



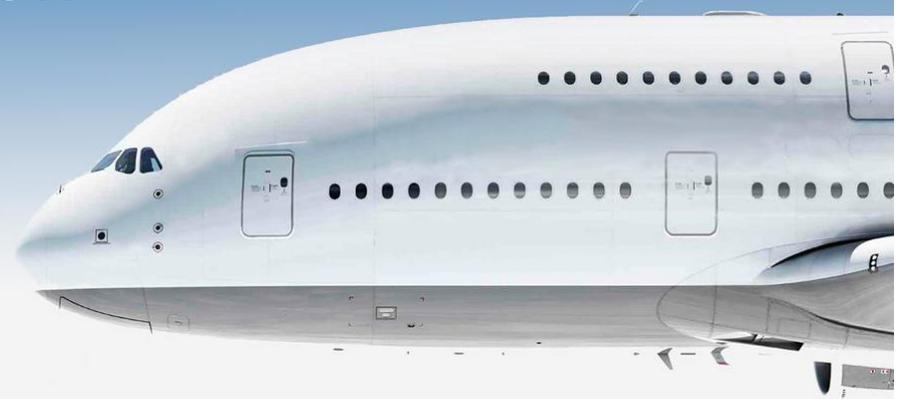
| ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



# Facilitation and Traveler Identification Programme: the role of the International Civil Aviation Organization



Christiane DerMarkar,

ICAO Traveller Identification Programme (ICAO/TRIP) Officer

13 April 2022



# Three interrelated Facilitation (FAL) Programmes

## Annex 9- Facilitation



## ICAO TRIP Strategy

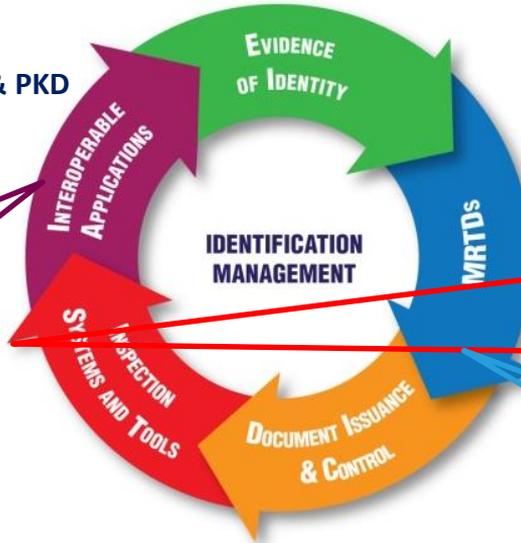


## ICAO PKD

Chapters 3, 8 & 9: main SARPs related to the TRIP & PKD

### API & PNR:

provide for timely, secure and reliable linkage of MRTDs and their holders to relevant data



Means to enhance security in cross-border movement.

Inspection Tool for ePassports verification, validation and authentication of the digital signatures and content of the chip



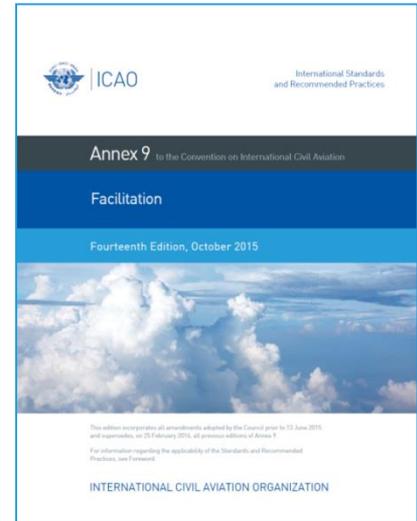
Manufacture of standardized MRTDs that comply with ICAO specifications (Doc 9303)



## Annex 9 - Facilitation

### Implementation of the Annex 9 Standards & Recommended Practices (SARPs) are essential to:

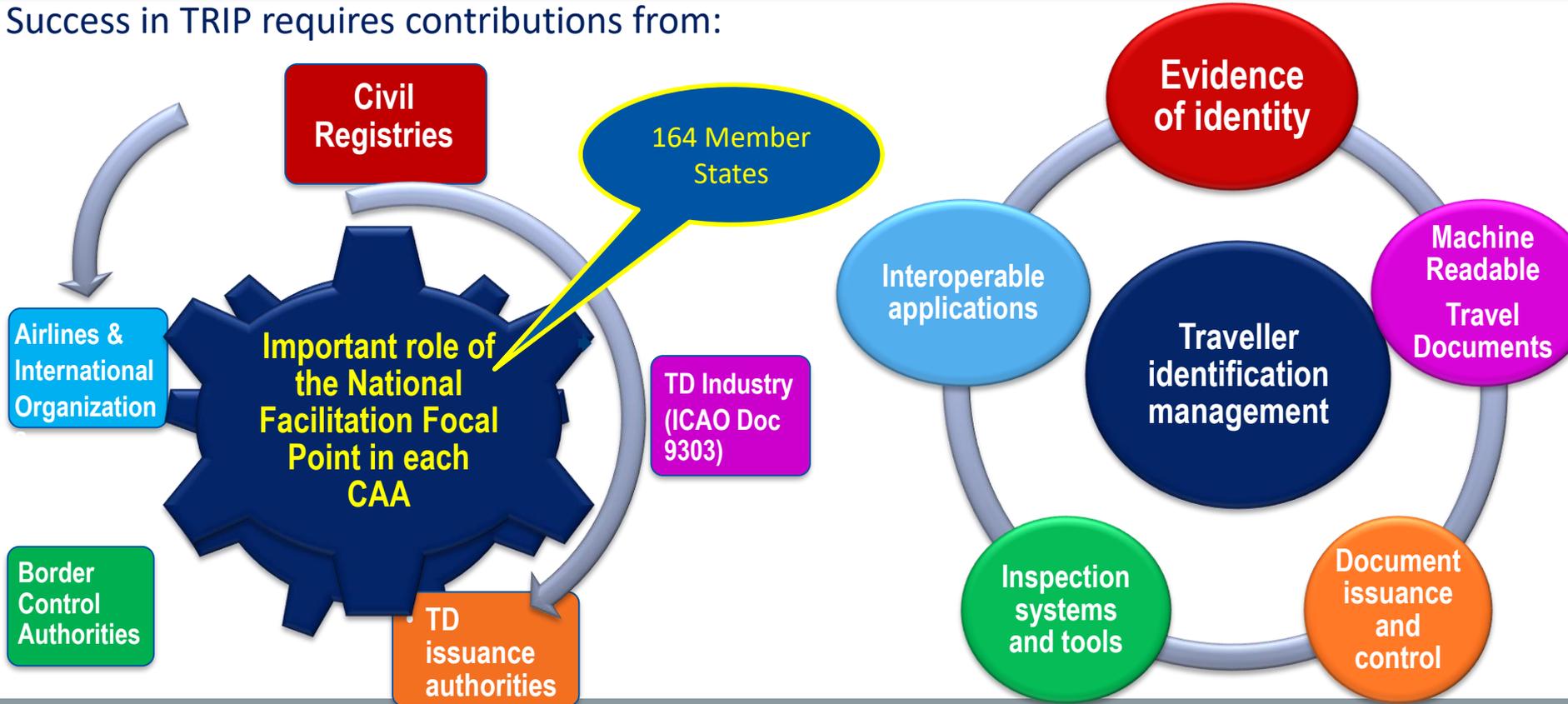
- Facilitate the clearance of
    - ✓ aircraft
    - ✓ passengers and their baggage
    - ✓ cargo and mail
  - Manage challenges in border controls and airport processes to maintain both the Security and the efficiency of air transport operations
- **Integrates function of agencies related to border control:**  
Travel documents, immigration, customs, quarantine, law enforcement, transport operators
- **Requires inter-agency and cross-border cooperation to implement Annex 9 obligations**





# National and Regional Collaboration

Success in TRIP requires contributions from:





ICAO

SECURITY & FACILITATION

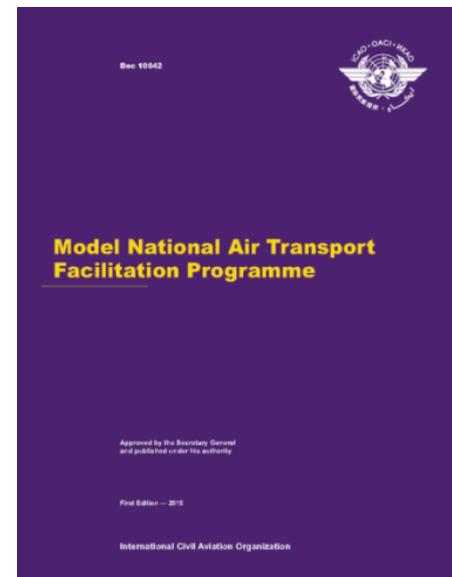
NO COUNTRY LEFT BEHIND



# National Air Transport Facilitation Programme (NATFP)

**Purpose:** Means of coordinating activities between national departments or agencies concerned with or responsible for various aspects of facilitation of national civil aviation

- ✓ Improve the effectiveness and efficiency of clearance control formalities
- ✓ Operationalization through national FAL committees
- ✓ NATFP and National Civil Aviation Security Programme are complementary

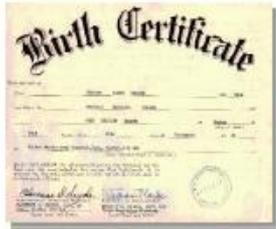


Establishing a NATFP  
is an ICAO Standard





# Traveller Identification Programme : ICAO TRIP Strategy

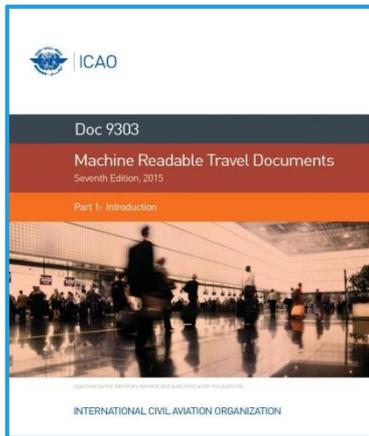






# Doc 9303: 13 Parts in all ICAO languages

MRP



eMRTD

Part 1: Introduction

Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs

Part 3: Specifications Common to all MRTDs

Part 4: Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs

Part 5: Specifications for TD1 Size Machine Readable Official Travel Documents (MROTDs)

Part 6: Specifications for TD2 Size Machine Readable Official Travel Documents (MROTDs)

Part 7: Machine Readable Visas

Part 8: Emergency Travel Documents

Part 9: Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs

Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)

Part 11: Security Mechanisms for MRTDs

Part 12: Public Key Infrastructure for MRTDs

Part 13: Visible Digital Seal (VDS)

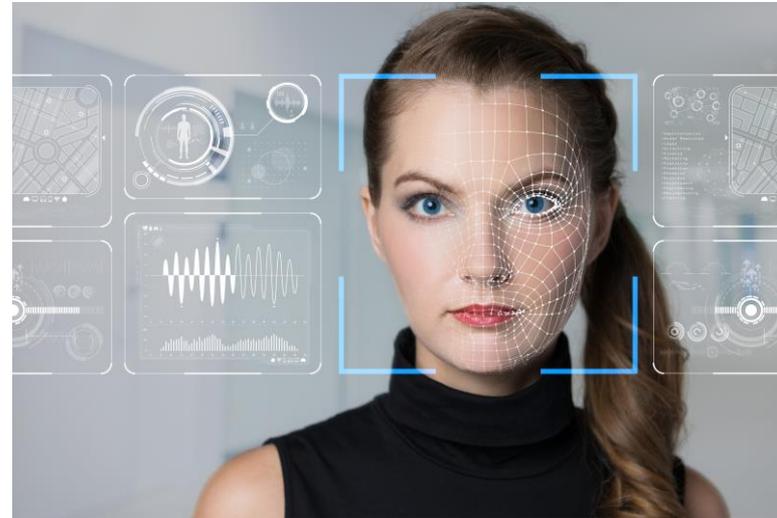




## Security of Travel Documents

### □ Biometrics Deployment: ICAO's choices

- Selection of biometrics for eMRTDs – facial image:
  - ✓ Least cultural obstructions;
  - ✓ Everybody has it;
  - ✓ Capture at a distance;
  - ✓ Interoperable (image);
  - ✓ Also usable without biometric verification;
- Optional additional biometrics - finger & iris:
  - ✓ Images.



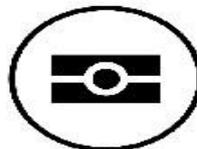


# ePassport or Biometric Passport

- ePassports are Machine Readable Passports (MRPs) with a chip (IC)
- The chip is an additional security feature and does not replace the MRZ
- Enhances security of the document
- Biometrics to confirm identity



e-Passport symbol





# ePassport/Biometric Passport Primer

		DATA ELEMENTS			
REQUIRED	ISSUING STATE OR ORGANIZATION DATA	Detail(s) Recorded in MRZ	DG1	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					
OPTIONAL	ISSUING STATE OR ORGANIZATION DATA	Encoded Identification Feature(s)	Global Interchange Feature	DG2	Encoded Face
			Additional Feature(s)	DG3	Encoded Finger(s)
		Displayed Identification Feature(s)	DG4	Encoded Eye(s)	
			DG5	Displayed Portrait	
		DG6	Reserved for Future Use		
		DG7	Displayed Signature or Usual Mark		
		Encoded Security Feature(s)	DG8	Data Feature(s)	
			DG9	Structure Feature(s)	
			DG10	Substance Feature(s)	
			DG11	Additional Personal Detail(s)	
DG12	Additional Document Detail(s)				
DG13	Optional Detail(s)				
DG14	Security Options				
DG15	Active Authentication Public Key Info				
DG16	Person(s) to Notify				

**Data Group 1 (DG1)**

- Issuing Organization
- Name of Holder
- Document Number
- Nationality
- Date of Birth
- Sex
- Date of Expiry...

**Data Group 2 (DG2)**

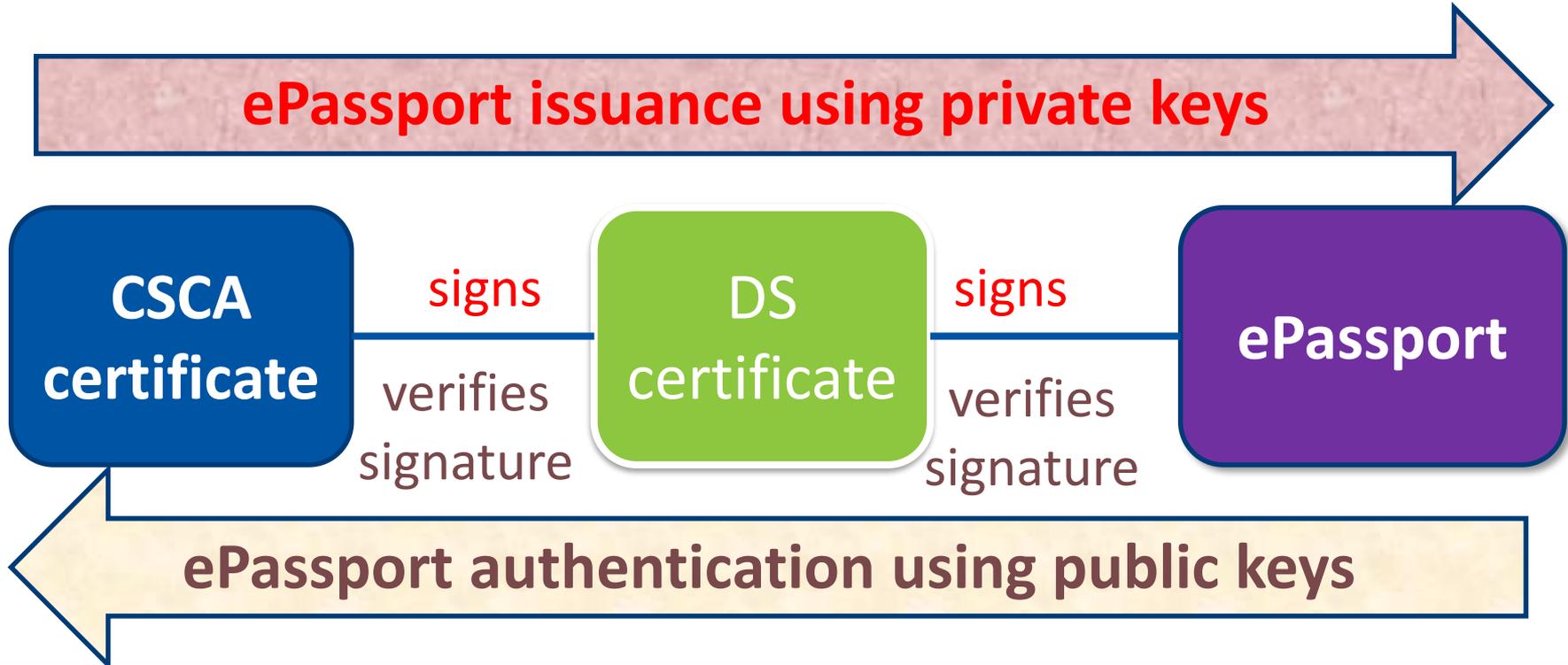
- Face

Data is added and encrypted at the time of issuance

- Approximately 145 ICAO Member States issue ePassports; 78 States participate in the ICAO Public Key Directory (PKD).
- The ePassport contains digitized identity information, including two mandatory elements (i.e. DG1 and DG2).
- Data can be authenticated and used to support passenger (e.g. facial matching, watchlist checking, etc.)



# Hierarchy of the ePassport certificates





# eMRTD Biometric Identity Verification

Subject to PKI authentication of the eMRTD, biometric images read from the eMRTD can be relied to verify identity by comparison of images taken of the same biometric feature of the traveller.

eMRTD biometric identity verification can be undertaken at different phases of the traveller journey, whenever the eMRTD is presented by the traveller.



ICAO Recommended Practice is for States to join the PKD and use the information available from the PKD to validate eMRTDs at border controls



## ICAO PKD: Key to the e-passport



### The e-passport

Facilitates travel

Enables automation

Increases security

But it can only be trusted if you verify the applied digital signature...

Which requires the appropriate public keys!



# Public key certificates

An electronic file storing *keys* required to authenticate an electronic travel document (e.g. ePassport)



- Sharing public keys is **necessary** – without the public keys, the party receiving the passport cannot trust the data on the chip – the passport is treated as a paper document, investment in electronic passports is wasted!
- Sharing public keys is **safe** – there is **no** possibility to issue false passports through knowledge of a public key
- Public keys are not personal information, there is no data protection concern with sharing

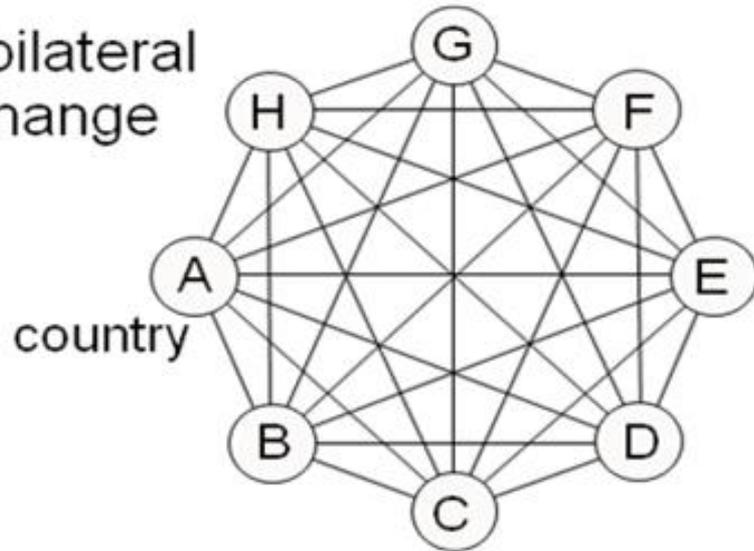
## A real ePassport public key (snippet):

```
30 82 02 0a 02 82 02 01 00 e4 fc 78 bb  
a0 64 98 19 42 ab 83 f2 5c 70 da 57 d2  
83 83 5b 22 4e 0f 4e 22 69 a8 a9 db 78  
08 f2 e5 de 59 5c bb 0e 43 a7 46 22 d2  
04 fd 15 49 81 cc f7 dd 91 1e d4 e2 af  
1c 0b 82 fb d1 ef c6 c8 12 b8 d4 04 14  
eb 86 ca 90 10 e3 da f5 c8 95 d9 ce ..
```



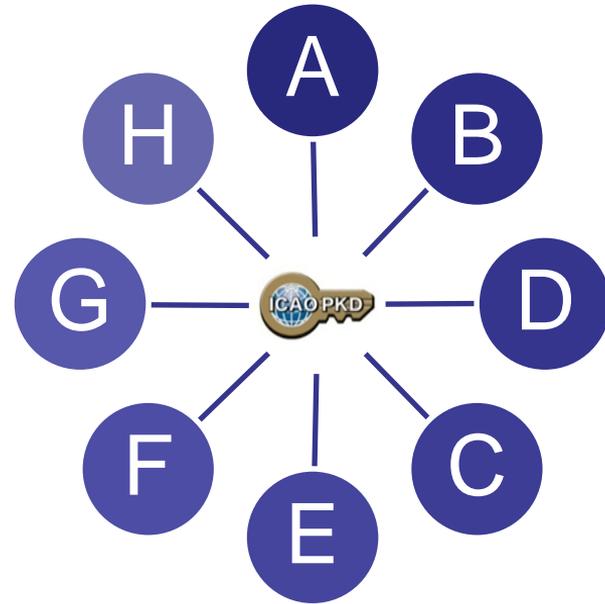
# The PKD makes sharing public key certificates convenient and reduces costs

via bilateral  
exchange



country

## Without the PKD



## With the PKD



ICAO

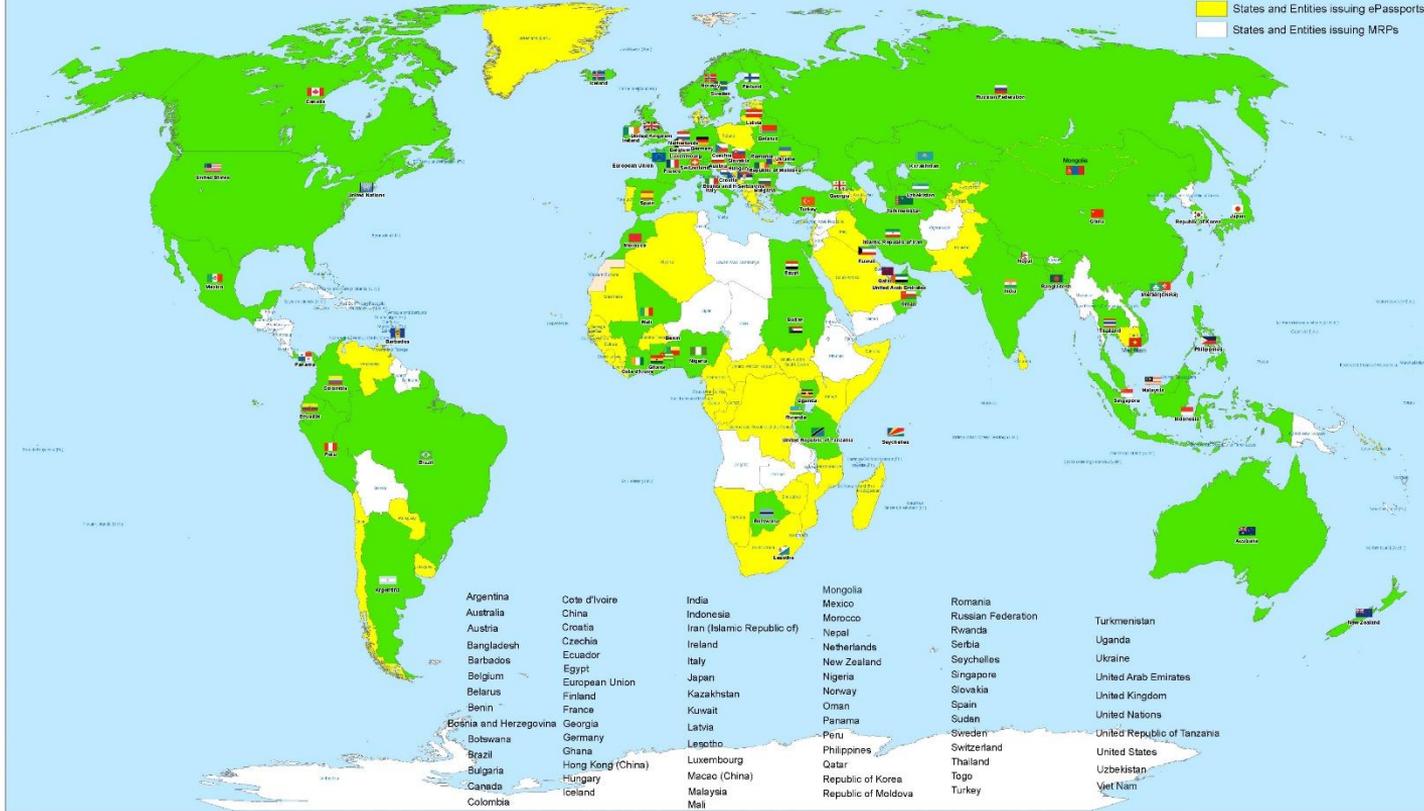
SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



### 82 PKD Participants and ePassports issuing States and Entities

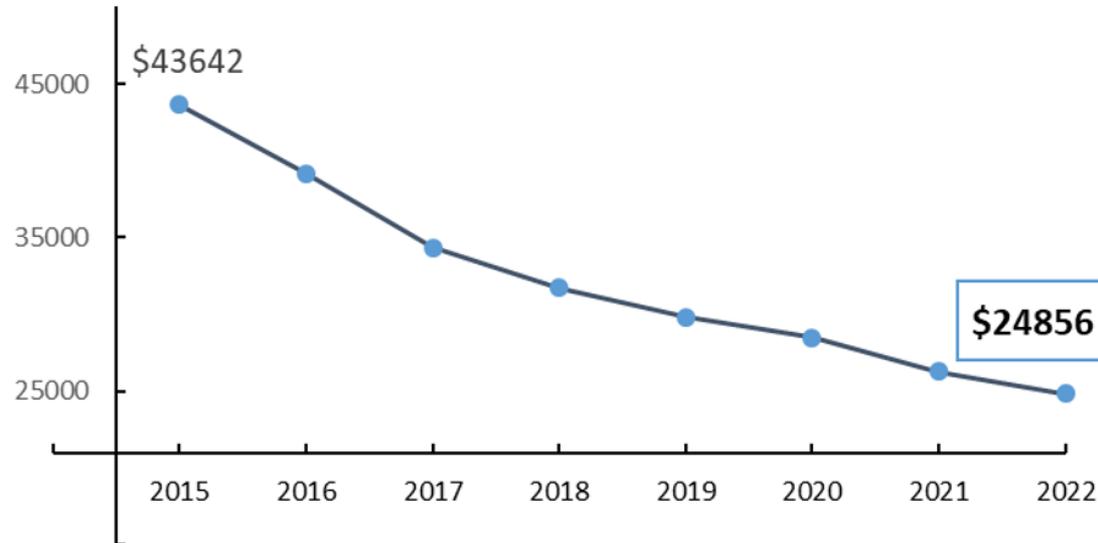
- Legend**
- PKD Participants
  - States and Entities issuing ePassports
  - States and Entities issuing MRPs





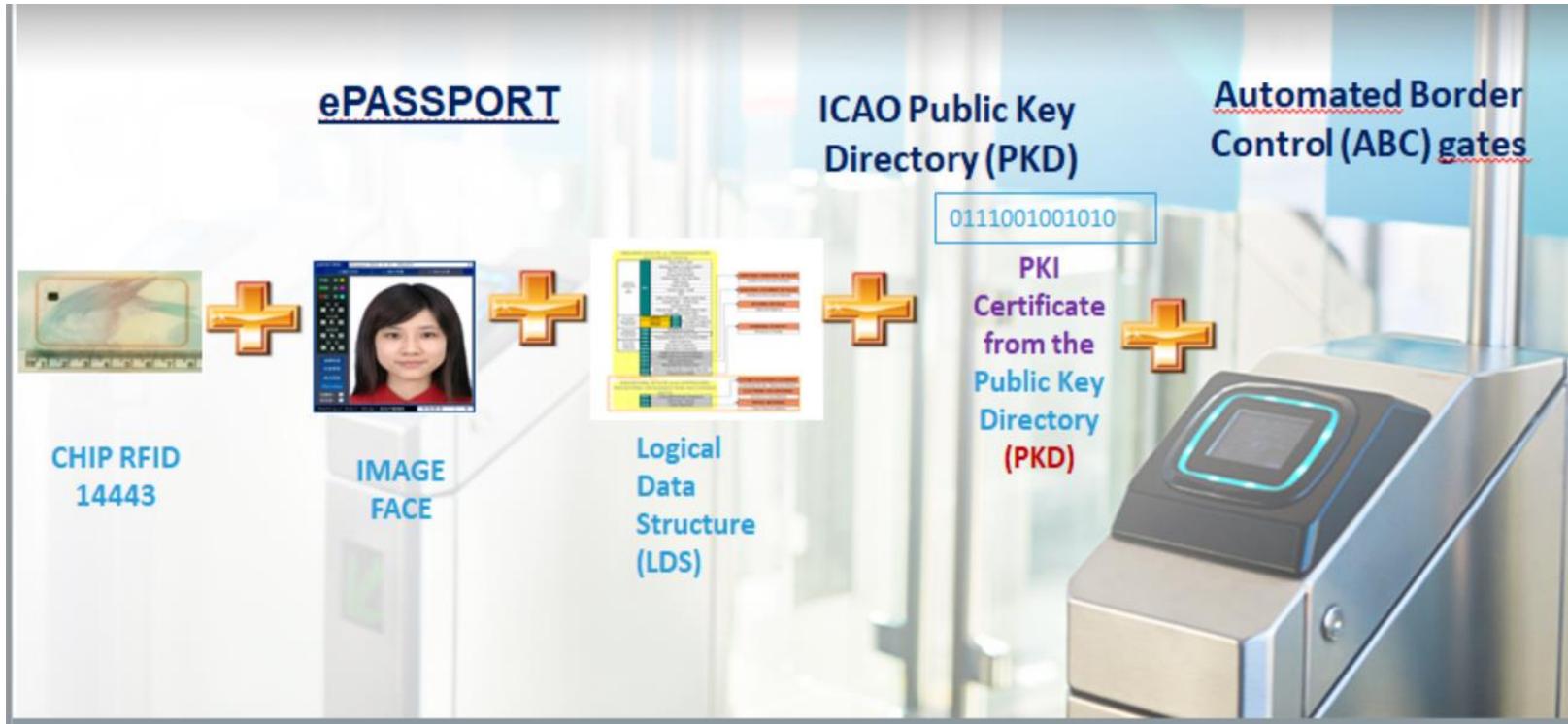
# Increasing participation increases accessibility for all States

PKD Annual Fee 2015-2022





# The benefits of associating ePassport, PKD, ABC gates & facial recognition





## Race to digital solutions

We increasingly turn to digital tools to solve problems. This is also true for facilitation of aviation.





# Future developments: Digital Travel Credential (DTC)

Specs of Type 1 DTC approved and  
To be published soon





| ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND

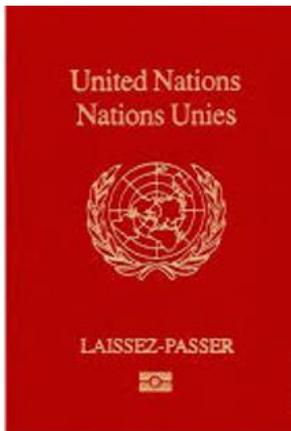


# ICAO Digital Travel Credential (DTC)

*“.....the ePassport must be used as the benchmark – it offers a secure, portable, verifiable and unclonable token. Anything that is pursued...must match this offering, while maintaining a balance between security and facilitation”*



# What if there is no physical passport anymore?



LAISSEZ-PASSER



LDS		DATA ELEMENTS		
REQUIRED	ISSUING STATE OR ORGANIZATION DATA	Detail(s) Recorded in MRZ	DG1	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
				Country Check Digit
			OPTIONAL	ISSUING STATE OR ORGANIZATION DATA
	Encoded Finger(s)			
	Encoded Eye(s)			
Displayed Identification Feature(s)	DG5	Displayed Portrait		
	DG6	Reserved for Future Use		
	DG7	Displayed Signature or Usual Mark		
Encoded Security Feature(s)	DG8	Data Feature(s)		
	DG9	Structure Feature(s)		
	DG10	Substance Feature(s)		
	DG11	Additional Personal Detail(s)		
	DG12	Additional Document Detail(s)		
	DG13	Optional Detail(s)		
	DG14	Security Options		
	DG15	Active Authentication Public Key Info		
	DG18	Person(s) to Notify		

DataGroup 1



DataGroup 2



- Document Type
- Issuing State
- Name of Holder
- Document Number
- Nationality
- Date of Birth
- Check Digit DOB
- Sex
- Date of Expiry
- ...



To proof integrity and authenticity of the data, the chip contains the Document Security Object

EF.SOD

Hash (DataGroup 1)

Hash (DataGroup 2)

Hash (DataGroup n)

DIGITAL SIGNATURE



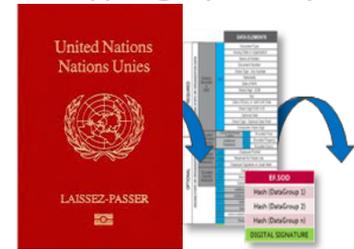


# The Hybrid Concept

**Hybrid Concept:** A DTC consists of a **Virtual Component** (DTC-VC) containing the digital representation of the holder's identity and one **Physical Component** (DTC-PC) that is cryptographically linked to the Virtual Component.

Three Types foreseen

1. *eMRTD bound*: DTC-VC with the eMRTD as the (only) DTC-PC.
2. *eMRTD-PC bound*: The physical device will serve as the DTC-PC, with the eMRTD as the alternate or as a fallback DTC-PC.
3. *PC-bound*: DTC-VC and DTC-PC but NO eMRTD anymore. Only the physical device will serve as the PC.





## Use cases

- Advanced information – sending the DTC-VC as part of an **Electronic Travel Authority** for early passenger screening and authentication
- Extracting data from an eMRTD (phone or kiosk) to create a DTC-VC and moving through points in the airport in a **seamless or 'touchless' manner** using biometrics

### Use of DTC for passenger facilitation



Pushing the border out



Biometric passenger pre-screening



Seamless arrival into the country

### Use of DTC for visitor program transformation



Improving the application experience



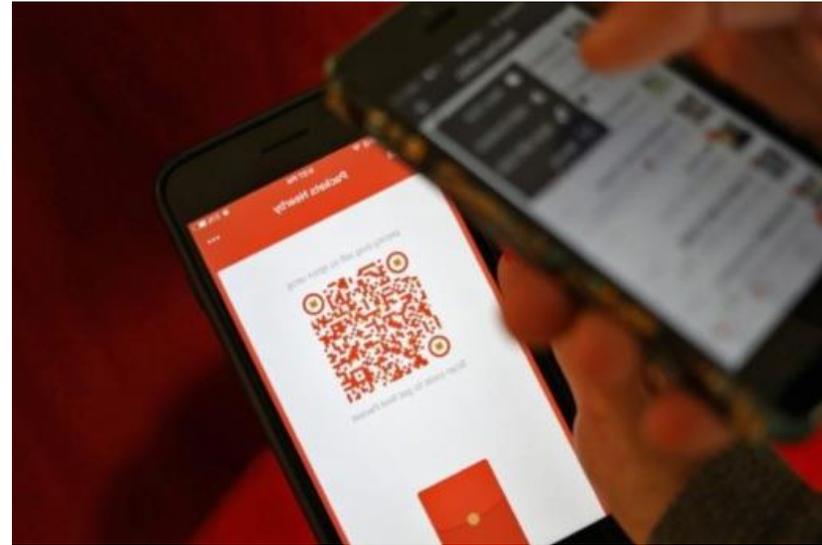
Expanding remote identity management



Enhancing data integrity and quality



# Visible Digital Seals (VDS) for Non-Electronic Documents – New Part 13, 9303, 8th Edition





## VISIBLE DIGITAL SEAL (VDS)

- The digital seal is a well established, fully ICAO standardized security feature which is already used for security documents.
- The implementation is relatively cheap and easy, various alternatives exist.
- Use of electronically signed bar codes standardized by ICAO
  - Visa
  - emergency travel documents
  - Can be applied to Digital Travel Authorizations (DTA)
  - Can be applied to health certificates (new Use Case) ... **VDS-NC**



ICAO

Doc 9303

Machine Readable Travel Documents  
Eighth Edition, 2021

Part 13: Visible Digital Seals



Approved by and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION







- Production class visa label
- 2D barcode 15x15mm<sup>2</sup>
- Barcode contains:
  - MRZ data
  - Passport number
  - Issuing date
  - Digital signature



# TRIP 2022

SEAMLESS AND CONTACTLESS  
Sharing data to accelerate the recovery

Mark your  
calendar

Montréal, Canada, 13-15 September 2022

Seamless and contactless: sharing data to accelerate the recovery

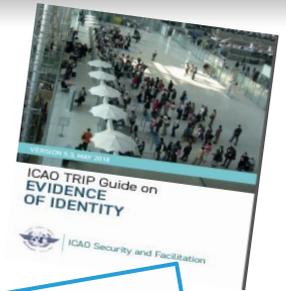


- ✓ a world-class forum
- ✓ for the exchange of information
- ✓ on all aspects of traveller identification management and the ICAO TRIP Strategy
- ✓ providing decision makers and technical experts
- ✓ with valuable insight on key current and emerging issues.



# New and Updated Guidance Materials

- **Technical Report - Digital Travel Credentials (DTC):  
Virtual Component Data Structure and PKI mechanisms – NEW**
- **Technical Report – VDS-NC - New**
- **Guidelines – VDS-NC for travel related health Proofs - New**
- Guide on Evidence of Identity
- **Doc 9303 Machine Readable Travel Documents (8<sup>th</sup> Edition) - New**
- Guide for Circulating Specimen Travel Documents
- Guidance on Migrating CSCAs
- Guide for Best Practice Guidelines for Optical Machine Authentication
- The Implementation Steps of Advance Passenger (API) System
- Passenger Name Record (PNR) information





| ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



# Questions?

Name: Christiane DerMarkar  
Email: [cdermarkar@icao.int](mailto:cdermarkar@icao.int)



THANK YOU!