

PART I: GUIDANCE

ICAO TRIP Guide on **BORDER CONTROL MANAGEMENT**



ICAO

SECURITY AND FACILITATION

VERSION 1, 2018

The International Civil Aviation Organization (ICAO) is a UN specialized agency established by States in 1944 to manage the administration and governance of the Convention on International Civil Aviation (Chicago Convention).

ICAO works with the Convention's 191 Member States and industry groups to reach consensus on international civil aviation Standards and Recommended Practices (SARPs) and policies in support of a safe, efficient, secure and economically sustainable and environmentally responsible civil aviation sector.

ICAO's mission is to serve as the global forum of states for international civil aviation, with the objective to support and enable a global air transport network that meets or surpasses the social and economic development and broader connectivity needs of global business and passengers.

Security & Facilitation is one of the five comprehensive Strategic Objectives of ICAO, meant to enhance global civil aviation security and facilitation. This Strategic Objective reflects the need for ICAO's leadership in aviation security facilitation and related border security matters.

Disclaimer

All reasonable precautions have been taken by ICAO to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied; nor does it necessarily represent the decisions or policies of ICAO. The responsibility for the interpretation and use of the material contained or referred to in this publication lies with the reader and in no event shall ICAO be liable for damages arising from reliance upon or use of the same. This publication shall not be considered as a substitute for the government policies or decisions relating to information contained in it. This publication contains the collective views of an international group of experts, believed to be reliable and accurately reproduced at the time of printing. Nevertheless, ICAO does not assume any legal liability or responsibility for the accuracy or completeness of the views expressed by the international group of experts.

Published by:

ICAO
Security & Facilitation
International Civil Aviation Organization
999 Robert-Bourassa Boulevard
Montréal, QC, Canada H3C 5H7

Email: fal@icao.int
Tel: + 1 514 954-9219
Fax: +1 514 954-6077
www.icao.int/Security/FAL/TRIP
www.icao.int

Printed by ICAO
2018 International Civil Aviation Organization

ICAO TRIP Guide on **BORDER CONTROL MANAGEMENT**

PART I: GUIDANCE



| ICAO SECURITY AND FACILITATION

Funded by the
Government
of Canada

Canada

The development of this guide was funded by the Government of Canada as part of a counter-terrorism capacity-building project implemented by the International Civil Aviation Organization for the benefit of its Member States.

Contributors to the ICAO TRIP Guide on Border Control Management:



CONTENTS

EXECUTIVE SUMMARY	4
ACKNOWLEDGEMENTS	5
ACRONYMS	6
DEFINITIONS	8
1. ABOUT THIS GUIDE – SCOPE AND APPLICATION	12
2. ICAO TRIP AND BORDER CONTROL MANAGEMENT	15
2.1 ICAO Traveller Identification Programme	15
2.2 Integrating Inspection Systems and Tools with Interoperable Applications	15
2.3 Identification of Travellers and Risk Assessment	18
3. NATIONAL STRATEGIES FOR BORDER CONTROL MANAGEMENT	21
3.1 Application of Technology	21
3.2 Strategic Frameworks	22
3.3 Environment and Travel Patterns	22
3.4 National Stakeholders	23
3.5 Regional Arrangements	27
3.6 International Law	28
4. INSPECTION SYSTEMS AND TOOLS	31
A. Visas and Electronic Travel Systems	32
B. Document Readers	37
C. Biographic Identity Verification	42
D. Biometric Identity Verification	45
E. National Watchlists	50
F. Entry and Exit Databases	54
G. Automated Border Controls	58
5. INTEROPERABLE APPLICATIONS	63
H. Advance Passenger Information and Interactive Advance Passenger Information	64
I. Passenger Name Record	71
J. Public Key Infrastructure and the ICAO Public Key Directory	76
K. eMRTD Biometric Identity Verification	82
L. INTERPOL's Stolen and Lost Travel Documents Database	86
M. International Watchlists	91
6. EXAMINATION OF TRAVELLERS AND TRAVEL DOCUMENT INSPECTION	95
6.1 Primary and Secondary Examination of Travellers	95
6.2 Manual and Visual Inspection of Travel Documents	97
7. HUMAN RESOURCE CONSIDERATIONS IN BORDER CONTROL MANAGEMENT	101
7.1 Personnel	101
7.2 Transparency and Governance	103
8. ASSISTANCE TO STATES	105
8.1 ICAO's Assistance to Member States	105
8.2 Other International Assistance	106
APPENDIX A – REFERENCE DOCUMENTATION	107

EXECUTIVE SUMMARY

ICAO is the United Nations Specialized Agency that has the mandate and responsibility for establishing, maintaining and promoting Standards and Recommended Practices (SARPs) related to the issuance and verification of machine-readable travel documents and related border control processes. Under the Traveller Identification Programme (TRIP) Strategy endorsed by the ICAO Assembly, ICAO is focused on ensuring a holistic and coordinated approach to traveller identification – from document issuance to Border Control Systems (BCS).

The ICAO TRIP Strategy is a framework for uniquely identifying travellers for enhancing border security and facilitation by bringing together the elements of identification management. Two TRIP elements relate to Border Control Management (BCM): **Inspection Systems and Tools** and **Interoperable Applications**.

The *ICAO Traveller Identification Programme Guide on Border Control Management* is intended for reference by States to optimize the use of the tools, systems and applications available to enhance their national BCM. The Guide includes 13 technical topics describing and categorizing the Inspection Systems and Tools and Interoperable Applications that can be applied for this purpose.

States combine the Inspection Systems and Tools and Interoperable Applications in their BCS – the integrated Information and Communication Technology (ICT) solutions that support BCM. The Guide identifies options available to States to enhance their national BCS and explains the interdependencies that link the Topics.

BCM is the sovereign responsibility of States. In their traveller border control arrangements States seek to maximise the economic, social and political benefits of travel while at the same time identifying and mitigating risks and threats.

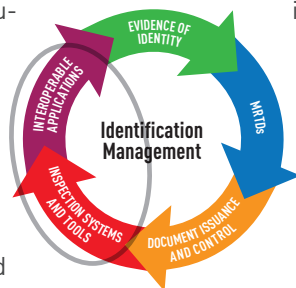
Identification of travellers and risk assessment of travellers, concepts introduced and explained in the Guide, can assist States in achieving these national objectives.

While States can be expected to have extensive knowledge of their own citizens and residents, they rely on foreign data and information about the identity and nationality of the citizens and residents of other States. Therefore, the SARPs and technical specifications published by ICAO play a critical role in ensuring that travel documents issued by States contain standardised traveller identity information in a standardised machine readable format and that the identity information can be communicated in a standardised, interoperable way.

The Guide discusses the contribution made by other United Nations (UN) agencies and international organisations to the traveller identification and risk assessment undertaken by States in their BCM. The Consolidated UN Security Council Sanctions List (CUNSCSL) and INTERPOL Red Notices identify potential travellers of security and law enforcement concern to States. Checks against INTERPOL's Stolen and Lost Travel Documents (SLTD) database are essential prior to relying on travel documents as evidence of identity.

Importantly, the Guide recognises that national BCM is most effective when it is applied across the travel continuum – when traveller identification and risk assessment is undertaken continuously by States and airlines at all phases of the traveller journey: pre-departure, pre-arrival, entry, stay and exit.

When applied in conjunction with its companion document, the Assessment Tool, the Guide can improve the traveller identification and risk assessment practice of States to achieve better security and facilitation outcomes in BCM.



ACKNOWLEDGEMENTS

The *ICAO Traveller Identification Programme (TRIP) Guide for Border Control Management* is a product of the project *Strengthening Border Control Management in the Caribbean Region*, funded by the Counter-Terrorism Capacity Building Programme of the Government of Canada.

Other activities of the project — two regional workshops (Antigua and Barbuda, and Jamaica) and four technical assistance missions (Barbados, Dominican Republic, Jamaica and Saint Lucia) — conducted in the Caribbean region

during 2017 were instrumental in informing the content of the Guide and its companion document, the Assessment Tool. ICAO is grateful for the contribution of the 13 States participating in the Project, the international and regional organizations and experts and consultants who have been involved in the activities of the Project.

Although this Guide and Assessment Tool have been developed as part of this project, they are intended for use by all Member States.

The content of the Guide reflects the invaluable contributions of:

- ICAO Implementation and Capacity Building Working Group (ICBWG)
- ICAO New Technologies Working Group (NTWG)
- European Border and Coast Guard Agency (FRONTEX)
- International Criminal Police Organization (INTERPOL)
- International Organization for Migration (IOM)
- Joint Regional Communication Centre (JRCC) of the Caribbean Community (CARICOM) Implementing Agency for Crime and Security (IMPACS)
- Organisation for Eastern Caribbean States (OECS)
- United Nations High Commissioner for Refugees (UNHCR)
- United Nations Office on Drugs and Crime (UNODC)
- United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED)

INTERNATIONAL CIVIL AVIATION ORGANIZATION

999 Robert-Bourassa Boulevard,
Montréal, Quebec H3C 5H7, Canada

Tel.: +1 514-954-8219

Fax: +1 514-954-6077

E-mail: FAL@icao.int

Internet: <http://www.icao.int>

ACRONYMS

1:1	One-to-one	ESTA	Electronic System for Travel Authorization (USA)
1:n	One-to-many	ETIAS	European Travel Information and Authorisation System
ABC	Automated Border Controls	EU	European Union
API	Advance Passenger Information	FADO	False and Authentic Documents Online
BCS	Border Control Systems	FAR	False Acceptance Rate
BCM	Border Control Management	FIND	Fixed INTERPOL Network Database
BSI	British Standards Institution	FRONTEX	European Border and Coast Guard Agency
CA	Certification Authority	FRR	False Rejection Rate
CARICOM	Caribbean Community	FTF	Foreign Terrorist Fighter
CAWG	Control Authorities Working Group (IATA)	iAPI	Interactive Advance Passenger Information
CCTV	Closed Circuit Television	IATA	International Air Transport Association
CRL	Certificate Revocation List	IBMTF	Integrated Border Management Task Force (INTERPOL)
CSCA	Country Signing Certification Authority	IC	Integrated Circuit
CUNSCSL	Consolidated United Nations Security Council Sanctions List	ICAO	International Civil Aviation Organization
DG	Data Group (in eMRTD IC)	ICC	Integrated Circuit Card
DS	Document Signer	ICT	Information and Communication Technology
DSA	Digital Signature Algorithm	IMPACS	Implementation Agency for Crime and Security (CARICOM)
DSC	Document Signer Certificates	INTERPOL	International Police Organization
EAC	Extended Access Control	INTERPOL-UNSC S/N	INTERPOL-United Nations Security Council Special Notices
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport	IOM	International Organization for Migration
eMRP	Electronic Machine Readable Passport		
eMRTD	Electronic Machine Readable Travel Document		
ETS	Electronic Travel Systems		

JRCC	Joint Regional Communications Centre
LDS	Logical Data Structure
LO	Liaison Officer
MIND	Mobile INTERPOL Network Database
MOU	Memorandum of Understanding
MRCTD	Machine Readable Convention Travel Document
MRP	Machine Readable Passport
MRTD	Machine Readable Travel Document
MROTD	Machine Readable Official Travel Document in the form of a card
MRV	Machine Readable Visa
MRZ	Machine Readable Zone
NATFP	National Air Transport Facilitation Programme
NCB	National Central Bureau
NIST	National Institute of Standards and Technology (USA)
NPKD	National Public Key Directories
NTWG	New Technologies Working Group
OCR	Optical Character Recognition
OECS	Organisation of Eastern Caribbean States
OHCHR	Office of the High Commissioner for Human Rights
OSCE	Organization for Security and Co-operation in Europe
PAXLST	Passenger List Message
PKD	Public Key Directory

PKI	Public Key Infrastructure
PNR	Passenger Name Record
PRADO	Public Register of Authentic travel and identity Documents Online
RBDES	Bali Process Regional Biometric Data Exchange Solution
SARPs	Standards and Recommended Practices
SLTD	Stolen and Lost Travel Documents
SOPs	Standard Operating Procedures
TRIP	Traveller Identification Programme (ICAO)
UAE	United Arab Emirates
UK	United Kingdom
UN	United Nations
UNCCT	United Nations Counter-Terrorism Centre
UNHCR	United Nations High Commission for Refugees
UNODC	United Nations Office on Drugs and Crime
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution
USA	United States of America
UV	Ultraviolet
VIZ	Visual Inspection Zone
WCO	World Customs Organization
XML	Extensible Markup Language

DEFINITIONS

The definitions included in the Guide are those adopted by ICAO in the publications Annex 9 – *Facilitation* and Doc 9303, *Machine Readable Travel Documents*.

AUTHENTICATION A process that validates the claimed identity of a participant in an electronic transaction.

AUTHENTICITY The ability to confirm that the Logical Data Structure and its components were created by the issuing State or organization.

AUTHORIZATION A security process to decide whether a service can be given or not.

BACKGROUND CHECK A check of a person's identity and previous experience, including where legally permissible, any criminal history, as part of the assessment of an individual's suitability to implement a security control and/or for unescorted access to a security restricted area.

BIOMETRIC A measurable, unique, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an enrollee.

BIOMETRIC DATA The information extracted from the biometric and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data).

BIOMETRIC IDENTIFICATION A means of identifying or confirming the identity of the holder of an MRTD by the measurement of one or more properties of the holder's person.

BIOMETRIC MATCHING The process of using an algorithm that compares templates derived from the biometric reference and from the live biometric input, resulting in a determination of match or non-match.

BIOMETRIC SAMPLE Raw data captured as a discrete, unambiguous, unique and linguistically neutral value representing a biometric characteristic of an enrollee as captured by a biometric system (for example, biometric samples can include the image of a fingerprint as well as its derivative for authentication purposes).

BIOMETRIC SYSTEM An automated system capable of:

- i. capturing a biometric sample from an end user for an MRP;
- ii. extracting biometric data from that biometric sample;

- iii. comparing that specific biometric data value(s) with that contained in one or more reference templates;
- iv. deciding how well the data match, i.e. executing a rule-based matching process specific to the requirements of the unambiguous identification and person authentication of the enrollee with respect to the transaction involved; and
- v. indicating whether or not an identification or verification of identity has been achieved.

BIOMETRIC VERIFICATION A means of identifying or confirming the identity of the holder of an MRTD by the measurement and validation of one or more unique properties of the holder's person.

CERTIFICATE A digital document which proves the authenticity of a public key.

CERTIFICATE REVOCATION LIST (CRL) A list of revoked certificates within a given infrastructure.

CERTIFICATION AUTHORITY

(CA) A trustworthy body that issues digital certificates for PKI.

COMPARISON The process of comparing a biometric sample with a previously stored reference template or templates. See also "One-to-many" and "One-to-one"

CONTACTLESS INTEGRATED CIRCUIT A semi-conductor device which stores MRTD data and which communicates with a reader using radio frequency energy according to ISO/IEC 14443.

COUNTERFEIT An unauthorized copy or reproduction of a genuine security document made by whatever means.

DATA PAGE The page of the passport book, preferably the second or penultimate page, which contains the biographical data of the document holder. See "Biographical data".

DIGITAL SIGNATURE The result of a cryptographic operation enabling the validation of information by electronic means. This is NOT the displayed signature of the MRTD holder in digital form.

DIRECTORY/PUBLIC KEY DIRECTORY (PKD) A repository for storing information. Typically, a directory for a particular PKI is a repository for the public key encryption certificates issued by that PKI's Certification Authority, along with other client information. The directory also keeps cross-certificates, Certification Revocation Lists, and Authority Revocation Lists.

DOCUMENT SIGNER A body which issues a biometric document and certifies that the data stored on the document is genuine in a way that will enable detection of fraudulent alteration.

ELECTRONIC MACHINE READABLE PASSPORT (eMRP) A TD3 size MRTD conforming to the specifications of Doc 9303-4, that additionally incorporates a contactless integrated circuit including the capability of biometric identification of the holder. Commonly referred to as “ePassport”.

ELECTRONIC MACHINE READABLE TRAVEL DOCUMENT (eMRTD) An MRTD (passport, visa or card) that has a contactless integrated circuit embedded in it and the capability of being used for biometric identification of the MRTD holder in accordance with the standards specified in the relevant Part of Doc 9303 — *Machine Readable Travel Documents*.

ELECTRONIC MRTD A TD1 or TD2 size MRTD conforming to the specifications of Doc 9303-5 or Doc 9303-6, respectively, that additionally incorporates a contactless integrated circuit including the capability of biometric identification of the holder.

ELECTRONIC TRAVEL SYSTEMS (ETS) The automated process for the lodgement, acceptance and verification of a passenger’s authorization to travel to a State, in lieu of the standard counterfoil paper visa.

ENROLMENT The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person’s identity.

EPASSPORT Commonly used name for an eMRP. See Electronic Machine Readable Passport (eMRP).

EXTRACTION The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.

FALSE ACCEPTANCE RATE (FAR) The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The false acceptance rate may be estimated as $FAR = NFA/NIIA$ or $FAR = NFA/NIVA$ where FAR is the false acceptance rate, NFA is the number of false acceptances, NIIA is the number of impostor identification attempts, and NIVA is the number of impostor verification attempts.

FALSE REJECTION RATE (FRR) The probability that a biometric system will fail to identify an enrollee or verify the legitimate claimed identity of an enrollee. The false rejection rate may be estimated as follows: $FRR = NFR/NEIA$ or $FRR = NFR/NEVA$ where FRR is the false rejection rate, NFR is the number of false rejections, NEIA is the number of enrollee identification attempts, and NEVA is the number of enrollee verification attempts. This estimate assumes that the enrollee identification/verification attempts are representative of those for the whole population of enrollees. The false rejection rate normally excludes “failure to acquire” errors.

FINGERPRINT(S) One (or more) visual representation(s) of the surface structure of the holder’s fingertip(s).

FORGERY Fraudulent alteration of any part of the genuine document.

HOLDER A person possessing an MRTD, submitting a biometric sample for verification or identification whilst claiming a legitimate or false identity. A person who interacts with a biometric system to enrol or have his identity checked.

HUMAN FACTORS PRINCIPLES. Principles which apply to design, certification, training, operations and maintenance and which seek safe interface between the human and other system components by proper consideration to human performance.

IDENTIFICATION/IDENTIFY The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the eMRTD holder whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with “Verification”.

IDENTITY The collective set of distinct personal and physical features, data and qualities that enable a person to be definitively identified from others. In a biometric system, identity is typically established when the person is registered in the system through the use of so-called “breeder documents” such as birth certificate and citizenship certificate.

IDENTITY DOCUMENT Document used to identify its holder and issuer, which may carry data required as input for the intended use of the document.

I-CHECKIT A screening solution that complements and enhances national border security systems. It allows trusted partners in the private sector to conduct advanced passenger checks in real-time, in collaboration with the law enforcement community.

IMPROPERLY DOCUMENTED PERSON A person who travels, or attempts to travel: (a) with an expired travel document or an invalid visa; (b) with a counterfeit, forged or altered travel document or visa; (c) with someone else's travel document or visa; (d) without a travel document; or (e) without a visa, if required.

IMAGE A representation of a biometric as typically captured via a video, camera or scanning device. For biometric purposes this is stored in digital form.

INSPECTION The act of a State or organization examining an MRTD presented to it by a traveller (the MRTD holder) and verifying its authenticity.

INSPECTION SYSTEM A system used for inspecting MRTDs by any public or private entity having the need to validate the MRTD, and using this document for identity verification, e.g. border control authorities, airlines and other transport operators, financial institutions.

INTEGRATED CIRCUIT (IC) Electronic component designed to perform processing and/or memory functions.

INTEGRITY The ability to confirm that the Logical Data Structure and its components have not been altered from that created by the issuing State or organization.

INTERFACE A standardized technical definition of the connection between two components.

INTEROPERABILITY The ability of several independent systems or sub-system components to work together.

ISSUING AUTHORITY The entity accredited for the issuance of an MRTD to the rightful holder.

ISSUING STATE The country issuing the MRTD.

ISSUING ORGANIZATION Organization authorized to issue an official MRTD (e.g. the United Nations Organization, issuer of the laissez-passer).

MACHINE ASSISTED DOCUMENT VERIFICATION A process using a device to assist in the verification of the authenticity of the document in respect to data and/or security.

MACHINE READABLE OFFICIAL TRAVEL DOCUMENT (MROTD) A document, usually in the form of a card of TD1 or TD2 size, that conforms to the specifications of Doc 9303-5 and Doc 9303-6 and may be used to cross international borders by agreement between the States involved.

MACHINE READABLE PASSPORT (MRP) A passport conforming with the specifications contained in Doc 9303-4. Normally constructed as a TD3 size book containing pages with information on the holder and the issuing State or organization and pages for visas and other endorsements. Machine readable information is contained in two lines of OCR-B text, each with 44 characters.

MACHINE READABLE TRAVEL DOCUMENT (MRTD) Official document, conforming with the specifications contained in Doc 9303, issued by a State or organization which is used by the holder for international travel (e.g. MRCTD, MRP, MRV, MROTD) and which contains mandatory visual (eye readable) data and a separate mandatory data summary in a format which is capable of being read by machine.

MACHINE READABLE ZONE (MRZ) Fixed dimensional area located on the MRTD, containing mandatory and optional data formatted for machine reading using OCR methods.

MATCH/MATCHING The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. A decision to accept or reject is then based upon whether this score exceeds the given threshold.

ONE-TO-MANY 1:n – Synonym for "Identification".

ONE-TO-ONE 1:1 – Synonym for "Verification".

PASSENGER DATA SINGLE WINDOW A facility that allows parties involved in passenger transport by air to lodge standardized passenger information (i.e. API, iAPI and/or PNR) through a single data entry point to fulfil all regulatory requirements relating to the entry and/or exit of passengers that may be imposed by various agencies of the Contracting State.

PKD PARTICIPANT An ICAO Member State or other entity issuing or intending to issue eMRTDs that follows the arrangements for participation in the ICAO PKD.

PRIVATE KEY A cryptographic key known only to the user, employed in public key cryptography in decrypting or signing information.

PUBLIC KEY The public component of an integrated asymmetric key pair, used in encrypting or verifying information.

PUBLIC KEY CERTIFICATE The public key information of an entity signed by the certification authority and thereby rendered unforgeable.

PUBLIC KEY DIRECTORY (PKD) The central database serving as the repository of Document Signer Certificates, CSCA Master Lists, Country Signing CA Link Certificates and Certificate Revocation Lists issued by Participants, together with a system for their distribution worldwide, maintained by ICAO on behalf of Participants in order to facilitate the validation of data in eMRTDs.

PUBLIC KEY INFRASTRUCTURE (PKI) A set of policies, processes and technologies used to verify, enrol and certify users of a security application. A PKI uses public key cryptography and key certification practices to secure communications.

REGISTRATION The process of making a person's identity known to a biometric system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.

SENSITIVE DATA Finger and iris image data stored in the LDS Data Groups 3 and 4, respectively. These data are considered to be more privacy sensitive than data stored in the other Data Groups.

SYSTEM A specific IT installation, with a particular purpose and operational environment.

VALIDATION The process of demonstrating that the system under consideration meets in all respects the specification of that system.

1 About this Guide – Scope and Application

The ICAO TRIP Guide on Border Control Management (BCM) is a product of the ICAO Traveller Identification Programme (TRIP) Strategy and a contribution to the global effort for enhancing security of borders.

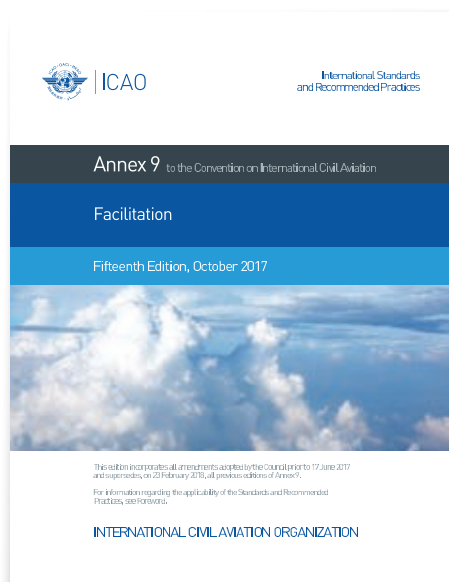
The regulatory framework of the ICAO TRIP Guide on BCM is found more prominently in:

- The Standards and Recommended Practices (SARPs) of Annex 9 – *Facilitation*,¹ specifically in:
 - Chapter 3. Entry and Departure of Persons and their Baggage;
 - Chapter 8. Other Facilitation Provisions; and
 - Chapter 9. Passenger Data Exchange Systems.
- The technical specifications of ICAO Doc 9303, *Machine Readable Travel Documents*.²

The Guide is principally concerned with BCM in the international air travel environment and focuses on the border controls applied to travellers. The TRIP Strategy, ICAO SARPs and technical specifications relating to traveller identification and risk assessment can also apply to all modes of transport, at all international borders.

The Guide is intended for reference by States to optimize the use of the tools, systems and processes available to enhance their national BCM. The Guide will help senior, middle and operational level management within national agencies responsible for immigration and border controls, as well as those other national agencies that rely on traveller identification data. This can include helping to inform strategy and policy development, budgetary planning, legislative reform initiatives, ICT systems change, operational planning, the identification of training needs, and the application of best practices.

The different starting positions of States and the very different border environments they face mean that it is not possible or desirable to specify to States a single path for improving their BCM. The guide can assist States in establishing a baseline for comparison and options for change.



1 *Annex 9 – Facilitation to the Convention on International Civil Aviation*, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

2 *Doc 9303, Machine Readable Travel Documents*, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

The Guide is composed of eight Sections:

1. About this Guide – Scope and Application introduces the Guide.

2. ICAO TRIP and Border Control Management provides a summary of how the TRIP Programme and the relevant ICAO SARPs and technical specifications contribute to BCM and to the underlying traveller identification and risk assessment.

3. National Strategies for Border Control Management describes how the border control environment unique to each State defines its security and facilitation challenges, and should thus inform its national BCM strategies.

4. National Border Inspections Systems and Tools comprises seven technical topics describing how States can capture, verify, match and record the data contained in MRTDs and about travellers:

- A. Visas and Electronic Travel Systems
- B. Document Readers
- C. Biographic Identity Verification
- D. Biometric Identity Verification
- E. National Watchlists
- F. Entry and Departure Databases
- G. Automated Border Controls

5. Interoperable Applications comprises six technical topics describing how States can access and share data about travellers and their travel documents:

- H. Advance Passenger Information and Interactive Advance Passenger Information
- I. Passenger Name Record
- J. Public Key Infrastructure and the ICAO Public Key Directory
- K. eMRTD Biometric Identity Verification
- L. INTERPOL's Stolen and Lost Travel Documents Database
- M. International Watchlists

6. Traveller Examination and Travel Document Inspection provides an overview of the responsibilities and roles of border agency personnel in the examination of the traveller and the inspection of travel documents.

7. Operational and Human Considerations in Border Control Management addresses some of the ways in which the facilitation and security of BCM depends not just on the use of technology, but also on the human application of technology, including overarching frameworks for governance and accountability.

8. Assistance to States outlines how the assistance available to States from ICAO and partner organizations can enhance their BCM.

The substantive content of the Guide is comprised of the 13 technical topics included under Sections 4 and 5. Each of the 13 technical topics is presented following a uniform structure:

UNIFORM STRUCTURE OF EACH OF THE 13 TECHNICAL TOPICS

TRAVELLER IDENTIFICATION & RISK

ASSESSMENT – Role and relative contribution of Inspection Systems and Tools and Interoperable Applications to identification of travellers and/or traveller risk assessment

KEY MESSAGES – A synopsis of the main points under that topic

OVERVIEW – A summary description of the topic

HOW IT WORKS – BORDER AGENCIES

Describes the role(s) and implication(s) for relevant border agencies

HOW IT WORKS – AIRLINES – Describes the role(s) and implication(s) for airlines

BENEFITS AND OPPORTUNITIES – Outlines the advantages that States can expect from effective implementation in relation to the topic

TECHNICAL ISSUES – Addresses some common challenges faced in implementation in relation to the topic

RELATED REQUIREMENTS – Lists additional factors or considerations that are critical to successful implementation in relation to the topic

RISKS AND COST MITIGATION – Provides some advice on managing or avoiding common challenges for implementation

BEST PRACTICE EXAMPLES – Identifies procedures, systems and techniques used by States that are recognized as, and have proven to be, effective and/or efficient

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES AND ICAO STATE LETTERS

– Includes extracts of relevant ICAO SARPs and State Letters

SOURCES FOR FURTHER INFORMATION

– References for literature specifically mentioned in the topic, and other information sources for readers who wish to investigate deeper into the subject matter

To further assist States in understanding and meeting their international obligations under the regulatory framework set by the Chicago Convention, extracts from the main SARPs of Annex 9 – *Facilitation* relevant to BCM are included in the Guide:

Difference between ICAO Standards and Recommended Practices:

STANDARD: Uniform application is recognized as necessary for the safety or regularity of international air navigation. States are obliged to report if they cannot implement a standard through a notification of differences.

RECOMMENDED PRACTICE: Uniform application is recognised as desirable in the interests of safety, regularity or efficiency of international air navigation. States should endeavour to conform.

Where relevant, the Guide also references ICAO State Letters:

An ICAO State Letter is the medium through which ICAO, under the authority of the Secretary General, officially communicates inter alia SARPs and policies with and obtains air transport data and information from its Member States.

In addition, State letters are used by the Regional Directors of the ICAO Regional Offices to officially communicate with the Member States in their area of accreditation.

The State Letter is available on the ICAO Secure Portal: <http://portallogin.icao.int/>
For more information, please refer to your national civil aviation authority.

The Assessment Tool, the companion document of the Guide, can be used by States to self-assess their BCM systems, processes and capabilities. The tool also provides a structured framework for technical experts to perform technical assistance missions to States. For ease of reference, the Assessment Tool follows an identical structure to that of the Guide.

Both the Guide and the Assessment tool are available for download at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>.

ICAO TRIP and Border Control Management

2.1 ICAO Traveller Identification Programme

ICAO is the United Nations Specialized Agency that has the mandate and responsibility for establishing, maintaining and promoting Standards and Recommended Practices (SARPs) related to the issuance and verification of machine-readable travel documents and related border control processes. Under the Traveller Identification Programme (TRIP) Strategy endorsed by the ICAO Assembly, ICAO is focused on ensuring a holistic and coordinated approach to traveller identification – from document issuance to Border Control Systems (BCS).

The ICAO TRIP Strategy³ is a framework for uniquely identifying travellers for enhancing border security and facilitation by bringing together the elements of identification management.

Effective traveller identification helps to optimize the economic, social and political benefits of international travel and to achieve the United Nations Sustainable Development Goals⁴. It also helps to manage security risks and to respond to threats at borders by enabling better targeting of resources towards persons of interest.

The 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.



National identification arrangements produce **Evidence of Identity** to support the issuance of **Machine Readable Travel Documents (MRTDs)**. Technical specifications contained in ICAO's Doc 9303, *Machine Readable Travel Documents*, along with the security of **Document Issuance and Control**, enhance the integrity of the travel document. Travel documents are therefore only as secure and reliable as the systems and protocols for their production and issuance, and the national identification arrangements behind them.

Inspection Systems and Tools enable border authorities to capture, verify and record data contained in the MRTDs and about travellers. Controls on the holders of travel documents can be performed at the **different phases of the journey: pre-departure, pre-arrival, arrival, stay and departure**. Those controls are enhanced by the global sharing of data about travellers and their travel documents achieved by **Interoperable Applications**.

The collection of traveller information completes the TRIP cycle by contributing additional evidence of identity concerning foreigners entering States.

Together, the elements of the ICAO TRIP Programme enable States to identify travellers and perform targeted traveller risk assessment.

2.2 Integrating Inspection Systems and Tools with Interoperable Applications

BCM consists of the regulatory framework, procedures, practices and technologies that are applied by national border control and law enforcement agencies and other stakeholders for managing the admission, stay, transit and departure of travellers. These measures are designed to complete traveller identification and risk assessment throughout the journey, consistent with international standards, recommended practices and obligations, to achieve the security and facilitation objectives of States.

The decisions and interventions made by States in BCM are sovereign in nature, and undertaken to regulate the flow of travellers in accordance with their national interest.

3 Proposal for an ICAO Traveller Identification Programme (A38-WP/11, Assembly – 38th session, 2013, available at: https://www.icao.int/Meetings/a38/Documents/WP/wp011_en.pdf)

4 *Sustainable Development Goals, United Nations*, United Nations, available at: <https://sustainabledevelopment.un.org/>

The flow of travellers overwhelmingly benefits States, and as such, BCM arrangements should facilitate timely and cost-efficient processing of genuine travellers while simultaneously identifying, managing and mitigating risks, and responding to threats.

Two of the five elements of the TRIP Strategy directly relate to BCM: **Inspection Systems and Tools** and **Interoperable Applications**.

Inspection Systems and Tools capture, verify, match and record the data contained in MRTDs and about travellers. Section 4 of this Guide discusses seven of them:

- A. Visas and Electronic Travel Systems
- B. Document Readers
- C. Biographic Identity Verification
- D. Biometric Identity Verification
- E. National Watchlists
- F. Entry and Departure Databases
- G. Automated Border Controls

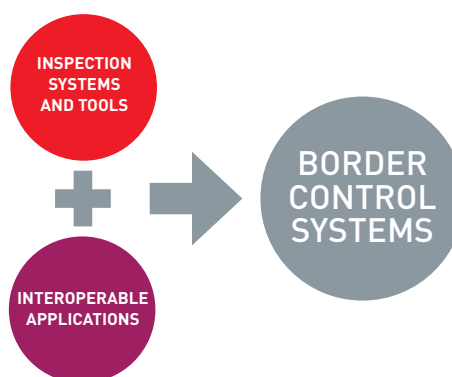
Interoperable Applications enable global sharing of data about travellers and their travel documents. Section 5 of this Guide discusses of them:

- H. Advance Passenger Information and Interactive Advance Passenger Information
- I. Passenger Name Record
- J. Public Key Infrastructure and the ICAO Public Key Directory
- K. eMRTD Biometric Identity Verification
- L. INTERPOL Stolen and Lost Travel Documents Database
- M. International Watchlists

BORDER CONTROL SYSTEMS

The BCS used by States integrate Interoperable Applications with Inspection Systems and Tools. Not all States employ all the available Inspection Systems and Tools and Interoperable Applications. Instead, they integrate them in different ways in their BCM. National BCM use different ICT architectures. When new features are added to legacy systems the architecture grows organically. When old architectures are replaced, the State may adopt a modular or service oriented architecture (e.g. with watchlist searches in one module, recording of entry and departure in another module).

The architecture used is less important than the results that are achieved.



States combine the Inspection Systems and Tools and Interoperable Applications in their BCS

All BCS, whatever their architecture, depend on the global interoperability of MRTDs. The analysis of data obtained from MRTDs when added to additional traveller identification and risk assessment data obtained from Interoperable Applications can be aggregated, disaggregated and analysed to produce statistics and actionable intelligence to facilitate and secure travel. The automated capture, verification and recording, along with those elements of analysis that are automated, is undertaken in the integrated BCS of States.

The integration of Inspection Systems and Tools with Interoperable Applications in national BCS allow traveller risk assessment to be undertaken throughout the traveller 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.

GLOBAL INTEROPERABILITY OF MRTDS: THE FOUNDATION OF BCM

The foundation of BCM is efficiently reading and effectively using the standardized, interoperable, machine readable data elements included in ICAO compliant MRTDs and eMRTDs.

The technical specifications for travel documents are published in Doc 9303, *Machine Readable Travel Documents*⁵. States should ensure the full application of these technical specifications to ensure that interoperability is achieved, and that the associated security and facilitation benefits are realised.

As traffic volumes grow and more States focus on how they can rationalize their border clearance processes with the employment of computerized databases and electronic data sharing, the MRTD plays a pivotal part in modern, enhanced BCSs.

Introducing document readers⁶ may require a substantial investment. But States can expect a return on their investment thanks to improvements in security, clearance speed and accuracy of verification that such systems provide. Document readers may also make it possible for States to eliminate both the requirement for paper documents, such

as passenger manifests and embarkation/disembarkation cards, and the administrative costs associated with the related manual procedures.

Data from the Machine Readable Zone (MRZ) enables the retrieval of identifying information about travellers from Advance Passenger Information (API)⁷ and Electronic Travel Systems (ETS)⁸. Data from the Integrated Circuit (IC) chip enables eMRTD Public Key Infrastructure (PKI) authentication⁹ and retrieval of biometric images in Automated Border Control (ABC)¹⁰ as well as in the processing of travellers undertaken by border control officers.

The data in ICAO compliant MRTDs and eMRTDs is designed to be read by machine readers configured to conform with Doc 9303 and to interface with the BCS of States. In practice, full standardisation is not always achieved. This has implications for the performance of the BCS of States.

Some factors influencing the efficient processing of travellers at border control points, include:

1. The proportion of travellers holding MRTDs and eMRTDs that meet interoperability standards for efficiently extracting data elements from them.
2. The availability and use of document readers capable of extracting data from the MRZ of MRTDs and eMRTDs, and from the IC chip of eMRTDs.
3. The integration of document readers with BCS that display reliable and consistent traveller details to border control officers.



5 The technical specifications for MRTDs and eMRTDs are published in the twelve Parts of *Doc 9303, Machine Readable Travel Documents*, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

6 See: *Topic B – Document Readers*

7 See: *Topic H – Advance Passenger Information and Interactive Advance Passenger Information*

8 See: *Topic A – Visas and Electronic Travel Systems*

9 See: *Topic J – Public Key Infrastructure and the ICAO Public Key Directory*

10 See: *Topic G – Automated Border Controls*

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Extracts from Annex 9 – *Facilitation*, Chapter 3. Entry and Departure of Persons and their Baggage¹¹:

D. Travel documents

3.11 All passports issued by Contracting States shall be machine readable in accordance with the specifications of Doc 9303, Part 4.

Note.—This provision does not intend to preclude the issuance of non-machine readable passports or temporary travel documents of limited validity in cases of emergency.

3.11.1 For passports issued after 24 November 2005 and which are not machine readable, Contracting States shall ensure the expiration date falls before 24 November 2015.

3.12 Contracting States shall ensure that travel documents for refugees and stateless persons (“Convention Travel Documents”) are machine readable, in accordance with the specifications of Doc 9303.

Note.—“Convention Travel Documents” are provided for in the 1951 Convention Relating to the Status of Refugees and the 1954 Convention Relating to the Status of Stateless Persons (cf. respective Article 28 of both Conventions).

3.13 **Recommended Practice.—** *When issuing identity documents or visas accepted for travel purposes, Contracting States should issue these in machine readable form, as specified in Doc 9303. ...”*



Identification of travellers informs, and is informed by, traveller risk assessment

2.3 Identification of Travellers and Risk Assessment

Identification of travellers is the essential foundation for traveller risk assessment.

States are transitioning from the traditional reliance on completing a single step traveller identification and risk assessment at entry controls, towards continuous identification of travellers and risk assessment repeated at each phase of the journey as new information becomes available.

This additional information collected at each phase of the journey is transmitted to the receiving/destination State’s border control agencies, who transform it into actionable intelligence for traveller risk assessment. Where this assessment calls into question the identity of a traveller, it is reassessed in an iterative process repeated until all questions of identity and risk are resolved.

11 *Annex 9 – Facilitation to the Convention on International Civil Aviation*, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

Watchlist searches and risk based targeting require the input of identity data. The risk analysis to develop actionable intelligence requires combining:

- Identity data;
- Travel data;
- Data from other agencies, including, for example, those responsible for security, customs, law enforcement, quarantine, public health; and
- Data from the public domain.

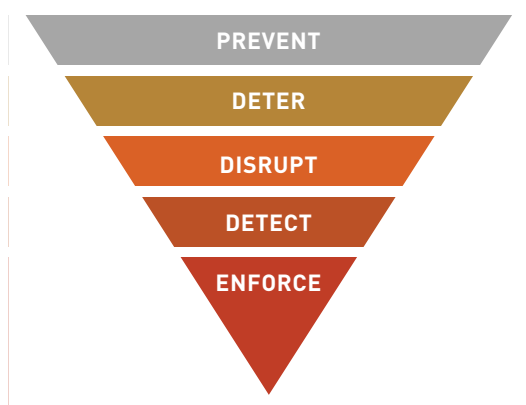
The scope of the risk assessment includes addressing all threats of concern to the State – including, among others, criminality, security, biosecurity and public health.

Each agency working at the border has particular responsibilities regarding the risk posed by a traveller – e.g. immigration for identification of travellers, customs agencies for goods, intelligence agencies for national security and police for law enforcement. It is important that agencies work together so that risk assessment information that brings into question the identity of travellers is shared with the agency primarily responsible for traveller identification.

The Inspection Systems and Tools and Interoperable Applications described in the Guide contribute, to different degrees, in the identification of travellers **and/or** to traveller risk assessment.

BORDER CONTROL MANAGEMENT INTERVENTIONS

As the assurance of traveller identification becomes more certain with each phase of travel, States can plan and implement risk based, intelligence led interventions. BCM interventions follow a hierarchy. BCM is most effective when it prevents the travel of those who represent a risk to States.



BCM Intervention Hierarchy

The basis of BCM interventions made by States — whether designed to prevent, deter or disrupt the travel of criminal and terrorists or to detect, detain and prosecute them — is the identification of travellers and the assessment of the risk they represent.

In best practice jurisdictions, more BCM resources are devoted to interventions that deter or disrupt, for example, improperly documented and other travellers determined by a State to be inadmissible from commencing or continuing travel.

Interventions applied in earlier phases of the journey are more readily achieved. It is easier to refuse a visa than to refuse at airline check-in; it is easier to deny boarding at embarkation than to remove a traveller from an aircraft at a transit point; and it is easier to refuse at entry than it is to locate a traveller after they enter a State.

BCM interventions — whether for prevention, deterrence, disruption, detection or enforcement — must be applied continuously throughout a traveller's journey. Not every person presenting a risk or threat will be prevented or deterred pre-departure, and some will enter States without being detected.

SEQUENCING INSPECTION SYSTEMS AND TOOLS AND INTEROPERABLE APPLICATIONS THROUGHOUT THE TRAVELLER JOURNEY

When a State manages traveller identification and risk assessment continuously across the traveller journey, the analysis of all relevant information can inform decisions about whether travel should be allowed to commence or continue to the next phase.

Pre-Departure Phase

The receiving/destination State may have information about the anticipated or expected travel of its own citizens (in the form of their national travel document databases) and of foreigners (in the form of their Visa and ETS databases). Once flight bookings are made, new information about travellers becomes available from airline reservation systems (in the form of Passenger Name Record (PNR)).

Pre-Arrival Phase

Additional information becomes available to the receiving/destination State from the departure control systems of airlines (in the form of API or interactive API (iAPI)). When transfer passengers join flights at transit points, the iAPI and API data available to States is updated. Liaison Officers (LOs) can operate at boarding gates assisting airlines to ensure that only properly documented travellers board flights.

Entry Phase

When travellers arrive at their final destination, States make decisions about whether to admit the traveller using all of the information collected in earlier phases and at entry. Entry databases record travel, providing a basis for States to determine who is present in their territory.

Stay Phase

Foreigners seeking to change the purpose or extend the duration of their authorised stay require permission. Details about changes to visa conditions made after entry and residence permits that are issued update databases of expected departures— data that is made available in BCS for exit controls.

Exit Phase

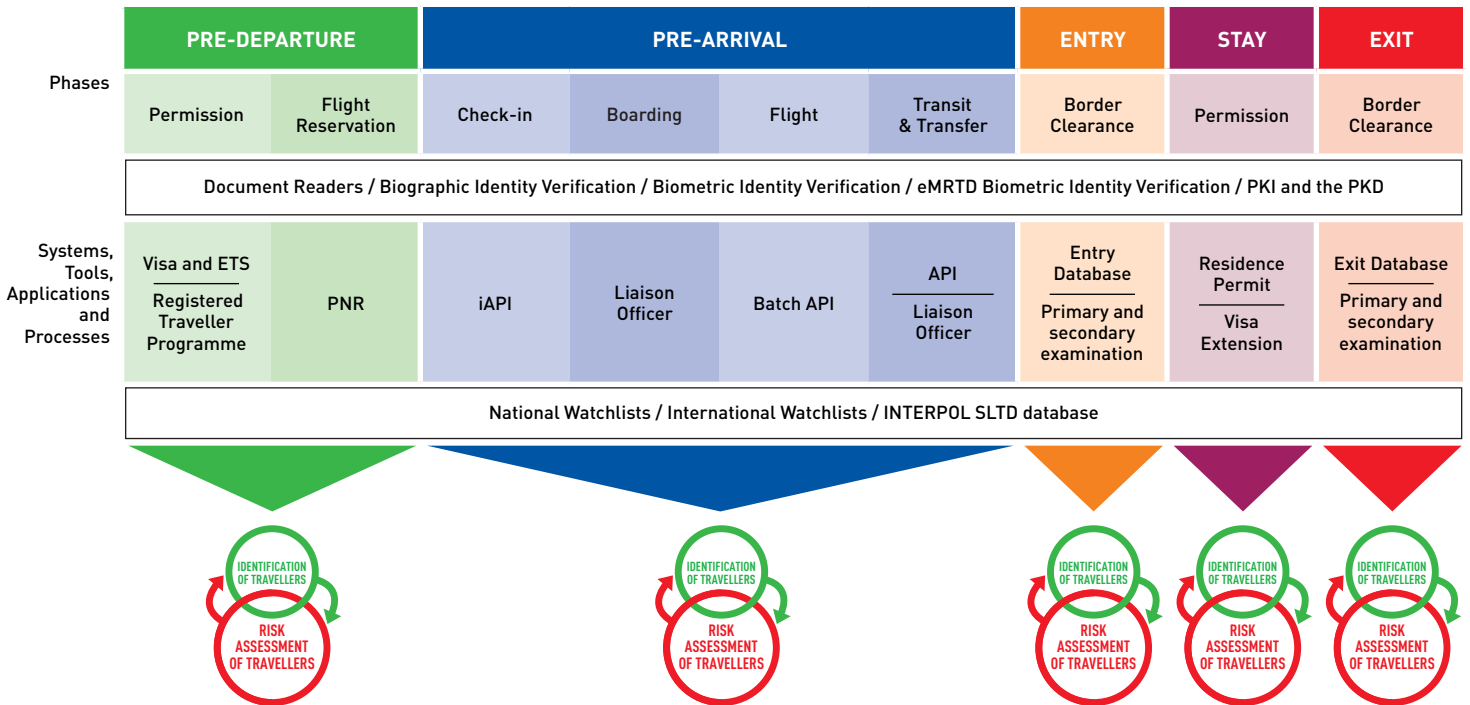
The departure of nationals and foreigners is recorded in an exit database, providing a basis of reconciliation of who is present in the State.

At all phases of the traveller 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 contribute to assuring traveller identification.

After traveller identity is established to a sufficient level of confidence, a State can check the INTERPOL SLTD database and national and international watchlists to inform a traveller risk assessment.

From the perspective of different States, the same traveller can at the same time be at different phases of the journey, e.g. a traveller at the exit phase for the State from which they are departing is at the pre-arrival phase for the State of destination. From the global perspective travel is a continuum, an interdependent system that requires enhanced cooperation between States, International and Regional Organizations and the private sector.



Traveller identification and risk assessment is repeated throughout the traveller journey as additional information becomes available to the receiving/destination State

National Strategies for Border Control Management

Historically, air transport has doubled in size every 15 years. In 2016, airlines worldwide carried around 3.8 billion travellers, and traffic is expected to reach over seven billion by 2030, according to ICAO forecasts.

This increase in the volume of air travel bring States different benefits, and different risks and threats. With more travellers from a larger number of States are travelling to States previously less visited, the challenge of identifying travellers to inform risk assessment and mitigate risks and threats has grown.

Effective national strategies for BCM are a response to the unique border control environment faced by the State and include:

- Appropriate application of technology;
- Strong policy, legal, system and organizational strategic frameworks;
- Consideration of environment and travel patterns;
- Effective engagement with stakeholders and between partner agencies;
- Complementary regional border arrangements; and
- Meeting State obligations under international law.

This Guide is concerned with the component of national BCM strategies that deals specifically with travellers. The BCM strategies adopted by States should enhance border security while facilitating the movement of legitimate travellers.

3.1 Application of Technology

Effective BCM is fundamental to national sovereignty. The national interest is served by regulating every phase of the traveller journey. The ICAO TRIP strategy recognizes that improved border control arrangements can be achieved, in part, by the application of technology. Inspection Systems and Tools and Interoperable Applications support the identification and risk assessment of travellers throughout the traveller journey.

The application of technology in BCM is expensive and carries a high risk of failure wherever objectives and solutions are not clearly aligned with the actual needs of States. Adding new tools and applications into national BCS is highly contingent on related requirements of legislation, other ICT systems and databases, and human capability and capacity. Some of these dependent interrelationships are noted in the *Related Requirements* sub-Sections in the 13 technical topics of Sections 4 and 5 of this Guide.



A strong business case must be developed prior to implementing technology solutions to ensure that benefits outweigh the cost of investment. The business case for investment will be a reliable basis for making investment decisions only if national BCM objectives are clearly identified.

3.2 Strategic Frameworks

The successful application of technology for BCM is dependent on a national strategic framework that includes:

- A **policy framework** that provides statements of strategy and objectives for translating the objectives of Governments into outcomes;
- A **legal framework** that provides the authority;
- A **systems framework** comprising business processes and an ICT framework; and
- **Organizational structures** and relationships within and between national agencies, and with external stakeholders.

For effective BCM, the national legal framework should:

- Provide clear authority (e.g. to allow travel to commence and continue, to approve entry into the State and to collect, retain, use, share and archive data about travellers);
- Incorporate contemporary concepts of identity and identity related fraud (e.g. in relation to biometric identifiers);
- Provide appropriate protection for the sensitive information collected from and about travellers – usually achieved in separate instruments in national legislation for the protection of data and privacy; and
- Be aligned with national economic and social development objectives, to ensure that the limited resources available to States are invested wisely.

The development and promotion of corporate planning documents that include mission and vision statements, and that relate activities and processes to measurable outputs and high-level outcomes, give purpose and focus to the work of national border control agencies. These plans should include descriptions of the intended response to business continuity and disaster recovery scenarios that anticipate disruption to normal operations caused by natural disasters, humanitarian crises or other foreseeable events. For critical ICT systems, business continuity and disaster recovery arrangements should, for example, ensure redundancy in the operation of national BCS, and contingencies for re-establishing processing when outages occur.

With a shared vision and common purpose, border control agencies can better identify their challenges and assess competing investment and development priorities. These insights enable decisions for adopting technology solutions that are an appropriate response to each national BCM environment.

3.3 Environment and Travel Patterns

Insight into a State's geopolitical, historical, social and economic circumstances is the key to understanding the influences on its current and future threats and opportunities to be taken into consideration into the national framework for BCM.

Landscape, topography, climate and proximity to neighbours shape the communication and transport access to neighbouring States and regions. Air travel to and through a State is influenced by the infrastructure of other modes of transport (ship, train and road) and their patterns of travel from and through the State. Some States, because of their geographic location and investment in infrastructure, are hubs for international civil aviation.

The movement of travellers has shaped and been shaped by conflicts, political instability, colonialism, human rights abuses, economic factors, and ethnic, religious and linguistic homogeneity or diversity. States can variously be a source and/or destination and/or point of transit for asylum seekers, victims of human rights abuses, the objects and perpetrators of people smuggling and the victims and perpetrators of human trafficking.

TRAVEL PATTERNS RELEVANT TO BORDER CONTROL MANAGEMENT

Overwhelmingly, travel is undertaken by properly documented travellers to, via and from official border control points. However, travel is also undertaken by imposters, improperly documented and other inadmissible persons – including FTFs and trans-national criminals.

The journeys undertaken by these criminals can be carefully contrived to evade effective traveller identification and risk assessment by using different transport modalities, and by targeting locations where BCM is weak. This evasion of border controls is sometimes referred to as broken travel.

Properly documented travellers undertake short term stays for international tourism and business travel; longer term stays for employment and education; and more permanent migration for economic and social purposes, including

refugee resettlement. A minority of properly documented travellers may have criminal or terrorist intentions, or otherwise be identified by States as inadmissible persons.

The various arrangements to facilitate properly documented travellers present opportunities for exploitation by criminals or terrorists.

National strategies and policies for traveller identification in BCM should seek to influence the future composition and scale of properly documented travellers for the benefit of the State, including in meeting their international obligations.

Improperly documented travellers subvert traveller identification in BCM by disguising their true identity and/or evading examination at border control points. Imposters and improperly documented travellers include vulnerable people seeking asylum and/or an improvement in their economic circumstances, and criminals exploit this vulnerability.

States can variously be a source, a destination and/or a point of transit for asylum seekers, victims of human rights abuses, and victims and perpetrators of people smuggling and human trafficking.

An understanding of the scale, composition and underlying causes of past and current improperly documented travel, and the incidence of imposters, is critical for States to assess the risk and threat of improperly documented travel and to apply the appropriate BCM intervention. Furthermore, the successful prevention, deterrence or disruption of improperly documented and other travellers determined by a State to

be inadmissible typically results in a displacement effect. These prospective travellers may attempt travel to other States. The BCM strategy of a State must anticipate and respond to these and other impacts of the BCM responses of other States.

3.4 National Stakeholders

The ICAO TRIP Strategy recognizes that traveller identification management requires cooperation within and between government agencies, and with international organizations and private stakeholders.

The complexity of BCM is reflected in the range of public and private stakeholders involved:

- Border control agencies responsible for customs, immigration and quarantine clearance;
- Agencies responsible for civil registration, and national identity card and travel document issuance;
- Agencies responsible for public health;
- Law enforcement and security agencies; and
- Airlines and airport operators.

Border controls are stronger when all BCM agencies consider the broader aspects of their interaction with travellers, not just those confined to their own jurisdiction. This 'all risks, all threats' approach to BCM is a feature of national arrangements in best practice jurisdictions.





Mutual understanding of roles and processes builds respect and trust as the foundation for effective communication, co-ordination and collaboration.

All BCM agencies and stakeholders rely on the ability of the agency responsible for immigration clearance at national borders to manage their own interventions. Through inter-agency cooperation, other national BCM agencies can obtain identification data of travellers from the agency responsible for immigration, as a foundation for their own investigation and intelligence analysis.

On the other hand, the agency responsible for immigration makes identity verification decisions based on information obtained from other national agencies and stakeholders:

- For its own **nationals**, based on the national travel document, authenticated against information recorded in the national passport and entry and exit databases; and
- For **foreigners**, based on the foreign travel document, authenticated against information obtained from airlines and information recorded in the national visa, residence permit and entry and exit databases.

The agencies responsible for civil registration, national identity card issuance and other large national identity databases

(e.g. driver's licenses) are typically not represented at the border. However, access to their data through modules or interfaces integral to the BCS enables the agency responsible for immigration to access richer data to achieve greater assurance in the identification of travellers.

The agency responsible for immigration requires insight into the business processes for visa and passport issuance that provide the starting point for traveller identification. Weaknesses in identity enrolment at visa and passport issuance can compromise effective BCM.

Commercial imperatives of airport operators and airlines need to be reconciled with the regulatory responsibilities of government agencies. Efficient processing of travellers, and a good passenger experience, need to be reconciled with efficient security screening.

BCM in international civil aviation operates in a challenging, time critical, high transaction volume, processing environment. ICAO Annex 9 – *Facilitation* includes time based Recommended Practices for the completion of entry and departure clearance formalities.

Extracts from Annex 9 – *Facilitation*, Chapter 3. Entry and Departure of Persons and their Baggage¹²:**J. Departure procedures**

“ ...

3.37 **Recommended Practice.**— *Contracting States, in cooperation with aircraft operators and airport management, should establish as a goal a total time period of 60 minutes in aggregate for the completion of required departure formalities for all passengers requiring not more than normal processing, calculated from the time of the passenger’s presenting himself at the first processing point at the airport (i.e. airline checkin, security control point or other required control point depending on arrangements at the individual airport).*

Note.— “Required departure formalities” to be completed during the recommended 60 minutes would include airline checkin, aviation security measures and, where applicable, the collection of airport charges and other levies, and outbound border control measures, e.g. passport, quarantine or customs controls. ...”

K. Entry procedures and responsibilities

3.40 **Recommended Practice.**— *Contracting States, with the cooperation of aircraft operators and airport operators, should establish as a goal the clearance within 45 minutes of disembarkation from the aircraft of all passengers requiring not more than the normal inspection, regardless of aircraft size and scheduled arrival time. ...”*

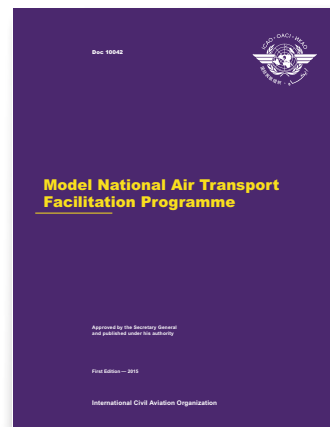
The Border Security Initiative of the United Nations Counter-Terrorism Centre (UNCCCT) and the Global Counterterrorism Forum highlights intra-agency, inter-agency and international cooperation among the 14 best practices to strengthen cross-border cooperation and border surveillance in a counterterrorism context¹³.

ICAO provides guidance to States on NATFP in the Annex 9 – *Facilitation* for which relevant SARPs are listed below and in the ICAO Doc 10042 Model National Air Transport Facilitation Programme¹⁴.

The work of the NATFP and the National Civil Aviation Security Programme are complementary. ICAO recommends that border control agencies participate in both national Facilitation and Aviation Security committees.

NATIONAL AIR TRANSPORT FACILITATION PROGRAMME

One important mechanism for achieving national inter-agency collaboration in BCM is the creation and effective operation of a National Air Transport Facilitation Programme (NATFP). The coordination of facilitation activities should take place under a National Air Transport Facilitation Committee and Airport Facilitation Committees, or similar coordinating bodies. The purpose of a NATFP is to facilitate the border-crossing formalities. The meetings of its committees are a forum for consultation and information sharing.



12 *Annex 9 – Facilitation to the Convention on International Civil Aviation*, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

13 Global Counterterrorism Forum, New York, 2016, available at: <https://www.thegctf.org/Cross-Cutting-Initiatives/Border-Security-Initiative>

14 *Model National Air Transport Facilitation Programme – First Edition*, Doc 10042, ICAO, Montreal, 2015, available to purchase at: <https://store1.icao.int/index.php/model-national-air-transport-facilitation-programme-doc-10042-english-printed-12870.html>

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES AND STATE LETTER

Extracts from Annex 9 – Facilitation, Chapter 8. Other Facilitation Provisions¹⁵:

G. Establishment of national facilitation programmes

8.17 Each Contracting State shall establish a national air transport facilitation programme based on the facilitation requirements of the Convention and of Annex 9 thereto.

8.18 Each Contracting State shall ensure that the objective of its national air transport facilitation programme shall be to adopt all practicable measures to facilitate the movement of aircraft, crews, passengers, cargo, mail and stores, by removing unnecessary obstacles and delays.

8.18.1 **Recommended Practice.**— *In establishing a national air transport facilitation programme, States should use the guidance material outlined in Appendix 12.*

8.19 Each Contracting State shall establish a National Air Transport Facilitation Committee, and Airport Facilitation Committees as required, or similar coordinating bodies, for the purpose of coordinating facilitation activities between departments, agencies, and other organizations of the State concerned with, or responsible for, various aspects of international civil aviation as well as with airport and aircraft operators.

8.20 **Recommended Practice.**— *Contracting States should endeavour to establish close coordination, adapted to circumstances, between civil aviation security and facilitation programmes. To this end, certain members of Facilitation Committees should also be members of Security Committees.*

8.21 **Recommended Practice.**— *In establishing and operating National Air Transport and Airport Facilitation Committees, States should use the guidance material outlined in Appendices 11 and 12.*

The ICAO State Letter “Nomination of a National Focal Point for Facilitation”, Ref.: EC 6/1 – 16/106, 14 December 2016, reminds States of the requirement for establishing a NATFP and requests States to nominate a focal point.

“The priorities for the next triennium (2017-2019) of the ICAO Traveller Identification Programme (TRIP) Strategy, as endorsed by the 39th Session of the Assembly, is one example where the establishment of an NATFP would facilitate coordination among Member States and ICAO. ...

Your Government is therefore requested to nominate, from within the State’s Civil Aviation Authority or the Ministry of Transport, a National Focal Point and an Alternate Focal Point, who would have access to the platform for secure communications with ICAO.”

The State Letter is available on the ICAO Secure Portal: <http://portallogin.icao.int/>
For more information, please refer to your national civil aviation authority.

¹⁵ *Standards and Recommended Practices, Annex 9 to the Convention on International Civil Aviation – Annex 9 – Facilitation*, Fourteenth Edition, ICAO, Montreal, October 2015, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

3.5 Regional Arrangements

States around the world come together under regional and bilateral agreements and treaties to strengthen economic, social and political relationships with their neighbours. Securing and facilitating intra-regional travel contributes to maximising these benefits.

Regional travel agreements shape and are shaped by regional travel patterns. Understanding regional factors is

therefore critical to developing effective national strategies and policies for the identification of travellers.

Many of these agreements include provisions that allow preferential access for travellers who are citizens or residents of the region. ICAO's SARPs and Doc 9303 support these arrangements by providing the flexibility for MRTDs to be issued in card as well as booklet formats. This enables national identity cards and driver licences to be used for travel between States and within regions – with benefits for quick, accurate border processing and consequently for security and facilitation.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Extracts from Annex 9 – *Facilitation*, Chapter 3. Entry and Departure of Persons and their Baggage¹⁶:

D. Travel documents

“ ...

3.13 **Recommended Practice.**— When issuing identity documents or visas accepted for travel purposes, Contracting States should issue these in machine readable form, as specified in Doc 9303. ...”

Regional travel concessions will typically be described in a treaty, Memorandum of Understanding or alternative legal instrument. The treaty obligation will be reflected in national legislation and policy, and may include shared infrastructure, data sharing or other applications of technology to mitigate risk – including the integration of Inspection Systems and Tools and Interoperable Applications that are the subject of this Guide.

Regional arrangements for BCM are typically built slowly over time, with the solutions adopted being unique to the challenges faced. Their foundation is mutual trust, shared policy objectives and compatible legislation, including strong and mature privacy and data protection arrangements. Active border control agency engagement with regional organizations makes an important contribution to national BCM strategic frameworks.

Notwithstanding regional differences, States considering the adoption of new regional or bilateral travel arrangements could benefit in adapting and adopting the existing legal and

institutional frameworks and policies used successfully in other regions.

Such arrangements may support sharing risks and threats, with a focus on security in the case of the Organization for Security and Co-operation in Europe (OSCE) and a focus on trans-national crime for the Bali Process:

- The OSCE publishes material that informs the development of the national border control strategy and policy of participating States. The OSCE's Border Security and Management concept provides strategic policy guidance. The Border Security and Management National Focal Point Platform facilitates the exchange of border-related information and experiences. The Border Management Staff College serves as a centre of excellence and a vehicle for the delivery of expertise and best practices in BCM and security.¹⁷
- Since 2002 the Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime has operated to raise awareness in the

¹⁶ *Standards and Recommended Practices, Annex 9 to the Convention on International Civil Aviation – Annex 9 – Facilitation*, Fourteenth Edition, ICAO, Montreal, October 2015, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

¹⁷ *Border Management*, Organization for Security and Co-operation in Europe, available at: <http://www.osce.org/secretariat/borders>

Asia-Pacific region of the consequences of people smuggling, trafficking in persons and related transnational crime. The Bali Process publishes guidance material¹⁸ and provides technical assistance to its participating States. In a recent initiative, the Bali Process has adopted a policy framework for sharing anonymised biometric data between member States¹⁹. The framework is significant for its strong privacy and data protection features.

Other regional arrangements have been created within organizations, with a focus on trade and travel facilitation:

- Over an extended period, notably including a common ETS for the 2007 Cricket World Cup, the Caribbean Community (CARICOM) has been innovative in establishing arrangements to share border control infrastructure and traveller data. Current arrangements include the Implementation Agency for Crime and Security (IMPACS) Joint Regional Communications Centre (JRCC) that is the central clearinghouse for receiving API. It acts on behalf of individual CARICOM Member States, pre-screening passengers from air and sea carriers travelling in the region. The JRCC analyses and screens the API data it receives, identifies targets and forwards alerts to its Member States.²⁰
- The effective implementation of European integrated border management in the free movement Schengen Area is the responsibility of the European Border and Coast Guard Agency (Frontex) and national BCM authorities. Effective implementation thus relies upon a shared and common use of information, capabilities and systems at national level and the response of Frontex at the European level. While the Member States retain primary responsibility for the management of their external borders, Frontex supports the application of the EU's measures relating to the management of its external borders by reinforcing, assessing and coordinating their actions²¹. Publications covering a range of topics relevant to BCM policy development can be found on the Frontex website²².

3.6 International Law

Since BCM is concerned with travel across international borders, it operates within a framework of international law. An understanding of the interaction between the various components of international law and national circumstances is therefore critical in determining a State's priorities in BCM.

An important objective of the UN is "to establish conditions under which justice and respect for the obligations arising from treaties and other sources of international law can be maintained"²³.

Major UN treaties with direct relevance to BCM include:

- **1944 Convention on International Civil Aviation**, which led to the establishment of ICAO;
- **1951 United Nations Convention Relating to the Status of Refugees** (and the *1967 Protocol Relating to the Status of Refugees*), for which the United Nations High Commission for Refugees (UNHCR) has supervisory responsibilities;
- **1954 United Nations Convention relating to the Status of Stateless Persons**, administered by UNHCR, which together with the 1951 Convention, inter alia establishes the legal foundation for Machine Readable Convention Travel Documents (MRCTDs);
- **2000 United Nations Convention against Transnational Organized Crime**, its 2000 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children and its 2000 Protocol against the Smuggling of Migrants by Land, Sea and Air, administered by the United Nations Office on Drugs and Crime (UNODC); and
- **1948 Universal Declaration of Human Rights** and the core international human rights instruments whose implementation fall under the broad responsibility of the United Nations Office of the High Commissioner for Human Rights (OHCHR).

18 *Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime*, available at : <http://www.baliprocess.net/regional-support-office/resources/>

19 *Policy Framework for the Regional Biometric Data Exchange Solution*, Bali Process, available at: <http://www.baliprocess.net/UserFiles/baliprocess/File/Policy%20Framework%20for%20the%20RBDES%20part09.pdf>

20 *CARICOM Implementing Agency for Crime and Security (IMPACS)*, CARICOM, available at: <http://www.caricom.org/about-caricom/who-we-are/institutions1/caricom-implementing-agency-for-crime-and-security-impacs>

21 Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 (pages 1-76) available at: http://frontex.europa.eu/assets/Legal_basis/European_Border_and_Coast_Guard.pdf

22 *Publications*, European Union's Border and Coast Guard Agency, available at: <http://frontex.europa.eu/publications/>

23 *Preamble Charter of the United Nations*, United Nations, San Francisco, 1945, <http://www.un.org/en/charter-united-nations/index.html>



The Refugee Convention and Protocol, the Convention against Transnational Organized Crime and the Universal Declaration of Human Rights share a focus on the protection of the basic human rights of vulnerable travellers. The Refugee Convention and its Protocol ensures the right to seek asylum for persons who are fleeing armed conflict, violence or persecution. The Refugee Convention and Protocol explicitly prohibits the forceful return of asylum-seekers to their country of origin, or another country where their life and freedom are at risk (the principle of “*non refoulement*”). The OHCHR has published *Recommended Principles and Guidelines on Human Rights at International Borders*²⁴ to provide guidance to States to ensure protection of these rights.

While virtually all UN Member States are members of ICAO, not all UN Member States have signed, ratified or acceded to all major treaties. Moreover, since States can lodge declarations, reservations or objections with UN Conventions and Protocols, and notify differences with ICAO SARPs²⁵, determining the precise status of multilateral instruments for each State is complex. To further complicate matters, there are international norms (such as the principle of “*non refoulement*”) which have the status of customary international law, and are therefore mandatory for all States, whether they have signed the relevant convention or not. The variance in adoption by States can become vitally important in BCM when, for example, they impact on the legal foundation for data sharing.

24 *Recommended Principles and Guidelines on Human Rights at International Borders*, OHCHR, 2014, available at: http://www.ohchr.org/Documents/Issues/Migration/OHCHR_Recommended_Principles_Guidelines.pdf

25 Article 38 of the Chicago Convention requires States to notify ICAO if they: Do not comply with a Standard in all respects; Do not bring its regulations or practices into full accord with any Standard; Adopt regulations or practices differing in any particular respect from the Standard. Notification can be performed online or offline.

In addition to their treaty obligations, Member States are obliged under the UN Charter to implement decisions made by the UN Security Council (UNSC)²⁶. Some of these provisions are concerned with regulating travel and BCM. Important examples include²⁷:

- **UNSC Resolution (UNSCR) 1373 (2001)**: A wide-ranging counter-terrorism resolution adopted following the 11 September terrorist attacks on the United States.
- **UNSCR 1267 (1999), 1989 (2011) and 2253 (2015)**: Established, then extended, the scope of the Consolidated United Nations Security Council Sanctions List (CUNSCSL)²⁸. The application of sanctions lists in BCM is discussed in *Topic N – International Watchlists of this Guide*.
- **UNSCR 2178 (2014)**: Adopted in response to the threat stemming from foreign terrorist fighters (FTFs) and requires Member States and the international community to strengthen border security and prevent FTF travel. Measures to be taken by Member States pursuant to resolution 2178 (2014) include:
 - Preventing the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents;
 - Preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents;
 - Preventing the entry into or transit through their territories of any individual seeking entry or transit for the purpose of participating in acts of terrorism; and
 - Requiring that airlines operating in their territories provide API to the appropriate national authorities.
- **UNSCR 2178 (2014)** notes that the activities of FTFs, and those who support them, may make them eligible for inclusion on CUNSCSL and therefore references UNSCR 1267 (1999), 1989 (2011) and 2253 (2015).
- **UNSCR 2309 (2016)**: Calls upon States to ensure the security of civil aviation by, inter alia, implementing ICAO Annex 9 “...standards and recommended practices relevant to the detection and prevention of terrorist threats involving civil aviation.”
- **UNSCR 2322 (2016) and UNSCR 2396 (2017)**: Calls upon States, inter alia, to share, where appropriate, biographic and biometric information about FTFs and other terrorists and to incorporate this information into national watchlists.

26 Chapter VII, Charter of the United Nations, available at: <http://www.un.org/en/sections/un-charter/chapter-vii/>

27 All United Nations Security Council Resolutions are available at: <http://www.un.org/en/sc/documents/resolutions/>

28 Consolidated United Nations Security Council Sanctions List, United Nations Security Council, <https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list>

Inspection Systems and Tools

Inspection Systems and Tools capture, verify, match and record the data contained in MRTDs and about travellers. Obtaining information contained in the travel document is the initial step for the identification of travellers. States and airlines perform travel document inspection at each phase of the journey: when travellers present their MRTD for visa issuance, at airline check-in, at boarding gates, at transfer desks, at entry and exit controls. In best practice jurisdictions the identification of travellers is informed by other relevant data — some obtained from the traveller, and some obtained from other sources.

Document readers provide an efficient and accurate mechanism to extract data from travel documents, automatically

triggering watchlist searches, enabling biographic and biometric identity verification, and recording the entry (or departure) of the traveller to (from) the State. In the ultimate expression of this automation of primary processing, travellers interact with self-service eGates and kiosks without input from border control agency personnel, thus releasing resources for redeployment to achieve other security or facilitation tasks.

The seven Inspection Systems and Tools described in this Section are used at specific or multiple phases of the traveller journey (pre-departure, pre-arrival, entry, stay and exit) and each contribute, to different degrees, to the identification of travellers and/or to traveller risk assessment.



A. VISAS AND ELECTRONIC TRAVEL SYSTEMS



Before travel begins, these **Inspection Systems for Traveller Identification & Risk Assessment** collect and analyse extensive contextual information to supplement the biographic and biometric data available from MRTDs.

KEY MESSAGES

- ✓ ICT-based systems to apply for and be issued a visa offer a more timely, efficient and secure solution for issuing authorities and travellers.
- ✓ In lieu of the standard counterfoil paper visa, these systems automate the process for the lodgement, acceptance and verification of a passenger’s authorization to travel to a State.
- ✓ These systems bring an additional benefit when they interface with other systems and databases (e.g. API and iAPI, national and international watchlists, INTERPOL SLTD).

OVERVIEW

The adoption of what became the standardized booklet format for travel documents during the twentieth century was a response to the needs of States to record permission for, and the details of, travel. These permissions typically commenced with a ‘visa’, a conditional permission granted by transit and destination States for a traveller to commence, continue and complete their journey.

For most of the twentieth century, consular and diplomatic officials of States used ink stamps to endorse visas directly into travel documents. Because these applications had to be made by representatives of the State, obtaining a visa was inconvenient and expensive. Because ink stamps are clumsy to endorse, easy to forge and alter, issuing a visa was inefficient; this resulted in security vulnerabilities for States.

In the latter part of the twentieth century, many States addressed these inefficiencies by waiving their visa requirements to facilitate travel. States that retained visa requirements progressively introduced machine printable, machine readable visas linked to centralised databases that made traveller data available to border control agencies.

In the more challenging security environment of the twenty-first century, many States have re-introduced the requirement to obtain permission prior to travel commencing. Improving upon the standard counterfoil paper visa-based system, these new arrangements use modern ICT systems, such as the internet, to make it easier for travellers to obtain permission to travel, while at the same time being more efficient and secure for issuing States.

These new generation solutions typically include:

- Online, self-service application and payment interfaces;
- Online issuance of an electronic permission to travel; and
- Creation of a State database of eligible travellers.

Some applications of national visa and ETS systems include a query and response interface with airline systems (i.e. iAPI)²⁹.



29 See: Topic H – Advance Passenger Information and Interactive Advance Passenger Information

Where States require additional information about previously unknown or other travellers they consider being higher risk, an intermediate step may be used. For many States, a distributed network of visa application centres, mostly operated by contracted third parties, allow additional screening such as interviews and the enrolment of biometric features. The processing locations of these centres can be determined by traveller demand rather than the points of presence of a diplomatic network; this makes them more conveniently located for travellers.

To further differentiate traveller risk, some States, airport operators and airlines engage in partnerships to offer trusted traveller programmes. These programmes facilitate travel and improve security by obtaining more detailed information, including biometric enrolment, from prospective travellers.

Each of these arrangements enables States to access the information they need to assess traveller risk at the pre-departure phase, with the least inconvenience and cost to potential travellers.

ETS are the most facilitative of these new generation solutions and the focus of the remainder of the discussion in this Topic. An ETS is the automated process for the lodgement, acceptance and verification of a passenger's authorization to travel to a State, in lieu of the counterfoil paper visas used by many States.

The back-end system of an ETS processes incoming data and submits it to watchlists or a decision engine — a rule-based software component that decides whether to grant authority to travel based on programmed logic. More advanced systems incorporate predictive analytic and other tools to identify and refer applications for human examination. Many States offer prospective tourists the option to make an online application, and to receive in return an electronic confirmation of their permission to travel within seconds or minutes of applying.

The online application interface allows States to collect more information about travellers. This additional data supplements traveller information, creating a powerful tool for superior traveller risk assessments. Additionally, it can provide an alternative to paper-based data collection from passenger embarkation/disembarkation cards for statistical purposes.

HOW IT WORKS – BORDER CONTROL AGENCIES

The national BCS retrieves eligible traveller data from the ETS database when the traveller completes entry border clearance formalities. When used in conjunction with an API

system, the two systems can match eligible traveller data when batch API data is received, at the pre-arrival phase.

ETS data can also be used to electronically compile statistics for national agencies, such as finance and tourism, avoiding the resource-intensive compilation of statistics from paper-based passenger embarkation/disembarkation cards.

Best practice jurisdictions maintain 24-hour, seven day per week operational support to review ETS errors and refusals. This minimizes traveller inconvenience while maintaining effective screening.

HOW IT WORKS – AIRLINES

Some airlines and other third parties may offer an ETS application interface. This can allow airlines to obtain ETS permissions for travellers as an alternative to denying boarding. The major site for ETS issuance is typically provided by the State. Airlines are instructed to warn passengers that an ETS permission is a requirement and that they will not be allowed to board without evidence that the ETS permission has been granted.

Like an airline eTicket, evidence that an ETS has been granted and is still valid will be available in the airline's departure control systems. However, travellers may still choose to carry a printed notice as evidence of having completed ETS formalities. Where travellers present paper evidence of a travel permission, airlines must still rely on the advice from the system, or an alternative confirmation of permission to travel received from the State.

BENEFITS AND OPPORTUNITIES

ETS expedite the pre-vetting and acceptance of low risk passengers into a State, while providing a secure method for governments and airlines to verify their acceptance for travel. ETS provide States with an added layer of border security.

Ultimately cheaper than a full-scale visa regime, an ETS requires no personnel or property infrastructure to receive and process visa applications. Decisions can be made automatically according to a set of rules and watchlist lookups.

The introduction of an ETS creates the opportunity to integrate with iAPI, enabling information to be received at check-in so passengers may be denied boarding if necessary.

ETS can replace visa on arrival arrangements with facilitation benefits for travellers in reducing the need to queue to obtain visas.

Best practice jurisdictions manage a clear separation between border control agencies responsible for the identification of travellers and processing, and the collection of visa or permit revenue. ETS is one mechanism to reduce or eliminate revenue collection at airports. In most ETS applications, the fee is collected electronically at the time of application. This has the additional benefit for States of improving the efficiency and integrity of revenue collection from visa fees.

While an ETS can be a cost effective, efficient and traveller-friendly alternative to a traditional visa system, they are technically complex – particularly if there is simultaneous introduction of an iAPI solution. States fully benefit from this technology when they can transform the data received from ETS into actionable intelligence to identify targets for border interventions. Prior to deciding to implement an ETS, States are advised to seek vendor independent, solution neutral advice and support..

TECHNICAL ISSUES

In best practice jurisdictions, a robust 24-hour ETS features a scalable web service with high availability, effective business continuity arrangements, and an iAPI integration with airline systems. ETS issuance requires connection to State BCS to perform watchlist checks. Since most ETS applications are designed to work in a lightly-supervised mode with a referral for human action required to deal only with exceptions, an ETS should feature careful case management design for automated decision making.

RELATED REQUIREMENTS

- ✓ National legislation to require collection and use of ETS data.
- ✓ ICT integration of ETS with national BCS (and the departure control systems of airlines for iAPI).
- ✓ Reliable, continuous ETS availability to prospective travellers for issuance.
- ✓ Reliable, continuous ETS availability for retrieval by BCS (and for “OK to Board” responses to airlines’ departure control systems for iAPI).
- ✓ Reliable, continuous network connectivity.

RISKS AND COST MITIGATION

A robust and secure ICT infrastructure is required so costs may outweigh benefits.

The support service for ETS may require additional personnel. Travellers may be rejected because of false watchlist matches and other logical errors. This could harm a State’s reputation and attractiveness as a tourist destination.

States are advised to carry out a full cost-benefit analysis.

BEST PRACTICE EXAMPLES

States should endeavour to keep information requirements to a minimum and make best use of the data elements received in an ETS to inform business intelligence about travel.

ETS work most effectively in combination with iAPI and the deployment of LOs at major departure airports to assist airline check-in personnel. The ETS systems used by Canada, the USA and Australia have these integration and support features.

In situations where a ‘common travel area’ exists — where multiple States allow free movement between one another — ETS data and alerts should be shared between participating States.

The proposed European Travel Information and Authorisation System (ETIAS) is an example of regional cooperation for border security. ETIAS will allow for advance checks and, if necessary, deny travel authorisation to visa-exempt third-country nationals travelling to the Schengen area. The system will apply to visa-exempt third country nationals, as well as those who are exempt from the airport transit visa requirement. They will need to obtain a travel authorisation before their trip, via an online application. The information submitted in each application will be automatically processed against other EU databases to determine whether there are grounds to refuse a travel authorisation. When no hits or elements requiring further analysis are identified, the travel authorisation will be issued automatically within a short time. If there is a hit or an element requiring analysis, the application will be handled manually by the competent authorities.³⁰

30 *European travel information and authorisation system – Council agrees negotiating position*, European Council, June 2017, available at: <http://www.consilium.europa.eu/en/press/press-releases/2017/06/09-etias/>

Travellers should be able to request clarification or reversal of adverse ETS decisions by letter, email or telephone, and have an official review the facts and logic leading to the decision.

The US ETS system, Electronic System for Travel Authorization (ESTA), provides for a 'redress number', a mechanism by which travellers that would otherwise be ineligible for an ETS permission can use the facility to obtain an ESTA and thereby have their travel facilitated.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Extracts from ICAO Annex 9 – *Facilitation* Chapter 3. Entry and departure of persons and their baggage³¹:

L. Transit procedures and requirements

“...

3.55 Contracting States shall keep to a minimum the number of States whose nationals are required to have direct transit visas when arriving on an international flight and continuing their journey to a third State on the same flight or another flight from the same airport on the same day. ...”

Extracts from ICAO Annex 9 – *Facilitation*, Chapter 9. Passenger Data Exchange Systems³²:

C. Electronic Travel Systems (ETS)

9.17 **Recommended Practice.**— *Contracting States seeking to establish an Electronic Travel System should integrate the pre-travel verification system with an interactive Advance Passenger Information system.*

Note.— *This will allow States to integrate with the airline departure control systems using data messaging standards in accordance with international guidelines in order to provide a real-time response to the airline to verify the authenticity of a passenger's authorization during check-in.*

9.18 **Recommended Practice.**— *Contracting States seeking to implement an Electronic Travel System (ETS) should:*

a) ensure a robust electronic lodgement platform where an online application for authority to travel can be made. A State should make clear that their platform is the preferred means for applying online in order to reduce the scope of unofficial third party vendors that may charge an additional fee for the purpose of lodging an individual's application.

b) include tools built into the application to assist individuals to avoid errors when completing the application form, including clear instructions as to the applicability of which nationalities require an ETS, and not allow application processing for non-eligible passengers (e.g. nationality and/or document type).

c) institute automated and continuous vetting of relevant alert lists.

d) provide electronic notification to the passenger to replace paper evidence of an individual's approval for travel.

31 *Annex 9 – Facilitation to the Convention on International Civil Aviation*, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

32 *Annex 9 – Facilitation to the Convention on International Civil Aviation*, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

e) ensure that the information required from the passenger is easily understood in accordance with the national laws and regulations of that State.

9.19 **Recommended Practice.**— Contracting States should allow for an implementation schedule that builds awareness regarding upcoming changes and develops communication strategies in multiple languages in cooperation with other governments, travel industry, airlines and organizations in order to communicate the planned implementation of an ETS.

9.20 **Recommended Practice.**— Contracting States should include a period of informed compliance after the initial implementation deadline, where passengers are allowed entrance into the country but informed of the new requirements. e.g. handing out a tear sheet with new requirements.

9.21 **Recommended Practice.**— Each Contracting State that requires an ETS should adopt policies that ensure that passengers are informed of the ETS requirements at the time of booking and should encourage aircraft operators to extend the ETS verification check to the point where travel originates rather than to the point of uplift for the last segment before entry into the country for which the ETS mandate applies.

Note.—This will depend on other aircraft operators' interline through check-in capabilities and the relationship between aircraft operators. ...”

SOURCES FOR FURTHER INFORMATION

References

Annex 9 – Facilitation to the Convention on International Civil Aviation, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

Standards and Recommended Practices, Annex 9 to the Convention on International Civil Aviation – Annex 9 – Facilitation, Fourteenth Edition, ICAO, Montreal, October 2015, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

European travel information and authorisation system – Council agrees negotiating position, European Council, June 2017, available on: <http://www.consilium.europa.eu/en/press/press-releases/2017/06/09-etias/>

Other sources

States seeking to establish an ETS system can also refer to the recommendations and suggested procedure(s) found in the *Best Practice for Electronic Travel Systems*, Version 1.0, IATA Control Authorities Working Group (CAWG), 27 October 2015, available at: https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/03-interactive_api/IATA%20CAWG%20Best%20Practice%20for%20Electronic%20Travel%20Systems%20revised%202016v1.pdf



MRZ images are captured in infrared to maximise image contrast, which improves the accuracy and reliability of the data that is read. The MRZ data elements identified in the infrared capture are sent to the national BCS.

More sophisticated readers can undertake machine based comparison of the images taken of travel documents with libraries of reference images that map the position and characteristics of security features observed in similar documents. Depending on the national BCS interface, all or some of the images, as well as reports on the results of the various comparisons, may be displayed to the border control officer. These reference library based tools require regular updates, and are therefore an ongoing service rather than a once only purchase.

Less commonly, some document readers can perform machine based authentication of proprietary security features that require specialized hardware and software interfaces³⁵.

The best document reader for a specific application has capabilities that complement and match the documents being presented.

Human examination of travel documents supports the interpretation of security features undertaken by document readers. All frontline border control officers should be trained in basic document examination techniques. In best practice jurisdictions, specialist forensic examiners support basic examination of documents at secondary examination.³⁶

HOW IT WORKS – AIRLINES

The document readers most often used by airlines are integrated into the keyboards used by check-in personnel. To read the passport, personnel swipe the bottom section of the data page containing the MRZ.

Data captured from the MRZ populates the corresponding data fields in the airline departure control system and are added to the API batch (or initiates the iAPI “OK to board” transaction with the State of final arrival)³⁷.

The examination to determine the authenticity of travel documents is a State responsibility. For this reason, airlines do not make extensive use of document readers that check and report on security features. However, since many States impose on airlines a financial liability for carriage of improperly documented travellers, there is an incentive for airlines to make basic checks of the authenticity of travel documents. Consequently, many airlines train their personnel to undertake visual and touch based checking of travel documents to assess their authenticity.



BENEFITS AND OPPORTUNITIES

National border control agencies have an important role to play in providing feedback to the national issuer(s) of MRTDs, to advise them how the travel documents they issue perform in practice.

35 For recommendations on operation of systems and processes involved in optical machine assisted authentication of MRTDs: *ICAO Guide for Best Practice Guidelines for Optical Machine Authentication*, Version 1, ICAO, Montreal, April 2016, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

36 See: *Section 6. Risk Assessment and Travel Document Inspection*

37 See: *Topic H – Advance Passenger Information and Interactive Advance Passenger Information*

RISKS AND COST MITIGATION

Document readers have been used in border control for more than 30 years, and have proven to be a reliable and robust application of technology. There is overwhelming evidence that machine reading the MRZ data elements into a national BCS is faster and more accurate than a border control officer manually typing travel document data into the national BCS.

However, MRZ misreads do occur for a range of reasons and cannot be wholly eliminated. Where misread error rates are high, it is important that their cause is analysed and understood. Document reader performance can be degraded by:

- Non-conformance of the MRZ of the MRTD or eMRTD in terms of positioning, infrared illumination features, typefaces and ink;
- Contamination of the MRZ (e.g. with dust or dirt) obscuring printed characters;
- Contamination of the optical plate on the reader;
- Heavy usage of the MRTD or eMRTD in harsh conditions that can damage the datapage material; and
- Environmental factors (e.g. document read accuracy may degrade if the optical reader plate is exposed to direct sunlight).

Effective use of the additional information provided by document readers that display images from multiple light sources depends in large part on the skills and knowledge of border control agency personnel, and how they are supported. Best practice jurisdictions support the primary processing undertaken by frontline officers with referrals of process exceptions to secondary examination. To mitigate the risk of project failure at implementation, the initial introduction of document readers requires skills development and training support, and changes to business processes.

A common implementation feature is for all the images captured by document readers and the results of the checks to be displayed to the processing officer at primary examination. In more sophisticated jurisdictions, less information is displayed unless a threshold discrepancy is identified. This mitigates somewhat the risk of sensory overload of officers.

The technical specifications described in ICAO Doc 9303 are extensive and complex. All of them are important for achieving MRTD and eMRTD interoperability. MRTD and

eMRTD projects require a significant investment; effective integration with the national BCS is critical to realising a return on investment. To mitigate implementation risks, States should undertake their own research and seek independent advice at the earliest stages of project planning, prior to decisions on solutions.³⁸

Non-compliance, whether minor, technical or more serious, does occur, and can have an impact on interoperability by making data more difficult to read from the MRZ and IC chip. It is critical that border control officers understand the non-compliance of their national MRTD and those of other States whose travellers often seek entry, and how this non-compliance impacts their inspection.

In more sophisticated jurisdictions, it is not unusual for the BCS to be reconfigured in minor ways each time an MRTD is introduced into circulation by their own MRTD issuer, or by MRTD issuers in other States. Non-compliance risks can be anticipated and mitigated by obtaining and testing specimens of new documents before they are issued to travellers. Inter-agency collaboration between travel document issuers and border control agencies is therefore essential.

BEST PRACTICE EXAMPLES

Quality assurance checks to assure machine readability are a standard feature of MRTD and eMRTD issuance. In best practice jurisdictions, the MRZ readers and the reader interface used for the quality assurance checks at passport issuance match as closely as possible those used at border inspection. By this simple alignment, the read performance at issuance can more closely approximate the actual read performance at border inspection.

Emerging practices include airlines deploying eMRTD readers that perform PKI authentication. This application involves partnerships with national authorities, where authentication provides operational benefits for all parties concerned.³⁹

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Refer to sub-Section 2.2 *Integrating Inspection Systems and Tools with Interoperable Applications* for ICAO SARPs that apply to MRTDs.

38 Guidance for authorities planning to implement major upgrades of their current travel documents and related systems, including all aspects of the procurement plan: ICAO Guide for *Collection of Best Practices for Acquisition of Machine Readable Travel Document Goods and Services*, Version 1, ICAO, March 2016, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

39 See: *Topic J – Public Key Infrastructure and the ICAO Public Key Directory*

SOURCES FOR FURTHER INFORMATION

References

Annex 9 – Facilitation to the Convention on International Civil Aviation, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

Doc 9303, Machine Readable Travel Documents, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

ICAO Guide for Best Practice Guidelines for Optical Machine Authentication, Version 1, ICAO, Montreal, April 2016, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

ICAO Guide for Collection of Best Practices for Acquisition of Machine Readable Travel Document Goods and Services, Version 1, ICAO, March 2016, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

Other sources

Guidelines on the security of travel document handling and issuance system are available in the *ICAO Guide for Assessing Security of Handling and Issuance of Travel Documents*, ICAO, Montreal, March 2017, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

triggering retrieval of other issuance data for comparison. For primary matching the travel document dataset used for this purpose may be an offline extract updated regularly in a batch process containing only the required data elements.

For secondary examination, where the primary process fails to match because of error or fraud, a more extensive extract is required to support resolution of traveller identity. Alternatively, full read-only access to the travel document database can be provided for a smaller number of border control agency personnel responsible for the resolution of doubt in the identification of travellers.

To protect data and maintain traveller privacy, agencies should implement appropriate controls and standard procedures to ensure searches of offline extracts (or of online full national identity and passport databases) are only undertaken when required and by the appropriate persons.

HOW IT WORKS – AIRLINES

In the absence of an operational imperative, and consistent with international privacy and data protection norms, airlines do not interface directly with the national identity or passport databases of States.

BENEFITS AND OPPORTUNITIES

At primary processing, automated database or database extract verification of MRTDs and eMRTDs issued by the State provides a strong foundation for the identity verification of travellers holding these documents.

For those documents that ‘fail to verify’, enquiry access to national identity and/or passport datasets at secondary examination provides a mechanism for prompt investigation and resolution of doubt in the identification of travellers. This capability can also be used in 24/7 border operations centres to provide advice to other States in resolving the ‘fail to verify’ instances they encounter at border control. Assisting in the resolution of these queries benefits the holders of the MRTDs and eMRTDs issued by the State by facilitating their continued travel.

Enquiry access to national identity and/or passport datasets at secondary examination and in 24/7 border operations centres is also essential in resolving referrals following INTERPOL SLTD database matches⁴¹.

TECHNICAL ISSUES

National BCS, national identity systems and national travel document issuance systems are most commonly proprietary systems that are unique to, or uniquely configured for, each State.

Where they exist as separate ICT systems, communication and data integration interfaces could link the various national systems to support comparisons at primary examination. However, this ICT integration is relatively complex compared to providing read-only access to national issuance databases at secondary examination.

National BCS of some States integrate a travel document issuance module. In this ICT architecture, automated comparisons at primary examination are likely to be more easily achieved. Similarly, enquiry access at secondary examination to the travel document issuance module is a simple matter of managing access permissions.

RELATED REQUIREMENTS

- ✓ National legislation and inter-agency agreements for BCM agencies to access national identity and/or passport databases.
- ✓ Protocols and business processes for the handling of personal information (biographic and biometric) that meet national privacy and data protection legislation.
- ✓ ICT integration of document readers with national BCS and reliable MRZ read performance of MRTDs and eMRTDs issued by the State⁴².
- ✓ ICT integration of national BCS with national identity and/or passport databases.
- ✓ Reliable, continuous supply of electricity and connectivity.

RISKS AND COST MITIGATION

The major risk and cost arises in those States that need to integrate unlinked, separate ICT systems for border control, travel document and national identity card issuance.

Because international airports operate continuously with high transaction volumes, communication costs can be a

41 See: *Topic L – INTERPOL Database of Stolen and Lost Travel Documents*

42 See: *Topic B – Document Readers*

significant factor. For those States where data bandwidth remains constrained or expensive or both, dataset extracts updated in batch processes provide business continuity and cost advantages.

In those States operating at lower volumes of travel document issuance and border traffic, the database national verification arrangements described in this Topic have cost advantages in comparison to investments in more complex solutions such as PKI authentication.

Where error, transliteration, cultural name variations (e.g. William, Wilhelm, Wim), the use of aliases or official traces of name changes (e.g. following adoption, marriage and divorce) create uncertainty in matching, alternative or additional verification may be required.

Alternative potential national resources for biographic verification may include: civil registries, national identity schemes, and functional systems that have identifying details recorded in tokens and/or databases (such as drivers' licenses, health insurance or pensions).

Consistent rules based transliteration provides a reliable basis for transforming names from one language to another. This is critical in MRTD issuance because the MRZ accommodates only the limited character set used in English. Inconsistent transliteration will result in the same name in the original language appearing with different Latin spellings in the MRZ. ICAO recommendations for transliteration are provided in Part 3 of Doc 9303⁴³.

SOURCES FOR FURTHER INFORMATION

Reference

Doc 9303, *Machine Readable Travel Documents*, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

United Nations Statistical Division (UNSD). 2014. *Principles and Recommendations for a Vital Statistics System – Third Edition*, <https://unstats.un.org/UNSD/demographic/standmeth/principles/M19Rev3en.pdf>

Further elaboration of these issues can be found in UN guidance on best practice in vital statistics⁴⁴.

BEST PRACTICE EXAMPLES

For States with a centralized national identification registry, the issuance of a travel document may follow a simplified process in which the national identity registry is acknowledged as the primary source of authentic information used to confirm the identity and citizenship of the traveller. A best practice in these jurisdictions is for border control agencies to also have access to the national identity database during secondary examination processes, to verify identity.

More generally, the secondary examination modules of more sophisticated national BCS include the ability to retrieve and reference data from national identity and passport issuance datasets to record the resolution of the referral of travellers due to identity data errors and, less commonly, identity fraud.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

The ICT interface(s) between national identity databases and national BCS are a sovereign matter for States, and are therefore not the subject of ICAO SARPs or technical specifications.

Other source

Best practices to prevent and mitigate security threats at every step of the travel document issuance process are available in the *ICAO Guide for Assessing Security of Handling and Issuance of Travel Documents*, ICAO, Montreal, March 2017, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

43 *Doc 9303, Machine Readable Travel Documents*, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

44 *Principles and Recommendations for a Vital Statistics System – Third Edition*, United Nations Statistical Division, New York, 2014, available at: <https://unstats.un.org/unsd/demographic/standmeth/principles/M19Rev3en.pdf>

D. BIOMETRIC IDENTITY VERIFICATION



These **Inspection Systems for Traveller Identification** compare images captured live from the traveller against biometric reference databases of enrolled images from visa, trusted traveller, travel document or other token issuance.

KEY MESSAGES

- ✓ Comparison of live biometric samples (face, fingerprint or iris) from a traveller with biometric templates held in national databases.
- ✓ Where integrated with eGates, kiosks and airline check-in processing, provides efficiency, security and facilitation benefits.

OVERVIEW

States have adopted a range of biometric⁴⁵ solutions for the identification of travellers. These solutions may use different biometric features, and obtain the reference image from different sources.

Biometric identity verification using reference images obtained from electronic eMRTDs is discussed in *Topic K – eMRTD Biometric Identity Verification*.

The present Topic describes solutions implemented in national BCS where the reference image for comparison is obtained from a source other than an eMRTD. The alternative sources for obtaining reference images of biometric features in these national systems include images enrolled in registered traveller programs, at visa or ETS issuance, or retrieved from the national identity or passport databases. In all these applications the reference image is accessed from a database.

Biometric comparisons for one-to-one (1:1) identity verification are in many cases implemented as one element of

Automated Border Controls (ABC) solutions⁴⁶ but can also be implemented in support of the processing of travellers by border control officers.

In addition to the 1:1 verification task, biometric comparisons can also be made between images captured of the traveller at border controls (whether face, fingerprint or iris) with images in a biometric watchlist database. This application of one-to-many (1: n) identification search comparisons is discussed in *Topic E – National Watchlists*.

Biometric comparisons are an application of probability, and results are subject to variance and error. Independently, while each of the three biometric features give a sufficiently high level of assurance of identity verification, the possibility of error remains. In closed systems, the statistical variance in matching can be modelled, estimated and expressed as False Acceptance Rates (FARs) and False Rejection Rates (FRRs). These simulations have only limited relevance to real world applications of biometrics, where additional sources of human error and statistical variance are present. For this reason, States should treat the claimed performance of biometric solutions with care.

In general, better results are achieved when high quality reference images are available and these are compared with high quality images of the live traveller. Guidance on image quality parameters is provided in the ICAO Doc 9303 Part 3: Specifications Common to all MRTDs⁴⁷.



45 ICAO Doc 9303 defines biometric identification as a generic term used to describe automated means of recognizing a living person through the measurement of distinguishing physiological or behavioural traits.

46 See: *Topic G – Automated Border Controls*

47 *Doc 9303, Machine Readable Travel Documents, 7th Edition*, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

HOW IT WORKS – BORDER CONTROL AGENCIES

Biometric systems cannot contribute to verifying the identity of a traveller if there is no previous record (a biometric sample and associated biographic detail) to compare against. In the national solutions that are the subject of this Topic, these reference samples are obtained and accessed from biometric images or templates and biographic details enrolled and captured previously and held in databases (e.g. visa, ETS, trusted traveller, residence permit or national identity card or national passport systems).

Biometric verification of traveller identity is used to confirm to an acceptable degree of confidence that the biometric sample obtained of the traveller presenting for border control matches the biometric available from the reference sample.

In cases where impersonation is suspected, or the biometric matching system produces an inconclusive result, further examination using a biometric matching system deployed at secondary examination can inform identity verification decisions. Identifying suspect cases for referral, and resolving non-match referrals requires skills, knowledge and experience in image comparison specific to each biometric feature (whether face, iris or fingerprints). The implementation of biometric identity verification solutions therefore requires careful consideration of the skills and training needs of border control officers.

HOW IT WORKS – AIRLINES

Emerging solutions use biometric identity verification to facilitate the movement of travellers through the various touch points at airports. In these solutions, airlines and airport authorities are investing in biometric technology to manage the access of travellers to restricted areas and boarding of flights.

Subject to appropriate ICT security and privacy and data protection, these solutions also have the potential to be integrated with a national BCS at departure processing. As these models mature it is likely that they will lead to the adoption of new international standards. In the meantime, it is important that airlines, airport operators and border control agencies work together to ensure that the commercial interests of airlines and airport operators are not compromised by arrangements that require substantial investment or impose ongoing transactional costs.

BENEFITS AND OPPORTUNITIES

Biometric matching for traveller identity verification is the foundation for ABC⁴⁸. The deployment of effective ABC solutions can reduce queue times to improve the traveller experience and provide process efficiency benefits for States. Biometric matching can also improve the accuracy and consistency of the identification of travellers, which could allow for redeployment of border control agency personnel to focus on risk-based interventions at secondary examination. These are important and significant facilitation and security benefits.

At departure control, a biometric traveller identity verification system can confirm that a previously encountered traveller has departed. Faked departures of imposters are a risk when traveller identity verification relies on human comparisons by border control agency personnel, or where departure control is not undertaken – a vulnerability that has been exploited, notably by foreign terrorist fighters.

Biometric records created during visa application or on entry can also be used for post-entry processing, for example, for residence permits or extensions of stay, to confirm that the traveller admitted is the one later applying to extend their stay.

Provided that comprehensive matching systems are employed, a biometric link between the traveller and his/her record ensures that multiple applications and multiple identities can be detected.

TECHNICAL ISSUES

Obtaining biometric sample images from travellers requires a BCS interface with:

- Visible light cameras for facial images;
- Infra-red cameras for iris images; and
- Specialized readers for fingerprints.

The quality of images obtained is subject to ambient lighting and other environmental factors, as well as presentation factors such as facial position for face and iris, or dry hands after long haul flights.

Accessing biometric reference samples for comparison requires a secure interface with the reference database containing the reference images and standardised data descriptors (metadata) to ensure the correct biometric samples are retrieved for comparison.

48 See: *Topic G – Automated Border Controls*



Exploiting biometrics requires capture devices that are accurate enough to capture images to create templates with sufficient detail to enable a good comparison between live and stored images.

The matching algorithm that performs the comparisons must be able to deliver timely reliable matching results for the volume of travellers that use the solution at airports and other border locations where the systems are to be deployed.

For all biometric types, there are inherent trade-offs in performance between:

- Speed and accuracy – a system that produces very accurate results may be unacceptable in terms of transaction times, and a faster system may deliver unacceptably high errors; and
- Referrals of genuine travellers (false rejections) and the possibility that an imposter will meet a match threshold and be allowed entry or departure (false acceptances).

The biometric matching systems need to be developed or purchased as an integrated system that includes careful calibration of capture devices and matching algorithms. Matching performance should be monitored to ensure that the settings are optimal. Algorithms should be regularly updated to new versions to take advantage of advances in technology, but this should only be done after testing that they closely simulate the environment in which the solution is deployed.

RELATED REQUIREMENTS

- ✓ National legislation to require travellers to provide a biometric sample image.
- ✓ Effective standard operating procedures.
- ✓ Legislative frameworks to collect, store, retrieve, compare, share, retain and dispose of biometric sample images and templates.
- ✓ National privacy and data protection legislation, systems and practices sufficient to protect biometric data from misuse.
- ✓ Secondary examination operating model with adequate staffing and accommodation for resolving traveller identity verification referrals.
- ✓ ICT integration of BCS with a biometric capture solution and a secure interface with the reference database containing biometric enrolments, and standardised metadata to ensure the correct biometric samples are retrieved for comparison.
- ✓ Reliable, continuous supply of electricity.
- ✓ Reliable, continuous, high bandwidth network connectivity sufficient for transmitting image files in real time.

RISKS AND COST MITIGATION

“Human recognition systems are inherently probabilistic, and hence inherently fallible. The chance of error can be made small but not eliminated. System designers and operators should anticipate and plan for the occurrence of errors, even if errors are expected to be infrequent.”⁴⁹

Each biometric modality (i.e. face, iris, finger) is at risk of artefact attacks, also known as ‘spoofing’. These attacks attempt to use a mask, contact lens or plastic fingerprint to trick the image capture device and interface into accepting a fake image. Protection against these attacks is critical to ensuring the integrity of the identification of travellers. As a result, all credible biometric solutions include ‘liveness’ detection features.

Very careful thought needs to precede planning for biometric systems. As with most information technology systems, biometric products are not cheap, and support and maintenance costs can be significant. There should be

⁴⁹ *Biometric Recognition: Challenges and Opportunities* US National Research Council, 2010, p.1, available at: <https://www.nap.edu/catalog/12720/biometric-recognition-challenges-and-opportunities>

a compelling business case for the introduction of biometric systems that includes such considerations as:

- Does the proposed system enhance national security?
- What are the risks and threats from existing and future border traffic?
- Does the volume of traffic at border posts justify the expenditure?
- What is the likely usage of the system by travellers?
- What is the likely effect on queue patterns and transaction times in arrival halls?
- Can all ports and offices of the immigration department and other agencies be connected to the system?
- Is the system appropriately protected against loss and unauthorised change or disclosure of biometric data?
- Are the biometric feature(s) selected interoperable with other systems?
- Is there a case for a Registered Traveller Programme?

The consideration of which biometric modality or modalities are to be used should be informed by the travel environment in the State, and the legacy biometric data available that could be used as reference samples. The application of biometrics requires a human interface with technology. This interface has a cultural dimension – solutions that are effective in one State may be less effective in another. Error should be anticipated, and statistical variance factors unique to the environment understood. Only after these analyses can a State determine a ‘concept of operations’ and

make an informed choice of biometric modality. States are encouraged to seek vendor independent, solution neutral advice to support their consideration.

Biometric technology continues to develop and mature. All applications of biometric technology in BCM are expensive to implement, and have ongoing operating costs.

BEST PRACTICE EXAMPLES

States have adopted a range of biometric solutions for the identification of travellers. These solutions use each of the three biometric features, and obtain the reference image from different sources. This variance in national practice reflects differences in perceived threat and risk, and the different efficiency and facilitation benefits implementing States are seeking to achieve. For example, in the United Arab Emirates (UAE), iris images enrolled at residence permit issuance are used to verify the identity of expatriate workers returning to the UAE.

Biometric matching can be applied to visa systems where biometric images (face and fingerprints) are collected at the time of application. This ensures that the person presenting a paper visa or electronic travel authorisation is the person to whom it was issued. This verification is used in Australia, United Kingdom (UK), United States of America (USA), and in the European Union (EU) visa systems where fingerprint readers at passport control capture one or more prints that are compared against the traveller’s visa record.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Extract from ICAO Annex 9 – *Facilitation*, Chapter 3. Entry and Departure of Persons and their Baggage⁵⁰:

D. Travel documents

3.11 All passports issued by Contracting States shall be machine readable in accordance with the specifications of Doc 9303, Part 4.

Note.—This provision does not intend to preclude the issuance of non-machine readable passports or temporary travel documents of limited validity in cases of emergency.

3.11.1 For passports issued after 24 November 2005 and which are not machine readable, Contracting States shall ensure the expiration date falls before 24 November 2015.

⁵⁰ Annex 9 – *Facilitation to the Convention on International Civil Aviation*, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

3.12 Contracting States shall ensure that travel documents for refugees and stateless persons (“Convention Travel Documents”) are machine readable, in accordance with the specifications of Doc 9303.

Note.—“Convention Travel Documents” are provided for in the 1951 Convention Relating to the Status of Refugees and the 1954 Convention Relating to the Status of Stateless Persons (cf. respective Article 28 of both Conventions).

3.13 **Recommended Practice.**— *When issuing identity documents or visas accepted for travel purposes, Contracting States should issue these in machine readable form, as specified in Doc 9303. ...”*

I. Inspection of travel documents

“ ...

3.34.4 **Recommended Practice.**— *Each Contracting State should consider the introduction of Automated Border Control (ABC) systems in order to facilitate and expedite the clearance of persons entering or departing by air.*

3.34.5 **Recommended Practice.**— *Contracting States utilizing ABC systems should, pursuant to 3.9.2 and 3.10.1, use the information available from the PKD to validate eMRTDs, perform biometric matching to establish that the passenger is the rightful holder of the document, and query INTERPOL’s Stolen and Lost Travel Documents (SLTD) database, as well as other border control records, to determine eligibility for border crossing. ...”*

SOURCES FOR FURTHER INFORMATION

References

Doc 9303, Machine Readable Travel Documents, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

Annex 9 – Facilitation to the Convention on International Civil Aviation, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

Biometric Recognition: Challenges and Opportunities, US National Research Council, 2010 available at: <https://www.nap.edu/catalog/12720/biometric-recognition-challenges-and-opportunities>

Other Sources

The United States National Institute of Standards and Technology (NIST) publishes biometrics standards and guidance on their implementation, testing and use. NIST documents are used as supplementary references by many States, for example in benchmarking biometric matching performance: *Biometrics*, NIST, available at: <https://www.nist.gov/programs-projects/biometrics>

National documents are also published describing the administrative governance and procedures that are critical to biometric projects. For example, the UK has published:

Code of practice for the implementation of a biometric system, PAS 92:2011, *British Standards Institution (BSI)*, 2011, available to purchase at: <http://shop.bsigroup.com/en/ProductDetail/?pid=00000000030213319>

Standards for the automated recognition of individuals based on their behavioural and biological characteristics, *British Standards Institution (BSI)*, 2010, available to purchase at: <http://shop.bsigroup.com/upload/Standards%20&%20Publications/BrochureDownload/BiometricsBrochure2010.pdf>

E. NATIONAL WATCHLISTS



These **Inspection Systems for Traveller Risk Assessment** compare biographical details or biometric images of the traveller against reference databases of known targets of concern compiled by the State from national and international sources.

KEY MESSAGES

- ✓ Checks traveller passport, biographical data or biometric samples against national databases of passport, nominal or biometric records.
- ✓ Enables risk-based interventions to target known or suspected criminals, terrorists, or unwanted or unauthorized travellers.
- ✓ Most effective when utilized as part of an integrated interface with the national BCS, allowing for real-time comparisons with traveller information.

OVERVIEW

Watchlists allow searches against biographic (name, date of birth, sex, nationality) and biometric (face, fingerprint, iris) identity attributes associated with known or suspected targets, as well as against a national lost, cancelled and stolen travel documents database along with the INTERPOL SLTD database.



Travellers are facilitated when their entry and stay are deemed beneficial to a State. Travellers who intend to engage in illegal or unwanted activities such as smuggling, illegal employment, terrorism or other crimes must be identified, so that appropriate interventions can be made to prevent travel or entry.

Fundamental to BCM is the application of intelligence gathering and analysis, and the ability to make risk-based interventions to prevent, deter and disrupt the travel of terrorists, criminals and other people who represent a risk or threat to States. The watchlist modules of national BCS are the principal tools for initiating these interventions.

The people whose identity attributes are included on watchlists represent a risk or threat based on their circumstances and prior conduct. This ranges from known terrorists and criminals, to people subject to administrative sanctions because of previous overstay or illegal employment, or those who may require a public health intervention.

Best practice jurisdictions gather intelligence and analyse data to target travellers who represent a risk. The collection of this intelligence uses all the tools described in the topics of this Guide. For example, a history of prior travel may reveal a pattern that might be confirmed by analysis when compared with visa records. This could result in a targeting alert to be triggered on the next occasion when API is received, signalling the pending arrival of the traveller.

In more sophisticated jurisdictions, the identification of risk-based targets is improved by using watchlists to apply risk-based profiles to information about travellers obtained from a range of sources. The watchlist entry will typically be created in real time when PNR, API, visa or ETS information is received, and may be deleted after the traveller is processed at entry control, if the intelligence analysis and targeting is resolved.

The interventions triggered by watchlist matches can be calibrated by the system to initiate action to:

- Process, record and advise;
- Initiate surveillance;
- Interview to obtain information;
- Arrange a person and/or baggage search; or
- Interview, detain and remove.

This level of detail can contribute to interventions to prevent, deter and disrupt threats as an alternative or in addition to action to detect threats and take enforcement action⁵¹.

51 See: Sub-Section 2.3 Identification of Travellers and Risk Assessment, Border Control Interventions

The application of watchlists is a basic functionality in all national BCSs.

HOW IT WORKS – BORDER CONTROL AGENCIES

Most States have moved from printed lists of targets for intervention to ICT based systems in which biographic and biometric details are searched to produce matches.

National watchlists are most effective when they include listings targeting *all* the risks and threats of *all* the agencies represented at the border. In these systems, the national watchlist module of the BCS is shared. The ICT infrastructure is used by agencies responsible for law enforcement, national security, customs and immigration.

In these jurisdictions with integrated national watchlists, the responses displayed to the border control officer are carefully calibrated so that they only see information relevant to their role. For some agencies, and in some situations, the inclusion on a watchlist can be facilitative for the traveller, for example where a traveller is included on a 'whitelist' to distinguish them from a 'blacklist' target that shares similar biographic or biometric or document attributes.

In best practice jurisdictions, watchlists are integrated with or included as a module in the BCS. Watchlist searches are initiated when the data from the MRZ is received by the document reader, or at pre-arrival from visa, ETS, API, iAPI or PNR data.

Name matching is a complex application of probability, subject to error and statistical variance. In best practice jurisdictions, different logical approaches are applied in combination to the name matching task. These include, among other techniques, algorithms that automate multiple wildcard search combinations, reference tables that anticipate alternative spellings of common names, the impact of transliteration, and cultural name variations. Watchlists should be configured to accept multiple listings for a single individual target, to accommodate known aliases and name changes.

Watchlist search algorithms can also be designed to anticipate and make additional searches for common typographic errors and phonetic misspellings.

In many jurisdictions, images of faces or other biometrics are associated with biographic records. Making these images

available at secondary examination can assist border control personnel in reconciling possible matches.

In some more advanced jurisdictions, watchlists of biometric identity attributes associated with the targets of national law enforcement, security, immigration and other agencies are being used. The 1:n identification searches performed in watchlist applications are significantly more complex than the more common 1:1 identity verification task⁵², and require sophisticated technical and human capability.

HOW IT WORKS – AIRLINES

The application of watchlists in the assessment of risks posed by the entry and stay of travellers is the sovereign responsibility of States.

In iAPI systems, when States respond to airline "OK to board" queries with a "refer to State authorities" response this may, in some instances, reflect a watchlist match where the State's chosen intervention is to prevent travel. When this occurs, it is important for the safety of airline check-in personnel that they remain unaware of the reason for the denial of check-in or boarding.

BENEFITS AND OPPORTUNITIES

Border control agencies maintain watchlists to assist in detecting and managing the travel of persons known to be associated with immigration or other offences. Other intelligence or law-enforcement agencies may also have their entries placed on the watchlist system so they can be informed and make an appropriate intervention if one of their targets arrives or departs.

Alerts to border officials of travellers who become persons of interest following API, ETS, PNR or other profiling or intelligence assessments are more reliably and effectively managed by watchlist entries than the former practice of oral or printed messages being passed to frontline border control officers.

⁵² See *Topic D – Biometric Identity Verification* for some explanations of the differences between 1:1 and 1:n biometric comparisons.

TECHNICAL ISSUES

Name matching is a challenging task:

- A traveller may have changed the spelling of his/her name;
- A traveller may have changed the number and order of name elements;
- Names may be truncated or spelled differently to fit into the machine-readable zone of modern travel documents;
- The name may have been transliterated from a non-Roman alphabet (e.g. Arabic, Cyrillic) in a way different to a previous record;
- Dates of birth may be inaccurate or incomplete, and vary between records;
- Names may have multiple spellings and diminutives (e.g. Robert and 'Bob');
- Officers may be under pressure to clear queues of passengers, and discouraged to look up all name variations;
- Simple watchlist systems may only cope with exact matches, and fail to uncover real matches that deviate slightly from the text entered for search; or
- The traveller may be using an alias.

RELATED REQUIREMENTS

- ✓ Protocols to enforce data quality standards for inclusion, for regular review, and for deletion of records from watchlists.
- ✓ ICT security arrangements to maintain restricted access to watchlist databases and to ensure watchlist searches are initiated only when required.
- ✓ Protocols and business processes for the resolution of watchlist matches, to confirm that the traveller is the subject of the watchlist entry.
- ✓ 24/7/365 operational support from all border control agency partners responsible for resolving national security, law enforcement, smuggling, public health, immigration and other alerts.
- ✓ Adequate interview and detention infrastructure at airports and other border locations.
- ✓ ICT integration of the watchlist module in the BCS.
- ✓ Appropriate ICT disaster recovery to ensure watchlists are searchable even if the BCS is unavailable.
- ✓ Reliable, continuous supply of electricity and connectivity at the 24/7 operations centre.

RISKS AND COST MITIGATION

The border control watchlist needs to be managed properly so that out-of-date and inaccurate entries are removed, thus preventing undue inconvenience to travellers. Depending on a State's data protection and privacy legislation, only necessary and relevant information should be kept on the system. Listings should be reviewed or automatically deleted after a defined period. The watchlist entries and the information supporting them should be classified and protected against unauthorised amendment, deletion and disclosure. Appropriate business continuity and disaster recovery arrangements are required. Travellers should not be able to view equipment or the screens displayed to border control officers.

Border control officers who access watchlist systems should be vetted to an appropriate standard. Access to the system should be controlled. The use of and access to the watchlist system or module should be audited and transactions logged, so that any misuse can be clearly identified. Management of the watchlist system or module should have a dedicated manager responsible for security and the prompt addition, updating and deletion of entries.

The transaction time for watchlist searches is a major factor in achieving facilitation standards. The performance impact of significant additions and changes to watchlist systems should therefore be carefully evaluated and modelled.

The introduction of biometric watchlists is a significant emerging opportunity in BCM. However, the effectiveness of biometric watchlists depends on whether biometric images of credible targets for border interventions are available to the State. It is likely that some combination of fingerprint, facial or iris images will in future be made available to States by INTERPOL, or to support the application of the CUNSCSL.

States wishing to invest in a biometric watchlist capability need to consider the legacy biometric data available to them that might be used to identify risk based targets, and how this data might be applied at the border to improve security outcomes. An example of relevant data might include fingerprint, face and iris images of travellers previously deported from the State who are at risk of attempting illegal re-entry using a fraudulent identity.

A clear concept of operations is required, and should be informed by sophisticated insights into probability and an understanding that biometric 1:n identification searches are subject to error rates *significantly higher* than biometric 1:1 verification searches. False positive errors — errors where a traveller is incorrectly identified as a target — can have

very serious consequences for travellers and for the reputation of States and their national border control agencies.

Commercial watchlist systems exist that may use either proprietary or third party name matching systems. It is recommended that such systems be procured after a competitive tender and full investigation of their performance in terms of speed, security and matching performance. Names have a cultural and ethnic dimension specific to national contexts, therefore name matching solutions that are effective for one State may be less effective in another. Name matching algorithms should be adapted to address issues of cultural equivalence, transliteration, aliases, and any other factors relevant to the environment in which they are being applied.

BEST PRACTICE EXAMPLES

It is desirable that additional watchlist datasets, as and when they become available, are integrated into national systems. These include the watchlists discussed in *Topic M – International Watchlists*.

In best practice jurisdictions, watchlist searches are undertaken at all phases of travel — at visa or ETS issuance,

at check-in, when interactive API is transmitted and the airline makes an “OK to Board” query, and finally during processing at entry.

In the USA, biometric watchlists of fingerprints available from national law enforcement databases, as well as tactical collections from war zones, have proven effective in detecting known and suspected criminals and terrorists at the US border.

The USA DHS Traveller Redress Inquiry Program (DHS TRIP) manages a ‘white list’, facilitating genuine travellers who would otherwise be inconvenienced by false watchlist matches⁵³.

In the UAE, biometric watchlists of the iris images of travellers who, during a previous stay, had their employment visa cancelled are being used for detecting and preventing entry under a false identity.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Not applicable.

SOURCES FOR FURTHER INFORMATION

Reference

Standards and Recommended Practices, Annex 9 to the Convention on International Civil Aviation – Annex 9 – Facilitation, Fourteenth Edition, ICAO, Montreal, October 2015, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

DHS Traveler Redress Inquiry Program (DHS TRIP), available at: <https://www.dhs.gov/dhs-trip>

Other sources

Biometric Recognition: Challenges and Opportunities, US National Research Council, 2010 available at: <https://www.nap.edu/catalog/12720/biometric-recognition-challenges-and-opportunities>

INTERPOL is developing such technology for police service and border control agency use and has published standards for image capture and exchange, *Forensics*, INTERPOL, available at: <https://www.interpol.int/INTERPOL-expertise/Forensics/Facial-recognition>

53 *DHS Traveler Redress Inquiry Program (DHS TRIP)*, available at: <https://www.dhs.gov/dhs-trip>

F. ENTRY AND EXIT DATABASES



These **Inspection Systems for Traveller Identification & Risk Assessment** compile comprehensive, searchable databases recording and indexing all the entries and departures of all travellers to and from the State.

KEY MESSAGES

- ✓ Computerised recording of details of arriving or departing travellers for border control and statistical purposes.
- ✓ Facilitates reconciliation of traveller entry and exit to manage stay.
- ✓ Additional data source for risk analysis based on traveller profile and history.
- ✓ Implementation should anticipate the technical challenge of compiling and maintaining large databases over extended periods of time.

OVERVIEW

Recording the entry and exit of all travellers is functionality basic to every national BCS. Recording travel informs States as to when their citizens and residents are abroad, and when foreigners and non-residents are present within their borders. This information has important applications, including in regulating the stay of travellers, and has domestic benefits such as protecting revenue through managing access to State entitlements.

The recording of entry and exit of travellers necessitates the creation of a travel history database. With the development of appropriate search and reporting tools, this travel history data combined with and analysed against other current data can be useful for investigative and intelligence purposes.

As a result, the value of a national database recording the entry and exit of travellers grows over time, providing more detailed insight into who is present in the State. With time, it becomes a richer source of historical data for analysis.

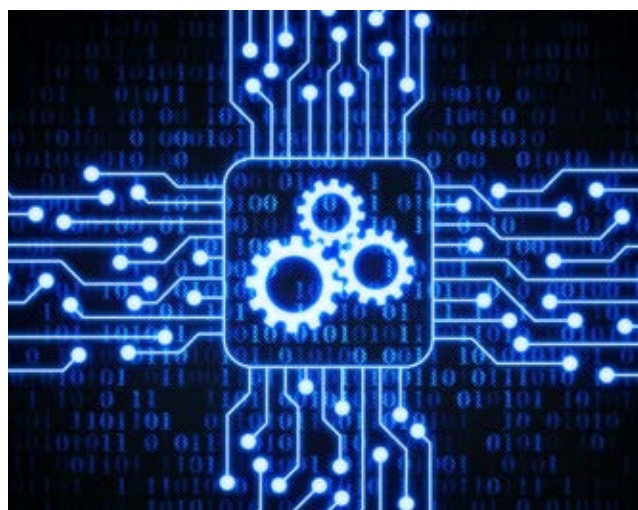
Yet growth in the size of such a database over time makes searching for matches a more challenging computational

task. It is therefore critical that traveller exit/entry databases be designed to scale from modest beginnings into larger databases capable of storing and effectively managing ever-expanding datasets. Also, traveller exit/entry databases contain sensitive personal information that must be adequately protected, from both a personal privacy and a broader data protection perspective.

The name matching required to reconcile entry and departure records of travellers to and from States can be challenging and difficult to achieve in practice. Biometric identity verification⁵⁴, when used to improve the accuracy and reliability of the identification of travellers, has the potential to improve entry and departure reconciliation⁵⁵.

In general, full reconciliation of traveller entry and departure is easier to achieve for States that have a small number of international border crossing points and are geographically isolated – such as small island States. These States have the opportunity to implement integrated national solutions covering all border crossings, to standardise national practice and business processes, and to identify and manage matching errors.

As a result, notwithstanding its critical importance to BCM, full entry/exit reconciliation has to date been used less in States that share extensive land borders with their neighbours. Still, because of the importance of travel history data in supporting the security and law enforcement response to emerging terrorist threats, more States are investing in national BCS with the capability to record and reconcile the entry and departure of travellers.



54 See: *Topic D – Biometric Identity Verification*

55 *The 9/11 Commission Report*, Washington, 2004, p. 389, available at: <http://govinfo.library.unt.edu/911/report/911Report.pdf>

HOW IT WORKS – BORDER CONTROL AGENCIES

Traveller data is read from the MRZ of MRTDs or eMRTDs via a document reader interface into BCS⁵⁶. Details of the arriving and departing flight are added, the data package is time stamped by the system to record the date of travel, and the travel record is added to the entry and exit database.

Where API data has been received, the flight details associated with the traveller can be retrieved and displayed on the screen along with the traveller details from the MRZ. In this way border control officers do not manually enter the flight details, thus reducing error and traveller processing time.

Travel databases typically allow a full set of cross-tabulated travel history searches using any combination or permutation of the available data elements, including: travel document number, name and date of birth, date of travel, nationality of traveller, document type, flight number and airline. When used in combination with API and PNR data, travel history searches contribute additional data for earlier analysis and risk-based targeting by security, customs, law enforcement, and immigration agencies.

HOW IT WORKS – AIRLINES

The recording of the entry and departure of travellers is a State responsibility, and not all States perform exit control. In some of these States, airline collection of API for transmission to the border control authorities of the airport of departure is undertaken.

In practice, API data is not sufficiently accurate to provide a basis for reliably recording traveller exit or entry. Where iAPI is available, MRZ data for each individual traveller has been added and authenticated by the border control agency. However, while iAPI data is in theory sufficiently accurate, since the data is collected by carriers at the start of air travel, *actual* entry or departure to/from the State needs to be separately confirmed to prevent substitution of travellers, faked departure and other identity related fraud.

For these and other reasons API is not, of itself, an alternative to border control agency examination of travellers at exit controls. It is important that States of flight origin intending to use the API data collected by airlines at departure understand the limitations of the data.

Better practice jurisdictions have State supervised exit controls in place, or are moving towards introducing them – in part as a response to emerging terrorism threats and the international requirement to prevent the travel of FTFs.

TECHNICAL ISSUES

Since all national BCS have as part of their basic functionality the ability to interface with document readers, obtain MRZ data, and process individual travellers for entry and/or departure, the creation of a travel database module is straightforward.

It's more challenging to design a module that anticipates the creation, protection and use of what quickly becomes a very large database.

Efficient database architecture, effective ICT access control and security and good search tools are necessary for success. The best options for each State will depend in part on the legacy systems and databases already in place, as these will determine the available options for change.

BENEFITS AND OPPORTUNITIES

The sustained growth of air transport and increasingly complex composition of travellers have made exit controls more important. The obligations of States under international law to prevent and deter transnational crime and apply travel related sanctions have increased in recent years. States can best meet these obligations where effective exit controls are in place.

In those States who record the entry and departure of all travellers at all border locations, a national travel history database provides the basis for managing the stay of foreigners within the territory of the State, and for recording the presence of citizens and residents.

Travel entry data is a rich source of data. When collated and analysed, it can contribute to investigative efforts to establish associations and relationships between criminals and terrorists.

States that previously did not record the exit of travellers may in the future consider doing it by using biometric verification in conjunction with API. This and other applications of biometric identity verification at exit control can improve

56 See: *Topic B – Document Readers*

the accuracy and completeness of exit data, and contribute to more reliable reconciliation of entry and departure records

A small number of States use iAPI data obtained from airlines at exit controls. In this case API data – in addition to being sent to the border authorities at transit and destination – is also used by the national BCS at departure. This provides another potentially valuable opportunity for the identification of travellers. It is especially useful in cases where all airlines operating from a State are already generating iAPI data for all departing travellers, and the additional impact on airlines is minimal. In such a case, the implementation is achieved simply by adding the exit control authorities of the State as an additional recipient of the existing iAPI data.

The potential benefits of achieving reconciliation of traveller entry and departure need to be weighed against the cost of the investment in systems and businesses processes to achieve it.

RELATED REQUIREMENTS

- ✓ National legislation to require border control agencies to collect, record, retain, search for, and use the entry and exit details of travellers crossing their borders.
- ✓ Protocols and business processes for the handling of personal information (biographic and biometric) that meet national privacy and data protection legislation.
- ✓ ICT integration of document readers with national BCS and reliable MRZ read performance of MRTDs and eMRTDs issued by the State⁵⁷.
- ✓ ICT integration of BCS to write to, and read from, a national entry and exit database.
- ✓ Reliable, continuous supply of electricity and network connectivity.
- ✓ Business continuity contingencies in case of failure of the system or for non-ICAO compliant MRTDs.

RISKS AND COST MITIGATION

Biographic matching can be a difficult task. Some travellers legitimately hold more than one national passport – including passports issued by more than one State – and

often with slight variations in their names due to transliteration, cultural name equivalence and other factors. When travellers replace their passports, their names and other biographic details may change. To account for this, States with effective systems for recording and reconciling the entry and departure of travellers employ extensive error management and error rectification tools. The travel history database design should anticipate and plan for managing error.

The travel history of individuals is personal and private and should be protected from misuse. Best practice in BCM includes comprehensive national privacy legislation to establish the individual right to privacy. On this foundation, border control personnel should be subject to specific controls that limit their access to the travel records of individuals to legitimate and lawful enquiries and investigations. There should be a provision for sanctions against personnel where access is inappropriate or unlawful.

The value of travel history databases as an intelligence analysis tool means that, once established, they become critical infrastructure for States. Best practice controls recognise that national BCS and travel history databases are critical to national security and law enforcement. States must take steps to ensure they are protected accordingly, including: appropriate data protection legislation, physical access control to server rooms, virtual access control and audit logs of searches, server and communication redundancy, and business continuity arrangements.

BEST PRACTICE EXAMPLES

National BCS in some States include functionality that identifies in real time unmatched departure of citizens and foreigners. By identifying these records, States can identify and resolve errors that would otherwise prevent a full reconciliation of the entry and departure of individual travellers. In addition to improving data quality, the unmatched departure of foreigners, citizens and residents can identify possible prior instances of evasion of border control points – a risk indicator that can then be investigated by border control agencies. These States have in common a small number of international airports and limited international travel by other transport modalities, but the achievement remains an example of best practice for other States.

In some States, the limitations and configurations of older airport infrastructure constrain the ability to achieve exit

57 See: *Topic B – Document Readers*

control. In the USA, airlines have in some circumstances been required to contribute data to national authorities to record traveller departure details. More recently, the USA has been trialling biometric departure processing using 1:1 verification of facial images. The reference images in these trials are obtained from the databases of the facial images of foreigners enrolled during visa issue, or at entry processing.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

The inclusion of travel history database functionality in their national BCS is a sovereign matter for States, and is therefore not the subject of ICAO SARPs. Interoperable Applications that are the subject of ICAO SARPs, such as iAPI and the ICAO PKD, can be leveraged to create more complete and more accurate travel history databases.

SOURCES FOR FURTHER INFORMATION

Reference

The 9/11 Commission Report Washington, 2004, available at: <http://govinfo.library.unt.edu/911/report/911Report.pdf>

G. AUTOMATED BORDER CONTROLS



*These **Inspection Systems for Traveller Identification & Risk Assessment** integrate other Inspection Systems and Tools and Interoperable Applications into a self-service automated processing solution.*

KEY MESSAGES

- ✓ Automated but supervised self-service passport control points for arriving or departing travellers.
- ✓ Enhances efficiency in traveller processing and identity verification, and enables redeployment of border personnel for targeted interventions to achieve facilitation and security objectives.
- ✓ ABCs require integration into the BCS.

OVERVIEW

Automated Border Control (ABC) is a collective term referring to ICT systems and interfaces that, in most applications:

- Read MRZ data from a MRTD, or read and PKI authenticate an eMRTD or read another identity token; and
- Establish that the passenger is the rightful holder of the document or token; and
- Interface with BCS and watchlists to determine eligibility to pass border controls according to pre-defined rules.

When ABCs are integrated with national BCS they can complete checking of eMRTD security features, authenticate the document as genuine and confirm that the data in the IC chip has not been altered. When these checks are completed, the biometric matching undertaken by the ABC can reliably confirm, in the absence of a successful presentation (i.e. spoofing) attack, that the traveller presenting at the kiosk or eGate is not an impostor.

ABC interfaces with travellers are typically kiosks that are configured as automated gates. The traveller presents the travel document to the kiosk document reader interface. The kiosk communicates with the BCS, which returns a

message allowing the traveller to pass, provided all the checks required by the programmed algorithm are met.

ABC solutions can improve the assurance of traveller identity, the efficiency of traveller processing and the traveller experience. ABC solutions can typically process each traveller in less than 30 seconds, simultaneously achieving security and facilitation benefits for States.

For their effective operation, ABCs use and rely on the implementation of the other technical topics of this Guide.

HOW IT WORKS – BORDER CONTROL AGENCIES

States determine traveller eligibility to use a national ABC solution. The eligibility criteria will be determined by security, efficiency and traveller convenience criteria. To maximise usage and benefits to citizens, adult nationals will usually be eligible. Young children may be excluded due to unreliable biometric matching performance, and the impact this would have on process efficiency and the reliability of identity verification. Foreign nationals might be allowed access to an ABC solution where, for example, security risks are low, efficiency benefits are high, and there is a close relationship between the States.

ABC allows eligible travellers to use a self-service border processing system when entering or leaving a State. In high volume processing environments where a cost benefit analysis justifies an ABC solution, self-service terminals can improve the personnel-to-traveller clearance ratio and allow the redeployment of border control officers to other security and facilitation tasks.

The system will admit travellers through the automatic gates, provided that the traveller meets the identity and eligibility requirements programmed into the solution. In the most common application of ABC, the eMRTD is used as the identity token, and checked as:

- Genuine and unaltered using ePassport Public Key Infrastructure (PKI) authentication⁵⁸;
- Carried by the genuine holder by a:
 - Search of INTERPOL's SLTD database⁵⁹; and
 - Comparison of the biometric – facial, iris or fingerprint – image read from the Integrated Circuit (IC) chip of the eMRTD with an image of the same feature taken from the traveller⁶⁰.

58 See: *Topic J – Public Key Infrastructure and the ICAO Public Key Directory*

59 See: *Topic L – Database of Stolen and Lost Travel Documents*

60 See: *Topic K – eMRTD Biometric Identity Verification*



Travellers approach the ABC system and present their eMRTD to the integrated passport reader. This may happen at the entrance to the eGate in double gate designs, at a separate kiosk, or within the biometric capture zone. Once the document's authenticity has been checked, data is typically sent to watchlists for automated matching. Watchlist matches result in referral to border control officers for resolution.

When the system refers travellers as 'failure to match', the biometric verification of identity undertaken in eGates needs to be supported by business protocols for confirming identity. The secondary examination must strike an appropriate balance between the likely error in the referral of a genuine identity and the much less common instance of actual identity fraud.

In best practice jurisdictions, ABC gates are monitored by border control officers working close to the eGates. The number of eGates to be monitored, and the period of monitoring to be completed in each shift need to be carefully designed to maintain officers' motivation and performance.

All ABC systems need to be linked to watchlists containing lists of both travel documents and travellers⁶¹. ABC systems integrated with API and/or PNR analysis systems can allow travellers to be risk-assessed *before* they use the ABC, so that targeted travellers can be directed immediately for secondary examination upon presentation of their MRTD to the ABC interface.

HOW IT WORKS – AIRLINES

In many States, airlines use self-service kiosks to wholly or partially automate the check-in process for travellers. These airline kiosks typically issue boarding passes and print baggage tags. Increasingly, applications of ABC involve partnerships between airport owners and border control agencies to install eGates.

More recently the trends towards automation of travel are converging in integrated solutions that use identifying information about travellers to link and automate airline and airport security processing to border controls – from check-in to boarding, and from disembarkation to leaving the airport terminal.

For some border control agencies, these integrated solutions that focus on the commencement of travel provide opportunities to invest in the creation of more accurate records of traveller details at the departure phase.

BENEFITS AND OPPORTUNITIES

ABC has process efficiency benefits, as it enables agencies to process a higher number of low-risk passengers quickly and conveniently, while maintaining border security and integrity. This helps optimize the process, and allows agencies to redeploy resources to focus on potentially higher-risk travellers.

The processing capacity of eGates is sustained over time – eGates perform repetitive and monotonous tasks without fatigue. Additionally, ABCs conduct an objective, repeatable set of checks to complete identity and document authentication that, subject to the programmed logic, can be more accurate and quicker to complete than similar checks conducted by humans.

Within the constraints of the physical space available, ABCs provide States with a scalable solution for meeting the processing challenge of increasing international air travel.

The eligibility checks undertaken at ABC checks are automatic and mandatory, reducing the opportunity for them to be forgotten or avoided, and ABC systems are readily auditable.

61 See: *Topic E – National Watchlists* and *Topic M – International Watchlists*

In some States, Registered Traveller (also known as ‘Trusted Traveller’) programmes use ABC to process a set of travellers who, because of their nationality or immigration status, are assessed as low risk. Participants in such programmes will be enrolled and vetted by border control agencies before being allowed to use the system. Enrolment may allow travellers to avoid more rigorous screening at the border, the requirement to make customs declarations and/or complete disembarkation cards. Watchlist checks will still be carried out, and travellers can be required to submit to comprehensive screening.

Extending the use of ABC to include registered travellers improves the business case for ABC implementation and allows officers at the conventional control to focus on high-risk travellers. Whether the various benefits outweigh the significant capital investment costs should be the subject of a cost/benefit or other analysis or evaluation. Since the quantum of the costs and benefits varies with each implementation, the required analysis is unique to each project.

TECHNICAL ISSUES

ABC solutions are heavily dependent on technology. While eGates themselves are modular, they generally require: a reliable, consistent power supply, extensive cabling, efficient support and maintenance, and an operating environment free from extremes of heat, dust, humidity and light.

For effective operation, eGates and kiosks at which travellers self serve must be designed with careful attention to human factors.

The positioning and content of signage and on-screen instructions, with coverage of languages aligned to usage, is critical. These human factors are in part culturally determined, and are also significantly influenced by the familiarity

of the local traveller population with similar technology interfaces. Kiosks and eGates should be located to facilitate efficient queuing and onward movement to the next airport touch point.

RELATED REQUIREMENTS

- ✓ ICT integration of eGate document readers with a national BCS.
- ✓ Reliable MRZ read performance of MRTDs and eMRTDs eligible to use the eGates⁶².
- ✓ Assurance that the evidence of identity presented by the traveller:
 - Is genuine and unaltered, e.g. by some combination of database verification and eMRTD PKI authentication⁶³; and
 - Is in the possession of the traveller to whom it was issued, e.g. by reference to national, international watchlists and the SLTD database⁶⁴.
- ✓ Verification of the identity of the traveller (e.g. by biometric comparison of images of travellers with reference samples⁶⁵).
- ✓ Integration with national watchlists, international watchlists and current and prior travel data into the BCS, to ensure automated assessment of traveller risk and appropriate interventions can be made.
- ✓ Access control arrangements to assure that travellers do not evade the ABC eGate or kiosk.
- ✓ ICT integration of a BCS to write to, and read from, a national entry and exit database⁶⁶.
- ✓ Reliable, continuous supply of electricity and network connectivity.



62 See: *Topic B – Document Readers*

63 See: *Topic J – Public Key Infrastructure and the ICAO Public Key Directory*

64 See: *Topics E – National Watchlists and L – INTERPOL Database of Stolen and Lost Travel Documents*

65 See: *Topics C – Biometric Identity Verification and K – eMRTD Biometric Identity Verification*

66 See: *Topic E – Entry and Exit Databases*

RISKS AND COST MITIGATION

ABC is an expensive investment and therefore deserves a comprehensive cost-benefit analysis and a strong business case. Many international airports are simply not busy enough to justify the capital investment in ABC. The cost impact on States of ABC systems would include: ongoing maintenance and support, development of a national ABC programme concept, acquisition of necessary software and hardware⁶⁷, BCS integration, a coherent plan for biometric enrolment, and training of relevant personnel.

ABC may be viewed negatively by personnel who feel that the system may put their jobs at risk or devalue their skills and experience. This may lead to demotivation, and possible lack of care in checking passengers rejected by the eGates. Comprehensive training, agreement of working conditions and business processes, and an internal communication plan are all important elements that need to be in place before the ABC system goes live.

To help genuine travellers, and to ensure that criminals or terrorists do not attempt to defeat the controls of the ABC system, eGates and kiosks should be located where they can be monitored by border control officers. This monitoring can include Closed Circuit Television (CTV) surveillance, but should also include a human presence.

Most eGate solutions interface with eMRTDs. In the most common implementations, ePassport PKI authentication is undertaken; then the facial (or fingerprint) image biometric from the eMRTD is used as a reference sample in a 1:1 biometric verification of identity. In these applications it is critical that the PKI certificate trust chain is fully checked and that certificate non-conformance issues are identified and managed.⁶⁸

However, there are also many eGate solutions that:

- Do not use eMRTDs as the token;
- Use eMRTDs as the token but do not undertake ePassport PKI verification; or
- Use ePassport PKI verification for establishing that the token is genuine and unaltered, but use a biometric reference sample obtained elsewhere (e.g. from a trusted traveller enrolment, or a visa or ETS enrolment, or an on-arrival enrolment).

In these alternative system architectures, it is critical that the ABC solution uses other mechanisms to confirm that the travel document is genuine, unaltered and remains in the hands of the traveller to whom it was issued. In national applications, this may be achieved, for example, by appropriate comparisons with traveller records in national databases⁶⁹.

The ABC solution should be designed to achieve adequate protection of the sensitive personal information of travellers.

There must always be a fall-back strategy if the ABC fails (e.g. because of a power outage) or is otherwise unavailable (e.g. because of lack of personnel) to ensure that the border clearance of travellers can continue to function.

Risk management of ABC systems is important for ensuring system continuity and the security and integrity of borders. The development of dedicated risk management plans and mitigation strategies for ABC systems and the completion of regular system audits are essential.

BEST PRACTICE EXAMPLES

Statistical modelling of traveller flow should be conducted before a case for ABC is made. Queue lengths and waiting time standards should be assessed and modelled.

The physical configuration and location of eGates needs to be planned carefully to ensure that they fit into the available floor space, allow adequate space for traveller queuing, and are not in an environment prone to sudden and extreme changes in temperature, ambient light or humidity.

To allow supervision of the eGates, monitoring stations should be near enough to allow border control officers to observe travellers' behaviour and, if necessary, to intervene to facilitate or secure travel.

It may be necessary to coordinate between agencies responsible for travel document issuance and BCM to ensure that ABCs have integrated access to the most recent PKI certificates, watchlist and other data required to securely facilitate passenger processing.

67 Guidance for authorities planning to implement major upgrades of their current travel documents and related systems including all aspects of the procurement plan: *ICAO Guide for Collection of Best Practices for Acquisition of Machine Readable Travel Document Goods and Services*, Version 1, ICAO, March 2016, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

68 See: *Topic J – Public Key Infrastructure and the ICAO Public Key Directory*

69 See: *Topic C – Biographic Identity Verification* and *Topic D – Biometric Identity Verification*

Border control officers should be adequately trained and have working conditions that promote healthy work and motivation. Border control officers monitoring an ABC system should be rotated regularly to other duties, to ensure their effectiveness is maintained.

Adequate signage and ensuing assistance to travellers who have difficulty using ABC kiosks is essential.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Extract from ICAO Annex 9 – *Facilitation*, Chapter 3 – Entry and departure of persons and their baggage⁷⁰:

I. Inspection of travel documents

“ ...

3.35.4 **Recommended Practice.**— *Each Contracting State should consider the introduction of Automated Border Control (ABC) systems in order to facilitate and expedite the clearance of persons entering or departing by air.*

3.35.5 **Recommended Practice.**— *Contracting States utilizing ABC systems should, pursuant to 3.9.2 and 3.10.1, use the information available from the PKD to validate eMRTDs, perform biometric matching to establish that the passenger is the rightful holder of the document, and query INTERPOL Stolen and Lost Travel Documents (SLTD) database, as well as other border control records to determine eligibility for border crossing.*

3.35.6 **Recommended Practice.**— *Contracting States utilizing ABC systems should ensure that gates are adequately staffed while operational to ensure a smooth passenger flow and respond rapidly to safety and integrity concerns in the event of a system malfunction....”*

SOURCES FOR FURTHER INFORMATION

References

Annex 9 – Facilitation to the Convention on International Civil Aviation, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

ICAO Guide for Collection of Best Practices for Acquisition of Machine Readable Travel Document Goods and Services, Version 1, ICAO, March 2016, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

Other Sources

Automated Border Control Implementation Guide, IATA, ACI and FRONTEX, December 2015, available at: <http://www.iata.org/whatwedo/passenger/Documents/ABC-Implementation-Guide-2nd-Edition.pdf>

Best Practice Operational Guidelines for Automated Border Control (ABC) Systems, FRONTEX, September 2015, available at: http://frontex.europa.eu/assets/Publications/Research/Best_Practice_Operational_Guidelines_ABC.pdf

Best Practice Technical Guidelines for Automated Border Control (ABC) Systems, FRONTEX, September 2015, available at: http://frontex.europa.eu/assets/Publications/Research/Best_Practice_Technical_Guidelines_ABC.pdf

Guidelines for Processing of Third Country Nationals through Automated Border Control, FRONTEX, September 2015, available at: http://frontex.europa.eu/assets/Publications/Research/Guidelines_for_Processing_of_Third_Country_Nationals_through_ABC.pdf

⁷⁰ *Annex 9 – Facilitation to the Convention on International Civil Aviation*, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

Interoperable Applications

Interoperable Applications enable global sharing of data contained in MRTDs and about travellers obtained from national, regional and international sources. They enable sharing of data created or obtained from outside a State to supplement data from national sources to inform traveller identification and risk assessment. Interoperable Applications are global. They provide a timely, secure and reliable linkage of inspection systems (e.g. airlines to State) or share additional data essential to authentication of the MRTD and/or identity verification (e.g. ICAO PKD, INTERPOL SLTD database and international watchlists).

Authenticated traveller identity data is available through visa systems and from BCS at entry and departure controls. The ICAO PKD extends and strengthens this authentication. Verified traveller identity data is available from airline departure control systems in the form of API. Additional unverified information about travellers is available from

airline reservation systems in the form of PNR. When combined with authenticated identity data and intelligence from national sources, airline data (API and PNR) support traveller identification and risk assessment.

In best practice jurisdictions, international watchlists – including the CUNSCSL and INTERPOL Red Notices, and the INTERPOL SLTD database – are integrated with BCS to prevent or to disrupt travel. International watchlists assist States in meeting their international obligations to combat terrorism and other transnational crime by identifying risk targets for border interventions.

The six Interoperable Applications described in this Section are used at specific or multiple phases of the traveller journey (pre-departure, pre-arrival, entry, stay and exit) and each contribute, to different degrees, to the identification of travellers and/or to traveller risk assessment.



H. ADVANCE PASSENGER INFORMATION AND INTERACTIVE ADVANCE PASSENGER INFORMATION



An *Interoperable Application for Traveller Identification & Risk Assessment* receives advance notice from airlines of travel, giving border control agencies additional time to complete a more detailed traveller identification and risk assessment. Such a system facilitates pre-clearance, and

in the case of iAPI, allows the State to prevent travel commencing by returning a message to airline check-in to refuse boarding.

KEY MESSAGES

- ✓ Travel document and flight information relating to arriving or departing travellers is sent directly to border control agencies by carriers.
- ✓ Facilitates process efficiencies for both border control agencies and airlines, including full or partial pre-clearance of flights and risk-based targeting of passengers prior to arrival.

OVERVIEW

API is an electronic communication system where data elements is collected and transmitted to border control agencies at check-in prior to flight departure (this includes joining travellers at points of transit) and made available to BCS at airports of subsequent transit and final destination. API data can be divided into two distinct categories: a) data relating to the flight, available to air transport operators from their own automated systems; and b) data relating to each individual passenger and aircraft crew member, corresponding to the items of data readable from the MRZ of MRTDs.

A standard electronic message, called the UN Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT) Passenger List Message (PAXLST) message

was developed to standardise the electronic transmission of passenger and aircrew manifests. The PAXLST message comprises two messages: the first a 'legacy' or 'batch' transmission for all passengers on the specified flight; and the second for crew members on that flight. The two messages may be transmitted separately or combined into one transmission.

API data can also be transmitted as individual records for each traveller, a configuration known as iAPI. iAPI is an electronic system that transmits API data elements collected by the aircraft operator during check-in directly to border control agencies. While the traveller is at passenger check-in, border control agencies return a standardized response message, called CUSRES (Custom Response) message, to the airline operator for each passenger and/or crew member. The response message confirms either that the traveller is "OK to board", or denies boarding authority and directs the carrier to "refer to national authorities".

WCO, IATA and ICAO have jointly agreed on the maximum set of API data that may be incorporated in the PAXLST message for transmission. For the message format for API data transmissions, ICAO mandates through Annex 9 – *Facilitation*⁷¹ that the API information required by States should conform to specifications for the PAXLST message.

This harmonised approach to collecting and transmitting data to border control agencies via a single and globally interoperable message structure and format avoids the unnecessary complexity in systems that would otherwise be needed to support multiple data exchange processes.

The UN/EDIFACT rules comprise a set of internationally agreed standards, directories and guidelines for the electronic interchange of structured data, particularly where it relates to trade in goods and services between independent, computerized information systems.

WCO, IATA and ICAO provide complete guidelines on API⁷² as well as a toolkit that outlines the basics on passenger data exchange⁷³.



71 *Annex 9 – Facilitation to the Convention on International Civil Aviation*, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

72 *Advance Passenger Information Guidelines*, Version 3.0, WCO/IATA/ICAO, October 2013, <https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx>

73 *IATA/WCO/ICAO Toolkit: presentation slides*, IATA, 2013, available at: <http://www.iata.org/iata/passenger-data-toolkit/presentation.html>

HOW IT WORKS – BORDER CONTROL AGENCIES

API can be used for risk-based targeting and to complete watchlist checks – either manually or automatically – since it contains the following data elements for all passengers and crew on a flight:

- Full name (as it appears on the MRTD, except where the name is truncated because it includes more than the available number of characters in the first line of the MRZ)
- Date of birth
- MRTD number
- State or organization issuing the MRTD
- MRTD expiry date
- Nationality
- Sex
- Data relating to the flight (including flight number, departure/entry date and time and airport of origin and destination)

Care should be taken to ensure name matching in watchlist systems is configured to search variations in name-order, the number of names, alternative spelling due to cultural and other factors, and any known name changes. Variations in spelling may be a result of transliteration from other alphabets, issuance errors or attempts to avoid detection. Watchlist searches should anticipate common phonetic and typographical errors and make compensatory searches. The application of watchlists is discussed further in *Topics E – National Watchlists* and *M – International Watchlists*. The initial design and configuration of watchlists is complex and technical assistance may be required.

Where States do not have an entry-departure recording system at both in and outbound controls, API can be used to reconcile entries and departures of travellers⁷⁴. Because some API data may be manually entered by airline check-in personnel, data accuracy is not always assured.

HOW IT WORKS – AIRLINES

Biographic data for API are typically captured either from travel documents at check-in or, as it is becoming more common, from declarations made by passengers themselves when making online reservations or checking in. In the latter case, the data is confirmed by the airline when the passenger presents their boarding pass at the airport.

Airlines may store API for frequent flyers so that it does not need to be captured before each flight, although this requires that airlines update details when travellers replace their travel documents.

Where airlines fail to send API data for some or all passengers, this may result in delayed departure of aircraft and charges or fines being levied by destination States.

For iAPI, traveller data can be sent progressively from when check-in opens from up to 72 hours in advance of travel until check-in is closed.

Adequate training of airline personnel is essential to ensure they understand the requirements of the States receiving the API data.

BENEFITS AND OPPORTUNITIES

Implementation of API, an ICAO Standard, supports States to fulfil their international obligations under UNSCR resolutions pertaining to counter-terrorism⁷⁵, notably 2178 (2014), 2309 (2016) and 2396 (2017).

Provided the API data is timely and accurate, they improve facilitation and reduce bottlenecks in border processing by enabling full or partial pre-clearance of flights. They also enable States to use border security resources more effectively and efficiently.

API can be used by border control agencies to complete automated searches:

- Of MRTD document numbers which have been reported as lost or stolen (by reference to the INTERPOL SLTD);
- To check the MRTD expiry date (including cross verification against entry and exit and travel document issuance databases),
- Of watchlists to identify suspect travellers; and
- To profile traveller attributes according to risk.

iAPI makes it possible to prevent travel, thus enhancing aviation security and border control processes.

⁷⁴ See: *Topic E – Entry and Departure Databases*

⁷⁵ See: *Section 3.6 International Law*

API can be analysed to provide entry and departure statistics (e.g. by nationality, sex, age, period of travel), and a basic reconciliation between the entry and departure of individual travellers⁷⁶.

Analysis of API can provide border control agencies with a more detailed picture of their State's border traffic, to identify emerging risks and threats.

API can be used to control access to ABC kiosks or eGates to passengers risk-assessed in advance by the national border control authorities.

For all these reasons, where implemented API should be used for *all* incoming and outgoing airlines so that API information is available on all travellers – whether arriving, departing or in transit.

TECHNICAL ISSUES

Collecting, formatting, transmitting, processing and storing API – 24 hours a day, 365 days a year – requires the procurement of a professionally designed system that can consistently and reliably handle these operations.

Since names are read from the MRZ, the transliteration from non-Latin alphabets may reduce matching performance with national or international watchlists.

The investment required for the development of a new API/iAPI capability is substantial. Significant costs are involved for software development (or acquisition), hardware (e.g. servers, switches), IT system linkage, testing and training. Ideally a 'Passenger Data Single Window', API should be received at a single point, and seamlessly distributed by the receiving agency to the other border control agencies that require it.

API relies on standardized, interoperable interfaces between airline and border control agency systems. Several ICT systems integrators and communication providers specialize in procuring API and iAPI solutions. States should seek vendor independent, solution neutral advice prior to decisions to implement API or iAPI. There will need to be a contract with a technical vendor; and day-to-day operation should be monitored to ensure compliance with technical and contractual standards. Reviews should take place from time to time to check that the contract delivers value for money.

iAPI requires 24/7 365-day operational support to manage the "OK to board" government responses to airline queries about every individual traveller. iAPI can be implemented independent of, or in conjunction with an ETS. When implemented in conjunction with an ETS, richer data is available to border control authorities for analysis, but the system integration is more complex and, as a result, more expensive.

API and iAPI processing centres need to be in a secure location with a backup power supply and reliable, secure communication links.

RELATED REQUIREMENTS

- ✓ National legislation requiring airlines to provide API data.
- ✓ MoUs with airlines.
- ✓ Protocols and business processes for sharing of API data between border control agencies to ensure single window collection.
- ✓ Handling of personal information from API to meet national privacy and data protection legislation.
- ✓ ICT integration of BCS to receive and interface with API data.
- ✓ Reliable, continuous supply of electricity and connectivity at a 24/7 operations centre.

RISKS AND COST MITIGATION

For travellers who do not require a visa, receipt of API data collected and transmitted by airlines is the first notice border control agencies receive of impending travel. A good relationship between border control agencies and each airline, supported by a clear legal framework and effective operating protocols, is required.

Airlines are responsible for collecting and transmitting API.

Border control agencies should have in place a system to receive, store securely, analyse and act upon API data. Failure to manage an API system properly could lead to a breakdown of cooperation with airlines and place the airline, and possibly the border control agency, at risk of litigation – especially if data is lost or disclosed in an unauthorised or illegal manner.

⁷⁶ See: *Topic E – Entry and Exit Databases*

Border control agencies should carefully consider how API is delivered and by whom. There may be transaction charges for each API message received and the fees can accumulate to be a significant cost.

API infrastructure can be shared at the regional level to extend access to API to Member States who might not otherwise have been able to make the required investment.

BEST PRACTICE EXAMPLES

There should be primary legislation in place to allow API to be collected and processed, and to require airlines to provide it. Delegated or secondary legislation (in the form of regulations or MoUs) are desirable to manage the everyday use of API. Guidance provided to airlines should clearly describe what is required from them. Delegated or secondary legislation should be reviewed from time to time to ensure it meets the needs of border control agencies in the face of changing travel patterns and threats.

States should ensure that API relationships with airlines are conducted with consistency and fairness, and with due regard to the commercial and operational realities of airline operations.

If API is obtained it should be *used*. States should seek to increase their capacity and capability to analyse and effectively use API data, and to sustain this capacity and capability over time.

Due regard needs to be paid to data protection and privacy legislation in each State handling API, and to the legitimate expectations of passengers that their personal data will be handled properly.

Depending on local legislation, data sharing agreements may be required where API is shared with regional partners or other government departments.

Sharing infrastructure is one way to reduce the cost and better utilize the human capability required for a successful API project. API infrastructure can be shared at the regional level to extend access to API to States that might not otherwise have been able to make the required investment.

One such example is an arrangement by the Implementing Agency for Crime and Security (IMPACS) of the Caribbean Community (CARICOM), through which the collection, processing and analysis of API data for regional traffic is carried out at the centralized Joint Regional Communications Centre (JRCC), which then relays alerts and advice on interventions to the relevant authorities at the destination States for their action prior to the entry of suspect travellers.

The appropriate elements of API should be matched against all agency and accessible international watchlists as soon as possible after receipt, and certainly before the arrival in the State of the flight.

Alerts raised by possible matches should be assessed for accuracy and relevance before dissemination to border control officers at primary inspection.

There should be an avenue of redress or appeal if a traveller claims not being the subject of the alert.

As a background activity, API should be analysed for changes in traffic patterns, profiles of passengers, or other items of intelligence interest.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Annex 9 – Facilitation, Chapter 9. Passenger Data Exchange Systems⁷⁷:

A. General

9.1 **Recommended Practice.**— *Contracting States requiring the exchange of Advance Passenger Information (API), interactive API (iAPI) and/or Passenger Name Record (PNR) data from aircraft operators should create a Passenger Data Single Window facility for each data category that allows parties involved to lodge standardized information with a common data transmission entry point for each category to fulfil all related passenger and crew data requirements for that jurisdiction.*

9.2 **Recommended Practice.**— *Contracting States and aircraft operators should provide the appropriate level on a 24/7 (continuous) basis, of operational and technical support to analyse and respond to any system outage or failure in order to return to standard operations as soon as practicable.*

9.3 **Recommended Practice.**— *Contracting States and aircraft operators should establish and implement appropriate notification and recovery procedures for both scheduled maintenance of information systems and non-scheduled system outages or failures.*

9.4 **Recommended Practice.**— *Contracting States and aircraft operators should provide the appropriate level (where practicable, a 24/7 arrangement) of contact support.*

B. Advance Passenger Information (API)

9.5 Each Contracting State shall establish an Advance Passenger Information (API) system.

Note.—The UN Security Council, in Resolution 2178 (2014), at paragraph 9, “[c]alls upon Member States to require that airlines operating in their territories provide advance passenger information to the appropriate national authorities in order to detect the departure from their territories, or attempted entry into or transit through their territories, by means of civil aircraft, of individuals designated by the Committee established pursuant to resolutions 1267 (1999) and 1989 (2011) (“the Committee”), and further calls upon Member States to report any such departure from their territories, or such attempted entry into or transit through their territories, of such individuals to the Committee, as well as sharing this information with the State of residence or nationality, as appropriate and in accordance with domestic law and international obligations.”

9.6 The API system of each Contracting State shall be supported by appropriate legal authority (such as, inter alia, legislation, regulation or decree) and be consistent with internationally recognized standards for API.

Note 1.— API involves the capture of a passenger’s or crew member’s biographic data and flight details by the aircraft operator prior to departure. This information is electronically transmitted to the border control agencies in the destination or departure country. Thus, passenger and/or crew details are received in advance of the departure or arrival of the flight.

⁷⁷ Annex 9 – Facilitation to the Convention on International Civil Aviation, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

Note 2.— The UN/EDIFACT PAXLST message is a standard electronic message developed specifically, as a subset of UN/EDIFACT, to handle passenger manifest (electronic) transmissions. UN/EDIFACT stands for “United Nations rules for Electronic Data Interchange For Administration, Commerce and Transport.” The rules comprise a set of internationally agreed standards, directories and guidelines for the electronic interchange of structured data, and in particular that related to trade in goods and services between independent, computerized information systems. The WCO, IATA and ICAO have jointly agreed on the maximum set of API data that should be incorporated in the PAXLST message to be used for the transmission of such data by aircraft operators to the border control agencies in the destination or departure country. It is to be expected that the UN/EDIFACT standard may be supplemented by modern message techniques, such as international xml standards or web-based applications.

Note 3.— Under its current format structure the UN/EDIFACT PAXLST message will not accommodate general aviation usage.

Note 4.—Internationally recognized standards for API are currently defined by the WCO/IATA/ICAO guidelines.

9.7 Recommended Practice.— *Each Contracting State developing legislation for the purpose of implementing an API system should consider developing aligned regulations that meet the needs of all involved agencies, defines a common set of API data elements required for that jurisdiction in accordance with message construction standards and appoints one government agency to receive API data on behalf of all other agencies.*

9.8 When specifying the identifying information on passengers to be transmitted, Contracting States shall require only data elements that are available in machine readable form in travel documents conforming to the specifications contained in Doc 9303. All information required shall conform to specifications for UN/EDIFACT PAXLST messages found in the WCO/IATA/ICAO API Guidelines.

9.9 When seeking to implement a national Advance Passenger Information (API) Programme, Contracting States that are unable to comply fully with the provisions contained in 3.48.1 9.8 with respect to data element requirements shall ensure that only those data elements that have been defined for incorporation into the UN/EDIFACT PAXLST message are included in the national Programme’s requirement or follow the WCO’s Data Maintenance Request (DMR) process for any deviation from the standard.

9.10 Recommended Practice.— *Contracting States should seek to minimize the number of times API data is transmitted for a specific flight.*

9.11 If a Contracting State requires API data interchange, then it shall seek, to the greatest extent possible, to limit the operational and administrative burdens on aircraft operators, while enhancing passenger facilitation.

9.12 Recommended Practice.— *Contracting States should refrain from imposing fines and penalties on aircraft operators for any errors caused by a systems failure which may have resulted in the transmission of no, or corrupted, data to the public authorities in accordance with API systems.*

9.13 Contracting States requiring that passenger data be transmitted electronically through an Advance Passenger Information system shall not also require a passenger manifest in paper form.

9.14 Recommended Practice.— *Each Contracting State should consider the introduction of an interactive Advance Passenger Information (iAPI) system.*

9.15 Recommended Practice.— *Contracting States seeking to implement an Interactive Advance Passenger Information (iAPI) system should:*

a) seek to minimize the impact on existing aircraft operator systems and technical infrastructure by consulting aircraft operators before development and implementation of an iAPI system;

b) work together with aircraft operators to develop iAPI systems that integrate into the aircraft operator's departure control interfaces; and

c) conform to the Guidelines on Advance Passenger Information (API) adopted by WCO/ICAO/IATA when requiring iAPI.

9.16 **Recommended Practice.**— Contracting States' and aircraft operators' API systems, including iAPI, should be capable of 24/7 operation, with procedures in place to minimize disruption in the event of a system outage or failure..."

SOURCES FOR FURTHER INFORMATION

References

Advance Passenger Information Guidelines, Version 3.0, WCO/IATA/ICAO, October 2013, <https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx>

Annex 9 – Facilitation to the Convention on International Civil Aviation, Fifteenth Edition, ICAO, Montreal, October 2017, available at purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

IATA/WCO/ICAO Toolkit: presentation slides, IATA, 2013, available at: <http://www.iata.org/iata/passenger-data-toolkit/presentation.html>

Threats to international peace and security caused by terrorist acts, S/RES/2178 (2014), United Nations, 2014, available at: <http://www.un.org/en/sc/documents/resolutions/>

Threats to international peace and security caused by terrorist acts: Aviation security, S/RES/2309 (2016), United Nations, 2016, available at: <http://www.un.org/en/sc/documents/resolutions/>

Other sources

IATA provides numerous supporting documents on Passenger data exchange systems, including API and iAPI:

IATA Control Authorities Working Group API Statement of Principles, IATA, May, 2007, available at: <http://www.iata.org/iata/passenger-data-toolkit/library.html>

IATA Control Authorities Working Group iAPI Statement of Principles, IATA, October, 2015, available at: <http://www.iata.org/iata/passenger-data-toolkit/library.html>

IATA Passenger and Airport Data Interchange Standards (PADIS) EDIFACT Implementation Guide, IATA Version 13.1 2013, available at: <http://www.iata.org/iata/passenger-data-toolkit/library.html>

IATA Air Transport & Travel Industry: Principles, Functional and Business Requirements PNRGOV IATA Version 13.1 August, 2013, available at: <http://www.iata.org/iata/passenger-data-toolkit/library.html>

IATA Guide to Facilitation, Second Edition, IATA, August 2015, available at: <http://www.iata.org/publications/Documents/toc-igf-02-20150709.pdf>

The following are sources of information about API, its contents and format:

A sample of legislation and guide lines for the supply of API is provided by the European Union: *The obligation of airlines to communicate passenger data offers some guidelines on API*, The European Union's Directive 2004/82/EC, European Union, 29 April 2004, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:261:0024:0027:EN:PDF>

An example of technical specifications for API supply by commercial carriers (to the USA): *Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels*, Vol. 72 No. 163, Department of Home Security, The United States government, 23/08/2007, available at: https://www.cbp.gov/sites/default/files/documents/apis_pre_departure_3.pdf

An example of technical specifications for API supply by general aviation (to the USA): *CBP Private Air APIS Guide*, Version 3.0, Office of Field Operations, US Customs and Border Protection, January 2015, available at: <https://www.cbp.gov/sites/default/files/documents/CPB%20Private%20Air%20Guide%203%200%20%28Jan%202015%29.pdf>

An example of quality standards for API supply (to the USA): *CBP Air APIS Guide – System Identified Errors and Manifest Sufficiency Rates: API Quality standards for the United States Bureau of Customs and Border Protection (CBP)*, Version 3, US CBP, April 2008, available at: https://www.cbp.gov/sites/default/files/documents/air_guide_2.pdf

An example of a schema for supply of API in XML format (to the UK Border Force): *explanatory-text.xls*: UK's format specification, UK Government 18/11/2011 available at: <https://www.gov.uk/government/publications/transfer-e-borders-data-general-aviation-and-maritime>

I. PASSENGER NAME RECORD



Obtained from airline reservation systems prior to travel commencing, this **Interoperable Application for Traveller Risk Assessment** consists of extensive contextual information to supplement the biographic and biometric data available from MRTDs and other sources.

KEY MESSAGES

- ✓ Arriving or departing traveller reservation information accessed by or sent to border control agencies for targeting individuals according to risk-based profiles.
- ✓ Useful for pre-entry / post-departure risk assessment, as well as identification of persons of potential higher risk based on patterns of travel over time.
- ✓ Most effective when used with other traveller data, including API and travel history.

OVERVIEW

The term Passenger Name Record (PNR) refers to data about travellers obtained from airline reservation systems collected at the time that flight bookings are made. Because the reservation systems of each airline and associated global distribution systems need to communicate with each other, airline systems are interoperable. The basis of this interoperability is the PNR unique record locator, a string of six alphanumeric characters. However, the scope and completeness of data collected varies between systems.

PNR data reveals and allows information to be inferred about when and how reservations were made:

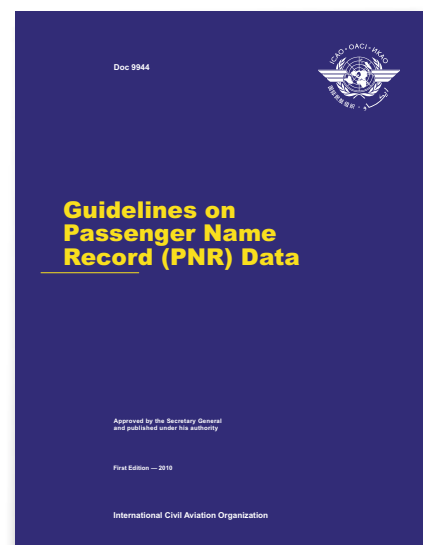
- The number of travellers;
- Their identifying details;
- The method of payment;
- Passenger contact information;
- Routing;
- Class of travel;
- Meal selection; and
- Other details about the traveller and intended travel.

Consequently, PNR data reveals sensitive, personal and financial information about travellers that, by its nature, requires adequate protection against misuse.

States requiring PNR information from airlines need clear national legislation defining: which data elements can be obtained, how and to where the data should be delivered, who can access the data, how they will be used and in what form, and for how long they will be retained. This legislative authority for the collection, use, retention and disposal of PNR data should be supported by a broader national framework of legislation, policy and practice for privacy and data protection.

The primary legal jurisdiction for airlines is the State in which they are incorporated. Airlines are also subject to the laws of the States in which they operate, including transit stops and flight paths over those countries. The net impact of operating in overlapping legal jurisdictions is that to provide PNR data, airlines must meet the legal requirements of all States of origin, transit and overflight.

PNR is most effective when it is obtained for all travellers, on all flights. Therefore, States intending to obtain and use PNR can do so only after establishing national frameworks of legislation, policy and practice that meet international privacy and data protection norms, as per the ICAO Doc 9944 Guidelines on PNR Data⁷⁸. Foreign airlines will, in general, only provide PNR to a State in which they are operating if MOUs or other inter-governmental agreements are in effect.



⁷⁸ *Guidelines on PNR Data*, First Edition, Doc 9944, ICAO, Montreal, 2010, available to purchase at: <https://store1.icao.int/index.php/guidelines-on-passenger-name-record-pnr-data-doc-9944-english-printed.html>

PNR data can also include API data elements. This is achieved by the airline reservation system requiring travel document details corresponding to the data elements in the MRZ of MRTDs. The data elements are obtained during booking, or subsequently, pre-departure. API exchange is an ICAO Standard to enable border authorities to better identify travellers and assess risk and threat⁷⁹.

The WCO, IATA and ICAO provide complete guidelines on PNR⁸⁰ and a toolkit that provides the basics on passenger data exchange⁸¹.

HOW IT WORKS – BORDER CONTROL AGENCIES

Depending on local legislation and the legislative obligations of operating airlines to other States, border control agencies will need to enter into a legal agreement or an MOU with airlines or reservation system owners to access PNR data. PNR data can be accessed via a dedicated airline terminal, or can be pulled or pushed to the border control agency's system via airline ICT systems.

There are commercially available systems that bundle PNR access with a set of processing and analysis tools.

PNR is most effective when used in combination with other data about travellers, such as travel history and API.

PNR can be used:

- Actively: To identify travellers whose combination of attributes suggests they pose a risk or threat; or to search data elements against those associated with known suspects (e.g. credit cards and telephone numbers); and
- Passively: As a reference database for the investigation of known suspects.

The active analysis of PNR data is a complex task requiring specialized skills, knowledge and experience. Vendors offer solutions with rules based algorithms to search for profiles or combinations of data elements. However, these profiles need to be checked for effectiveness and continually updated and tuned as known patterns of fraud and abuse change and new suspect travel patterns emerge.

Certain PNR elements (for example credit card and telephone numbers) can be compared against intelligence databases to identify known suspects or methods of offending.

Consistent with ICAO's SARPS, it is important that border control agency use of PNR minimizes the commercial impact on airlines. PNR should therefore be received by one single State system or agency – the Passenger Data Single Window – and disseminated, whether in raw form or after being processed into usable intelligence, to other agencies.

HOW IT WORKS – AIRLINES

Airlines hold personal data relating to travellers as well as details about their travel plans. PNR is the mechanism by which airline reservation systems share details about passengers who travel on more than one airline during their journey (i.e. interlining passengers). In a competitive business environment there is sensitivity about sharing such data unless there are enforceable guarantees about confidentiality. In addition, data sharing of the sensitive personal information is covered by data protection and privacy laws, and is only allowed once enabling legislation is in place.

Airline collection of PNR is for commercial purposes, using long established networks and protocols. The variation in the data elements available between airlines is a feature of PNR that cannot be changed easily or economically to suit border control agencies.

BENEFITS AND OPPORTUNITIES

Implementation of PNR allows States to support pre-entry/ departure risk assessment activities, thus improving the efficiency of border controls. Effective analysis of PNR data can often identify potential threats to aviation security and/ or national security and lead to pre-travel interventions.

The analysis of PNR data can link travellers to organized criminal activity, for example by identifying common elements with known past patterns of travel associated with the smuggling or trafficking of people, drugs and other contraband. These indicators can include unusual and illogical travel attributes.

79 See: *Topic H – Advance Passenger Information and Interactive Advance Passenger Information*

80 *Passenger Name Record Guidelines*, Version 13.1, WCO/IATA/ICAO, October 2013, <https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx>

81 *IATA/WCO/ICAO Toolkit: presentation slides*, IATA, 2013, available at: <http://www.iata.org/iata/passenger-data-toolkit/presentation.html>

TECHNICAL ISSUES

The value of PNR is that it contains additional information about travellers beyond the identity information available from travel documents. However, because these additional data elements differ from the biographic and biometric identity information recorded in BCS, PNR data requires specialized database and data analysis tools.

The richness of PNR data makes human analysis of the raw data impractical. Commercial systems are available to automatically search PNR for sequences of letters and groups of text and associations between individual records. This allows border control agencies to look for patterns that indicate to them that traveller behaviour is outside statistical norms or matches characteristics identified in intelligence analysis.

The logical search rules that allow such automatic triggers are developed as an investigative hypothesis and established in the PNR data analysis system, either by the solution provider or by national border control personnel, and reviewed and amended in the light of experience.

RISKS AND COST MITIGATION

PNR projects require multi-disciplinary expertise. Vendors offering PNR solutions can offer integration of ICT and can assist in developing human capability, but are less able to assist in establishing the necessary legal frameworks.

The analysis of PNR data requires sophisticated human capability to identify patterns, develop targeting hypotheses, and tune algorithms. For PNR data to be used effectively this analysis capability needs to be sustained and developed over time.

The analysis of PNR data takes time; consequently, PNR is less effective for short haul flights with a high proportion of late ticketing of travel. Like any application of technology, PNR projects should fit and reflect local circumstances.

PNR can be expensive to implement and operate. While the benefits can be significant, they can also be difficult to realise and sustain. A careful analysis of likely costs and expected benefits should be undertaken prior to any decision to invest in PNR, and States should seek solution neutral, vendor independent sources of advice.

Since carriers bear the costs of batching and transmitting PNR data, States have a responsibility to ensure the PNR data they request are consistent with ICAO SARPS, meet their needs, and that the data, once received, are actually used.

RELATED REQUIREMENTS

- ✓ National legislation authorising collection of PNR from airlines, including adequate privacy and data protection safeguards as described in ICAO Doc 9944, Guidelines on Passenger Name Record (PNR) Data.
- ✓ MOUs with airlines.
- ✓ Protocols and business processes for lawful sharing of PNR data between border control agencies.
- ✓ Data tools to combine for analysis data from national border inspection with PNR data.
- ✓ 24/7/365 capability to analyse PNR data in real time to develop actionable intelligence to identify suspects and target interventions according to risk.
- ✓ Reliable, continuous supply of electricity and connectivity at a 24/7 operations centre.

BEST PRACTICE EXAMPLES

Sharing infrastructure is one way to reduce the cost and better ensure the human capability required for a successful PNR project. PNR infrastructure can be shared at the regional level through an arrangement to extend access to PNR to States that might not otherwise have been able to make the required investment.

In many States, PNR data is analyzed in joint targeting centres staffed by representatives of immigration, customs, law enforcement and security agencies. By operating from a single location 24/7/365, targets can be identified and tasked to the appropriate border control agency prior to the entry of the traveller. Joint targeting centres help ensure that BCM is a response to multiple risks and threats faced by States.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Extracts from ICAO Annex 9 – Facilitation, Chapter 9. Passenger Data Exchange Systems⁸²:

A. General

9.1 **Recommended Practice.**— *Contracting States requiring the exchange of Advance Passenger Information (API), interactive API (iAPI) and/or Passenger Name Record (PNR) data from aircraft operators should create a Passenger Data Single Window facility for each data category that allows parties involved to lodge standardized information with a common data transmission entry point for each category to fulfil all related passenger and crew data requirements for that jurisdiction.*

9.2 **Recommended Practice.**— *Contracting States and aircraft operators should provide the appropriate level on a 24/7 (continuous) basis, of operational and technical support to analyse and respond to any system outage or failure in order to return to standard operations as soon as practicable.*

9.3 **Recommended Practice.**— *Contracting States and aircraft operators should establish and implement appropriate notification and recovery procedures for both scheduled maintenance of information systems and non-scheduled system outages or failures.*

9.4 **Recommended Practice.**— *Contracting States and aircraft operators should provide the appropriate level (where practicable, a 24/7 arrangement) of contact support. ...”*

D. Passenger Name Record (PNR) Data

9.22 Each Contracting States requiring Passenger Name Record (PNR) data shall align their data requirements and its handling of such data with the guidelines contained in ICAO Doc 9944, *Guidelines on Passenger Name Record (PNR) Data*, and in PNRGOV message implementation guidance materials published and updated by the WCO and endorsed by ICAO and IATA.

9.22.1 Contracting States requiring the transfer of PNR data, shall adopt and implement the EDIFACT-based PNRGOV message as the primary method for airline-to-government PNR data transferal to ensure global interoperability.

Note 1.— The PNRGOV message is a standard electronic message endorsed jointly by WCO/ICAO/IATA. Depending on the specific airline’s Reservation and Departure Control Systems, specific data elements which have been collected and stored by the airline, can be efficiently transmitted via this standardized message structure.

Note 2.—This provision is not intended to replace or supersede any messages exchanged between airlines and customs administrations to support local airport operations.

Note 3.— In addition to the mandatory EDIFACT-based PNRGOV message, Contracting States may also, optionally, consider implementation of the XML PNRGOV message format as a supplemental method of PNR data transfer, thereby allowing those airlines with XML capability a choice of format for the transmission of PNR data.

9.23 **Recommended Practice.**— *Contracting States requiring PNR data should consider the data privacy impact of PNR data collection and electronic transfer, within their own national systems and also in States. Where necessary, Contracting States requiring PNR data and those States restricting such data exchange should engage in early cooperation to align legal requirements.*

⁸² Annex 9 – Facilitation to the Convention on International Civil Aviation, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

SOURCES FOR FURTHER INFORMATION

References

Annex 9 – Facilitation to the Convention on International Civil Aviation, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

Guidelines on PNR Data, First Edition, Doc 9944, ICAO, Montreal, 2010, available to purchase at: <https://store1.icao.int/index.php/guidelines-on-passenger-name-record-pnr-data-doc-9944-english-printed.html>

IATA/WCO/ICAO Toolkit: presentation slides, IATA, 2013, available at: <http://www.iata.org/iata/passenger-data-toolkit/presentation.html>

Passenger Name Record Guidelines, Version 13.1, WCO/IATA/ICAO, October 2013, <https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx>

J. PUBLIC KEY INFRASTRUCTURE AND THE ICAO PUBLIC KEY DIRECTORY



This *Interoperable Application supports Traveller Identification* by assuring that the data read from the IC chip in the eMRTD are unaltered, and were written to the chip by a genuine issuing authority.

KEY MESSAGES

- ✓ The authentication of passport data stored in the IC chip of eMRTDs using digital certificates.
- ✓ Adds an additional layer of assurance of the authenticity and integrity of an eMRTD.
- ✓ ICAO's PKD reduces the certificate distribution burden on State authorities responsible for eMRTD issuance, and the certificate collection burden on States undertaking eMRTD PKI authentication at border controls.
- ✓ A NPKD or an alternative repository enables access to certificates at border controls.

OVERVIEW

The technical specifications of ICAO for global interoperability of eMRTDs ensure that properly configured document readers can accurately read data from the IC chip of properly configured eMRTDs. The interoperability standards for eMRTDs are published in ICAO Doc 9303⁸³.

PKI cryptography is used to secure eMRTDs, ensuring that only eMRTDs issued by recognized issuing authorities are accepted at border control.

PKI is a cryptography-based system in which private 'keys' are generated and held in a central repository, and used to create and distribute public 'keys' for system users, as a means of authentication. The keys are created in the form of digital certificates. PKI cryptography is asymmetric, i.e. the public keys can be distributed, shared and authenticated without revealing the private key. PKI is also used in many States in national applications that securely deliver online services to citizens.

The application of PKI in eMRTD issuance and the exchange of digital certificates enable States to determine that an eMRTD presented by a traveller at border controls:

- Has been issued by a genuine authority;
- Contains data that is unaltered; and
- Does not contain certificates that have been revoked.

The arrangements for authentication of eMRTDs rely on the global distribution between States of certificates and revocation lists from passport issuers to border control agencies. While States could exchange the necessary information bilaterally, the volume of information being exchanged would result in a highly complex and ineffective system that would be susceptible to errors.

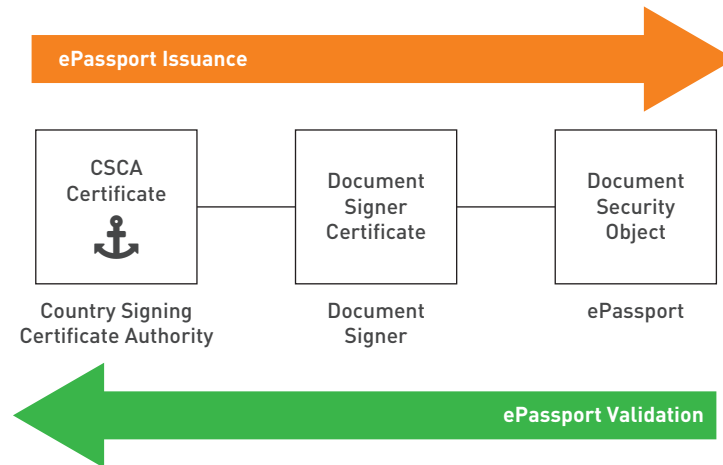
ICAO maintains the PKD to reduce the certificate distribution burden on national authorities responsible for eMRTD issuance, and the certificate collection burden on national authorities undertaking eMRTD authentication at border inspection. By playing the role of central broker, the ICAO PKD provides an efficient means for States to upload their own information and download that of other States.



Authentication relying on certificates downloaded from the ICAO PKD can be undertaken for all eMRTDs that are accepted for travel purposes by a State, including, for example, travel documents issued in card formats and refugee travel documents. However, the most common use of the ICAO PKD by Member States is to authenticate ePassports.

The ICAO PKD is the global repository of the digital certificate lists required to authenticate data in eMRTDs, including: the Country Signing Certification Authority (CSCA) certificate, Document Signer Certificates (DSC), CSCA Master Lists and Certificate Revocation Lists (CRL). The PKD has the

83 Doc 9303, *Machine Readable Travel Documents*, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>



Trust chain of ePassport and validation

additional benefit of enabling quality assurance checks to ensure that the certificates and revocation lists being uploaded to it meet interoperability specifications.

The DSC, CSCA Master Lists and revocation lists required to perform authentication of eMRTD are available to all States for free download from the PKD in a single batch file. Membership of the PKD is not required for this basic access.⁸⁴ For PKD members, downloads are available in an easier to use, transaction ready, format.

Given global travel volumes, the PKD operates offline in batch processes and is not designed to support online individual authentication transactions. Instead, States download certificates and revocation lists from the ICAO PKD to their NPKD (or an alternate library or repository that supports real time access). The State's NPKD is the national reference database containing the certificates and revocation lists downloaded from the ICAO PKD or obtained by bilateral exchange with other State's authorities responsible for eMRTD issuance. The State's NPKD can then be accessed by BCS.

The role of the NPKD in supporting eMRTD authentication at the border is different from the national PKI infrastructure that supports ePassport issuance and uploads to the ICAO PKD. Establishing and operating a NPKD is a significant, ongoing administrative and technical commitment independent of eMRTD issuance and ICAO PKD uploads.

HOW IT WORKS – BORDER CONTROL AGENCIES

The authentication check of the certificate trust chain, completed in the background, is fully automated and typically takes just a few seconds⁸⁵:

1. Travellers present their eMRTD (most commonly an ePassport) to a border control officer, or place their document onto an ABC interface.
2. A machine reader optically reads the MRZ of the eMRTD⁸⁶. The data read from the MRZ initiate a transaction to access the data from the IC chip, in most cases completing an optional privacy protection protocol that relies on data being read from the MRZ.
3. Data is retrieved from the IC chip of the eMRTD.
4. A comparison is made between the digital certificates retrieved from the eMRTD with the DSC and CSCA Master List or link certificates downloaded from the NPKD. In each method, certificate matches confirm that the eMRTD was genuinely issued and is unaltered.
5. A further check against the most recent revocation list obtained from the ICAO PKD confirms that the certificates remain trusted by the issuing authority.

⁸⁴ For downloading the certificates and revocation lists: *ICAO PKD data download*, ICAO, Montreal, <https://pkddownloadsg.icao.int/>

⁸⁵ More information on the fundamentals of eMRTDs are found at *ePassport Basics*, ICAO, Montreal, available at: <https://www.icao.int/Security/FAL/PKD/Pages/ePassportBasics.aspx>

⁸⁶ See: *Topic B – Document Readers*

The authentication of eMRTDs at border controls does not require States to issue eMRTDs. However, States issuing eMRTDs will already have in place some of the security infrastructure necessary to establish and manage a NPKD.

Membership of the ICAO PKD is available to all States issuing eMRTDs, or intending to strengthen their border controls. Membership requires application and payment of a one-off joining fee and an ongoing annual fee⁸⁷. New members of the PKD have up to 15 months to commence the upload of certificates for their eMRTDs, the milestone for commencing active participation.

Members of the PKD share advice and support from fellow members, the PKD Board, the PKD Operator and the PKD Secretariat. Bilateral collection of CSCAs is inefficient and time consuming. In contrast, PKD members have transaction ready access to CSCA Master Lists – a more efficient collection method.

Membership of the PKD is growing. The list of current participants is available at: <https://www.icao.int/Security/FAL/PKD/Pages/ICAO-PKDParticipants.aspx>

HOW IT WORKS – AIRLINES

Authentication of eMRTDs is a State responsibility. However, there is no technical obstacle to airlines downloading digital certificates and revocation lists from the ICAO PKD for authentication of eMRTDs.

BENEFITS AND OPPORTUNITIES

The ICAO PKD provides an efficient, secure and sustainable means to obtain the certificates and revocation lists necessary to undertake authentication of eMRTDs.

Authentication of eMRTDs means that the document can be used with confidence as the identity token in ABC systems. When PKI certificates fail to authenticate, eGates can be configured to refer travellers for human inspection and clearance.

Authentication of eMRTDs provides a reliable, automated mechanism to determine the integrity of the travel document presented by the traveller.

TECHNICAL ISSUES

Authentication of eMRTDs is a State responsibility requiring significant investment to:

- Create and maintain the necessary ICT infrastructure;
- Compile and maintain the necessary repository of certificates and revocation lists; and
- Carry out transactions between them.

State BCS need to maintain systems that can read eMRTDs both optically and electronically. The electronic interface must access the up-to-date digital certificates obtained from all States issuing eMRTDs, so that the necessary authentication can take place. The NPKD, as the State's certificate storage system, must be connected to the ICAO PKD so that updates to the certificate list can be made automatic.

Most modern commercially available document readers include functionality to present the necessary data to a BCS. The BCS must include functionality for authentication of eMRTDs and for referring "fail to authenticate" instances to border control officers.

RISKS AND COST MITIGATION

Authentication of eMRTDs at border inspection relies on an extensive technical infrastructure and adherence to demanding administrative protocols and practices⁸⁸, including:

- The document readers deployed at border controls need to be capable of handling eMRTDs;
- A robust and secure ICT infrastructure is required to download certificates and revocation lists from the ICAO PKD into the NPKD, and for the data from the NPKD to be made available at border controls; and
- Certificates and revocation lists must be updated regularly. Earlier certificates need to be retained for as long as the travel documents they authenticate remain valid.

87 The latest PKD fee are available in the folder PKD Finance Documents: *Publications*, ICAO, Montreal, <https://www.icao.int/Security/FAL/PKD/Pages/Publications.aspx>

88 Guidance for authorities planning to implement major upgrades of their current travel documents and related systems including all aspects of the procurement plan: *ICAO Guide for Collection of Best Practices for Acquisition of Machine Readable Travel Document Goods and Services*, Version 1, ICAO, March 2016, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

A BCS that does not authenticate against up to date certificates and revocation lists has the potential to falsely reject good documents and falsely accept compromised documents.

The PKI technical standards leave some room for interpretation in their application and as result certificates available from the PKD can from time to time have unusual conformance characteristics or not fully meet technical specifications⁸⁹. States relying on eMRTD authentication need to develop an understanding of potential and actual PKI certificate and interface non-conformance defects and how those defects will impact on their national BCS.

The arrangements for the creation and distribution of the Deviation Lists which are the formal mechanism for notification of identified defects and non-compliance are described in Part 2 of ICAO Doc 9303. Membership of the PKD provides access to a community of practice where defects are identified and discussed and workaround solutions are shared.

States intending to undertake authentication of eMRTDs where fingerprints or iris images are to be read from the IC chip will, in most cases, face the additional complexity of managing the multiple layers of PKI authentication required by the optional Extended Access Control (EAC) protocol⁹⁰. The certificates required for EAC are not available from the ICAO PKD and must instead be obtained bilaterally from eMRTD issuers. States contemplating an EAC implementation are encouraged to seek independent advice to carefully review the experience of other States before committing to this option.

A careful appraisal of administrative capacity and capability should precede consideration of the implementation of eMRTD authentication.

RELATED REQUIREMENTS

- ✓ National legislation authorising creation of a NPKD, downloads from the ICAO PKD and eMRTD authentication at border controls.
- ✓ State membership of the ICAO PKD, to ensure the timely distribution and receipt of digital certificates and revocation lists.
- ✓ A NPKD to receive and store digital certificates and revocation lists downloaded from the ICAO PKD.

- ✓ Administrative capacity and capability to sustain an up to date NPKD.
- ✓ eMRTD capable document readers.
- ✓ Integration of the NPKD with BCS and document readers to access the certificates and revocation lists necessary to complete eMRTD PKI authentication for travellers.
- ✓ Capacity, capability and organizational arrangements to manage referrals from primary examination of travellers, and to resolve PKI “fail to authenticate” instances at secondary examination.
- ✓ Reliable, continuous supply of electricity and network connectivity.

BEST PRACTICE EXAMPLES

Certificates of Identity and Convention Travel documents issued by the Australian Government are issued in eMRTD format and are authenticated at the Australian border.

Membership of the ICAO PKD should be managed by a designated position within the border control agency, to ensure continuity of membership and communication between the NPKD and the ICAO PKD.

The NPKD should be regularly audited for integrity and completeness.

eMRTD readers and NPKD BCS interfaces should be audited regularly to ensure that they are accessing up to date certificates from the NPKD.

Where eMRTDs fail to authenticate, officers should carefully examine the document to ensure that the document is properly issued and belongs to the holder. A defect in authentication or verification of IC chip data may be an indication of identity fraud or other malpractice.

Emerging practices include airlines deploying eMRTD readers that perform PKI authentication. This involves partnerships with national authorities where authentication provides operational benefits for all parties.

89 Examples of non-conformance are discussed in *PKD Machine Readable Error Codes*, ICAO PKD Board, Montreal, 2011 and *PKD Upload Contents Checks*, ICAO PKD Board, Montreal, 2011 available at: <https://www.icao.int/Security/FAL/PKD/Documents/PKDTechnicalDocuments/PKD%20Machine%20Readable%20Error%20Codes.pdf> and <https://www.icao.int/Security/FAL/PKD/Documents/PKDTechnicalDocuments/PKDUUploadContentsChecks.pdf>

90 See: *Topic K – EMRTD Biometric Identity Verification*

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Extracts from ICAO Annex 9 – *Facilitation* Chapter 3. Entry and departure of persons and their baggage⁹¹:

C. Security of travel documents

3.9 **Recommended Practice.**— *Contracting States should incorporate biometric data in their machine readable travel documents in a contactless integrated circuit chip, as specified in Doc 9303, Machine Readable Travel Documents.*

Note.— *Doc 9303 does not support the incorporation of biometric data in visas.*

3.9.1 **Recommended Practice.**— *Contracting States issuing or intending to issue eMRTDs should join the ICAO Public Key Directory (PKD) and upload their information to the PKD.*

3.9.2 **Recommended Practice.**— *Contracting States implementing checks on eMRTDs at border controls should join the ICAO Public Key Directory (PKD) and use the information available from the PKD to validate eMRTDs at border controls. ...”*

ICAO State Letter

ICAO has issued the State Letter “ICAO Public Key Directory (PKD)”, Ref.: EC 6/8.3 – 16/70, 25 July 2016, which notably includes the action to “join the ICAO Public Key Directory (PKD) and verify the digital signatures embedded in ePassports.”

“The ICAO PKD is a secure and cost-effective system for sharing up-to-date, globally trusted and validated public keys essential for verifying and authenticating ePassports.”

The State Letter is available on the ICAO Secure Portal: <http://portallogin.icao.int/>
For more information, please refer to your national civil aviation authority.

91 *Annex 9 – Facilitation to the Convention on International Civil Aviation*, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

SOURCES FOR FURTHER INFORMATION

References

Annex 9 – Facilitation to the Convention on International Civil Aviation, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

Doc 9303, Machine Readable Travel Documents, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

ICAO Guide for *Collection of Best Practices for Acquisition of Machine Readable Travel Document Goods and Services*, Version 1, ICAO, March 2016, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

ICAO Public Key Directory (PKD), ICAO State Letter No. EC 6/8.3 – 16/70, 25 July 2016. The State Letter is available on the ICAO Secure Portal: <http://portallogin.icao.int/>. For more information, please refer to your national civil aviation authority.

ICAO PKD data download, ICAO, Montreal, available at: <https://pkddownloadsg.icao.int/>

ICAO PKD Participants, ICAO, Montreal, available at: <https://www.icao.int/Security/FAL/PKD/Pages/ICAO-PKDParticipants.aspx>

ePassport Basics, ICAO, Montreal, available at: <https://www.icao.int/Security/FAL/PKD/Pages/ePassportBasics.aspx>

PKD Machine Readable Error Codes, ICAO PKD Board, Montreal, 2011 available at: <https://www.icao.int/Security/FAL/PKD/Documents/PKDTechnicalDocuments/PKD%20Machine%20Readable%20Error%20Codes.pdf>

PKD Upload Contents Checks, ICAO PKD Board, Montreal, 2011 available at: <https://www.icao.int/Security/FAL/PKD/Documents/PKDTechnicalDocuments/PKDUUploadContentsChecks.pdf>

Publications, PKD Finance Documents, ICAO, Montreal, available at: <https://www.icao.int/Security/FAL/PKD/Pages/Publications.aspx>

Other Sources

Guideline on requirements for inspection of machine readable (electronic) identity and travel documents produced by the German Federal Office for Information Security, the Federal Criminal Police Office and the Federal Police: *Machine Authentication of MRTDs for Public Sector Applications*, Technical Guideline BSI TR-03135, Version 2.2.0, Federal Office for Information Security of Germany, Bonn, 2017, available in English at: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03135/index_hm.html

Information on the ICAO PKD including the basics, validation, publications, governance, participants, why to join, and how to participate: *ICAO PKD*, ICAO, Montreal, available at: <https://www.icao.int/Security/FAL/PKD/Pages/default.aspx>

Video on PKD, with statements from PKD participants: *ICAO Public Key Directory*, ICAO, Montreal, available at: <http://www.icao.int/Security/FAL/Pages/PKD-Video.aspx>

K. eMRTD BIOMETRIC IDENTITY VERIFICATION



These *Interoperable Applications for Traveller Identification* enable States to perform biometric verification of universal and mandatory face images and, in more limited circumstances, of optional fingerprints and iris images.

KEY MESSAGES

- ✓ Comparison of live biometric samples (face, fingerprint or iris) from a traveller with biometric images read from the chip in eMRTDs.
- ✓ Where integrated with eGates, kiosks and airline check-in processing, provides efficiency, security and facilitation benefits.



OVERVIEW

States able to undertake the eMRTD PKI authentication at border controls⁹² can rely on the biometric images⁹³ available in eMRTDs as being genuine and unaltered.

States wishing to undertake eMRTD biometric identity verification at border controls can inspect facial images, and may be able to inspect fingerprint or iris images.

The primary facial biometric image is available to *all* States with compliant reader solutions from every ICAO compliant eMRTD. The facial image is stored in Data Group (DG) 1 of the Logical Data Structure (LDS) in the IC chip in each eMRTD⁹⁴.

States may be able to access the optional fingerprint or iris images stored in DG 3 or 4 in eMRTDs where they have been included. Most States that include those biometric images in their eMRTDs restrict access to this sensitive personal information. The mechanism most commonly used to achieve this restricted access is the EAC protocol. EAC allows the

eMRTD issuing authority to determine which document readers at which airports and other border control points can read biometric images from DG 3 or 4.

The eMRTD biometric identity verification can be implemented at primary examination in fully automated kiosks and eGates⁹⁵, or can be used to support inspection by border control officers. eMRTD biometric identity verification can also be undertaken at secondary examination, to resolve cases of suspected identity fraud or other “fail to match” referrals of travellers from primary examination, including from eGates.

HOW IT WORKS – BORDER CONTROL AGENCIES

A camera or other image capture device is used to obtain an image of the biometric features of the traveller, to be used in the comparison with the image read from the eMRTD.

⁹² See: *Topic J – Public Key Infrastructure and the ICAO Public Key Directory*

⁹³ The technical specifications for MRTDs and eMRTDs are published in the twelve Parts of *Doc 9303, Machine Readable Travel Documents*, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

⁹⁴ *Doc 9303, Machine Readable Travel Documents*, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC), 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

⁹⁵ See: *Topic G – Automated Border Controls*

An eMRTD document reader accesses the biometric image from the IC chip of the traveller. During the chip access process, the PKI certificate trust chain of the eMRTD is checked to ensure that the public key certificate is genuine and has not been revoked.⁹⁶

Templates are created from both biometric images by the biometric software engine. The templates are compared and a match result is returned to the BCS. Biometric matching is an application of probability. Where the match result exceeds a pre-determined threshold, the traveller will be processed as meeting biometric identity verification. Where the match result is below the pre-determined threshold, the traveller will be processed as not meeting biometric identity verification.

The challenge with the identification of travellers is to determine whether:

- Each traveller is the holder of a genuine travel document;
- Each traveller has a genuine claim to the identity represented in the travel document; and
- The identity represented is a true identity.

Biometric identity verification provides strong evidence that the person represented in the document is the traveller. When combined with eMRTD PKI authentication, strong evidence is added that the travel document is genuine and unaltered. It remains for State border authorities to assess whether the traveller has a genuine claim to the identity, and whether the identity is a true identity.

Biometric identity verification comparisons are therefore just one element in the broader consideration of the identification of travellers.

HOW IT WORKS – AIRLINES

Airlines and port authorities are investing in biometric technologies linked to eMRTDs to automate check-in, baggage drop, perimeter security and boarding. Convergence between airline systems and BCS is emerging.

TECHNICAL ISSUES

Biometric identity verification matching is advisory, not definitive. Biometric identity verification can reduce, but not eliminate, the statistical variance and error that is a feature of all ICT applications involving probability.

BENEFITS AND OPPORTUNITIES

In eGate applications, the biometric facial image identity verification available from eMRTDs provides a universal, extendable, scalable solution that has efficiency, security and facilitation benefits for States. It is for this reason that the combination of the eMRTD token and the face biometric modality is a feature of the most commonly deployed Automatic Border Control (ABC) solutions operating globally.

Biometric identity verification using eMRTDs at primary examination can help to mitigate the risk of imposters using travel documents issued to other people. Biometric matching against a stored image can be used separate from ABC solutions to confirm that an individual is the genuine holder of an eMRTD.

Using eMRTD biometric identity verification at secondary examination can facilitate and expedite the assessment of identity of “failure to match” cases referred from primary examination.

RISKS AND COST MITIGATION

Fingerprints and iris images are generally regarded as sensitive personal information, so access to this data should be more restricted. As a result, most States that include fingerprints or irises in their eMRTDs as secondary biometrics secure this data with the additional layers of PKI that are specified in Doc 9303 Part 11 – Security Mechanisms for MRTDs⁹⁷, using either the optional EAC protocol or alternative encryption.

EAC provides a mechanism for the State passport issuing authority to manage access to the secondary biometric images contained in Data Group 3 or 4 on the IC chip. Access is restricted to authorised terminals (i.e. approved eMRTD document readers being used at approved border locations). In EAC the exchange of certificates to manage the

⁹⁶ See: *Topic J – Public Key Infrastructure and the ICAO Public Key Directory*

⁹⁷ The technical specifications for MRTDs and eMRTDs are published in the twelve Parts of *Doc 9303, Machine Readable Travel Documents*, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

chip authentication and terminal authentication protocols is bilateral between States.

The ICAO PKD does not support the exchange of the certificates required by EAC because EAC requires the approval by an issuing authority direct to a border authority to allow this sensitive access.

Consequently, EAC can be extremely challenging to implement from both a technical and administrative standpoint. Multi-country implementations of EAC require inter-governmental agreements to precede the adoption of technical solutions. As such, EAC solutions are most often limited to national solutions.

Biometric systems are complex and expensive to implement and operate. It is therefore important that vendor independent, solution neutral advice informs consideration of options prior to committing to solutions or biometric modalities⁹⁸.

RELATED REQUIREMENTS

- ✓ National legislation to authorise eMRTD biometric identity verification.
- ✓ National legislation to collect, store, retrieve, compare, share, retain and dispose of biometric sample images and templates.
- ✓ Privacy and data protection legislation, systems and practices, sufficient to protect biometric data from misuse.
- ✓ A secondary examination operating model with adequate staffing and accommodation for resolving traveller identity verification referrals.
- ✓ Sufficient eMRTD document readers and image capture devices to meet current and future traveller volumes.
- ✓ Creation of a NPKD as the repository for the certificates and revocation lists, relied on at the border control to confirm that the eMRTDs from which biometric samples are taken are genuine and unaltered.
- ✓ ICT integration of the BCS with biometric capture and an eMRTD PKI authentication interface, to ensure that the biometric sample read from the IC chip is genuine and unaltered.

- ✓ For accessing secondary biometrics (i.e. fingerprints or iris images) from the eMRTDs of foreigners:
 - Approval from the State issuing authority; and
 - Technical ability to manage EAC terminal and chip authentication with document readers.
- ✓ Reliable, continuous supply of electricity.
- ✓ Reliable, continuous, high bandwidth network connectivity sufficient for transmitting image files in real time.

BEST PRACTICE EXAMPLES

A large number of States undertake biometric identity verification using images read from eMRTDs as one element of their ABC solutions:

- Australia, Finland, Germany, New Zealand, Portugal and the UK, among other States, use facial images; and
- France, Hong Kong, Malaysia and Singapore, among other States, use fingerprint images.

The UK uses a standalone facial image matching system when there is doubt about the identity of the holder of an eMRTD. This provides border control officers with additional objective information that can help to resolve traveller identity.

Systems can be configured to make multi-dimensional comparisons of images taken of the traveller with the images printed in the document, read from the chip and retrieved from a database.

⁹⁸ Guidance for authorities planning to implement major upgrades of their current travel documents and related systems including all aspects of the procurement plan: ICAO Guide for *Collection of Best Practices for Acquisition of Machine Readable Travel Document Goods and Services*, Version 1, ICAO, March 2016, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Extracts from ICAO Annex 9 – *Facilitation*, Chapter 3. Entry and departure of persons and their baggage⁹⁹:

A. General

“ ...

3.3 Contracting States that use integrated circuit (IC) chips or other optional machine readable technologies for the representation of personal data, including biometric data, in their travel documents shall make provision whereby the encoded data may be revealed to the holder of the document upon request. ...”

C. Security of travel documents

“ ...

3.9 **Recommended Practice.**— *Contracting States should incorporate biometric data in their machine readable travel documents in a contactless integrated circuit chip as specified in Doc 9303, Machine Readable Travel Documents.*

Note.— *Doc 9303 does not support the incorporation of biometric data in visa. ...”*

SOURCES FOR FURTHER INFORMATION

References

Annex 9 – Facilitation to the Convention on International Civil Aviation, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

ICAO Guide for *Collection of Best Practices for Acquisition of Machine Readable Travel Document Goods and Services*, Version 1, ICAO, March 2016, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

Doc 9303, Machine Readable Travel Documents, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

⁹⁹ *Annex 9 – Facilitation to the Convention on International Civil Aviation*, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

L. INTERPOL'S STOLEN AND LOST TRAVEL DOCUMENTS DATABASE



This **Interoperable Application** supports **Traveller Identification & Risk Assessment** by providing further assurance that passports genuinely issued by States remain in the hands of travellers entitled to use them.

KEY MESSAGES

- ✓ Checks against a global database of more than 76 million records of stolen, stolen blank, lost and revoked travel documents reported by INTERPOL member countries.
- ✓ Accessible by both border control agencies and airlines, via multiple INTERPOL technical solutions (FIND, MIND and I-Checkit).
- ✓ Supplements the use of national and international watchlists at every stage of the traveller journey.

OVERVIEW

The international police organization (INTERPOL) enables police in member countries to work together to fight international crime. It provides a range of policing expertise and capabilities, supporting three main crime programmes: Counter-terrorism, Cybercrime, and Organized and Emerging Crime.¹⁰⁰

INTERPOL operates from its General Secretariat in Lyon, France, 24 hours a day, 365 days a year and has seven regional offices worldwide. Each INTERPOL member country maintains a National Central Bureau (NCB) staffed by its own highly trained law enforcement officers.

The Integrated Border Management Task Force (IBMTF) is the central point of contact and coordination for international border security activities at INTERPOL¹⁰¹.

The IBMTF supports law enforcement officers working at the frontline of border security by:

- Assisting them with access to INTERPOL's policing capabilities, including portable temporary access to border-related databases at border points that do not have regular access to these;
- Delivering capacity building and training courses; and
- Coordinating operational activities at border points.

INTERPOL offers a range of policing capabilities that can help States to enhance their own border security procedures, and to integrate their efforts with those of their neighbours.

INTERPOL's SLTD database enables INTERPOL, NCBs and other authorized law enforcement entities – including border control agencies responsible for the identification of travellers – to determine, within seconds, whether the travel document presented by the traveller has been previously reported as being stolen, stolen blank, lost or revoked.



The SLTD database was created in 2002, following the 11 September 2001 terrorist attacks in the USA, to help States secure their borders and protect their citizens from terrorists and other dangerous criminals who use fraudulent and fraudulently obtained travel documents.

The SLTD database is a compilation of all the travel documents reported as stolen, stolen blank, lost and revoked to INTERPOL by each NCB. In turn, the NCB in each INTERPOL member country relies on input and advice from their travel document issuing authority, national police and border authorities for details of such travel documents that come to their notice. The NCB reports the details of these documents to INTERPOL headquarters for inclusion in the SLTD database.

¹⁰⁰ INTERPOL, <https://www.interpol.int/>

¹⁰¹ Border management, INTERPOL, <https://www.interpol.int/INTERPOL-expertise/Border-management>

Travel document holders are advised that they should not attempt to travel with a document that has been reported as stolen or lost. Nonetheless, some travellers who report their travel document as lost or stolen do attempt to use the document when they later find it. Travel documents reported stolen or lost may be fraudulently used by impostors or fraudulently altered to be used by other criminals. As such, the presentation by a traveller of a passport reported as stolen or lost should be treated as a potentially significant risk to the integrity of border controls.

Despite the ready availability of the SLTD database, not all States conduct searches to determine whether an individual is using a passport previously reported as stolen or lost. To increase the use of the SLTD database worldwide, INTERPOL encourages each State to extend access to INTERPOL's I-24/7 network – which serves as the interface for accessing its criminal databases, including the SLTD database – to international airports and other border crossings.

This access requires the installation of equipment and specialized software. Having undertaken the necessary equipment and systems integration, border control officers in an INTERPOL member country can screen passenger information directly against the SLTD database. In best practice jurisdictions, this screening is carried out automatically for all travellers at primary examination.

Airlines can access INTERPOL SLTD database through I-Checkit, a system interface specially developed for them.

HOW IT WORKS – BORDER CONTROL AGENCIES

The exchange of SLTD database information is key to strengthening border controls and mitigating the impact of identity theft and immigration fraud. The ICAO Doc 9303 Part 2: Specifications for the Security and Design, Manufacture and Issuance of MRTDs¹⁰², discusses the operational procedures to:

- Communicate proactively with document holders;
- Maintain national databases of stolen, lost and revoked travel documents;
- Share information on stolen, stolen blank, lost and revoked travel documents with INTERPOL, and systematically verify documents against INTERPOL databases at primary inspection; and
- Check to determine whether a holder is presenting a stolen, lost or revoked document at a border crossing.

When border control officers receive an SLTD database alert via their BCS interface, the first step is to determine whether the travel document is being presented by the person to whom it was issued. If the travel document remains in the hands of the genuine holder, then the traveller should be advised to replace the travel document. If the travel document is being presented by a person other than to whom it was issued, then further investigation of the travel document and the traveller's intentions is necessary. In both cases, the travel document is seized for eventual return to the issuing authority to prevent its further use.

Details of stolen and lost passports are submitted directly to the SLTD database by INTERPOL NCBs via INTERPOL's I-24/7 secure global police communications system. Only the State that issued a document can add it to the database. INTERPOL is not automatically notified of all passport thefts occurring worldwide, and the SLTD database is not connected to national lists of stolen, lost, stolen blank and revoked passports. This requires States to be proactive in submitting notice of such documents to INTERPOL.

It should be noted that simply because a travel document is flagged as stolen, lost or revoked does not imply that the holder of the document is engaged in illegal activity, or that they should be summarily refused entry. Enquiries should be made with the holder of the document and the issuing authority (via the INTERPOL network) to establish the circumstances behind the database entry. It will be helpful if the agency that detects such a questioned document can check its security features to determine whether any unauthorised change has taken place, and if so whether any observed forgery or counterfeiting techniques should be circulated to frontline officers, INTERPOL and the original issuer.

INTERPOL developed the I-24/7 system to connect law enforcement officers in all its member countries. It enables authorized users to share sensitive and urgent police information with their counterparts around the globe, 24 hours a day, 365 days a year.

With I-24/7 installed at every NCB, INTERPOL is now focusing on extending access to its services beyond the NCB to frontline officers with law enforcement responsibilities, including border control officers responsible for the identification of travellers.

102 Doc 9303, *Machine Readable Travel Documents*, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

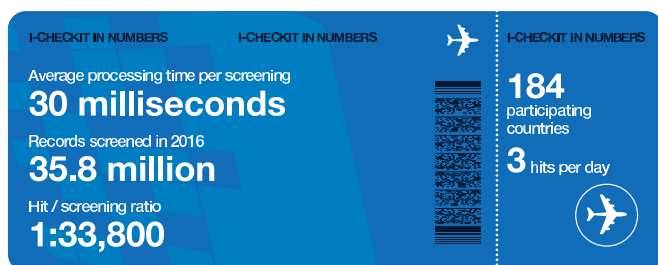
For access to its SLTD database, INTERPOL offers real time and batch update interfaces. Either can be integrated with national BCS for primary and/or secondary processing of travellers.

SLTD database can also be implemented as a separate, additional screening check to support secondary examination. However, full integration with a national BCS is preferable, as the INTERPOL SLTD database enhances assurance of identification of travellers at primary processing.

HOW IT WORKS – AIRLINES

To help identify and stop criminals from using stolen or lost travel documents before they reach the airport or the border, INTERPOL has developed I-Checkit¹⁰³. This initiative allows trusted partners in the travel industry to submit travel documents for screening against the SLTD database when customers book an airplane ticket. The data screened does not include names of individuals.

A database match triggers an instant alert to initiate investigation. Notifications are sent to INTERPOL's General Secretariat Command and Coordination Centre, to the INTERPOL NCB in the States concerned, and to other relevant national law enforcement entities. In some cases, the travel industry operator's security teams are also alerted, to enable them to further examine the document and refer it to local law enforcement agencies.



I-Checkit is only fully effective when border control agency advice and support is available to the airlines using the tool.

BENEFITS AND OPPORTUNITIES

A single global database of many millions of suspect travel and identity documents that can be readily accessed by police and border control agencies is an essential tool in disrupting

and limiting the market in misused travel documents. The value of a stolen, stolen blank, lost or revoked document is significantly reduced if it cannot be used for international travel. By increasing the risk for unauthorised holders (for example terrorists, criminals, and those seeking to enter a country when improperly documented) of being detected and denied boarding or check-in, the value of fraudulently obtained travel documents can be reduced, and their use deterred.

Subject to support from border control agencies, airline use of the I-Checkit system can disrupt travel using such documents, even in jurisdictions without full exit controls.

With full integration into primary processing, checks of the INTERPOL SLTD database can be initiated when the MRTD is placed on the document reader without any other processing input from border personnel. Integration to this level reduces error and increases process efficiency, while at the same time delivering security benefits for States and facilitation benefits for travellers.

TECHNICAL ISSUES

Border control agencies have two main methods for accessing the SLTD database: the Mobile INTERPOL Network Database (MIND), and the Fixed INTERPOL Network Database (FIND). MIND and FIND facilitate searches by border control agencies of SLTDs, people, and even stolen motor vehicles. The key difference between them is that FIND allows real-time online access to INTERPOL databases, which are continuously updated, while MIND contains a copy of these databases. This offline copy is updated periodically, usually within 48 hours. Thus, FIND provides more up-to-date data; however, this advantage will dissipate over time as MIND is updated more regularly.

Depending on their infrastructure, States may rely on FIND, MIND, or both. However, the development of FIND is recommended to avoid the risk of carrying out searches against outdated databases. An additional advantage of the FIND network is that it allows access to information on individuals who are the subject of INTERPOL Notices, discussed in *Topic N – International Watchlists*, while MIND does not contain these personal data.

States should also keep a national list of travel documents reported to them as stolen, stolen blank, lost, revoked or otherwise suspect, and ensure that border and law enforcement agencies can easily access the list.

103 I-Checkit, INTERPOL, <https://www.interpol.int/INTERPOL-expertise/I-Checkit>

RELATED REQUIREMENTS

- ✓ National legislation for border control agencies to access and act on SLTD database matches is an INTERPOL requirement for the implementation of MIND/FIND.
- ✓ Protocols and business processes for the resolution of SLTD database matches.
- ✓ 24/7/365 operational support for contacting the passport issuing agencies of other States (via their NCBs) to resolve SLTD database matches.
- ✓ ICT integration of BCS with INTERPOL MIND/FIND.
- ✓ Reliable, continuous supply of electricity and connectivity.
- ✓ Properly trained border control officers and a secured location.

BEST PRACTICE EXAMPLES

Establish a good working relationship with the local INTERPOL NCB to allow for quick searches of INTERPOL resources, and timely responses to database matches.

Where infrastructure and finances allow, install or upgrade primary line and targeting centre links to INTERPOL's SLTD database via MIND or FIND, and ensure 24/7 accessibility. Make document checking an automatic process within entry and exit controls.

Check travel document country code data against the SLTD database on a routine basis at all entry and exit controls.

Ensure that a response to a suspect document query from another State is sent within one hour from receipt at the NCB.

Ensure that citizens are aware that they should report the loss or theft of a travel document without delay to the relevant authority, and that the details are checked and placed on the SLTD database as soon as possible.

RISKS AND COST MITIGATION

Primary processing or joint targeting centre access to the SLTD database will require upgrades and integration with ICT systems. Where ICT systems are outsourced and subject to transaction-based pricing, this could result in substantial additional costs. To reduce transaction-based costs, border control agencies should consider covering air borders by means of API details being run through the SLTD database via a central system before travel commences.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Annex 9 – Facilitation, Chapter 3. Entry and departure of persons and their baggage¹⁰⁴:

C. Security of travel documents

“ ...

3.10 Contracting States shall promptly report accurate information about stolen, lost, and revoked travel documents, issued by their State, to INTERPOL for inclusion in the Stolen and Lost Travel Documents (SLTD) database.

3.10.1 **Recommended Practice.**— *Each Contracting State should, as far as practicable, query, at entry and departure border control points, the travel documents of individuals travelling internationally against the INTERPOL Stolen and Lost Travel Documents (SLTD) database. ...”*

¹⁰⁴ Annex 9 – Facilitation to the Convention on International Civil Aviation, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

ICAO State Letter:

ICAO State Letter “Annex 9 — *Facilitation*: provisions on the Stolen and Lost Travel Documents (SLTD) database of INTERPOL”, Ref.: EC 6/3 – 17/92, 24 July 2017, includes the required action to implement Standard 3.10 and comply, as practicable, with Recommended Practice 3.10.1 of Annex 9.

“This SLTD database was created to ascertain the validity of travel documents at border control points. In order to protect the security and integrity of passports, to enhance international cooperation to counter threats to civil aviation, and to prevent the use of travel documents for acts of unlawful interference against civil aviation, the ICAO Assembly has encouraged Member States to report on a regular basis stolen and lost passports to the database.”

The State Letter is available on the ICAO Secure Portal: <http://portallogin.icao.int/>
For more information, please refer to your national civil aviation authority.

SOURCES FOR FURTHER INFORMATION

References

Annex 9 – Facilitation: Provisions on the Stolen and Lost Travel Documents (SLTD) database of INTERPOL, ICAO State Letter, Ref.: EC 6/3 – 17/92, 24 July 2017. ICAO State Letters are available on the ICAO Secure Portal: <http://portallogin.icao.int/>. For more information, please refer to your national civil aviation authority.

Annex 9 – Facilitation to the Convention on International Civil Aviation, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

Border management, INTERPOL, <https://www.interpol.int/INTERPOL-expertise/Border-management>

Doc 9303, Machine Readable Travel Documents, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

I-Checkit, INTERPOL, <https://www.interpol.int/INTERPOL-expertise/I-Checkit>

INTERPOL, <https://www.interpol.int/>

Machine Readable Travel Documents, Doc 9303, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

Standards and Recommended Practices, Annex 9 to the Convention on International Civil Aviation – Annex 9 – Facilitation, Fourteenth Edition, ICAO, Montreal, October 2015, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

Other Sources

INTERPOL contact for SLTD database, INTERPOL Database Management Unit: databasemanagement@interpol.int

M. INTERNATIONAL WATCHLISTS



These *Interoperable Applications for Risk Assessment* supplement national watchlists with additional targets who may otherwise remain unknown to them, thus helping States secure their own borders and meet their international obligations to combat terrorism and other trans-national crime.

KEY MESSAGES

- ✓ Lists issued by the United Nations and INTERPOL of individuals who are subject to arrest, notification or travel ban.
- ✓ Provide additional resources against which to check the identity and information presented by a traveller on departure or entry, and facilitate information sharing between States concerning potentially high-risk travellers.
- ✓ Best practice is integration of international watchlist data into national watchlist systems.

OVERVIEW

Member States of the UN have obligations and responsibilities that include the enforcement of UN imposed sanctions. To support the enforcement of its sanctions, the UN publishes the CUNSCSL, which includes all individuals and entities subject to sanction measures imposed by the UNSC¹⁰⁵. The sanctions can take different forms, including targeted measures such as arms embargos, travel bans, and financial and commodity restrictions.

A notice related to a travel ban intended to prevent an individual from entering or transiting certain States may not constitute a requirement for arrest, detention or other enforcement action. However, key UNSCR on counter-terrorism request States to prevent the mobility of terrorists and the travel of FTFs, whether or not they are listed under CUNSCSL.

Additionally, INTERPOL member countries have obligations and responsibilities in relation to international law enforcement. INTERPOL publishes Notices that include both

international requests for cooperation and alerts allowing police in member countries to share critical crime-related information with other law enforcement-related agencies, including those responsible for BCM¹⁰⁶. These Notices are published by INTERPOL's General Secretariat at the request of National Central Bureaus (NCBs) and other authorized entities.

Types of INTERPOL Notices:



A request to locate and provisionally arrest an individual pending extradition. It is issued by the General Secretariat at the request of a member country or an international tribunal on the basis of a valid national arrest warrant. However, it is not an international arrest warrant.



A request to collect additional information about a person's identity, location or activities in relation to a crime.



Issued to provide warnings and/or intelligence about persons who have committed criminal offences and might repeat these crimes in other countries.



A request to help locate missing persons, often minors, or to help identify persons who are unable to identify themselves.



Issued to warn of an event, a person, an object or a process that represents a serious and imminent threat to public safety.

105 *Consolidated United Nations Security Council Sanctions List*, United Nations Security Council, <https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list>

106 *Notices*, INTERPOL, <https://www.interpol.int/INTERPOL-expertise/Notices>

In the case of Red Notices, the specified persons are wanted¹⁰⁷ by national jurisdictions for prosecution, or to serve a sentence based on an arrest warrant or court decision. In such a case, INTERPOL's role is to assist the national police forces in identifying and locating these persons with a view to their arrest and extradition, or similar lawful action.

Notices are also used by the UN, international criminal tribunals and the International Criminal Court to seek persons wanted for committing crimes within their jurisdiction: notably genocide, war crimes, and crimes against humanity.



INTERPOL also leverages its network and established arrangements for publishing and distributing INTERPOL-UNSC Special Notices (INTERPOL-UNSC S/N). Like other INTERPOL Notices, Special Notices

are circulated to all INTERPOL member countries through INTERPOL's secure I-24/7 global communications system. The Special Notice seeks to alert law enforcement agencies worldwide that a given individual or entity is subject to UN sanctions.¹⁰⁸

States must prevent the mobility of terrorist and FTFs and have the responsibility to search traveller data against the CUNSCSL and INTERPOL's coloured Notices. This is most efficiently achieved by integration of the INTERPOL nominal database into the national watchlist modules of BCS.

HOW IT WORKS – BORDER CONTROL AGENCIES

In best practice jurisdictions, international watchlists should be integrated into national watchlist systems so that they are consulted at visa or ETS issuance and during the border processing of travellers – both at eGates and when processing is completed by border control officers.

This integration is facilitated by:

- The publication of the CUNSCSL in standardised, downloadable .xml, .html and .pdf formats; and
- Interfaces of the national BCS and other law enforcement systems with the INTERPOL FIND solution.

HOW IT WORKS – AIRLINES

The purpose of watchlists is to trigger a BCM intervention from the relevant State authority to more closely examine the risk posed by a traveller. Airlines cannot be responsible for such regulatory interventions because their powers to act are limited to offloading or refusing to board passengers.

BENEFITS AND OPPORTUNITIES

States that incorporate searches of international watchlists into their BCS are meeting their international obligations and helping to combat terrorism and other transnational crime. States also have an important role to play by contributing additions, updates and amendments to these international watchlists.

For the time being international watchlists available at border control are largely limited to biographic listings, and as a result rely on searches by name, date of birth and nationality. The use of international biometric watchlists is growing, and models are emerging for managing the related privacy and data protection issues. UNSCR 2322 (2016) and UNSCR 2396 (2017) call upon States to share biometric and biographic information on FTFs and individual terrorists, and to implement biometric watchlist functionality in their BCS.

States planning to create a biometric watchlist capability should anticipate the possible future inclusion of listings from international sources. INTERPOL have extensive holdings of facial and fingerprint images and this data may become available for frontline application in border control in the future.

TECHNICAL ISSUES

INTERPOL's Criminal Information System is available to the NCBs of its member countries 24 hours a day, 7 days a week. For border control agencies and frontline officers, INTERPOL offers standalone and integrated solutions, with either batch or online real-time updates.

Via its public facing website, INTERPOL offers a limited search capability of its coloured Notices. However, using this interface to conduct separate searches of the UN Sanctions and INTERPOL watchlists is impractical and would excessively impact process efficiency and traveller

107 View Red Notices, INTERPOL, <https://www.interpol.int/notice/search/wanted>

108 Special Notices, INTERPOL – United Nations Security Council Special Notice, INTERPOL, <https://www.interpol.int/INTERPOL-expertise/Notices/Special-Notices>

facilitation. Some level of integration with national BCS is desirable for effective implementation.

RISKS AND COST MITIGATION

Data quality is a critical risk in watchlists. The effectiveness of watchlists is determined by matching performance. Watchlists of persons rely primarily on name matching, with nationality and date of birth playing secondary roles. Name matching is challenging and errors in international watchlist matching have two potentially serious consequences:

- Allowing the travel of known criminals or terrorists (false acceptance matches); and
- Disrupting or preventing the travel of innocent travellers (false rejection matches).

To minimize the margin of error, name matching algorithms should anticipate cultural name variations, aliases, transliteration, legal name changes and phonetic translation and typographical transcription errors.

Matching will be less likely wherever the watchlist data do not match the details included in the MRTD. For international watchlists, States are reliant on the quality of the identifying details provided at the time the watchlist record was created, and the identifying details included in the MRTD at the time of issuance. This matching challenge is further complicated by the behaviour of criminals and terrorists, who take active steps to disguise their identity.

To mitigate the impact on process efficiency and facilitation, it is desirable that States integrate international watchlist datasets into the national watchlist modules of their BCS. In these integrated arrangements, a document reader capturing the MRZ can be used to initiate simultaneous searches of all national and international watchlist datasets of persons who are known to represent a possible risk or threat, as well as of travel documents reported stolen or lost that might be used to disguise identity.

Since a watchlist match initiates a secondary process to determine whether that match is true or false, it is essential that national watchlist databases are subject to active management. This is to ensure that:

- Only listings that meet national data quality standards are included;

- Listings include clear advice on the action required from border control personnel;
- Listings are subject to regular review; and
- Reviews that are undertaken confirm that the requesting agency or organization continues to require the listing, and remains available to support action if the person is detected.

It is likely that in the future the current biographic and document number watchlists of known terrorists and criminals will be supplemented by biometric watchlists of facial, fingerprint and iris images, or other biometric identifiers. The application of biometrics to watchlists has the potential to improve matching performance, while at the same time introducing new sources of error. These errors will need to be anticipated and mitigated in the design and planning of solutions.

States that delay participation in international watchlist arrangements risk criticism for failing to meet their international obligations. At the same time, States that attempt to participate without mature capability to sustain effective watchlist management are susceptible to failure. The reputational risk of integrating international watchlists into national BCS prematurely or incorrectly should be carefully evaluated.

RELATED REQUIREMENTS

- ✓ National legislation for border control agencies to take the action requested by the international watchlist (e.g. INTERPOL Red Notices require provisional arrest pending extradition).
- ✓ Protocols and business processes for the resolution of watchlist matches, to confirm that the traveller who comes to notice is the subject of the watchlist entry.
- ✓ 24/7/365 operational support for contacting the law enforcement or security authorities in the country responsible for the original listing. In general, this requires collaboration with national law enforcement and security authorities.
- ✓ ICT integration of BCS with CUNSCSL and other international watchlists.
- ✓ Reliable, continuous supply of electricity and network connectivity.

BEST PRACTICE EXAMPLES

The Bali Process Regional Biometric Data Exchange Solution (RBDES)¹⁰⁹ from the Asia-Pacific region is an example of a regional biometric watchlist application intended to foster greater regional cooperation to reduce the irregular movement of people. It enables participating members to exchange information in a consistent and harmonized manner by aligning legal, technical, privacy and operational processes with domestic and international frameworks.

The RBDES is a simple channel of communication that allows members to exchange anonymised biometric data, with associated biographical data being provided according to agreed protocols in the event of a positive match. Participation in the RBDES is voluntary and non-binding;

Bali Process members can opt in and opt out of the RBDES at any time, and endorsement of the RBDES does not commit any member to using it.

The significance of the RBDES arrangement: since the initial transaction uses anonymised data, privacy and data protection is inherently strong. Since the protocols for the exchange of associated biographical data can be agreed and configured on a bilateral basis, the framework can be adjusted to account for the legislation and privacy and data protection protocols of each member country.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Not applicable.

SOURCES FOR FURTHER INFORMATION

References

Annex 9 – Facilitation to the Convention on International Civil Aviation, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

Consolidated United Nations Security Council Sanctions List, United Nations Security Council,

<https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list>

Special Notices, INTERPOL – United Nations Security Council Special Notice, INTERPOL, <https://www.interpol.int/INTERPOL-expertise/Notices/Special-Notices>

Notices, INTERPOL, <https://www.interpol.int/INTERPOL-expertise/Notices>

Threats to international peace and security caused by terrorist acts S/RES/1516 (2003), United Nations, 2003, available at: <http://www.un.org/en/sc/documents/resolutions/>

View Red Notices, INTERPOL, <https://www.interpol.int/notice/search/wanted>

Regional Biometric Data Exchange Solution (RBDES), Bali Process,

<http://www.baliprocess.net/regional-support-office/regional-biometric-data-exchange-solution/>

Other sources

Tool to help Member States implement key Security Council resolutions on terrorism: *Technical guide to the implementation of Security Council resolution 1373 (2001) and other relevant resolutions*, CTED, 2017, available at: <https://www.un.org/sc/ctc/blog/2017/08/21/counter-terrorism-committee-submits-updated-technical-guide-to-security-council/>

¹⁰⁹ *Regional Biometric Data Exchange Solution (RBDES)*, The Bali Process, <http://www.baliprocess.net/regional-support-office/regional-biometric-data-exchange-solution/>

Examination of Travellers and Travel Document Inspection

The examination of travellers and inspection of their travel documents is a core responsibility and function of border control agencies. Effective identification of travellers requires travel document authentication as one component of verification of identity.

While the use of technology plays a central role, skilled and capable border control personnel remain an important safeguard for deterring irregular movement across borders and preventing harm from smuggling, trafficking, terrorism, and other forms of organized criminal activity.

The Inspection Systems and Tools and Interoperable Applications described in Sections 4 and 5 support faster and more accurate BCM decisions. But where there is no such technology – or where the technology fails – border officers need the skills, training, and experience to judge whether travel documents are valid, genuine, free from forgery or alteration, and are being presented by the rightful holder.

The workspace in which border officers are performing traveller examination and travel document inspection, and the procedures by which they do so, are important determinants of the effectiveness and efficiency of those efforts.

6.1 Primary and Secondary Examination of Travellers

Entry controls are the final opportunity for a State to perform traveller identification and risk assessment to determine admissibility of a traveller. When doubts arise about traveller identity or risk at primary examination, the authentication of travel documents may need to be supplemented by secondary examination processes and tools, including forensic inspection of MRTDs, interviews and/or alternative or additional biometric comparisons.

PRIMARY EXAMINATION	SECONDARY EXAMINATION
	
<p>Travellers 99% clearance Automation = simplification of processing</p> <p>Immigration Agency 80% of border control agency personnel work at primary examination The number and share of border agency personnel working at primary examination is decreasing in best practice jurisdictions.</p>	<p>Travellers 1% referral of watchlist matches and targets, PKI, SLTD More targets, more matches, more false positives = Increasingly complex Increasing complexity = Increasing error</p> <p>Immigration Agency 20% of border control agency personnel work at secondary examination The number and share of border agency personnel working at secondary examination is increasing in best practice jurisdictions.</p>

Comparing Primary and Secondary Examination¹¹⁰

110 The suggested ratios are illustrative only and can be expected to vary between States.

PRIMARY EXAMINATION

Primary examination presents an opportunity for border officers to address several key questions before allowing a traveller to proceed. These include: Is the traveller the rightful holder of the travel document being presented? Is the document valid and authentic? Is the traveller's immigration status defined by their travel document (e.g. citizen of the country, citizen of a regional free travel area, diplomat)? Does the traveller qualify for entry or departure according to national or regional immigration legislation? Is the traveller admissible at his/her next destination?

In determining the answers to these questions, there are several additional questions a border officer conducting primary examination might consider. For example: Does the traveller's language or dialect, appearance and manner fit with their description in the travel document? Does the traveller's explanation of the purpose and length of stay seem valid and reasonable? Is the traveller deemed a 'person of interest' based on a watchlist match or intelligence assessment?

Where there is doubt, an officer may decide to carry out more thorough questioning and request that the traveller produce evidence to support their statements. Where it does not prejudice intelligence or law enforcement operations, any adverse information may be discussed with the traveller with the response observed and noted. A search of the traveller's person and/or baggage may be undertaken, where authorised by national law.

The presentation of a defective or damaged eMRTD where the data on the chip are unreadable should alert border officers to the possibility that the holder may be an impostor.

SECONDARY EXAMINATION AND REMOVAL

Standard Operating Procedures (SOPs) for interventions at secondary examination should be published, accessible to and understood by border control officers. The procedures should anticipate all the circumstances where referrals to secondary examination are required.

Effective secondary examination requires adequate interview and detention rooms located close to the primary processing of arriving and departing travellers. BCS should include modules to record and manage the resolution of referrals at secondary examination.

SOPs should highlight to border control officers the protection obligations of the State to vulnerable travellers. These include the right to seek asylum for persons fleeing armed conflict or persecution, and procedures to identify victims of human trafficking, objects of people smuggling and other abuses of human rights. Where custody is required it should be administrative, non-punitive and the conditions should preserve the dignity of travellers. The period of detention should be kept to a necessary minimum.

Decisions regarding a traveller's admissibility should always be made in accordance with the relevant national legislation, international law, and based on the evidence presented by the traveller. Travellers should be informed of adverse decisions in writing, and advised of their appeal rights

If a decision is made to deny entry, the traveller should be removed in accordance with national legislation and the SARPs of Chapter 5. Inadmissible Persons and Deportees of Annex 9 – *Facilitation*¹¹¹.

PHYSICAL ARRANGEMENTS FOR TRAVELLER AND DOCUMENT INSPECTION

The full benefit of the verification of traveller identity to help prevent and deter the travel of persons of interest can only be achieved when *all* travellers are subject to border controls. For effective BCM it is essential that international airports have adequate and reliable access control arrangements, to prevent travellers from circumventing departure and entry controls.

This can happen when travellers are assisted in avoiding border control points, when entries and departures are not recorded or processed in BCS, or when watchlist checks are not performed or watchlist alerts are ignored.

The mixing of departing travellers with transit and transfer travellers can be exploited by transnational criminals. Boarding pass swaps are one means to facilitate human trafficking or people smuggling.

Left unmitigated, the risks from border controls being evaded compromise security and reduce trust and confidence.

Implementing some simple measures can reduce the risk of border control evasion and related conspiracies to facilitate improperly documented and other inadmissible travel at border control. The introduction of snake queues can help

111 *Annex 9 – Facilitation to the Convention on International Civil Aviation*, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

disrupt conspiracies involving facilitators, corrupt officers and airline check-in personnel. Ensuring that travellers are randomly presented to airline and border personnel makes it difficult to be processed by a chosen officer or check-in agent. Snake queues have the additional benefit of being more time and space efficient.

Having airline or airport management personnel direct travellers to the primary line in order of entry can also reduce the risk of would-be offenders attempting to be processed by officers known to them for purposes of evading border controls. An unpredictable workstation rotation can also be used to make it difficult for corrupt border control officers to be on duty at a time and place coordinated with travellers attempting improperly documented and other inadmissible travel.

Another effective measure for reducing the risk of insider-enabled conspiracies is to enact a policy prohibiting border officers from having or using their mobile phones while on duty. When border control officers need to be contacted, this should be made through a landline phone located in a monitored central location.

6.2 Manual and Visual Inspection of Travel Documents¹¹²

Passports and travel documents have included printed and other physical security features since they first appeared in booklet form in the 1920s. These features *authenticate* the document, to provide assurance that the document is genuine and unaltered, and issued by the government of its State of origin. The security features in travel documents have increased in number and sophistication since they were first introduced. Nonetheless, fraud in the form of forgery or alteration, or the issuance to, or use of a genuine document by an imposter, persists.

The use of technology is invaluable but the need for human inspection of MRTDs remains. All front-line border control officers should be trained in basic document inspection

and verification techniques, including the identification of fraudulent or altered documents and imposters.

The ICAO training package “Control of the Authenticity and Validity of Travel Documents at Airport Borders – Level 1”¹¹³ is available to assist States in achieving this capability.

Other similar training courses for primary and secondary inspection are offered by international organizations, including the International Organization for Migration (IOM)¹¹⁴ and UNODC¹¹⁵, various States as part of their bilateral cooperation programme, and the private sector.



A good practice is to ensure that frontline border officers have access to some basic tools that can assist in document inspection and verification. Magnifying devices are a simple and inexpensive tool that can be part of the personal equipment of each frontline officer. Another good practice is for basic frontline inspection to be supported by forensic specialists at secondary examination.

Officers working in secondary examination should have access to additional and more sophisticated tools for document examination, including microscopes for more detailed analysis of document security features. UV and other light sources can be used at secondary examination to expose altered or counterfeit text, or to identify disturbance to printed areas, paper or other substrate that may indicate document abuse. Whatever equipment is deployed, it is necessary to provide training in its use.

112 The manual and visual inspection of travel documents is the subject of a range of other publications and as a result is not dealt with exhaustively in this Guide. The intention of the content of this sub-Section is only to highlight that human inspection of travel documents remains of vital importance to effective BCM.

113 *ICAO Training Package Control of the Authenticity and Validity of Travel Documents at Airport Borders – Level 1*, ICAO, 2016, <https://www.icao.int/Training/Pages/TDexam.aspx>

114 *Passport Examination Procedure Manual (Second Edition)*, IOM, 2016, to make an order: <https://publications.iom.int/books/passport-examination-procedure-manual-second-edition>

115 *Guide for the development of forensic document examination capacity*, UNODC, New York, 2010, available at: https://www.unodc.org/documents/scientific/Forensic_Document_Examination_Capacity.pdf

Border control officers should be expert in inspecting and verifying the security features of their own national travel documents, as well as those of other States' travel documents that are commonly encountered on their border¹¹⁶. Relevant training to achieve this expertise should be a high priority for border control agencies.

States have access to databases and image libraries that contain the descriptions and detail the security features of genuine travel documents. These databases include:

- Electronic Documentation Information System on Network (EDISON TD)¹¹⁷;
- The EU database of False and Authentic Documents Online (FADO) – which is only available for EU law-enforcement agencies – and its public version, the Public Register of Authentic travel and identity Documents Online (PRADO)¹¹⁸; and
- Other commercial solutions.

In addition, INTERPOL has developed the Digital INTERPOL Alert Library-Documents Database (Dial-Doc) to counter the illicit use of fraudulent travel documents and foster international cooperation by exchanging national alerts on recently detected forms of false travel documents through INTERPOL's I-24/7¹¹⁹.

It is a practical reality that some travellers will present themselves for inspection without travel documents. The circumstances vary – from scenarios where travel documents are lost by accident to others where the loss is deliberate. In the latter case, identification cards and travel documents presented by the traveller at the start of a journey may have been discarded or destroyed or passed to another traveller for future reuse. SOPs and BCS design should anticipate that they will encounter undocumented travellers. In preparation, detail how interviews should be conducted and provide for the capture and recording of the identity details of travellers. The procedures adopted need to protect the human rights of asylum seekers, victims of trafficking, and objects of human smuggling who may be among the undocumented travellers who may be encountered¹²⁰.

WORKING WITH AIRLINES, AIRPORT MANAGEMENT AND OTHER BORDER AGENCIES

It is an increasingly widespread practice for airlines to check the travel documents of travellers at boarding. While airline check-in and gate agents cannot be expected to be document examination experts, they nonetheless constitute a valuable additional layer in the traveller identification process.

Border control authorities should keep airline personnel operating in their border space informed about trends in improperly documented and other inadmissible travel (including specific examples of travel document fraud) and travellers known to present a risk, so that airline personnel can be more effective in contributing to identification of travellers.

In major embarkation and transit airports, airline check-in and boarding gate personnel are assisted by LOs – State officials seconded to airlines to help ensure that only properly documented travellers board.



116 It is essential that States distribute specimens of their passports to other States, for facilitating international travel and for supporting forensic comparison. Guidance for this distribution can be found in the ICAO Guide for Circulating Specimen Travel Documents, Version 1, ICAO, Montreal, March 2016, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

117 EDISON Travel Documents, available at: <http://www.edisontd.net/>

118 Public Register of Authentic travel and identity Documents Online (PRADO), Council of the European Union, available at: <http://www.consilium.europa.eu/prado/en/prado-start-page.html>

119 Databases, INTERPOL, available at: <https://www.interpol.int/INTERPOL-expertise/Databases>

120 New York Declaration for Refugees and Migrants UN Security Council, New York, 19 September 2016

Border control authorities should also collaborate with airport operators and airlines for the design and operation of access control arrangements¹²¹. Airlines or airport personnel should ensure that all disembarking travellers are escorted to the immigration inspection area and presented promptly to border control officers. Transit passengers should be made to proceed directly to transfer desks or

the transit lounge; these areas should also be secured with appropriate access controls.

Depending on a State's national legislation and the policy of the border control agency, airlines may share responsibility for removing and facilitating the escort of inadmissible travellers. The policies and procedures for escorts should be clearly communicated to airline personnel.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Extracts from ICAO Annex 9 – *Facilitation* Chapter 3. Entry and departure of persons and their baggage¹²²:

I. Inspection of travel documents

3.32 Contracting States shall assist aircraft operators in the evaluation of travel documents presented by passengers, in order to deter fraud and abuse.

3.33 **Recommended Practice.**— *Contracting States should consider making arrangements with other Contracting States to permit the positioning of liaison officers at airports in order to assist aircraft operators to establish the validity and authenticity of the travel documents of embarking persons.*

3.34 Aircraft operators shall take necessary precautions at the point of embarkation to ensure that persons are in possession of the documents prescribed by the States of transit and destination for control purposes as described in this chapter.

3.34.1 The public authorities of each Contracting State shall seize fraudulent, falsified or counterfeit travel documents. The public authorities shall also seize the travel documents of a person impersonating the rightful holder of the travel document. Such documents shall be removed from circulation immediately and returned to the appropriate authorities of the State named as issuer or to the resident Diplomatic Mission of that State, except in cases where public authorities retain documents for law enforcement purposes. The appropriate authorities of the State named as issuer or the Diplomatic Mission of that State shall be notified of such retention by the public authorities that seize the travel documents in question.

3.34.2 Contracting States shall not require aircraft operators to seize documents referred to in Standard 3.34.1.

3.34.3 Contracting States shall not require an aircraft operator to carry a passenger from a point of departure or transit, to the intended final destination, when the travel document presented by that passenger is determined by the State to be fraudulent, falsified or counterfeit, or is held by a person other than to whom the document was legitimately issued.

Note.— Nothing in this provision is to be construed so as to prevent the return of inadmissible passengers whose travel document(s) are fraudulent, falsified or counterfeit or held by an imposter, and have been seized by a Contracting State, in accordance with Standard 3.34.1 and who are travelling under a covering letter issued in accordance with Standard 5.7. ...”

121 Chapter 4 of the *Annex 17 – Security Safeguarding Civil Aviation Against Acts of Unlawful Interference to the Convention on International Civil Aviation*, Tenth Edition, ICAO, Montreal, April 2017, available to purchase at: <https://www.icao.int/Security/SFP/Pages/Annex17.aspx>

122 *Annex 9 – Facilitation to the Convention on International Civil Aviation*, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

J. Departing procedures

“ ...

3.38 **Recommended Practice.**— *Contracting States that require inspection by the public authorities of the travel documents of departing passengers should, in cooperation with airport management, use applicable technology and adopt a multi-channel inspection system, or other means of streaming passengers, in order to expedite such inspections. ...”*

K. Entry procedures and responsibilities

“ ...

3.41 In order to expedite inspections, Contracting States, with the cooperation of airport operators, shall use applicable technology and adopt a multichannel immigration inspection system, or other means of streaming passengers, at international airports where the volume of passenger traffic justifies such measures. ...”

“ ...

3.43 The public authorities concerned shall expeditiously accept passengers and crew for examination as to their admissibility into the State.

Note.— *A passenger or crew member is “accepted for examination” when he makes his first appearance at the arrivals control point after disembarkation, to seek entry into the country concerned, at which time the control officer makes a determination whether he should be admitted or not. This does not include the sighting of travel documents, which may be carried out immediately upon disembarkation. ...”*

“ ...

3.47 Except in special circumstances, Contracting States shall make arrangements whereby the identity documents of visitors need to be inspected only once at times of entry and departure. ...”

“ ...

3.52 After individual presentation by passengers and crew of their travel documents, the public officials concerned shall, except in special individual cases, hand back such documents immediately after examination.

3.53 **Recommended Practice.**— *Contracting States should make arrangements whereby a passenger and his baggage, arriving on an international flight making two or more stops at international airports within the territory of the same State, are not required to be cleared through border control formalities at more than one airport of the State concerned.*

L. Transit procedures and requirements

3.54 Where airport facilities permit, Contracting States shall make provision by means of direct transit areas or other arrangements, whereby crew, passengers and their baggage, arriving from another State and continuing their journey to a third State on the same flight or another flight from the same airport on the same day may remain temporarily within the airport of arrival without undergoing border control formalities to enter the State of transit. ...”

Human Resource Considerations in Border Control Management

While the Inspection Systems and Tools and Interoperable Applications described in Sections 4 and 5 can contribute significantly to effective and efficient BCM, they are not the only contributing factors in achieving these outcomes.

Irrespective of the technology used, no border is secure or efficient without: effective leadership and management, a competent and motivated workforce, clear prioritization of work, sufficient staffing levels and resources, and an overarching policy framework that is robust and adaptive.

7.1 Personnel

This sub-Section addresses key principles and practices for achieving: appropriate staffing levels, training, career opportunities, adequate remuneration, recognition and utilization of personnel skills and experience, communicating to border control officers clear and attainable objectives, required standards of behaviour, and the agreed values of the border agency.

RECRUITMENT AND RETENTION

Border control officers should be recruited and selected for their individual aptitude and capability. Recruitment should target candidates with a strong general education and some insight into and understanding of other cultures, especially those commonly encountered in the border environment where they will work.

The ability to speak foreign languages may be desirable. Consideration should be given to achieving a balanced representation of gender and social backgrounds. Candidates should undergo a thorough background check during the hiring process, and once hired should thereafter be subjected to regular vetting and oversight.

Matching staffing numbers to the demands placed upon them is essential. Border controls cannot be secure if not enough officers are deployed to carry out the processes and use the Inspection Systems and Tools and Interoperable Applications described elsewhere in this Guide. Sufficient border control officers are required to ensure a balance between adequately inspecting all travellers and preventing undue delays.

The salaries and allowances for border officers are a matter for States to determine but it is essential that levels of remuneration be set to attract and retain good candidates. Additional benefits – including housing, transport, meal and travel allowances, and pensions – may serve as motivating factors for retaining border control officers and promoting compliance with border control agency objectives.

MOTIVATION AND TRAINING

Working in border control can at times be routine to the point of monotony. It is important that processes, policies and procedures be in place to keep border control officers alert and fresh. Shifts should be structured so that border control officers are not on duty for too long, and that adequate breaks are built into schedules.

Border control officers should be rotated through front-line and back office duties, to broaden their experience and keep them up to date with changes in policy or procedure. While there are clear benefits to developing ‘specialists’ (for example in document examination, enforcement and intelligence analysis), it is also beneficial that border control officers can carry out the widest possible range of duties relevant to their operational environment.

Border control officers should be given the opportunity to develop their professional skills and experience, either through in-service training or, where possible and appropriate, secondments to other authorities engaged in aspects





of BCM. Shadowing and mentoring programs engaging the skills and experience of senior officers is good practice.

Personnel appraisals provide an opportunity to identify, understand, and address sub-standard performance, as well as to identify career development opportunities. Appraisals should be impartial, aligned with published agency standards and objectives.

PROFESSIONAL STANDARDS

The senior management of border control authorities should set clear and attainable objectives and standards and defined values for the agency. These should be formal, published, and easily accessible for all personnel. While they can be expressed as vision statements and objectives, it is also important that they be sufficiently concrete and concise to be understood by all personnel.

Publicizing and demanding agency-wide adherence to a clear Code of Conduct can reduce the risk of corruption and improve traveller trust.

Documented SOPs contribute to maintaining professional standards, and for providing a basis against which any deviation from accepted practices can be identified. A casework module integrated with BCS can assist in monitoring and auditing border control officer activity, including in recording individual actions and decisions.

Measurable performance indicators should be identified to assess border control personnel. These might include transaction times and queuing times at entry and departure. Performance reporting should be analysed to identify personnel shortages, misaligned work priorities, and ineffective processing methods. One technique is the 'mystery shopper', where an external expert is placed in the traveller queue to observe the border process and personnel performance.

Good practice is for border control agencies to have a professional standards unit, or to have regular external inspection and auditing. External review is an important means of maintaining the confidence of other border control agencies, citizens and travellers in the efficiency and integrity of border officers.

Personnel should be encouraged to make suggestions as to how to improve their jobs and the overall performance of BCM. Personnel who report unprofessional practices of any sort should be protected, and their concerns investigated.

HUMAN FACTORS

Appropriate attention to human factors allows border control officers to perform their duties at the highest level. A human factor is a physical, physiological or cognitive property of an individual or an individual working in a team. Human factors influence and are influenced by human interactions and interfaces with technological systems and their applications.



Human factors are multidisciplinary in nature. They impact on two broad areas, which interrelate so closely that in many cases their influences overlap and factors affecting one may also affect the other:

- Effectiveness of the system (safety and efficiency); and
- Well-being of operational personnel.

For example, motivated individuals perform with greater effectiveness than unmotivated individuals. Some of the many factors that may influence the well-being of operational personnel working in border control include fatigue, body rhythm disturbance, and sleep deprivation or disturbance.

Senior management should identify and mitigate the negative impact of human factors (e.g. ineffective communication, complacency, skill and knowledge gaps, environmental distractions, fatigue) while maximising positive impacts (e.g. team building, skills development).

7.2 Transparency and Governance

Transparency and good governance is essential for maintaining public trust and upholding management and operational standards in BCM. Some simple transparency and governance-related measures and practices have proven effective where implemented by border control agencies.

Two simple good practices for establishing a degree of transparency (as well as deterring corruption) are the use of uniforms and name badges by all border control personnel. This ensures that all border control officers are clearly identifiable by travellers, making them more accountable for performing their duties in a consistent and professional way. In jurisdictions where border control personnel may have concerns relating to their own security about displaying their name, identification by a personal number is a possible alternative.

Organizational-wide implementation of such a policy is preferable, both as a demonstration of support for the practice among senior management, and to promote solidarity between personnel in headquarters and in operational, traveller contact positions.

Having a functional and accessible system for travellers and other customers to report complaints, or simply to provide feedback on their entry or departure experience can increase transparency and achieve good governance in BCM.

Having all border control personnel follow protocols for signing in and out of their shifts is an important way of ensuring individual accountability among border personnel. This accountability commences with a sign on at the start of each shift, and a sign off at the end of each shift.

National BCS typically include session and transaction audit features. For these to be effective, clear protocols need to be developed and enforced. Whenever a frontline officer

takes a seat at an immigration or emigration counter, or at a work station in an office at the airport, they should log on to the system(s) and be required to log out of the system(s).

In the use of such systems, login credentials and passwords should be unique to each authorized officer. The sharing of login credentials or passwords should be strictly prohibited, under any circumstances, and violations should be subject to sanction.

Establishing and enforcing these simple rules is fundamental for accounting for the time of frontline border control officers, as well as for ensuring:

- That the entry of all travellers and crew is processed by the BCS at primary inspection or control; and
- That all referrals to secondary processing are recorded in, and managed by, the BCS.

In scenarios where a traveller cannot be processed through the BCS, those exceptions need to be documented and ultimately rectified, to ensure that all traveller identification and processing is recorded.

It may also be appropriate to monitor interactions between officers and travellers by closed-circuit television (CCTV) and audio. This creates an objective record that can be used in subsequent discussions with personnel, or as supporting evidence in an investigation or a case of complaint.

Taken together, the transaction audit functionality of a BCS can be used in conjunction with login and logoff, timestamping and CCTV recordings to perform transaction pattern analysis of the work of frontline border control officers, yielding useful information about BCM performance.

Finally, a customary practice in many border control agencies is to require that a more senior officer approve of certain courses of action – for example detention, confiscation of a document, or refusal of entry. Engaging this ‘second pair of eyes’ can help to deter arbitrary and unwarranted actions, and to leverage the judgement of an officer with more experience who may be able to suggest a better alternative if one is merited.

Reflecting current priorities, opportunities and challenges, ICAO works with its 192 Member States, international and regional organizations and industry groups to maintain and develop the SARPs related to Annex 9 – *Facilitation, the technical specifications of Doc 9303* and the ICAO TRIP Strategy.

In addition to its core civil aviation standards and policy work, ICAO also provides guidance and assistance to States to implement ICAO requirements.

Assistance to States

8.1 ICAO's Assistance to Member States

ICAO State Letters are one mechanism by which ICAO, under the authority of the Secretary General, officially communicates with Member States and relevant organizations regarding its SARPs and policies. ICAO State Letters are available on the ICAO Secure Portal: <http://portallogin.icao.int/>. For more information on State Letters, please refer to your national civil aviation authority.

ICAO is committed to assisting Member States in the development and maintenance of a NATFP¹²³ and the implementation of the ICAO TRIP Strategy. To enhance the services offered, a secure web-based platform has been developed for use by Member States as a one-stop source of facilitation related information. Upon nominating their National Focal Point and Alternate Focal Point for Facilitation matters, States are granted access to the platform¹²⁴.

IMPLEMENTATION OF THE ICAO TRIP STRATEGY

An action plan for national implementation of the ICAO TRIP Strategy is available to States. The ICAO TRIP Implementation Roadmap for Member States details the actions, organizations responsible, references, supporting resources, proposed timeframes, and the corresponding Annex 9 provisions for each of the five TRIP elements.¹²⁵ Implementation of the Road Map under the National Air Transport Facilitation Committee and Programme is coordinated by the national focal point for facilitation matters¹²⁶.

The ICAO TRIP website includes publications and other resources including technical guidelines, the bi-annual TRIP Magazine and the TRIP Compendium¹²⁷. Publications relevant to BCM are referenced throughout the Guide and in Appendix A.

Through the network of ICAO Regional Offices, the Secretariat provides direct assistance to States¹²⁸. In parallel, in the context of the *No Country Left Behind* initiative, ICAO develops



a resource mobilization strategy – involving Member States, international and regional organizations, manufacturers and stakeholders – to provide States, on request, with technical assistance including funding, capacity-building and technology transfer. This enables States to effectively implement the ICAO SARPs and the TRIP roadmap.

INTERNATIONAL FORA

ICAO encourages States to engage in international fora to keep abreast of contemporary best practices in BCM and to contribute to the development and review of ICAO SARPs and technical specifications.

In this regard, States are invited to attend the annual the ICAO TRIP Symposium and Exhibition in Montreal. The Symposium enables the exchange of information on all aspects of traveller identification management while also providing decision makers and technical experts with insight into current and emerging TRIP related issues.

In collaboration with host Member States, ICAO also arranges regional seminars and workshops around the world. Participation in these events helps attendees to develop their national policies and implementation plans. By engaging with international experts and counterparts from other States, attendees can share experience and best practices. Information on past and upcoming events

123 See: sub-Section 3.4 Border Control Management Agencies and Stakeholders

124 *Nomination of a National Focal Point for Facilitation*, ICAO State Letter No. EC 6/1-16/106, 14 December 2016 available at: <http://portallogin.icao.int/>.

125 *ICAO Traveller Identification Programme (TRIP) Implementation Roadmap for Member States*, ICAO, July 2017, available at: <https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Implementation%20Roadmap.%20July%202017.pdf>

126 *ICAO TRIP Implementation Roadmap for Member States*, ICAO State Letter No. EC 6/3-17/96, 11 August 2017. ICAO available at: <http://portallogin.icao.int/>.

127 *TRIP Compendium*, ICAO, Montreal, 2017 available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

128 *ICAO's Regional Presences*, ICAO, available at: <https://www.icao.int/secretariat/RegionalOffice/Pages/default.aspx>

is available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Events.aspx>. States interested in hosting regional seminars or workshops are invited to write to: FAL@icao.int.

Additionally, States are encouraged to participate as members or observers in the Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP). The main objective of the TAG is to advise and support the ICAO Secretariat in developing policy, recommendations and proposals for the implementation of the ICAO TRIP Strategy, including the development and maintenance of MRTD standards and specifications¹²⁹.

All States are invited to nominate experts in: Evidence of Identity, MRTDs, Document Issuance and Control, Inspection Systems and Tools, and Interoperable Applications to participate in the TAG/TRIP. For more information on the TAG/TRIP and for membership, please visit: <https://www.icao.int/Security/FAL/TRIP/Pages/Panels.aspx>.

States seeking broader exposure to the Annex 9 SARPs relating to BCM can attend as observers the periodic meetings of the ICAO Facilitation (FAL) Panel. Further information on the FAL Panel can be found at: <https://www.icao.int/Security/FAL/ANNEX9/Pages/Panel.aspx>.

To ask questions or communicate with the Facilitation Section, States are invited to write to: FAL@icao.int.

8.2 Other International Assistance

ICAO works with numerous international organizations to coordinate policy development and assistance to States.

As described in Section 3, ICAO complements the policy and assistance work of the UN Counter-Terrorism Committee Executive Directorate (CTED) and the UN CTITF inter-agency Working Groups to help States with implementation of the UNSCR¹³⁰ related to counter-terrorism.

Outside ICAO, representatives of BCM agencies from many States meet their airline partners in the IATA Control Authorities Working Group (IATA/CAWG)¹³¹, a forum for ongoing dialogue between airlines and Immigration officials regarding the control of illegal migration.

For operational implementation of API and PNR¹³², ICAO works in partnership with the WCO and IATA.

ICAO and INTERPOL work closely together to help States integrate their BCS with the mechanisms of INTERPOL, including the SLTD database¹³³. A memorandum of understanding signed by ICAO and IOM in 2016 formalised the partnership for delivering BCM and other MRTD related technical assistance to States. IOM, the UN migration agency, has more than 400 offices worldwide. IOM is a project based organization that works among others to implement ICAO SARPs, and technical specifications, through migration and border management projects¹³⁴. IOM is well placed to deliver strategic and operational advice and support to States that are working to develop and enhance their BCM.

Engaging with these organizations, committees and panels, and relying on their publications can provide States with deep insights into contemporary best practice, thus informing national BCM policy development and implementation.

129 *Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP)*, ICAO, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Panels.aspx>

130 *Security Council Resolutions*, United Nations Security Council, available at: <http://www.un.org/en/sc/documents/resolutions/>

131 IATA/Control Authorities Working Group (IATA/CAWG), IATA, available at: <http://www.iata.org/whatwedo/workgroups/Pages/icawg.aspx>

132 See: *Topics H- Advance Passenger Information and Interactive Advance Passenger Information and Topic I - Passenger Name Record*

133 See: *Topic L - INTERPOL SLTD Databases*

134 *Immigration and Border Management*, International Organization for Migrations, available at: <https://www.iom.int/>

Appendix A

Reference Documentation

1. ICAO

Chicago Convention and Annexes

Annex 9 – Facilitation to the Convention on International Civil Aviation, Fifteenth Edition, ICAO, Montreal, October 2017, available to purchase at: <https://store1.icao.int/index.php/annex-9-facilitation-english-printed-13239.html>

Annex 17 – Security Safeguarding Civil Aviation Against Acts of Unlawful Interference to the Convention on International Civil Aviation, Tenth Edition, ICAO, Montreal, April 2017, available to purchase at: <https://www.icao.int/Security/SFP/Pages/Annex17.aspx>

Convention on International Civil Aviation, Ninth Edition, Doc 7300/9, ICAO, Montreal, September 2006, available at: https://www.icao.int/publications/Documents/7300_9ed.pdf

Manuals and Documents

Doc 9303, Machine Readable Travel Documents, 7th Edition, ICAO, Montreal, 2015, available at: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

Guidelines on PNR Data, First Edition, Doc 9944, ICAO, Montreal, 2010, available to purchase at: <https://store1.icao.int/index.php/guidelines-on-passenger-name-record-pnr-data-doc-9944-english-printed.html>

Model National Air Transport Facilitation Programme – First Edition, Doc 10042, ICAO, Montreal, 2015, available to purchase: <https://store1.icao.int/index.php/model-national-air-transport-facilitation-programme-doc-10042-english-printed-12870.html>

Guidelines

All ICAO TRIP guidance material is available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

ICAO Guide for Assessing Security of Handling and Issuance of Travel Documents, ICAO, Montreal, March 2017

ICAO Guide for Best Practice Guidelines for Optical Machine Authentication, Version 1, ICAO, Montreal, April 2016

ICAO Guide for Circulating Specimen Travel Documents, Version 1, ICAO, Montreal, March 2016

ICAO Guide for Collection of Best Practices for Acquisition of Machine Readable Travel Document Goods and Services, Version 1, ICAO, March 2016

ICAO TRIP Implementation Roadmap for Member States, ICAO, July 2017

Working Papers

Proposal for an ICAO Traveller Identification Programme (*ICAO TRIP*) Strategy, A38-WP/11, Assembly – 38th session, 2013, available at: https://www.icao.int/Meetings/a38/Documents/WP/wp011_en.pdf

State Letters

State Letters are available on the ICAO Secure Portal: <http://portallogin.icao.int/>. For more information, please refer to your national civil aviation authority.

ICAO TRIP Implementation Roadmap for Member States, ICAO State Letter No. EC 6/3-17/96, 11 August 2017

Annex 9 – Facilitation: Provisions on the Stolen and Lost Travel Documents (SLTD) database of INTERPOL, ICAO State Letter, Ref.: EC 6/3 – 17/92, 24 July 2017

Nomination of a National Focal Point for Facilitation, ICAO State Letter No. EC 6/1-16/106, 14 December 2016

ICAO Public Key Directory (PKD), ICAO State Letter No. EC 6/8.3 – 16/70, 25 July 2016

ePassport Basics, ICAO, Montreal, available at: <https://www.icao.int/Security/FAL/PKD/Pages/ePassportBasics.aspx>

Other ICAO publications

ICAO PKD, ICAO, Montreal, available at: <https://www.icao.int/Security/FAL/PKD/Pages/default.aspx>

ICAO PKD data download, ICAO, Montreal, available at: <https://pkddownloadsg.icao.int/>

ICAO PKD Participants, ICAO, Montreal, available at: <https://www.icao.int/Security/FAL/PKD/Pages/ICAO-PKDParticipants.aspx>

ICAO Public Key Directory Video, ICAO, Montreal, available at: <http://www.icao.int/Security/FAL/Pages/PKD-Video.aspx>

ICAO's Regional Presence, ICAO, available at: <https://www.icao.int/secretariat/RegionalOffice/Pages/default.aspx>

ICAO Training Package “Control of the Authenticity and Validity of Travel Documents at Airport Borders – Level 1”, ICAO, Montreal, 2016, <https://www.icao.int/Training/Pages/TDexam.aspx>

Passenger Name Record Guidelines, Version 13.1, WCO/IATA/ICAO, October 2013, <https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx>

PKD Machine Readable Error Codes, ICAO PKD Board, Montreal, 2011 available at: <https://www.icao.int/Security/FAL/PKD/Documents/PKDTechnicalDocuments/PKD%20Machine%20Readable%20Error%20Codes.pdf>

Publications, PKD Finance Documents, ICAO, Montreal, available at: <https://www.icao.int/Security/FAL/PKD/Pages/Publications.aspx>

Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP), ICAO, available at: <https://www.icao.int/Security/FAL/TRIP/Pages/Panels.aspx>



2. United Nations

Charter

Chapter VII, Charter of the United Nations, available at: <http://www.un.org/en/sections/un-charter/chapter-vii/>

Preamble Charter of the United Nations, United Nations, San Francisco, 1945, <http://www.un.org/en/charter-united-nations/index.html>

United Nations Security Council Resolutions

Consolidated United Nations Security Council Sanctions List, United Nations Security Council, <https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list>

Security Council Resolutions, United Nations Security Council, available at: <http://www.un.org/en/sc/documents/resolutions/>

Other UN Documentation

Principles and Recommendations for a Vital Statistics System – Third Edition, United Nations Statistical Division, New York, 2014, available at: <https://unstats.un.org/unsd/demographic/standmeth/principles/M19Rev3en.pdf>

Sustainable Development Goals, United Nations, available at: <https://sustainabledevelopment.un.org/>

3. International Organizations

Advance Passenger Information Guidelines, Version 3.0, WCO/ IATA/ICAO, October 2013, <https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx>

Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime, available at: <http://www.baliprocess.net/regional-support-office/resources/>

Border management, INTERPOL, <https://www.interpol.int/INTERPOL-expertise/Border-management>

Border Management, Organization for Security and Co-operation in Europe, available at: <http://www.osce.org/secretariat/borders>

CARICOM Implementing Agency for Crime and Security (IMPACS), CARICOM, available at: <http://www.caricom.org/about-caricom/who-we-are/institutions1/caricom-implementing-agency-for-crime-and-security-impacs>

Good Practices in the Area of Border Security and Management in the Context of Counterterrorism and Stemming the Flow of Foreign Terrorist Fighters, Global Counterterrorism Forum, New York, 2016, available at: <https://www.thegctf.org/Cross-Cutting-Initiatives/Border-Security-Initiative>

Guide for the development of forensic document examination capacity, UNODC, New York, 2010, available at: https://www.unodc.org/documents/scientific/Forensic_Document_Examination_Capacity.pdf

IATA/WCO/ICAO Toolkit: presentation slides, IATA, 2013, available at: <http://www.iata.org/iata/passenger-data-toolkit/presentation.html>

IATA/Control Authorities Working Group (IATA/CAWG), IATA, available at: <http://www.iata.org/whatwedo/workgroups/Pages/icawg.aspx>

I-Checkit, INTERPOL, <https://www.interpol.int/INTERPOL-expertise/I-Checkit>

Immigration and Border Management, International Organization for Migrations, available at: <https://www.iom.int/INTERPOL>, <https://www.interpol.int/>

Notices, INTERPOL, <https://www.interpol.int/INTERPOL-expertise/Notices>

View Red Notices, INTERPOL, <https://www.interpol.int/notice/search/wanted>

Passport Examination Procedure Manual (Second Edition), IOM, 2016, to make an order: <https://publications.iom.int/books/passport-examination-procedure-manual-second-edition>

Passenger Name Record Guidelines, Version 13.1, WCO/ IATA/ICAO, October 2013, <https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx>

Recommended Principles and Guidelines on Human Rights at International Borders, OHCHR, 2014, available at: http://www.ohchr.org/Documents/Issues/Migration/OHCHR_Recommended_Principles_Guidelines.pdf

Special Notices, INTERPOL – United Nations Security Council *Special Notice*, INTERPOL, <https://www.interpol.int/INTERPOL-expertise/Notices/Special-Notices>

I-Checkit, INTERPOL, <https://www.interpol.int/INTERPOL-expertise/I-Checkit>

View Red Notices, INTERPOL, <https://www.interpol.int/notice/search/wanted>

4. Regional Organizations

EDISON Travel Documents, available at: <http://www.edisontd.net/>

European travel information and authorisation system – Council agrees negotiating position, European Council, June 2017, available on: <http://www.consilium.europa.eu/en/press/press-releases/2017/06/09-etias/>

Policy Framework for the Regional Biometric Data Exchange Solution, Bali Process, available at: <http://www.baliprocess.net/UserFiles/baliprocess/File/Policy%20Framework%20for%20the%20RBDES%20part09.pdf>

Public Register of Authentic travel and identity Documents Online (PRADO), Council of the European Union, available at: <http://www.consilium.europa.eu/prado/en/prado-start-page.html>

Publications, European Union's Border and Coast Guard Agency, available at: <http://frontex.europa.eu/publications/>

Regional Biometric Data Exchange Solution (RBDES), The Bali Process, available at: <http://www.baliprocess.net/regional-support-office/regional-biometric-data-exchange-solution/>

5. National and Others

Biometrics Program downloads, NIST (US), available at: <https://www.nist.gov/programs-projects/biometrics>

Biometric Recognition: Challenges and Opportunities National Research Council (US), 2010 available at: <https://www.nap.edu/catalog/12720/biometric-recognition-challenges-and-opportunities>

Code of practice for the implementation of a biometric system, PAS 92:2011, British Standards Institution (BSI), 2011, available to purchase at: <http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030213319>

DHS Traveler Redress Inquiry Program (DHS TRIP), available at: <https://www.dhs.gov/dhs-trip>

Machine Authentication of MRTDs for Public Sector Applications, Technical Guideline BSI TR-03135, Version 2.2.0, Federal Office for Information Security of Germany, Bonn, 2017, available in English at: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03135/index_hm.html

Standards for the automated recognition of individuals based on their behavioural and biological characteristics, British Standards Institution (BSI), 2010, available to purchase at: <http://shop.bsigroup.com/upload/Standards%20&%20Publications/BrochureDownload/BiometricsBrochure2010.pdf>

The 9/11 Commission Report (US) Washington, 2004, available at: <http://govinfo.library.unt.edu/911/report/911Report.pdf>

