Authority
- Date of Issue
- Other Person(s) Included on MRTD
- Endorsement/Observations
- Tax/Exit Requirements
- Image of Front of MRTD
- Image of Rear of MRTD

Optional Detail(s)
- Optional Detail(s)

Person(s) to Notify
- Name of Person(s) to Notify
- Contact Details of Person(s) to Notify

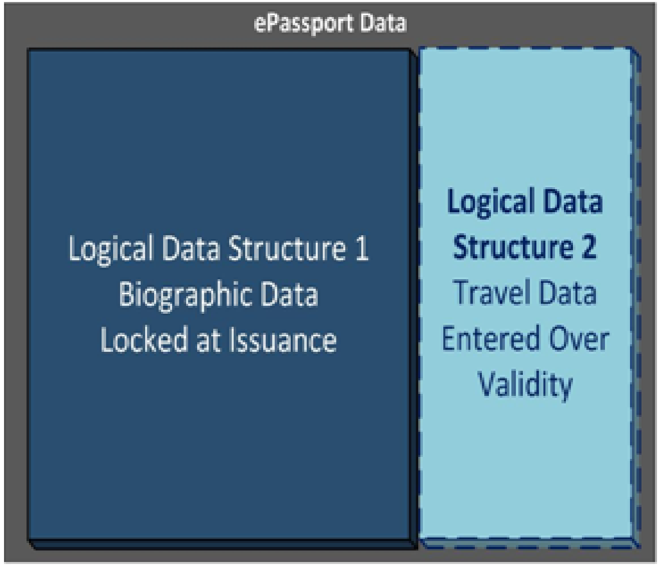
Part 1: Context

- 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.

Part 1: ePassport Developments

- 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.



ePassport Data

Logical Data Structure 1
Biographic Data
Locked at Issuance

Logical Data Structure 2
Travel Data
Entered Over Validity

Part 1: LDS2 Applications

1. Electronic Travel Stamps

- Standardized content and format, and protection from tampering.

- The benefit of adding this travel data in digital format include: greater consistency; enhanced security; and ease of access and viewing.

Drawbacks/Limitations

- Not all States may choose to implement this application, which could result in some stamps stored in the chip (and manually added) and others just being manually added.
- Tracking/monitoring concerns.

Part 1: LDS2 Applications

2. 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

3. 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 storage

Part 1: 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.

Part 2: International 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

Part 2: 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

VISA RECORDS

TRAVEL RECORDS

BIOMETRICS

Part 2: Logical Data Structure

VISA RECORDS

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 2: Logical Data Structure

Travel Records

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

TRAVEL RECORDS

Part 2: Logical Data Structure

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)

BIOMETRICS

Part 2: Protocols

Data authenticity / integrity

- Passive Authentication

Copy / Clone protection

- Active Authentication
- Chip Authentication

Access Control / Communications encryption

- PACE

Read / Write authorization

- Terminal Authentication

Part 2: Protocols

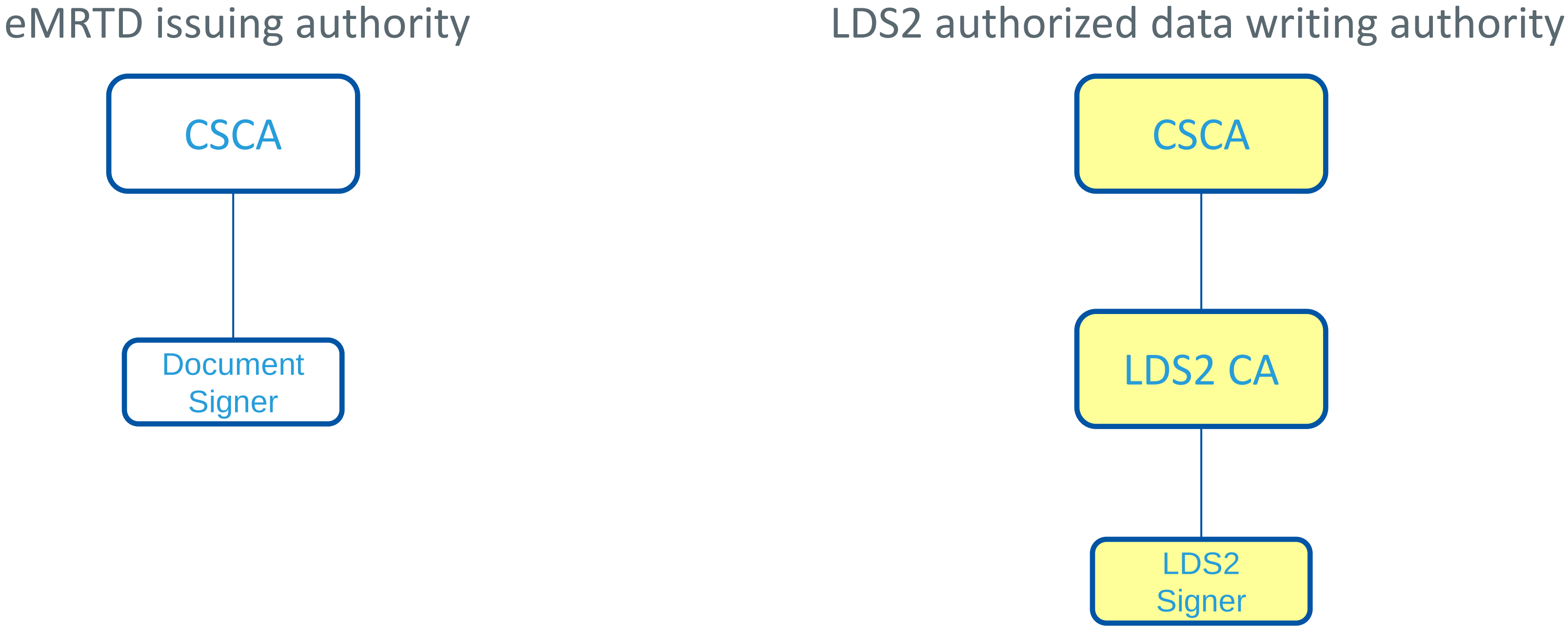
Authorization matrix

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. All States / defined Organizations. Default allow policy with selective denial.
2. Defined States / Organizations. Default deny with selective allow.

Part 2: Public Key Infrastructure

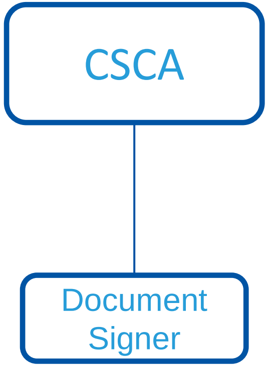
Signature PKI



Part 2: Public Key Infrastructure

Signature PKI

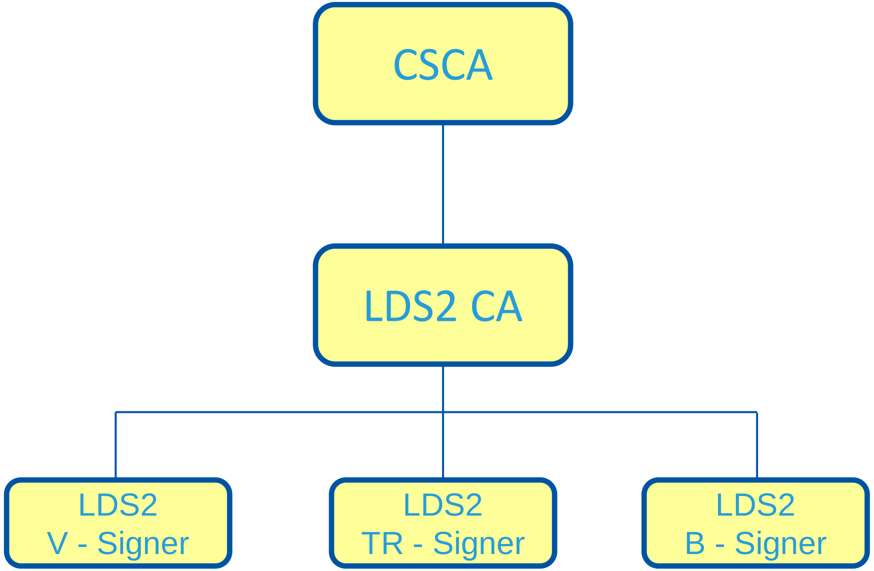
eMRTD issuing authority



CSCA

Document Signer

LDS2 authorized data writing authority



CSCA

LDS2 CA

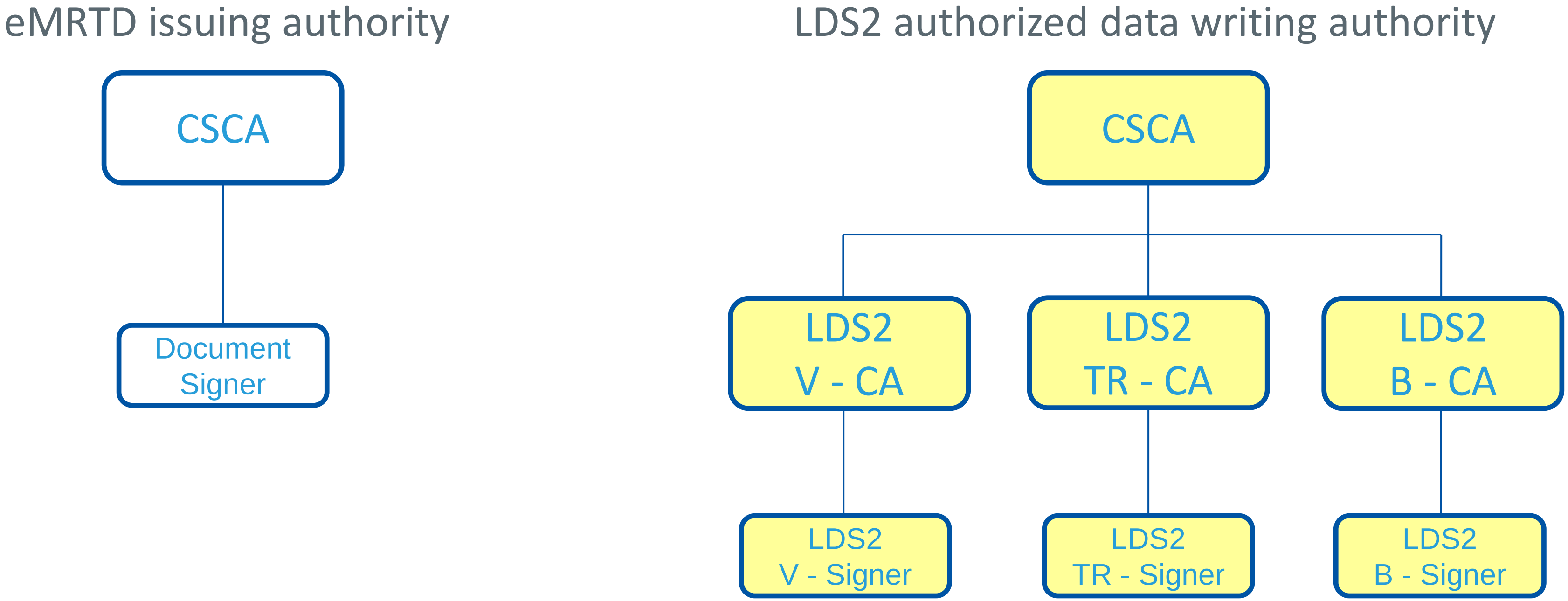
LDS2 V - Signer

LDS2 TR - Signer

LDS2 B - Signer

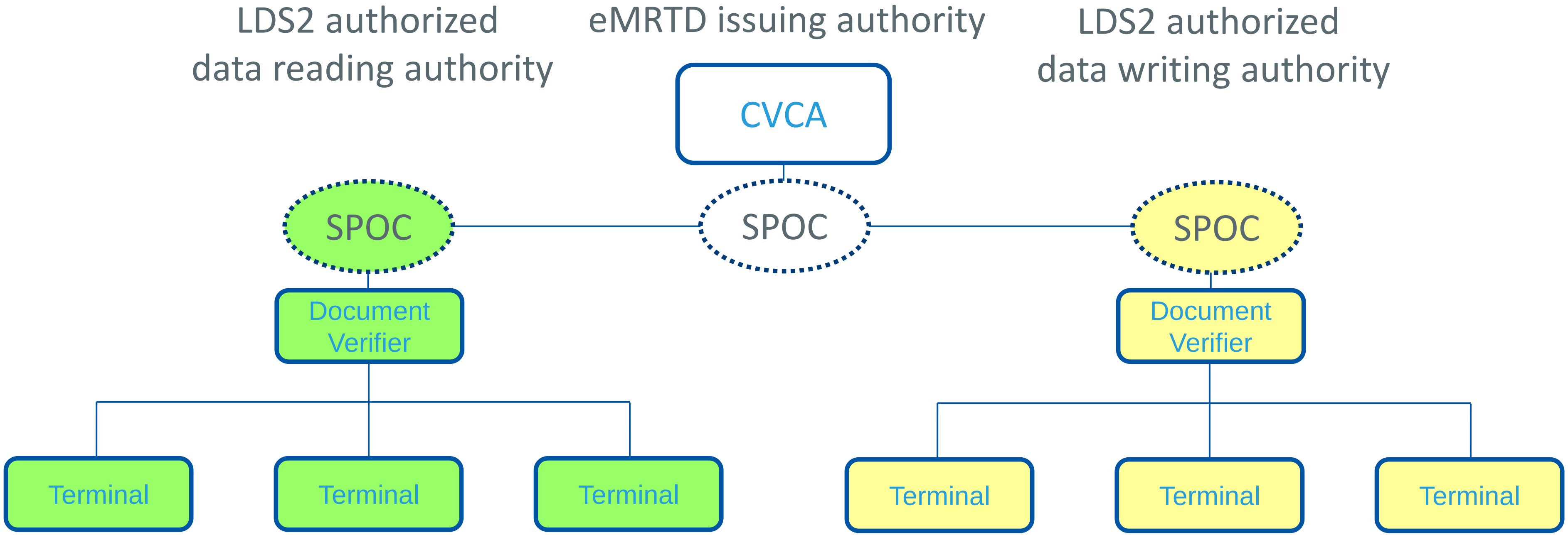
Part 2: Public Key Infrastructure

Signature PKI

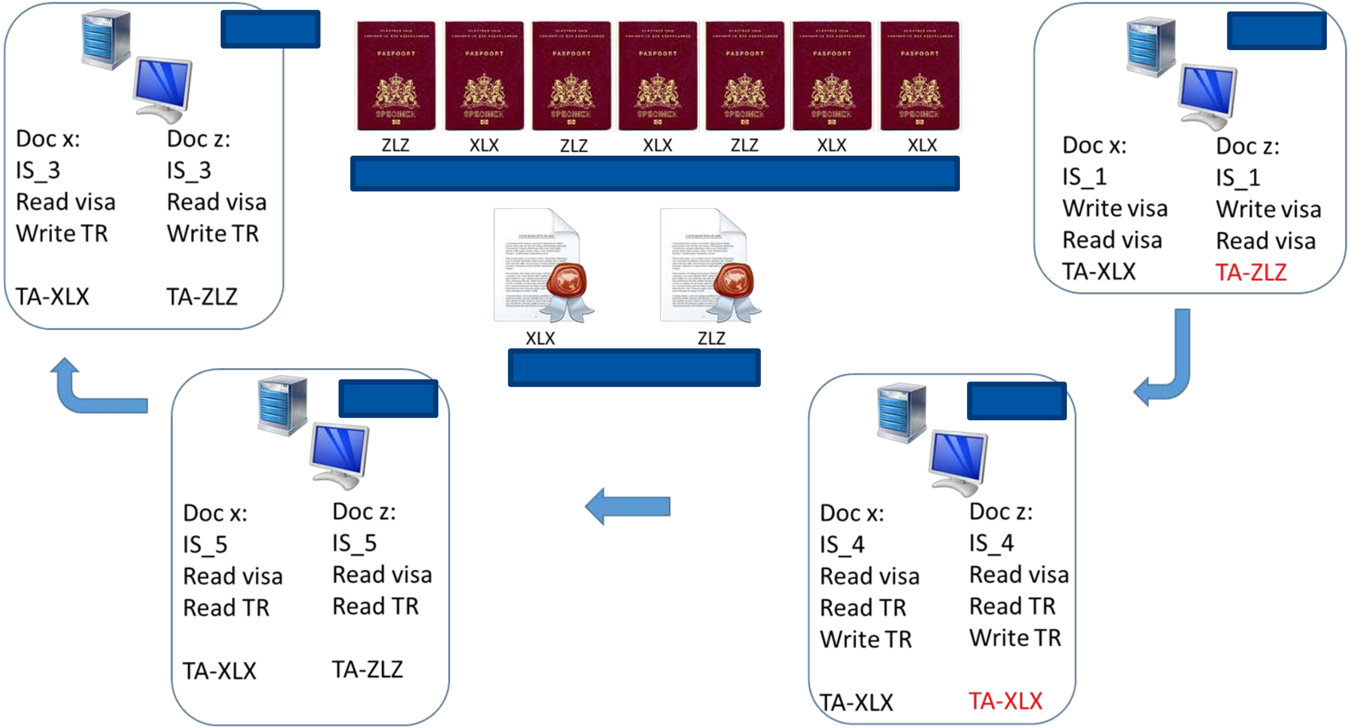


Part 2: Public Key Infrastructure

Authorization PKI



Part 3: LDS2 Demonstrator



Doc x:	Doc z:
IS_3	IS_3
Read visa	Read visa
Write TR	Write TR
TA-XLX	TA-ZLZ

Doc x:	Doc z:
IS_1	IS_1
Write visa	Write visa
Read visa	Read visa
TA-XLX	TA-ZLZ

Doc x:	Doc z:
IS_5	IS_5
Read visa	Read visa
Read TR	Read TR
TA-XLX	TA-ZLZ

Doc x:	Doc z:
IS_4	IS_4
Read visa	Read visa
Read TR	Read TR
Write TR	Write TR
TA-XLX	TA-XLX

Contact Details

Names:	Justin Ikura; and Tom Kinneging
Emails:	justin.ikura@cic.gc.ca; and tom.kinneging@safrangroup.com