International Civil Aviation Organization

WORKING PAPER

A40-WP/7
EX/4
5/7/19
(Information Paper)

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 14: Facilitation Programmes

BENEFITS OF PARTICIPATION IN THE ICAO PUBLIC KEY DIRECTORY (PKD)

(Presented by the Council of ICAO)

EXECUTIVE SUMMARY

This paper presents information on the ICAO Public Key Directory (PKD) highlighting the benefits to be derived by States from membership in the ICAO PKD. The ICAO PKD was established to support States in gaining access to public key information required to validate and authenticate ePassports. It is an essential part of the ICAO Traveller Identification Programme (TRIP) Strategy as it supports processes of reading and verifying travel documents in an efficient and cost-effective manner. Verification of ePassports using the associated public key infrastructure certificates can provide border control authorities with assurance that travel documents are genuine and unaltered, which in turn authenticates the biometric information contained in ePassports and allows for automation of aspects of the border clearance process. The validation of ePassports is an essential element in capitalizing on the investment made by States in developing such travel documents, contributing to improved border security, combatting terrorism and crime, and promoting secure air travel globally. As the ICAO PKD serves both facilitation and security needs at the same time, making use of the ICAO PKD will help to counter gaps in the security of a country's border control systems, while at the same time, enhancing the travellers' experience during their journey. The PKD currently comprises 66 participants. ICAO encourages all Member States to join the PKD and actively use it with a view to enhancing the efficiency and effectiveness of ePassport validation.

Strategic Objectives:	This working paper relates to Strategic Objective — *Security and Facilitation*
Financial implications:	No additional resources are required.
References:	C – DEC 216/2 Doc 9303 (7th Edition), *Machine Readable Travel Document* A40-WP/6, Developments pertaining to the ICAO Public Key Directory (PKD) A40-WP/8, Developments pertaining to the ICAO Traveller Identification Programme (ICAO TRIP) Strategy

1. BACKGROUND

1.1 An electronic passport (ePassport) is a Machine Readable Passport (MRP) with an integrated circuit (IC) chip with encrypted data that stores the biographical information visible on page two of the passport related to its holder. When an ePassport is personalized by the issuing State, it is locked and hence cannot be modified, adding a layer of security to MRPs.

1.2 In addition to the biographic traveller information on the passport data page, an ePassport chip (Appendix A) stores State-specific digital security features, known as a State's digital signature. These digital signatures are unique to each State and are securely stored in the chip of the ePassport as the Document Security Object (SOD) allowing them to be verified through Public Key Infrastructure (PKI) of the issuing State. Appendix B sets out the links between the issuance and verification of an ePassport can be done and how its authentication can be confirmed using the ICAO Public Key Directory (PKD). When an ePassport is scanned and the chip data is read, its authenticated digital signature tells border authorities that the data on the chip is authentic, that it was issued by the State, and that it has not been altered.

1.3 This authentication, usually referred to as ePassport validation, is the process of validating the authenticity and integrity of an ePassport by verifying the digital signature on the chip. For the border control of a receiving State to authenticate the ePassport of a foreign traveller, the receiving State must have access to certain information from the issuing State.

1.4 There are more than 140 States and non-State entities, such as the United Nations, currently issuing ePassports or electronic Machine Readable Travel Documents (eMRTDs), with about one billion ePassports in circulation. Although the State's digital signatures can be exchanged bilaterally, the increasing number of States issuing ePassports and the correspondingly high volume of ePassports in circulation would result in a highly complex, ineffective system that could delay the facilitation process and create errors. The ICAO PKD has been created to be a central repository for exchanging the information required to authenticate ePassports. Therefore it provides an efficient means for States to upload their own information and download that of other States for the purpose of using it at the border controls to enhance both facilitation and security. Not all States issuing ePassports are PKD participants, as shown in Appendix C.

2. THE PKD ROLE IN THE ICAO TRAVELLER IDENTIFICATION PROGRAMME (TRIP) STRATEGY

2.1 The ICAO TRIP Strategy employs an approach consisting of five interlinked elements that help States to establish and confirm the identity of travellers. The five elements are complementary and mutually reinforcing. Effective traveller identification helps to optimize the economic, social and political benefits of international travel and also helps to manage security risks and to respond to threats at borders by enabling better targeting of resources towards persons of interest.

2.2 Together, the elements of the ICAO TRIP Programme enable States to identify travellers and perform targeted traveller risk assessment, notably by linking Inspection Systems and Tools (IST) and Interoperable Applications (IA). The collection of traveller information completes the ICAO TRIP cycle by contributing additional evidence of identity concerning foreigners entering States.

2.3 Inspection Systems and Tools enable border authorities to capture, verify and record data about travellers contained in the Machine Readable Travel Documents (MRTDs). Controls on the holders of travel documents can be performed at the different phases of the journey: pre-departure, pre-arrival, entry, stay and exit. Those controls are enhanced by the

global sharing of data about travellers and their travel documents achieved by Interoperable Applications. These two of the five elements of the ICAO TRIP Strategy directly relate to Border Control Management (BCM). The Border Control Systems (BCS) used by States integrate Interoperable Applications with Inspection Systems and Tools.

2.4 Inspection Systems and Tools capture, verify, match and record the data contained in MRTDs and about travellers while Interoperable Applications enable global sharing of data about travellers and their travel documents. The integration of IST with IA in national BCS allow traveller risk assessment to be undertaken throughout the different phases of a traveller's journey. This assessment is informed by the identification of travellers using the new information that becomes available to transit and destination States at each phase of the journey. The description of the ICAO TRIP elements, some items under IST and IA, and how they interact with the different phases of a typical traveller's journey, are shown in Appendix D.

2.5 The foundation of an efficient Border Control Management is to effectively read the MRTD data elements by using standardized and interoperable MRTDs and eMRTDs, compliant with the technical specifications of ICAO Doc 9303, *Machine Readable Travel Documents* at https://www.icao.int/publications/pages/publication.aspx?docnum=9303. States should comply with the full application of these technical specifications to ensure that interoperability is achieved, and that the associated security and facilitation benefits are realised.

3. BENEFITS OF USING THE PKD AT THE BORDERS

3.1 From the point of view of the issuer State, the use of modernized issuance technologies with secure network and PKI infrastructures is enhancing both trust in passports issued by the State and participation in international security initiatives. Furthermore, it allows flexibility for newer initiatives such as Electronic Travel Authorization (ETA), Automated Border Control (ABC) gates and all modern tools available based on ePassports' technology. To fully leverage the benefits of being a PKD member, the use of the PKD should go hand-in-hand with enhanced border inspections.

3.2 In 2014, the United Nations Security Council (UNSC) adopted resolution 2178 which notably states: "reaffirms that all States shall prevent the movement of terrorists by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents". Joining and using the ICAO PKD can help Member States in implementing this UNSC resolution as it is recognized as a valuable instrument, currently without a viable alternative. From the State perspective it is a proactive approach in both contributing to enhance passenger travel experience and fighting international terrorism.

3.3 Without the ability of validating the electronic data in an ePassport at a foreign border, the travel document must be treated exactly as an MRP and provides no added security. The ICAO PKD enables a simple, fast and cost-efficient way of validating ePassports. Only the use of an ePassport reader pre-loaded with PKD data at border controls can confirm the authenticity of an ePassport data chip. Therefore, using the PKD tool at the borders ensures that timely information is available to validate ePassport authenticity. This process simplifies the ePassport validation process at borders, and facilitates fast and secure cross-border movement by enabling the prompt detection of compromised or false chips.

3.4 From the perspective of an ePassport-issuing State, it is important to ensure that border authorities around the world are validating their ePassports. Fees for PKD membership are low, in comparison to the investment required to maintain a bilateral infrastructure to connect to all ePassport-issuing participants. Sharing data via the PKD channel reduces such related administrative costs under a bilateral approach. Furthermore, the PKD fees decrease with the increased number of PKD participants.

3.5 Using PKD at the borders provides strong trust in physical and electronic security of ePassports. Physical data page and chip data can be matched to visible inspection, while facial recognition can be applied to a photo of the arriving passenger. Imposters and counterfeiters therefore have many challenges to achieve entry if inspection is done properly.

3.6 Participating in the ICAO PKD offers first-serve-access for the issuing State's border control agencies. Validating ePassports in line with Part 12 of Doc 9303 provides confidence to the border authority that a travel document under inspection has been issued by the proper authorities and that the information recorded on the document has not been tampered. Doc 9303 Part 12 details the PKI specifications, an important component of the overall security of MRTDs, as it provides the requirements needed for the information technology specialists who are tasked with developing the national PKI (NPKI) ystem for the States and covers topics such as roles and responsibilities, key management, distribution mechanisms, PKI trust and validation. The ICAO PKD tool provides reliable and cost-effective access to the NPKI published by other States making a robust ePassport validation possible.

3.7 Furthermore, becoming a PKD participant enables an ePassport-issuing State to share experiences with other States and to benefit from their experience, while gaining the efficiencies of multilateral data exchange and facilitating international travel for its own citizens.

3.8 Finally, it is noteworthy that the PKD Board is finalizing a Master List, expected to be available end 2019, representing a significant addition to the current services offered by the ICAO PKD.

4. CONCLUSIONS

4.1 Joining the ICAO PKD should be part of strengthening overall national identity management. Preventing criminals from obtaining a genuine ePassport under a false identity is vital and linking issuing systems with civil registry data is essential.

4.2 The introduction of the PKD should be properly prepared. States should ensure compliance with ICAO specifications from the start. States need to address national and international administrative steps and technical issues related to their system's integration into the ICAO PKD. The practical steps to implement the ICAO PKD are detailed in Appendix E.

4.3 Owing to ICAO's standards, recommended practices and specifications, every state today has the opportunity to benefit from this framework, which has created a truly globally interoperable system for reading and verifying passports at international borders.

4.4 It represents a significant contribution to global security, and facilitates immigration processes at airports, as well as at land and sea borders. Adding biometric features, such as facial images, to the contactless chip in MRPs shows that the level of security has grown substantially. It is now up to the border management agencies worldwide to upgrade their infrastructure to be able to read these features and use them in their border systems to verify the identity of bearers.

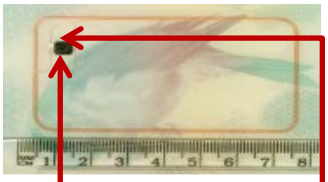
— — — — — — — —

APPENDIX A

WHAT IS AN ePASSPORT?

ICAO defines ePassport as a Machine Readable Passport (MRP) containing a contactless integrated circuit (IC) chip within which is stored data from the MRP data page, a biometric measure of the passport holder and a security object to protect the data with a cryptographic technology, and which conforms to specifications contained in Doc 9303-4.

MRP **Chip**



Logical Data Structure (LDS) **State Digital Signature**

The LDS contains biographic and mandatory biometric data (image face) in addition to other information.

ISSUING STATE or ORGANIZATION RECORDED 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		
Encoded Identification Feature(s)	GLOBAL INTERCHANGE FEATURE	DG2	Encoded Face	
	Additional Feature(s)	DG3	Encoded Finger(s)	
		DG4	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	Reserved for Future Use		
	DG15	Active Authentication Public Key Info		
	DG16	Person(s) to Notify		

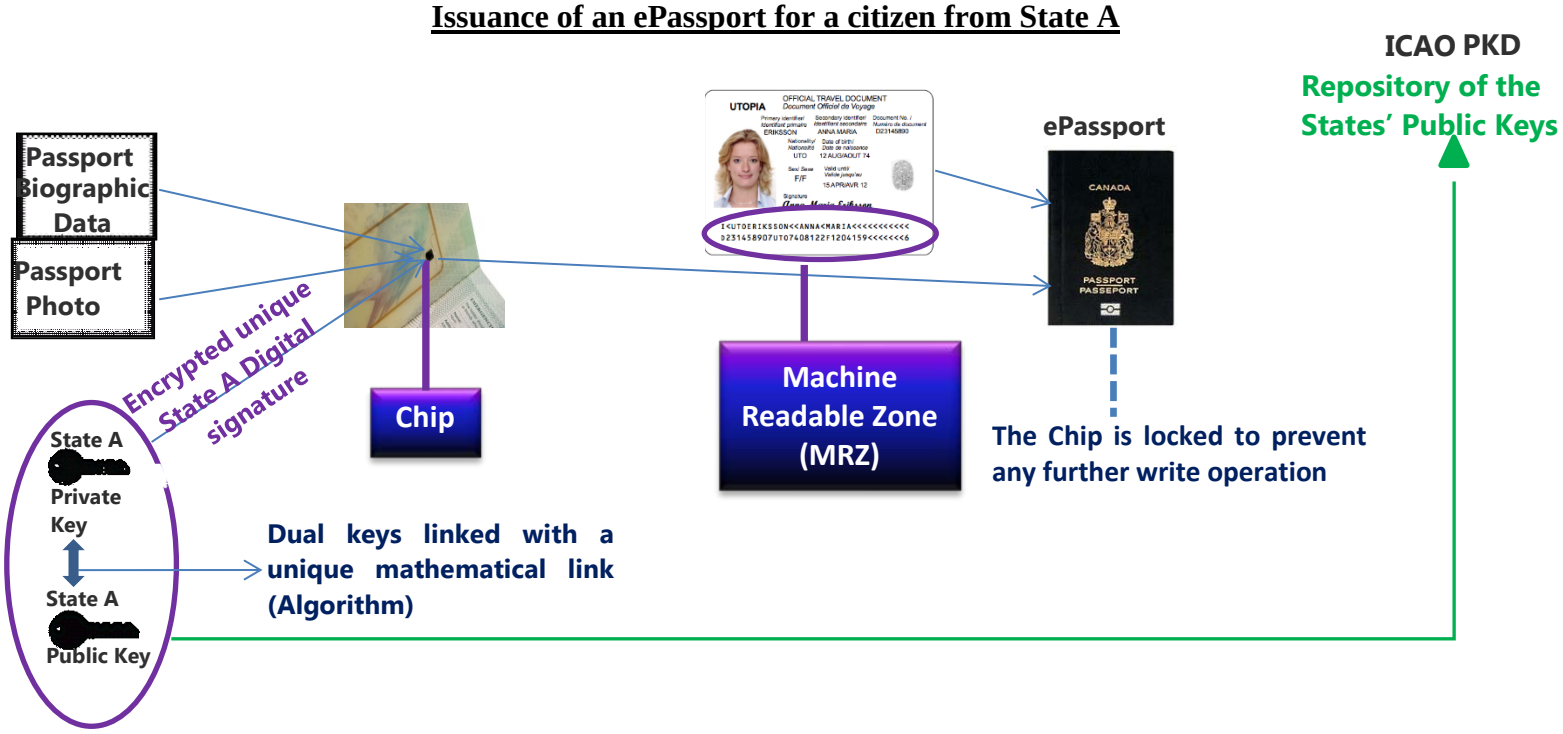
Proper validation of the issuing State Digital Signature on an ePassport's chip points to the authenticity and integrity of the data placed in the LDS portion of the chip.

— — — — — — — —

APPENDIX B

FROM THE ISSUANCE OF AN EPASSPORT TO ITS VERIFICATION AT THE BORDERS: THE TRUST CHAIN

Issuance of an ePassport for a citizen from State A



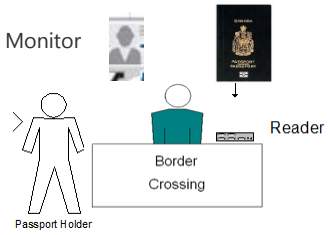
Checking Steps when the citizen from State A arrives at the State B border

Step 1

- The MRZ data is simply a representation of some of the printed information on the data page, allowing computers to electronically read the printed information accurately.
- The officer scans the passport through a reader to read the MRZ which allows the ePassport chip to be accessed.
- The contents of the MRZ contain a key which is used to access the chip and the chip is only allowed to communicate with a reader if the key matches.
- If it is the case, the data and photo are retrieved and the checking goes to Step 2.

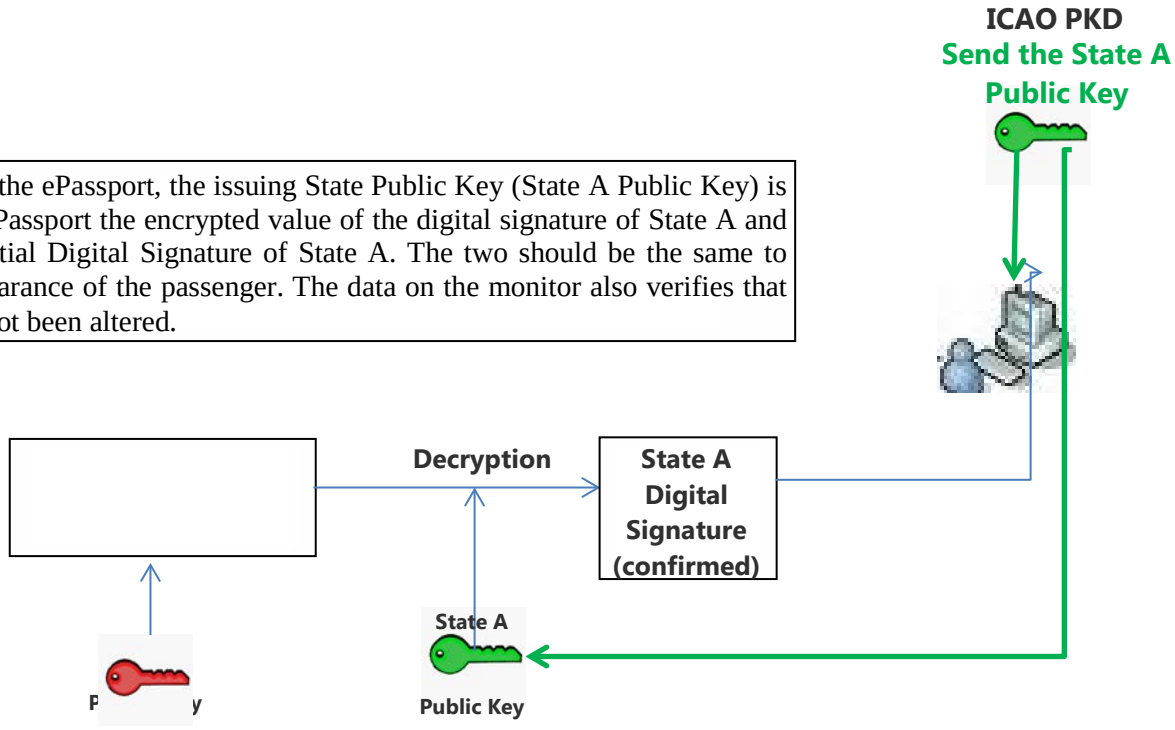
Step 2

The chip is opened and the officer checks that the holder matches the photo in the passport as well as the data and the photo in the passport' s chip as shown on the monitor. The next step consists in verifying that the passport was issued by a legitimate authority and it has not been altered since its issuance.



Step 3

In order to authenticate the ePassport, the issuing State Public Key (State A Public Key) is used to decrypt in the ePassport the encrypted value of the digital signature of State A and to compare it to the initial Digital Signature of State A. The two should be the same to allow the successful clearance of the passenger. The data on the monitor also verifies that the passport data have not been altered.

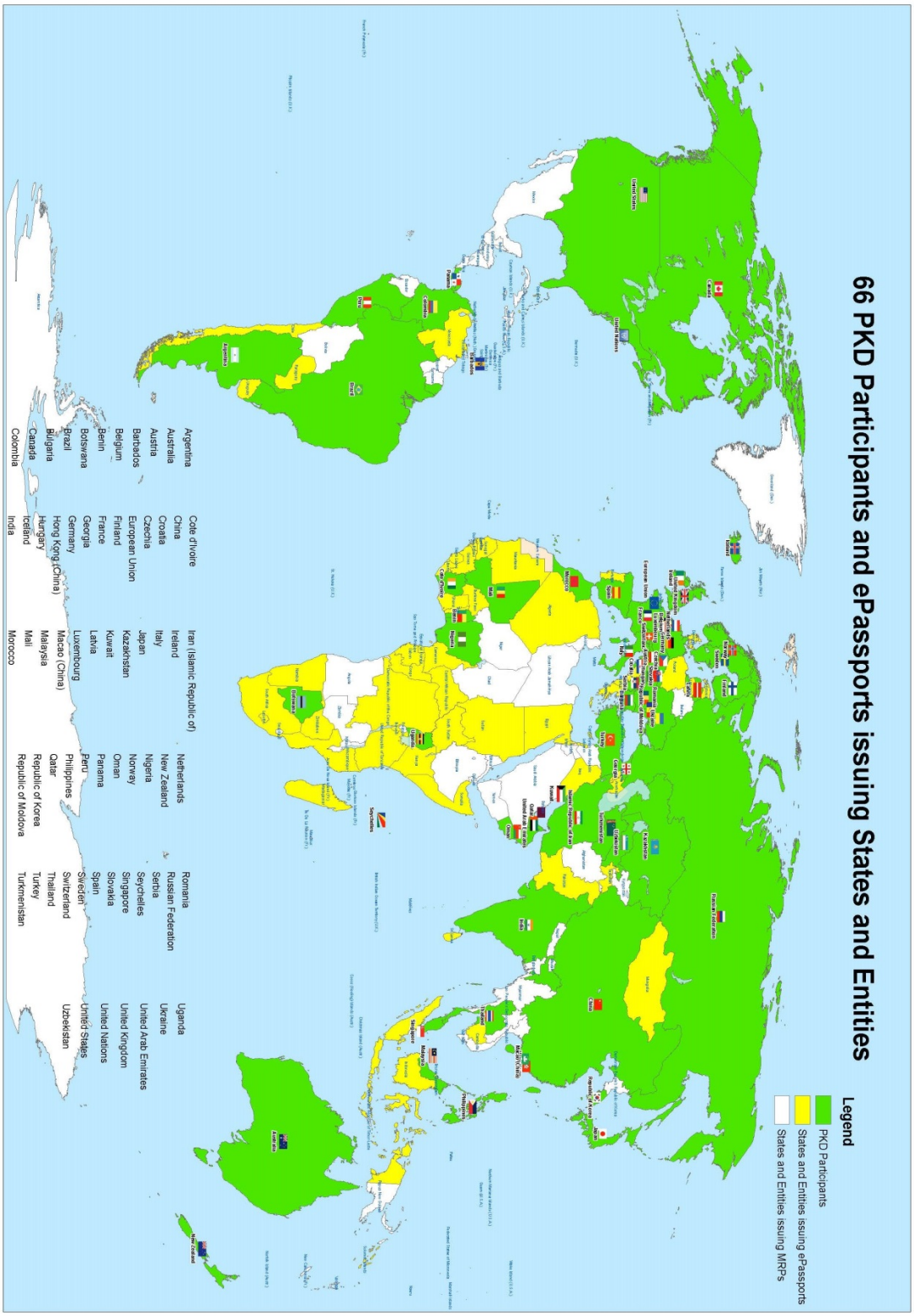


The role of the ICAO PKD is to validate the authenticity of each State's Public Key otherwise the whole set of data of the ePassport could be counterfeit. This is confirmed through the official import ceremony of each PKD participant Public Key. However, the ICAO PKD does not guarantee identity of the passport holder as it only guarantees that the data in the ePassport are unchanged since the production by a specific producer.

— — — — — — — —

APPENDIX C

STATES AND ENTITIES ISSUING ePASSPORTS AND PKD PARTICIPANTS

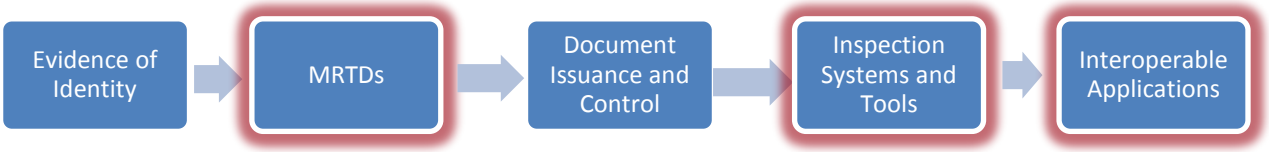


— — — — — — — — —

APPENDIX D

THE ICAO TRIP STRATEGY AND BORDER CONTROL MANAGEMENT

The five elements of the ICAO TRIP Strategy: Three of them are linked to the PKD use



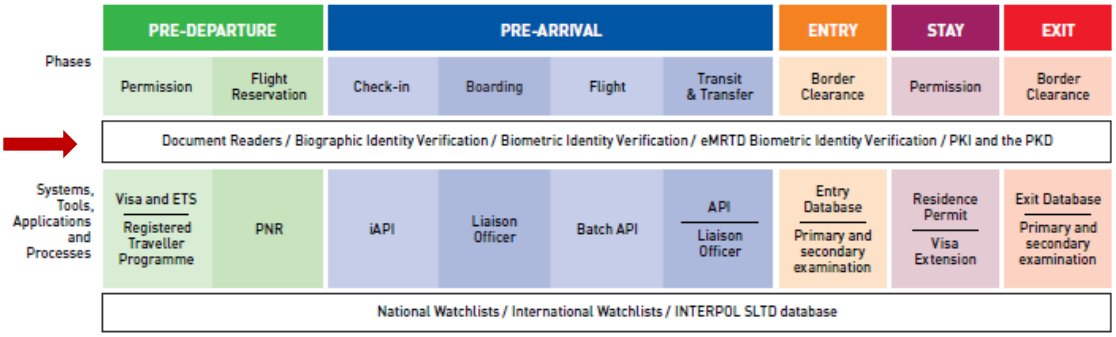
Some examples of the different items for the Fourth and the Fifth elements of the ICAO TRIP Strategy are highlighted in the table below

INSPECTION SYSTEMS AND TOOLS	INTEROPERABLE APPLICATIONS
Visas and Electronic Travel Systems (ETS)	Advance Passenger Information (API) and Interactive API (iAPI)
Document Readers	Passenger Name Record (PNR) data
Public Key Infrastructure (PKI)	Public Key Infrastructure (PKI)
ICAO Public Key Directory (PKD)	ICAO Public Key Directory (PKD)
Biographic Identity Verification	eMRTD Biometric Identity Verification
Biometric Identity Verification	INTERPOL Stolen and Lost Travel Documents (SLTD) Database
National Watch Lists	International Watch Lists
Entry and Departure Databases	Automated Border Controls (ABCs)
Automated Border Controls (ABCs)	

The different phases of a traveller's journey

The preparation for the use of the ICAO PKD tool should start at the Pre-Departure phase when issuing the eMRTD (2nd TRIP element). At the Entry phase, the ICAO PKD tool (4th TRIP element) would be used to authenticate the eMRTD and its interoperability (5th TRIP element) would enable to link the eMRTD to the other interoperable applications.

Issuance of the eMRTD with the State Digital Signature



AT ALL PHASES OF THE JOURNEY: Document readers are used for the reliable, efficient capture of traveller identity details. Biographic identity verification checks are undertaken using the data read from travel documents. Where available, biometric identity verification and PKI authentication, thanks to the use of the PKD tool, contribute to assuring traveller identification. After traveller identity is established to a sufficient level of confidence, a State can check the INTERPOL Stolen and Lost Travel Documents (SLTD) database and national and international watch lists to inform a traveller risk assessment.

— — — — — — — —

APPENDIX E

PRACTICAL STEPS TO JOIN THE ICAO PKD

1) Review national legislation: A thorough review of the national legislative framework is essential before introducing ePassports and participating in the ICAO PKD.

2) Define roles and responsibilities and implement an NPKD: States have the responsibility to ensure the quality of the material they share via the ICAO PKD. This requires that roles and responsibilities of national stakeholders are clearly defined, and technical standards are adhered to and maintained. This applies especially to National Public Key Directories (NPKDs) which will upload and download certificates to and from the ICAO PKD, and the CSCA.

3) Join the ICAO PKD: The initial step to take for a State is to sign the PKD Memorandum of Understanding (MoU) with ICAO. This is followed by a window of 15 months to connect the NPKD to the ICAO PKD and to start active upload and download. States willing to become an ICAO PKD participant should consult the Secretariat regarding the registration process details.

4) Integrate the NPKD with the ICAO PKD: The final step involves the full integration of the NPKD of the State with the ICAO PKD. This includes NPKDs uploading and downloading certificates and revocation lists to and from the ICAO PKD.

— END —