VERSION 1, DRAFT 4, NOVEMBER 2017

STATUS: Working Final Draft

ACTION: Please send your comments before 4 December 2017 to: kboulet@icao.int with copy to dsterland@icao.int and ross@identitymatters.net.au

ICAO TRIP Guide on BORDER CONTROL MANAGEMENT

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:

IMPACS

CTED
UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE

INTERPOL

International Organization for Migration (IOM)
The UN Migration Agency

ECS

UNHCR
The UN Refugee Agency

UNODC
United Nations Office on Drugs and Crime

CONTENTS

EXECUTIVE SUMMARY

The International Civil Aviation Organisation (ICAO) is the only 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. While in the past ICAO concentrated on the physical security of travel documents, under the Traveller Identification Programme (TRIP) Strategy endorsed by the ICAO Assembly, ICAO's mandate has expanded to include traveller identification. ICAO is focused on ensuring a holistic and coordinated approach to traveller identification - from document issuance to border control solutions. The ICAO TRIP Strategy is a framework for uniquely identify travellers for enhancing border security and facilitation by bringing together the elements of identification management.

Border Control Management (BCM) is the sovereign responsibility of States. In their traveller border control arrangements States seek to maximise the economic, societal and political benefits of travel while at the same time identifying and mitigating risks and threats. To achieve these national objectives, States must identify travellers and assess traveller risk.

States combine the Inspection Systems and Tools and Interoperable Applications of the TRIP Strategy in their Border Control Systems (BCS) – the integrated ICT solutions that support BCM.

While States can be expected to have extensive knowledge of their own citizens and residents, they rely on advice from other States about the identity and nationality of the citizens and residents of other States.

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 way.

Other United Nations (UN) agencies and international organisations contribute to BCM undertaken by States. The UN sanctions watchlist and INTERPOL Red Notices identify potential travellers of security and law enforcement concern to States. Checks against INTERPOL's Stolen and Lost Travel Documents database are essential prior to relying on travel documents as evidence of identity.

The *ICAO Traveller Identification Programme (TRIP) Guide on Border Control Management* describes the contribution made by ICAO, other UN agencies and INTERPOL to traveller identification and risk assessment. The Guide explains the interdependencies that link the traveller identification and traveller risk assessment undertaken by States.

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

The Guide is intended for practical application by States to optimize the use and interoperability of the tools, systems and processes available to enhance their national Border Control Management. The guide includes 13 technical topics describing and categorizing the Inspection Systems and Tools and Interoperable Applications endorsed by ICAO's Traveller Identification Programme Strategy that can be applied for this purpose.

The national border inspection systems and tools and interoperable applications **together comprise** the BCS used by States.

Differences in national BCS reflects differences in which inspection systems, tools and interoperable applications are used and how they are combined and integrated. The Guide identifies options to enhance national BCS, to improve traveller identification and risk assessment, 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.

The other activities of the project, regional workshops (Antigua and Barbuda, and Jamaica) and 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, and International and Regional Organizations, 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 global use and for all Member States of ICAO.

THE CONTENT OF THE GUIDE REFLECT THE INVALUABLE CONTRIBUTIONS OF:

- ICAO Implementation and Capacity Building Working Group (ICBWG)
- ICAO New Technologies Working Group (NTWG)
- 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

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

LDS	Logical Data Structure
LO	Liaison Officer (airline/immigration)
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
UNSCR	United Nations Security Council Resolution
USA	United States of America
VIZ	Visual Inspection Zone
WCO	World Customs Organization
XML	Extensible Markup Language

DEFINITIONS

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 unforgettable.

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 of:
  - 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 set forth in ICAO Doc 9303, *Machine Readable Travel Documents*[2].

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

The Guide is intended for practical application by States to optimize the use and interoperability 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, policy development, budgetary planning, legislative reform initiatives, Information and Communication Technology (ICT) systems change, operational planning, the identification of training needs, and the application of best practices.

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. Environment and Strategy describes how the different circumstances faced by individual States define their security and facilitation challenges, and should thus inform their national BCM strategies.

4. National Border Inspections Systems and Tools comprises seven technical topics describing how States can capture, verify, record, and utilize data about travellers and their travel documents:

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 additional data about travellers - nationally, regionally and internationally:

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 Database of Stolen and Lost Travel Documents
M. International Watchlists

6. Traveller Examination and Travel Document Inspection provides an overview of the responsibilities and roles of border agency staff 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 national practices in BCM.

The substantive content of the Guide is comprised of the 13 technical topics under sections 4 and 5, as described above. These have been developed to allow for standalone use, thus acronyms are reintroduced for each topic. Each of the 13 technical topics is presented following a uniform structure:

Uniform structure of each of the 13 technical topics	
	Key Messages – a synopsis of the main points under that topic.
	Overview – a background or overview 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 and citations for literature specifically mentioned in the topic, and other information sources for readers that wish to make deeper investigation 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 Assessment Tool, the companion document of the Guide, can be used by States to self-assess their BCM system, processes and capabilities. It 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.

2 ICAO TRIP and Border Control Management

2.1 ICAO Traveller Identification Programme

The International Civil Aviation Organisation (ICAO) is the only 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. While in the past ICAO concentrated on the physical security of travel documents, under the Traveller Identification Programme (TRIP) Strategy endorsed by ICAO Assembly, ICAO's mandate has expanded to include traveller identification.

ICAO is now focused on ensuring a holistic and coordinated approach to traveller identification - from document issuance to border control systems. The ICAO TRIP Strategy[3] 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 Goals.[4] It also helps to manage security risks and to respond to threats at borders by enabling better targeting of resources on 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 supportive.

Evidence of Identity - credible evidence of identity to create, trace, link and verify identity against breeder documents to ensure authenticity of identity;

MRTDs - the design and manufacture of standardized MRTDs, including ePassports, that comply with ICAO specifications;

Document Issuance & Control – processes and protocols for document issuance by appropriate authorities to authorized holders, and controls to prevent theft, tampering and loss;

Inspection Systems and Tools – inspection systems and tools for the efficient and secure reading and verification of MRTDs, including the use of the ICAO PKD[5]; and

Interoperable Applications - global systems for the timely, secure and reliable linkage of MRTDs and their holders to relevant data during inspection operations.

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.

National border **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 sharing of national, regional and international data about travellers and their travel documents with **Interoperable Applications**. Together, these mechanisms enable States to identify travellers and to perform targeted traveller risk assessment.

3 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

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

5 For the purpose of the ICAO TRIP Guide on BCM, ICAO Public Key Directory (PKD) is treated as an Interoperable Application.

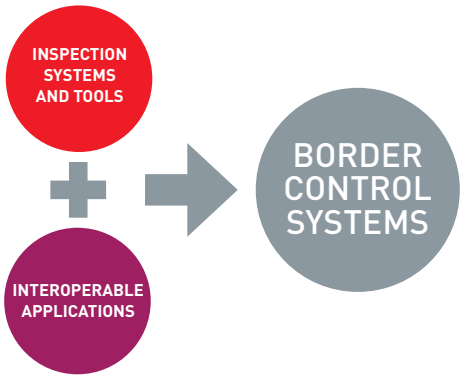
2.2 Integrating national border Inspection Systems and Tools with Interoperable Applications

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 to, stay in, and departure of travellers. These measures are designed to realise 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 the national interest. 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**.

The Border Control Systems (BCS) used by States integrate interoperable applications with national inspection systems and tools. Not all States employ all of the available inspection systems, tools and interoperable applications that are supported by the ICAO SARPs and technical specifications. Rather, interoperable applications are integrated with national inspection systems and tools in different ways and in differing ICT systems architectures by different States.



States combine the Inspection Systems and Tools and Interoperable Applications of the TRIP Strategy in their Border Control Systems (BCS)

The ICAO TRIP Guide on BCM is intended to assist States in identifying options to improve their current BCS, and as a result to support better BCM outcomes.

Global interoperability of MRTDs enables Inspection Systems and Tools to capture, verify and record the data contained in 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 both facilitate and secure travel.Section 4 of this Guide discusses seven Inspection Systems and Tools:

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 national, regional and international data about travellers to be shared, subject to appropriate privacy and data protection legal frameworks, within and between national border agencies and internationally with counterpart border agencies, airlines and international organizations.

Section 5 of this Guide discusses six Interoperable Applications:

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 Database of Stolen and Lost Travel Documents
M. International Watchlists

The integration of national border Inspection Systems and Tools with Interoperable Applications in national BCS allow traveller risk assessments to be undertaken throughout the traveller journey, informed by the identification of travellers using the new information that becomes available to the receiving/destination State at each phase of the journey.

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

The distinction made in the TRIP Strategy between national border inspection systems and tools and interoperable applications disappears in well integrated national border control systems. In States with effective BCM, the BCS achieves traveller identification and traveller risk assessment in a circular process repeated throughout the journey.

GLOBAL INTEROPERABILITY OF MRTDS: THE FOUNDATION OF BCM

Efficiently reading and effectively using the standardized, interoperable, machine readable data elements included in ICAO compliant Machine Readable Travel Documents (MRTDs) and electronic MRTDs (eMRTDs) is the foundation of BCM.

The technical specifications for travel documents are published in Doc 9303, *Machine Readable Travel Documents*[6]. 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 interchange, the MRTD plays a pivotal part in modern, enhanced compliance systems.

Equipment to read the documents and access the databases may entail a substantial investment, but this can be expected to be returned by the improvements in security, clearance speed and accuracy of verification which such systems provide. Use of MRTDs in automated border control systems 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) is the key to retrieving 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) authentication[9] and retrieval of biometric images in Automated Border Control (ABC) [10] and human processing solutions.

The extent to which MRTDs and eMRTDs contribute to efficient processing of air travellers depends on the combined impact of three factors:

1. The proportion of travellers holding MRTDs and eMRTDs, and how reliably and consistently these documents meet interoperability standards determines how efficiently data elements can be extracted from them. For most States, their own citizens form the largest single group of travellers while travellers from a small number of other States make up a significant proportion of the remaining travellers.
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 national border control systems achieving reliable and consistent presentation of traveller details to border inspection officials.

6 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

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 Baggage[11]:

"...

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.*

..."

2.3 Identification of Travellers and Risk Assessment

International best practice in border processing is to integrate the identification of travellers and risk assessment, and to repeat the assessment at each phase of the journey as new information becomes available to the receiving/destination State.

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, police for law enforcement.

The MRTD provides border control authorities with a convenient, efficient means to examine and record biographic and biometric identity data and to record travel history providing evidence of continuity of the identity that is claimed by the traveller.

Many States are transitioning from the traditional reliance on completing a single step traveller identification and risk assessment at entry controls, towards the best practice of continuous risk assessment informed by information about travellers obtained at and before the commencement of their journey. Watchlist searches and risk based targeting require the input of identity and nationality data. The risk analysis to develop actionable intelligence requires combining identity data with travel and other data.

Identification of Travellers: The essential foundation for Risk Assessment of Travellers

The identification of travellers, informs, and is informed by risk assessment. When doubts arise about traveller identity, the risk assessment needs to be revisited. When new or additional risk factors are identified, the identification of travellers may need to be reassessed.

Additional information collected about travellers at each phase is transmitted to the receiving/destination State's border agencies that analyze, review, develop and enhance it to transform it into actionable intelligence useful in the assessment of traveler risk. The scope of the assessment includes all matters of concern to the State, typically criminal, security, biosecurity and public health risks and threats.

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

Before travel commences, the receiving/destination State may have information available to them about the anticipated or expected travel of their 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 reservations systems (in the form of Passenger Name Record (PNR)).

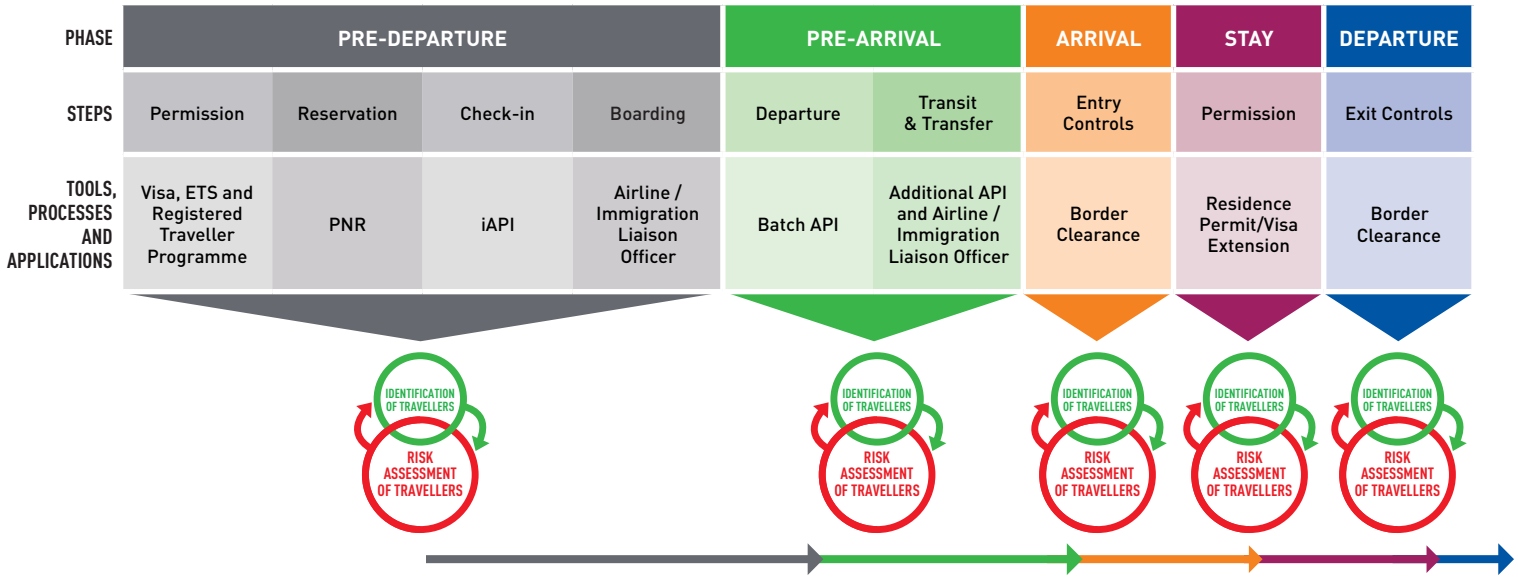
Once travel commences, additional information becomes available from the departure control systems of airlines (in the form of iAPI and/or API). When travellers transit, transfer and then arrive at their final destination, States can obtain new information about travellers, whether via human interactions with border officials or automated interactions at kiosks and eGates.

When traveller identification and risk assessment is managed continuously across the traveller journey, the analysis of all relevant information can inform decisions about whether travel should be allowed to commence or continue, whether entry or departure should be allowed, and whether an extension of stay and residence permit will be allowed, if it is sought. Not every person presenting a risk or threat will be prevented or deterred pre-departure, and some will enter States without being detected.

Enabling this integration of national border inspection systems and tools with interoperable applications is the objective of the TRIP Strategy.

*Some of the inspection systems and tools and interoperable described later in the Guide contribute primarily to the identification or travellers **or** to traveller risk assessment. Other inspection systems and tools and interoperable contribute strongly to both the identification of travellers **and** to traveller risk assessment.*

The key messages that commence each of the 13 technical topic details in Sections 4 and 5 of the Guide describe the role each plays, and the relative contribution they make, to either identification of travellers, or traveller risk assessment, or both.



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

3 Environment and Strategy

The regulatory framework, procedures, practices and technologies for BCM described in this guide are the product of the response of national border control agencies, ICAO, the United Nations (UN) and other international organizations to both the opportunities and challenges that arise from the growth in civil aviation.

Historically, air transport has doubled in size every fifteen years. In 2016, airlines worldwide carried around 3.8 billion travellers, and it's expected to reach over 7 billion by 2030, according to the ICAO long-term traffic forecasts.

In addition to this increase in the volume of air travel, more travellers from a larger number of countries are travelling to countries previously less visited. As a result, the challenge of identification and risk assessment of travellers has grown. The international response to emerging threats includes new interoperable applications to combat the threat of terrorism and other trans-national crime.

To be effective, the national strategic frameworks for BCM implemented by States need to incorporate the identification of travellers as a foundation to informing the assessment and mitigation of risks and threats, to ensure that the economic, social and political benefits of travel can continue to be realised. It is critical also that national strategic frameworks are a response to the unique border control environment and the pattern of travel (including intra-regional travel) faced by each State.

3.1 Strategic framework for Border Control Management

Effective BCM is fundamental to national sovereignty. It is the central responsibility of government agencies with responsibilities for border control to regulate travel, entry, transit, stay and departure in the national interest. A national BCM strategy should enhance border security while facilitating the movement of legitimate travellers.

The ICAO TRIP strategy recognizes that improved border control arrangements can be achieved, in part, by the application of technology. National border inspection systems and tools and interoperable applications support the identification and risk assessment of travellers, an iterative process applied at all phases of 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 border control systems 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 that comprise Sections 4 and 5 of this Guide.

A strong business case must be developed prior to implementing technology solutions to ensure that benefits in increasing the security and facilitation of travel 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 in the business case.

As a result, the successful application of technology is dependent on a national strategic framework that includes:

- A policy framework that provides statements of strategy and objectives. Policy is about translating the objectives of Governments into outcomes.
- A legal framework that provides the "authority" to do things.
- A systems framework comprising:
  - business processes that determine "how" things are done; and
  - an ICT framework that determines how technology supports, enables and constrains "how" things are done.
- Organizational structures and relationships that contribute to the achievement of BCM national objectives.

In best practice jurisdictions, the expression of a Government's intentions in the policy framework is formalized into a set of binding rules in the legal framework, which determines the structure for the systems framework which are supported by organizational arrangements.

For effective BCM, the national legislative 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 incorporate mission and vision statements, that relate activities and processes to measurable outputs and high-level outcomes, give purpose and focus to the work of national BCM 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.

With a shared vision and common purpose, BCM agencies are better placed to understand their capability and capacity gaps, and assess their competing investment and development priorities. Without these insights States are more likely to invest in expensive ICT solutions that are an inappropriate response to their national BCM environment.

3.2 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 natural hubs for international civil aviation.

The movement of travellers has shaped and been shaped by conflicts, political instability, colonialism, human rights abuses, economic factors including labour migration, 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, and victims and perpetrators of people smuggling and human trafficking.

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. Overwhelmingly, travel is undertaken by properly documented travellers to, via and from border control points designated by States. However, properly documented travellers may have criminal or terrorist intentions, or otherwise be identified as inadmissible persons.

Travel is also undertaken by imposters, improperly documented[12] and other inadmissible persons, including Foreign Terrorist Fighters (FTFs) and other trans-national criminals. The journeys undertaken by these travellers can be carefully contrived to evade identification and border controls by using broken or complex travel schemes using different transport modalities, and by targeting locations where border controls are weak. Persons of interest may seek opportunities to take advantage of the various arrangements to facilitate properly documented travellers. Imposters and improperly documented travellers include vulnerable people seeking asylum or an improvement in their economic circumstances.

The sustained growth of air transport and increasingly complex composition of travellers have made effective identification of travellers at exit control more important.

National strategies and policies for BCM should seek to influence the future composition and scale of properly documented travellers, and to minimize the incidence of improperly documented travellers, for the benefit of the State - while at the same time meeting the State's international obligations.

3.3 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"[13].

12 Annex 9 defines an improperly documented person as: "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."

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

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 foundations for Machine Readable Convention Travel Documents (MRCTDs);
- 2000 United Nations Convention against Transnational Organized Crime (and the 2000 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children and the 2000 Protocol against the Smuggling of Migrants by Land, Sea and Air), 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).

The Refugee Convention and Protocol, the Convention against Transnational Crime and the human rights instruments whose implementation are the broad responsibility of UNHCR, UNODC and OHCHR, respectively, share as their focus the protection of the vulnerable. Their application in BCM is critical to ensure that the basic human rights of vulnerable travellersare protected. The Refugee Convention and its Protocol ensures the right to seek asylum for persons who are fleeing armed conflict or persecution, and 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 whose implementation ensures protection of these rights[14].

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 SARPs[15], 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"* mentioned above) 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.

Extracts of the main ICAO SARPs relevant to BCM are included throughout the Guide.

In addition to their treaty obligations, Member States are obligated under the UN Charter to implement decisions made by the UN Security Council[16]. Some of these provisions are concerned with regulating travel, and are therefore directly relevant to BCM. UN Security Council Resolution (UNSCR) 2178 (2014) [17] was adopted in response to the threat stemming from foreign terrorist fighters (FTFs) which has increased the pressure on Member States and

14 *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

15 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. For further information, please consult *Manual on Notification and Publication of Differences*, Doc 10055, ICAO, Montreal, YYYY, available at: TO BE PUBLISHED.

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

17 *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/

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.

In separate provisions UNSCR 2178 references Council Resolutions 1267, 1989 and 2253, which established, then extended, the scope of the Consolidated United Nations Security Council Sanctions List (CUNSCSL). UNSCR 2178 notes that the activities of FTFs, and those who support them, may make them eligible for inclusion on a sanctions list.[18] The application of sanctions lists in BCM is discussed in *Topic N – International Watchlists of this Guide*.

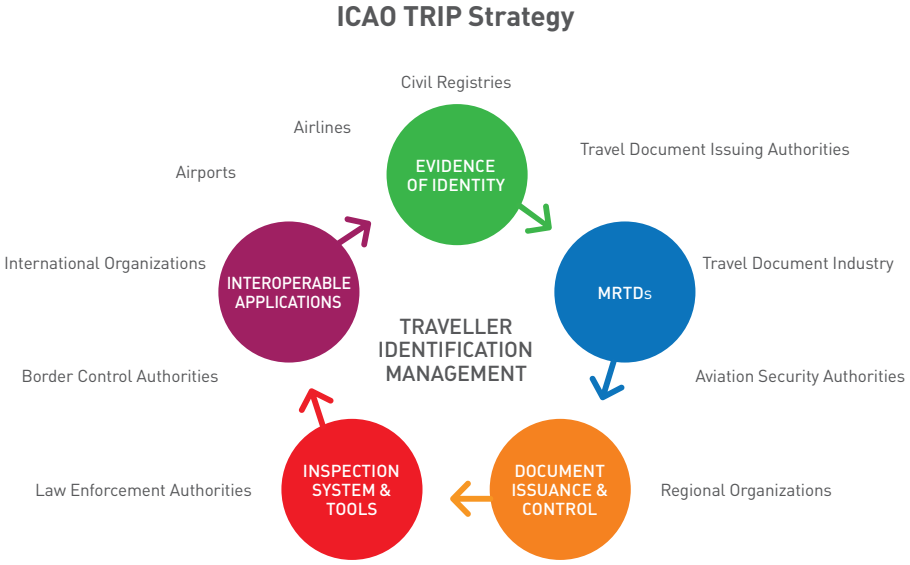
UN SCR 2309 (2016) is a direct call to States to ensure the security of civil aviation by, inter alia, implementing ICAO Annex 9 "...standards and recommended practices relevant to the detection and prevention of terrorist threats involving civil aviation."[19]

3.4 Border Control Management Agencies and Stakeholders

The ICAO TRIP Strategy recognizes that traveller identification management requires cooperation within and between government agencies, and with international organizations and private stakeholders. BCM in international civil aviation operates in a challenging, time critical, high transaction volume, processing environment. ICAO Annex 9 includes time based Recommended Practices for the completion of entry clearance formalities for this reason.

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

19 *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/



"...

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 check-in, 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 check-in, 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 complexity of BCM and the underlying identification and risk assessment of travellers throughout the traveller journey is reflected in the range of public and private stakeholders involved:

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

Border controls are stronger when all border agencies consider the broader aspects of their interaction with travellers, not just those confined to their own jurisdiction. An "all risks, all threats" approach to BCM is a feature of effective 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 so that they can manage their interventions throughout the journey to inform the traveller risk assessment.

As such, national law enforcement and security agencies should maintain close relationships with the agency responsible for immigration clearance, because they rely on the identification of travellers as a foundation for investigation and intelligence analysis.

In best practice States, the national agency responsible for immigration clearance at national borders makes identity verification decisions based on information provided by other national agencies and stakeholders:

- For its own **nationals**, based on the national passports they present to airlines and border agencies, verified against information recorded in the national passport and travel movement databases; and
- For **foreigners**, based on the foreign passports the travellers hold, information obtained from airlines and information recorded in the national visa, residence permit and travel movement databases.

The agencies responsible for civil registration, national identity card issuance and/or other large national identity databases (e.g. driver's licenses) are typically not represented at the border, but access to their data through modules integrated in the border control system provides critical support to BCM.

The agency responsible for immigration clearance requires insight into the different business processes for visa and passport issuance that lead to traveller processing at the border.

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. Threats and risks that are the narrow responsibility of individual agencies need to be managed in a broader context of serving the national interest, and meeting international obligations.

The Border Security Initiative of the United Nations Counter-Terrorism Centre (UNCCT) 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 context[20].

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 that must be accomplished with respect to aircraft engaged in international operations and their passengers, crew and cargo. The meetings of its committee are a forum for consultation and information-sharing amongst the participants.

While the primary responsibility for the NATFP rest with the civil aviation authority, the coordination should be taking place with the participation of other ministries and agencies (agriculture/environment, customs, foreign affairs, identification card issuing authorities, immigration, passport/visa issuing authorities, public health, security and narcotics control, quarantine and tourism), public and private airport operators, international airline operators further to other governmental of non-governmental entities that have a role in promoting the international tourism and trade.

ICAO provides guidance to States on NATFP in the Annex 9 – *Facilitation* for which relevant SARPs are available below and in the ICAO Doc 10042 Model National Air Transport Facilitation Programme[21].

The work of the NATFP complements and is complemented by the National Civil Aviation Security Programmes and Committees given that facilitation and security are complementary matters in international civil aviation. ICAO recommends that members of border control agencies participate in both national Facilitation and Aviation Security committees.

20 *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

21 *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

Relevant ICAO Standards and Recommended Practices and State Letter

Extracts from Annex 9 – *Facilitation*, Chapter 8. Other Facilitation Provisions[22]:

"...

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 al 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.

REGIONAL BORDER MANAGEMENT ARRANGEMENTS

States around the world come together under regional and bilateral agreements and treaties, designed to strengthen and develop economic, social and political relationships with their neighbours.

Many of these agreements include provisions which provide preferential access for travellers - whether restricted to travel in border regions; or applied more broadly to all travel; or applied to all travel to and from particular ports or airports; or applied to all travel using particular transport modalities.

Whatever their detail, current and prospective regional and bilateral agreements for facilitated travel shape and are shaped by regional travel patterns. Insight into these local factors is critical in formulating effective national strategies and policies for the identification of travellers for BCM.

Where regional arrangements include "free movement" concessions, the associated identity and security risks can be mitigated by data sharing – whether between national inspection systems or by using interoperable applications.

22 *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

Regional organizations can provide a legal and institutional framework to facilitate the sharing of data to contribute to traveller identification and risk assessment:

- The Organization for Security and Co-operation in Europe (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 and 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[23].
- Since 2002 the Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime has operated to raise awareness in the Asia-Pacific region of the consequences of people smuggling, trafficking in persons and related transnational crime. The Bali Process publishes guidance material[24], 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 States[25]. The framework is significant for its strong privacy and data protection features.

Whereas the regional focus of the OSCE (security) and Bali Process (trans-national crime) are defined by a focus on specific shared risks and threats, other regional (and bi-lateral) frameworks for BCM have been created within organizations with a trade and travel facilitation focus:

- 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 clearing house for the receipt from airlines of Advance Passenger Information (API). The JRCC analyses and screens the API data it receives, identifies targets and forwards alerts to its member States[26].
- The European Border and Coast Guard Agency (FRONTEX), promotes, coordinates and develops European border management in line with the European Union (EU) fundamental rights charter and the concept of integrated border management. FRONTEX publications[27] cover a range of topics relevant to BCM policy development. The work of FRONTEX at the EU's external borders facilitates the Schengen common travel area.

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 BCM agency engagement with regional organizations is an important input to national BCM strategic frameworks.

23 *Border Management*, Organization for Security and Co-operation in Europe, available at: http://www.osce.org/secretariat/borders
24 *Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime*, available at : http://www.baliprocess.net/regional-support-office/resources/
25 *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
26 *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
27 *Publications,* European Union's Border and Coast Guard Agency, available at: http://frontex.europa.eu/publications/

4

National Border Inspection Systems and Tools

Modern border control systems provide States with the ability to prevent the travel of people who are assessed as representing a risk or threat. This is made possible by obtaining information about travellers prior to their arrival in the receiving/destination State, analysing the information and transforming it into actionable intelligence to inform decisions about whether travel should be allowed to commence or continue, and whether entry should be allowed. This is achieved by establishing the identity of the traveller to a sufficient level of confidence, then undertaking a traveller risk assessment.

Travel document inspection is the critical initial step in the identification of travellers. Travel document inspection is undertaken physically in visa issuance, and virtually in online ETS applications and thereafter is repeated at each step of the travel continuum - when MRTDs are presented at airline check-in, at boarding gates, at transfer desks and at entry. In best practice jurisdictions the identification of travellers is informed by other relevant data, some of it obtained from the traveller, and some of it 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 traveller primary processing, travellers interact with self-service eGates and kiosks in the entry (or departure) clearance process without processing input from border agency staff, thus releasing resources for redeployment to achieve other security or facilitation objectives.

The border Inspection Systems and Tools employed within national BCS integrate traveller identification and risk assessment, ensuring that relevant data is not only used by agencies responsible for immigration but that it is shared routinely with other border agencies.

TRIP Strategy Element: Inspection Systems and Tools	
Purpose	Capture, verify and record data in the MRTDs and about travellers
Objective	To transform the data into actionable intelligence to secure and facilitate travel
Where	National level, at different point in time during the traveller journey
Who	Within and between BCM agencies. Primarily agencies performing the immigration clearance functions at international airports and national security and law enforcement agencies for analysis and investigation activities.
Topics in the Guide	A. Visas and Electronic Travel Systems B. Document Readers C. Biographic Identity Verification D. Biometric Identity Verification E. National Watchlists F. Entry and Exit Databases G. Automated Border Controls

A. VISAS AND ELECTRONIC TRAVEL SYSTEMS

National Border Inspection Systems for Traveller Identification & Risk Assessment *- by the collection and analysis, prior to travel commencing, of 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 both issuing authorities and travellers.
- ✓ In lieu of the standard counterfoil paper visa, the process for the lodgement, acceptance and verification of a passenger's authorization to travel to a State is automated.
- ✓ An additional benefit is the allowance for interfacing with other systems and databases (iAPI, national watch and international watch lists, INTERPOL, civil registries, etc.)

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 the visa endorsement was made directly into travel documents by the consular and diplomatic officials of States using ink stamps. Because these applications had to be made to representatives of the State, obtaining a visa was inconvenient and expensive, and because ink stamps are clumsy to endorse, easy to forge and fraudulently alter, issuing a visa was inefficient, and created document security vulnerabilities for States.

In the latter part of the twentieth century many States, in response to these inefficiencies, waived their visa requirements to facilitate travel. States that retained visa requirements progressively introduced machine printable, machine readable visas linked to centralised databases which 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 Information and Communication Technology (ICT) systems, such as the internet, to make permission to travel easier and cheaper for the traveller to obtain, 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. interactive Advance Passenger Information (iAPI)).

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. Since the processing locations of these centres can be determined by traveller demand rather than the points of presence of a diplomatic network, they are more conveniently located for travellers.

To further differentiate traveller risk, some States, airport operators and airlines in various partnerships offer trusted traveller programmes, which share the same objectives of facilitated travel and improved security, and can secure more detailed information (including biometric enrolment) from prospective travellers in advance. Each of these arrangements mean that States access the information they need to assess traveller risk pre-departure, at the least inconvenience and cost to potential travellers.

Electronic Travel Systems (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.

A back-end system processes the incoming data and submits it to watch lists or a decision engine – a rule-based software

component which 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 to prospective tourists to make an online application, and receive an electronic confirmation of their permission to travel within seconds or minutes of applying.

The online application interfaces of this modern permission to travel allow States to ask for more information about travellers. This additional information, when integrated with Advance Passenger Information (API)[28] data, supplements traveller information creating a powerful tool for superior traveller risk assessments, and can in addition provide an alternative to data collection from passenger cards for statistical purposes.

HOW IT WORKS – BORDER AGENCIES

The various national systems for managing permission to travel (e.g. the ETS) contribute to a single database of eligible travellers.

Eligible traveller data is retrieved from the ETS database by the national border control system when the traveller completes entry border clearance formalities. When used in conjunction with an API system the eligible traveller data can be matched when batch API data is received, prior to the entry of the traveller. In more advanced jurisdictions ETS data is integrated to enhance iAPI data

ETS data can also be used to compile accurate statistics for the Ministry of Finance or Ministry of Tourism, avoiding the need for resource-intensive compilation of figures from paper cards.

In best practice jurisdictions, 24-hour, 7 days per week operational support is maintained to review ETS errors and refusals, to minimize traveller inconvenience whilst 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, the evidence that an ETS has been granted and is still valid will be available in the airline's departure control systems, but 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 on 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 applications, governments, and airlines to verify their acceptance for travel. ETS provide States with an added layer of border security.

An ETS is ultimately a cheaper option than a full-scale visa regime since it requires no staff or accommodation to receive and process visa applications (either owned or outsourced); decisions can be made automatically according to a set of rules and watch list lookups; and fees are collected electronically instead of in cash.

The introduction of an ETS creates the opportunity to integrate with iAPI, which enables information to be received in advance of the traveller's departure so that they 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 at the end of their journey. In most ETS applications, a 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.

Best practice jurisdictions manage a clear separation between border 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.

While an ETS can be a cost effective, efficient and traveller-friendly alternative to a traditional visa system, they are technically complex – particularly if the intention is the simultaneous introduction of an iAPI solution. Full realization

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

of benefits is possible only for those States able to transform the data received from ETS into actionable intelligence to identify traveller targets for border interventions. States are advised to seek vendor independent, solution neutral advice and support prior to deciding to implement an ETS.

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 classified State systems to perform watchlist checks. Since most ETS applications are designed to work in a lightly-supervised mode with human intervention only required to deal 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 border control system (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 border controls systems (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, but the costs may outweigh the benefits. A persuasive business case is required.

The support service for ETS may require additional staff. Travellers may be rejected because of false watch list matches and other logical errors. This could harm the States reputation and attractiveness as a tourist destination. A full cost-benefit analysis should be conducted.

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 airline/immigration Liaison Officers (LOs) at major departure airports to assist airline check-in staff. 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 themselves - ETS data and alerts should be shared between those States in the same way as API and Passenger Name Record (PNR) data are shared.

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[29].

Travellers should be able to request clarification or reversal of adverse ETS decisions by letter, email or telephone, and have an officer of the border agency 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.

29 *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/

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Extracts from ICAO Annex 9 – *Facilitation* Chapter 3. Entry and departure of persons and their baggage[30]:

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 Systems[31]:

"...

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.

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. ..."*

30 *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

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

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

B. DOCUMENT READERS

National Border Inspection Tools supporting Traveller Identification & Risk Assessment *- by the fast, accurate capture of biographic, cryptographic and biometric data from MRTDs in automated inspection processes applied throughout the travel continuum.*

KEY MESSAGES

- ✓ Entails the capture of data from an ICAO 9303-compliant travel document via optical-electronic reader equipment.
- ✓ Enables verification of traveller identity more quickly and with higher degree of confidence.
- ✓ Where interoperable with other national systems and databases, facilitates cross-checking of travel document data with greater efficiency and accuracy.
- ✓ Used throughout the traveller journey, by States at visa issuance, entry and departure, and by airlines at check-in, transfer and boarding.

OVERVIEW

Efficiently reading and using the standardised, interoperable, machine readable data elements included in Machine Readable Travel Documents (MRTDs) and electronic MRTDs (eMRTDs) issued in an ICAO compliant format[32] is the foundation of border control management (BCM).

Travel documents, machine readers and the interfaces between them vary in standard, depending on when they were introduced to the border control systems currently in use. They may not reach current standards even if they did when they were introduced. To ensure interoperability is achieved, all new elements in the border control systems need to be fully compatible with all the older elements. This is called "backwards compatibility", and is a very important aspect of maintaining interoperability. Travel documents typically remain valid for 5 or 10 years, so currently valid travel documents always include those that have been issued in prior configurations.

At the same time, the installed base of systems globally ranges from the most sophisticated ABC systems to the absence of readers and computer interfaces. Modern

Example of a VIZ and MRZ from an MRTD – ICAO Figure 1 p3 Doc 9303 Part 3 7th Edition

national border control systems are reliable and resilient but outages do occur. Even in the most sophisticated jurisdictions human examination of travel documents is necessary at primary processing, and is required always and everywhere for secondary examination – when the genuineness of the traveller's purpose, and/or their identity/document is in doubt[33].

Consequently, the data page in ICAO compliant MRTDs includes both a machine readable zone (MRZ) and a visual inspection zone (VIZ).

MRTDs include a range of security features. While physical security features are typically placed throughout the document, they are used most intensively on the data page. Modern document readers can identify, interpret and report on these security features.

HOW IT WORKS – BORDER AGENCIES

Document readers are available with different capabilities. All include the ability to perform a simple MRZ read; some offer a level of forensic document examination or the ability to interpret machine verification features, and some can read the data from the chip and perform ePassports PKI authentication on eMRTDs.

Document readers most often used by border agencies are full page readers with good tolerance for variations in placement of the travel document on the reader plate. All ICAO conformant document readers have an infrared light source and camera which illuminates the MRZ and captures an image of the data page. MRZ images are captured in

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

33 See *Section 6 Risk Assessment and Travel Document Inspection*

infrared to maximise image contrast to improve the accuracy and reliability of the data that is read. The MRZ data elements identified in the infrared capture are sent to the national border control system.

More sophisticated readers available from a number of reader vendors 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 border control system interface, all or some of the images, as well as reports on the results of the various comparisons, may be displayed to the border official. 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 interfaces[34].

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

The interpretation of security features undertaken by document readers is supported by human examination of travel documents. All frontline border officials should be trained in basic document examination techniques. Basic examination of documents is supported by specialist forensic examiners at secondary examination in best practice jurisdictions. The tools and techniques used by border control officials to examine documents are briefly discussed in *Section 6. Risk Assessment and Travel Document Inspection*.

HOW IT WORKS – AIRLINES

The document readers most often used by airlines are integrated into the keyboards used by check-in staff. The passport read is achieved by a swipe of the bottom section of the MRTD or the eMRTD data page containing the MRZ.

The data captured from the MRZ populates the corresponding data fields in the airline departure control system and is added to the Advanced Passenger Information (API) batch (or initiates the interactive API (iAPI) "OK to board" transaction with the State of final arrival)[35].

The examination to determine the genuineness 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, many airlines do train their staff to undertake visual and touch based checking of travel documents to assess their genuineness. Many States impose on airlines a financial liability for carriage of inadequately documented travellers, further incentivizing airlines to make basic checks of the genuineness of travel documents.

34 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

35 See: *Topic H* - Advance Passenger Information and Interactive Advance Passenger Information

It is possible that in future airlines may deploy eMRTD readers that perform Public Key Infrastructure (PKI) authentication. This is perhaps more likely in applications involving partnerships with national authorities, where authentication provides operational benefits for all parties concerned.

BENEFITS AND OPPORTUNITIES

MRTDs are issued for the primary purpose of facilitating travel. Consequently, national BCM 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.

Document readers improve the speed and reliability of capturing the MRZ data elements. Routine usage of document readers releases human resources which can be used for other tasks to improve security and facilitation outcomes.

For their own operational purposes, and to meet their obligations to provide API data to border control authorities in transit and destination States, airlines have a strong incentive to install and use document readers at their check-in desks and boarding gates. The self-service check-in kiosks which in some airports have begun to offer an alternative check-in experience for travellers usually include an MRTD MRZ reader. With the universal adoption of MRTDs approaching completion, the operational and efficiency benefits for airline use of document readers continues to increase.

National BCM authorities can and should encourage airlines to install and use document readers so that the accuracy of the API information provided to other States is maximised.

TECHNICAL ISSUES

The data encoded in the MRZ includes a series of check digits to ensure that misreads of characters can be identified. The purpose of this data validation is to manage accuracy and ensure interoperability. Because fraud often occurs on less sophisticated travel documents, a check sum digit failure is a risk indicator for closer examination of the travel document, and in many instances fraudulent alteration of travel documents can be detected by this method. However, since the check digit algorithm is published and freely available, check sum calculations can't be considered a wholly reliable security feature of MRTDs and eMRTDs, and should not be solely relied upon as a means of authenticity verification.

Ultraviolet images of MRTD and eMRTD data pages display their fluorescent security features. It is important that border inspection officials are trained to recognise the basic security features of the documents they encounter most often – their own national passport, and the national passports of the States that most travellers they encounter are from. Ultraviolet features can be subject to variability at issuance, and ultra violet fluorescence degrades over time. This variability and change gradient is a good subject for the more advanced training of border inspection officials.

RELATED REQUIREMENTS

- ✓ National legislation requiring travellers to present themselves and their travel documents for examination.
- ✓ Adequate standard operating procedures describing traveller examination process.
- ✓ MRTD/eMRTD booklet design must meet ICAO Doc 9303 technical specifications in the areas critical to machine readability performance. For example:
  - The ink used in personalisation must absorb light in the near infra-red spectrum and the paper or other substrate used for the data page must be dull when illuminated by the document reader to maximise contrast with the printed MRZ data elements; and
  - The MRZ must be printed within the area defined for it on the data page, and the typeface size and ink used for personalisation of the data page must be readable under infra-red light in accordance with the optical character recognition (OCR)-B standard
- ✓ National MRTD/eMRTD issuance practices at personalisation must include quality assurance steps to ensure consistency in the readability performance of the MRZ of MRTDs and eMRTDs, and of the IC chips in eMRTDs.
- ✓ Sufficient document readers need to be installed at every international airport in the State with functionality appropriate to the characteristics of the MRTDs and eMRTDs being presented by travellers.
- ✓ ICT integration with the national border control system (e.g. to ensure travel history is recorded accurately and that watchlist and INTERPOL databases of Stolen and Lost Travel Documents (SLTD) checks are completed).
- ✓ Reliable, continuous supply of electricity and network connectivity to ensure business continuity of document readers and national border control system
- ✓ Disaster recovery contingencies to ensure traveller processing can continue in the event of outages and systems failures

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 incorporating machine reading of the MRZ data elements into a national border control system is faster and more accurate than a border control official manually typing travel document data into the national border control system.

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, infra-red 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 which can damage the datapage material
- Document reader performance can be compromised by 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 multiple images depends in large part on the skills and knowledge of border agency staff, and how they are supported. Best practice jurisdictions support the primary processing undertaken by front line officials with referrals of process exceptions to secondary examination. To mitigate the risk of project failure at implementation, the application of new technology in border control requires skills development and training support, together with effective business process change.

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 inspection. In more sophisticated jurisdictions, less information is displayed unless a threshold discrepancy is identified. This mitigates somewhat the risk of sensory overload of officials.

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, and effective integration with the national border control system 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.[36]

Non-compliance, whether minor, technical or more serious, does occur, and can impact on interoperability at the most fundamental level, either by making data more difficult to read from the MRZ, eMRTD and/or IC chip. It is critical that border officials undertaking border inspection understand the areas where the MRTDs and eMRTDs issued by their own State, and by States whose travellers often seek entry, are non-compliant, and how this non-compliance impacts on their inspection.

In more sophisticated jurisdictions it is not unusual for the national border control system to be reconfigured in minor ways each time a new MRTD is introduced into circulation. These impacts can be anticipated and mitigated by obtaining and testing representative specimens of new documents before they are issued to travellers. Inter-agency collaboration between travel document issuers and border agencies is critical to ensure minor and technical non-compliance risks are mitigated.

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 quality assurance checks at passport issuance match as closely as possible those used in the national border inspection system. By this simple alignment, the read performance at issuance can more closely approximate the actual read performance at border inspection.

36 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

Extract from ICAO Annex 9 – *Facilitation*, Chapter 3. Entry and Departure of Persons and their Baggage[37]:

"...

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.*

..."

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

37 *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

C. BIOGRAPHIC IDENTITY VERIFICATION

***National Border Inspection Systems for Traveller Identification** - by integrating national travel document issuance database verification searches into primary processing, and making more extensive search results available to support secondary examination.*

KEY MESSAGES

- ✓ A data link between the physical presentation of a travel document and the database which supports issuance and management of documents.
- ✓ Facilitates more efficient and reliable confirmation that the datapage of the travel document is authentic and corresponds to the presenting national traveller.
- ✓ Enhances process efficiency for border inspection officers at primary and secondary inspection.

OVERVIEW

For most States, it is their own citizens who comprise the largest percentage of air travellers by nationality passing through their airports. Confirmation of the identity and nationality of a State's own citizens mitigates the risk of substitutions of persons, whether citizens or foreigners, attempting to fraudulently use travel documents issued by the State. These substitutions might otherwise enable foreigners to pose as nationals and avoid border screening scrutiny, or nationals to assume an alternative national identity.

Comparing biographic data elements from the travel document with the data elements of the same document recorded in the national issuance database can confirm that the datapage remains unaltered. This comparison can be managed in different ways to meet the privacy and data protection laws of each State.

For process efficiency, the interface for verification of national travel documents should be integrated into national border control system, such that the verification operates in real time with very high system availability and fast response time.

For older national passports and other travel documents that may be issued in Machine Readable Travel document (MRTD) format such as Emergency Travel Documents, Certificates of Identity, Documents of Identity and/or United Nations Convention Travel Documents, PKI authentication may not be available, and database comparison could provide a necessary alternative means of authentication.

The Public Key Infrastructure (PKI) provides a readily integrated and automated authentication alternative for States who issue electronic passports (ePassports)[38]. However, this authentication is limited to information to the data included in the travel document.

For all States, when fraud is suspected or an error has occurred, it is essential that border control agency staff can make further comparisons in secondary processing to resolve and distinguish between instances of fraud and error. Importantly, national law enforcement and security agencies are dependent on advice in this area from the agency responsible for immigration clearance. Access to the travel document issuance database provides a much richer source of additional data to support verification of identity and citizenship. This additional data can include addresses, telephone numbers, email addresses and details of family members, as well as details of the circumstances and timing of the application and issue of the travel document.

HOW IT WORKS – BORDER AGENCIES

Citizens present their MRTD or eMRTD at border control. A document reader captures and validates the MRZ details, then transmits the MRZ data to the national border control system.

Data elements sufficient to uniquely match the MRTD or eMRTD presented by the traveller (e.g. travel document number, family name, date of birth) to the identity in the database used to retrieve the travel document details 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 agency staff responsible for the resolution of doubt in the identification of travellers.

38 See: *Topic J - Public Key Infrastructure and the ICAO Public Key Directory*

To ensure data is protected and traveller privacy is maintained, appropriate controls should be implemented, and standard procedures adopted, 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 assist other States in resolving the "fail to verify" instances they encounter in their border control systems. 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 Stolen and Lost Travel Document (SLTD) matches[39].

TECHNICAL ISSUES

National border control systems, national identity systems and national travel document issuance systems are most commonly proprietary systems that in many cases are unique to, or uniquely configured for, each State.

Where they exist as separate Information and Communication Technology (ICT) systems, communication and data integration interfaces are required to link the various national systems. In general, ICT integration in establishing an automated interface for comparisons of traveller MRZ data with travel document datasets will be relatively complex, compared to providing read-only access to travel document and/or national identity databases at secondary examination.

National border control systems of some States include an integrated travel document issuance module. In this ICT architecture, verification integration for automated primary comparisons is likely to be more easily achieved, and enquiry access to the travel document issuance module is a simple matter of managing access permissions.

RELATED REQUIREMENTS

- ✓ National legislation and inter-agency agreements for border control management 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 border control system and reliable MRZ read performance of MRTDs and eMRTDs issued by the State[40]
- ✓ ICT integration of national border control systems 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 and travel document and national identity card issuance.

Because international airports operate on or close to full time operations with high transaction volumes, communication costs can be a 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 interoperable applications such as PKI authentication.

39 See: *Topic L - INTERPOL Database of Stolen and Lost Travel Documents*
40 See also: *Topic B* - Document Readers

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 BCM agencies to also have access to the national identity database in secondary examination processes, to verify identity.

More generally, the secondary examination modules of more sophisticated national border control systems 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.

Database comparisons that establish an alternative basis for authentication are a best practice investment in redundancy and business continuity, for situations when a National Public Key Directory (NPKD) is unavailable.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

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

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

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

D. BIOMETRIC IDENTITY VERIFICATION

***National Border Inspection Systems for Traveller Identification** - by comparisons of images captured live from the traveller against biometric reference databases of enrolled images from visa or trusted traveller or 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 or airline check-in procedures, provides efficiency, security and facilitation benefits.

OVERVIEW

A range of biometric[41] solutions for the identification of travellers have been adopted by States. These solutions may use different biometric features, and obtain the reference image from different sources. Biometric identity verification using reference images obtained from electronic Machine Readable Travel Document (eMRTDs) is discussed in *Topic K-eMRTD Biometric Identity Verification.*

This Topic describes solutions implemented in national border control systems 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 Electronic Travel Systems (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 1:1 identity verification are in many cases implemented as one element of Automated Border Controls (ABC) solutions[42] but can also be implemented in support of human processing of travellers.

In addition to the 1:1 verification task, biometric comparisons can also be made between images captured of the traveller at border inspection (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 MRTDs[43].

All biometric types are at risk of artefact attacks, also known as "spoofing", which entail an attempt to use a mask, plastic fingerprint, or contact lens to trick the image capture device and interface into enrolling a fake image. Protection against these attacks is critical to ensure the integrity of the identification of travellers. As a result, all credible biometric solutions include "liveness" detection features.

HOW IT WORKS – BORDER 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).

41 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.

42 See: *Topic G – Automated Border Controls*

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

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 inspection 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 stand-alone biometric matching system can inform identity verification decisions at secondary examination. Identifying suspect cases for referral, and resolving non-match referrals, requires skills, knowledge and experience in image comparison specific to each biometric type. The implementation of biometric identity verification solutions therefore requires careful consideration of the skills and training needs of border officials.

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 border control system 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 agencies work together to ensure that the commercial interests of airlines and airport operators are not compromised by arrangements which require substantial investment or impose ongoing transactional costs.

BENEFITS AND OPPORTUNITIES

Biometric matching for traveller identity verification is the foundation for ABC[44]. The deployment of effective ABC solutions can reduce queue times to improve the traveller experience and provide process efficiency benefits for States. It can also improve the accuracy and consistency of the identification of travellers, which could allow for redeployment of border agency staff to focus on risk-based interventions at secondary examination. These are all important and significant facilitation and security benefits.

At exit 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 agency officials, or where exit control is not undertaken; a vulnerability which 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 for extended stay or refugee status.

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

TECHNICAL ISSUES

Obtaining biometric sample images from travellers requires a border control system 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, and 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 (meta data) to ensure the correct biometric samples are retrieved for comparison.

Exploiting biometrics requires capture devices which 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 which 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.

44 See: *Topic G - Automated Border Controls*

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

- Speed and accuracy – a system which produces very accurate results may be unacceptable in terms of transaction times, and a faster system may deliver unacceptably high errors.
- 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 updated to new versions to take advantage of advances in technology, but this should only be done after testing that closely simulates 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 practice 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 border control system 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.
- ✓ 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 Extended Access Control (EAC) terminal authentication and chip authentication at all border inspection document readers.
- ✓ Reliable, continuous supply of electricity.
- ✓ Reliable, continuous, high bandwidth network connectivity sufficient for transmitting image files in real time.

RISKS AND COST MITIGATION

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 a compelling business case for the introduction of biometric systems which 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?

Border agencies should seek expert help when specifying and procuring biometric systems, and should at least consider the following questions:

Question	Observations
Does the technology work robustly and reliably?	Are there operational sites where the biometric systems can be seen in operation? If not, can the vendor arrange credible demonstrations?
Does it work in your business environment?	Consider the type of passenger traffic; the environmental conditions (ambient light, temperature, humidity, space availability); legislation (is the capture of such sensitive personal data allowed?); social perspective (will travellers comply?)
Will there be tangible benefits?	In terms of reduced queues; staff savings; increased security, and integrity of the control.

The consideration 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. It is only after this analysis that a "concept of operations" can be determined, and an informed choice of biometric features can be made. States are encouraged to seek vendor independent, solution neutral advice.

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

A range of biometric solutions for the identification of travellers solutions have been adopted by States. 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. In the United Arab Emirates, 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 the passport control capture one or more prints which 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 Baggage[45]:

"...

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.*

..."

45 *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

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

Other Sources

The United States National Institute of Standards and Technology (NIST) publishes biometrics standards covering the three biometric features considered here and guidance on their implementation, testing and use. NIST documents are used as supplementary references by many States, for example in benchmarking matching performance: *Biometric*, 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=000000000030213319
- 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

National Border Inspection Systems for Traveller Risk Assessment *- by comparisons of biographical details (or biometric images) captured from the traveller against reference databases of known targets of concern compiled by the State from national and international sources.*

KEY MESSAGES

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

OVERVIEW

There are no absolutes when it comes to deciding the admissibility of travellers. For most States, citizens have an unrestricted right to enter and depart from their State. Some travellers have a restricted right, such as citizens of common travel areas who may be refused entry on certain grounds. Some travellers may be admitted after a brief examination to determine their residence status. Other travellers need to be assessed to determine whether they qualify for admission according to the legal requirements of the State.

For non-citizens, the right of entry to a State is conditional. Travellers are facilitated when their entry and stay are deemed beneficial to 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 security interventions can be made to prevent travel or entry.

Fundamental to border control management (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 border control systems are the principal tool for initiating these interventions.

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 lost, cancelled and stolen travel documents that could be misused to disguise their true identities.

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 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 which 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 Advance Passenger Information (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 in real time to apply risk-based profiles to information about travellers obtained from a range of sources. In these applications, the watchlist entry will typically be created when Passenger Name Record (PNR), Advance Passenger Information (API), visa or Electronic Travel System (ETS) information is received, and deleted after the traveller is processed at entry.

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.

HOW IT WORKS – BORDER AGENCIES

Most States have moved from printed or manuscript lists of suspects to Information and Communication Technology (ICT) based systems in which names and personal details are searched, to produce a range of matches.

In best practice jurisdictions, watchlists are included as a module within the border control system, and watchlist searches are initiated by the document reader when the data from the Machine Readable Zone (MRZ) is received.

In contrast, when watchlist searches are initiated after the data processing at entry, error is more likely and processing times compromised. For these reasons, 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.

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 border control system is shared information. Thus, the ICT infrastructure is used by agencies responsible for law enforcement, national security, customs and immigration. In the jurisdictions where national watchlists have these characteristics, the responses displayed to the border inspection agency staff are carefully calibrated so that staff only see information relevant to their role. For some agencies, and in some situations, the inclusion on a watchlist can be facilitative, for example to ensure an appropriate public health response.

Name matching is a complex application of probability, subject to error and statistical variance. In best practice jurisdictions, a number of different logical approaches are applied to the name matching task. These include, amongst other techniques, algorithms which automate multiple wildcard search combinations, reference tables that anticipate alternative spellings of common names and the impact of transliteration.

In many jurisdictions, images of faces or other biometrics are associated with biographic records. Making these images available at secondary examination can assist border agency staff 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 one to many (1:n) identification searches performed in watchlist applications are significantly more complex than the more common one-to-one (1:1) identity verification task, and require sophisticated technical and human capability. Refer to *Topic D - Biometric Identity Verification* for a more detailed explanation of 1:1 and 1:n.

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 interactive API (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 staff that they remain unaware of the reason for the denial of check-in or boarding.

BENEFITS AND OPPORTUNITIES

Most border agencies maintain watch lists, and these assist officers to detect and manage 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 watch list system so they can be informed if one of their targets arrives or departs.

Travellers who become persons of interest because of API, ETS, PNR or other profiling or intelligence assessments, are most effectively managed by short term watchlist entries, rather than being alerted verbally or by paper messages to front-line inspection officers.

TECHNICAL ISSUES

There are problems in matching names in travel documents against watch lists for the following, not exhaustive, reasons.

- 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 watch list systems may only cope with exact matches, and fail to uncover real matches which deviate slightly from the text entered as a search term
- 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 the border 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 border control system.
- ✓ Appropriate ICT disaster recovery to ensure watchlists are searchable even if the border control system is unavailable.
- ✓ Reliable, continuous supply of electricity and connectivity at 24/7 operations centre.

RISKS AND COST MITIGATION

The border control watch list needs to be managed properly so that out-of-date and inaccurate entries are removed, to prevent 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, and it should be reviewed or automatically deleted after a fixed period. The watch list entries and the information supporting them should be security-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 display screens.

Watch lists in many countries are classified documents, and may contain sensitive material obtained from covert sources. Border control staff that use such systems should be security vetted up to the relevant standard. Access to the system should be by frequently-changed password and/or a physical token issued individually to staff. Ideally, use of the system should be audited and transactions logged, so that any misuse can be clearly identified. It is recommended that a watch list system has its own system manager who is responsible for security and the prompt addition, updating and deletion of entries.

The transaction time for searches is also a major factor in keeping traveller queues moving at ports of entry, and this should be evaluated when specifying new or upgraded systems.

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 Consolidated United Nations Security Council Sanctions List (CUNSCSL).

In the meantime, 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 high 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 -- that is, 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 agencies.

BEST PRACTICE EXAMPLES

Commercial watch list 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 flexibility of matching. Names have a cultural and ethnic dimension specific to national contexts, therefore name matching solutions that are effective for one State may be significantly less effective in another.

In the United States, 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 border.

In the United Arab Emirates (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

Other sources

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

F. ENTRY AND EXIT DATABASES

***National Border Inspection Systems for Traveller Identification & Risk Assessment** - by compiling over extended periods of time comprehensive, searchable databases recording and indexing all the entries and departures of all travellers to and from the State.*

KEY MESSAGES

- ✓ Manual or computerised recording of details of arriving or departing travellers, for law enforcement or statistical purposes.
- ✓ Facilitates reconciliation of traveller entry and exit, and risk analysis based on traveller profile and history.
- ✓ Implementation should anticipate the technical challenge of collecting and maintaining this information over time.

OVERVIEW

Recording the entry and exit of all travellers 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, and a richer source of historical data for analysis.

Yet the 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 which must be adequately protected, from both a personal privacy and 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 verification[46], when used to improve the accuracy and reliability of the identification of travellers, has the potential to improve entry and departure reconciliation. [47]

In general, full reconciliation of traveller entry and departure is easier to achieve for States who 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 -- albeit without the organisational scale and resources to make developing the capability easy.

As a result, notwithstanding its critical importance to Border Control Management (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, States are now investing more in national border control systems with the capability to record and reconcile the entry and departure of travellers.

HOW IT WORKS – BORDER AGENCIES

Traveller data is read from the Machine Readable Zone (MRZ) of Machine Readable Travel Documents (MRTDs) or electronic Machine Readable Travel Documents (eMRTDs) via a document reader interface into border control systems[48]. 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.

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 Advance Passenger

46 See: *Topic D - Biometric Identity Verification*
47 *The 9/11 Commission Report*, Washington, 2004, p. 389, available at: http://govinfo.library.unt.edu/911/report/911Report.pdf
48 See: *Topic B* - Document Readers

Information (API) and Passenger Name Record (PNR) data, travel history searches contribute additional data for earlier analysis and risk-based targeting by security, customs, law enforcement, and immigration agencies.

Where API data has been received by the border control system, the flight details associated with the traveller can by retrieved by the border control system from the MRZ read and displayed on the screen along with the traveller details. This alternative enables confirmation by the border official without their having to key in the additional details, thus reducing error and traveller processing time.

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 destination airports is undertaken.

In practice, API data is not sufficiently accurate to provide a basis for reliably recording traveller entry and departure. In contrast, where interactive API (iAPI) is available, MRZ data for each individual traveller has been added and verified by the State border agency. However, despite the fact that 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 State border agency examination of travellers at exit control. 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 them – in part as a response to emerging terrorism threats and the international requirement to prevent the travel of foreign terrorist fighters.

TECHNICAL ISSUES

Since all national border control systems 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.

More difficult is a design that anticipates the creation, protection and use of what quickly becomes a very large database.

Efficient database architecture, effective Information and Communication Technology (ICT) access control and security and good search tools are necessary for success. With each element, 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

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 within the State of citizens and residents.

Travel entry data is a rich source of data which when collated and analysed can contribute greatly 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 by using biometric verification in conjunction with API. This and other applications of biometric identity verification at exit control can improve 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 border control systems at departure. This provides another potentially valuable opportunity for the identification of travellers, especially 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.

For each State, the benefits of achieving reconciliation of traveller entry and departure would need to be weighed against the cost of the investment in systems and businesses processes to achieve it.

RELATED REQUIREMENTS

- ✓ National legislation to require BCM 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 border control system and reliable MRZ read performance of MRTDs and eMRTDs issued by the State.[49]
- ✓ ICT integration of border control system 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. 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 agency staff should be subject to specific controls that limit their access to the travel records of individuals to legitimate and lawful enquiries and investigations, and there should be a provision for sanctions against staff 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 should recognise that national border control systems and travel history databases are critical to national security and law enforcement, and take steps to ensure they are protected accordingly. These controls should include 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 border control systems in some States include functionality that identifies in real time unmatched departure of citizens and foreigners. By identifying these records, errors which would otherwise prevent a full reconciliation of the entry and departure of individual travellers are identified and resolved. In addition to improving data quality, the unmatched departure of foreigners, citizens and residents can identify possible prior instances of evasion of border controls – a risk indicator that can then be investigated by border 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 island States.

In some States, the limitations and configurations of older airport infrastructure constrains the ability to achieve exit control. In the United States (US), airlines have in some circumstances been required to contribute data to national authorities to record traveller departure details. More recently, the United States has been trialling biometric departure processing using one-to-one (1:1) verification of facial images. The reference images in these trials are obtained from the ePassports of US citizens and databases of the facial images enrolled during visa issue, or the US-VISIT entry processing of foreigners.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

The inclusion of travel history database functionality in their national border control systems is a sovereign matter for States, and is therefore not the subject of ICAO Standards and Recommended Practices (SARPs) or technical specifications.

Interoperable applications that are the subject of ICAO SARPs, such as iAPI and the ICAO Public Key Directory (PKD) can be leveraged to efficiently 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

49 See: *Topic B* - Document Readers

G. AUTOMATED BORDER CONTROLS

National Border Inspection Systems for Traveller Identification & Risk Assessment *- by integrating inspection systems and tools and interoperable applications into a self-service automated processing solution achieves process efficiency gains that release border agency resources to achieve other facilitation and security objectives.*

KEY MESSAGES

- ✓ Automated but supervised self-service passport control points for arriving or departing travellers.
- ✓ Appropriately implemented, enhances efficiency in traveller processing and identity verification, and enables redistribution of border personnel for targeted intervention.
- ✓ ABCs readily integrated into the national border control systems and related interoperable applications.

OVERVIEW

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

- read a Machine Readable Travel Document (MRTD), read and authenticate an electronic Machine Readable Travel Document (eMRTD) or read another identity token;
- establish that the passenger is the rightful holder of the document or token; and
- interface with border control systems and watchlists to determine eligibility to pass border inspection controls according to pre-defined rules.

ABCs are readily integrated with national border control systems, and with interoperable applications. ABC provides routine checking of eMRTD security features, authenticates the document as genuine, and confirms that the data in the Integrated Circuit (IC) chip has not been altered. In addition, these systems are typically capable of matching the biometrics stored in an eMRTD to that captured from a traveller. This biometric matching ensures, 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 their travel document to the kiosk document reader interface. The kiosk communicates with the border control system, which sends a return message allowing the traveller to pass only if all the checks required by the approval 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. ABC solutions thereby simultaneously achieve security and facilitation benefits for States.

For their effective operation, ABCs use and rely on the 12 other technical topics of this Guide.

HOW IT WORKS – BORDER 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 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 staff-to-traveller clearance ratio and allow the redeployment of border inspection officers.

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) authentication50;
- In the hands of the genuine holder by:
  - search of INTERPOL's database of Stolen and Lost Travel Document (SLTD)[51] ; and
  - the biometric fingerprint or facial image read from the Integrated Circuit (IC) chip of the eMRTD being compared to an image of the same feature taken from the traveller[52].

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 watch lists for automated matching. Possible watchlist matches result in referral to a border official for resolution.

The biometric verification of identity completed in eGates, whatever the biometric features (facial, fingerprint or iris) used, needs to be supported by business protocols for confirming identity when the system refers travellers as "failure to match". 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 officials working from locations close to the eGates. The number of eGates to be monitored, and the period of monitoring to be completed in each session, need to be carefully designed to ensure motivation and performance is maintained.

As described above, ABC systems relying on eMRTDs as the identity token need to be linked to watch lists (for both travel documents and travellers) and to a digital certificate checking system interface with the ICAO Public Key Directory (PKD).

ABC systems integrated with Advance Passenger Information (API) and/or Passenger Name Record (PNR) analysis systems can allow travellers to be risk-assessed *before* they use the ABC, so that targeted travellers can be directed for human examination according to assessed risk.

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 inspection 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 control – from check-in to boarding, and from disembarkation to leaving the airport terminal.

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

BENEFITS AND OPPORTUNITIES

ABC has process efficiency benefits, as it enables the processing of increased number of low-risk passengers quickly and conveniently, while maintaining the security and integrity of borders. This helps optimize the process, and allows resources to be focused on potentially higher-risk travellers.

The processing capacity of eGates is sustained over time - eGates don't get tired – and reduces human resource related costs driven by increasing passenger traffic. Additionally, ABCs conduct an objective repeatable set of checks to

50 See: *Topic J - Public Key Infrastructure and the ICAO Public Key Directory*
51 See: *Topic L - Database of Stolen and Lost Travel Documents*
52 See: *Topic K - eMRTD Biometric Identity Verification*

complete identity and document authentication which, 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 to meet the processing challenge of increasing international travel by air.

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.

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. Usually participants in the scheme will be enrolled and vetted by border officers before being allowed to use the system. Enrolment in these schemes may allow travellers to avoid more rigorous screening and the requirement to make customs declarations or complete disembarkation cards. Watch list checks will still be carried out, and travellers can be required to submit to formal inspection at any time. Extending the use of ABC to include registered travellers improves the business case for ABC implementation, and allows officers at the conventional control to concentrate 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 will, in general, 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

- ✓ National legislation required for the implementation of ABC.
- ✓ Information and Communication Technology (ICT) integration of eGate document readers with a national border control system.
- ✓ Reliable Machine Readable Zone (MRZ) read performance of MRTDs and eMRTDs eligible to use the eGates[53].
- ✓ Assurance that the evidence of identity presented by the traveller:
  - is genuine and unaltered, e.g. by some combination of database verification and ePassport Public Key Infrastructure (PKI) authentication[54] ; and
  - is in the possession of the traveller to whom it was issued, e.g. by reference to national, international watchlists and the SLTD.[55]
- ✓ Verification of the identity of the traveller (e.g. by biometric comparison of images of travellers with reference samples[56]).
- ✓ Integration with national watchlists, international watchlists and current and prior travel data into a border control system, 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 border control system to write to, and read from, a national entry and exit database.[57]
- ✓ Reliable, continuous supply of electricity and network connectivity.

53 See: *Topic B – Document Readers*
54 See: *Topic J - Public Key Infrastructure and the ICAO Public Key Directory*
55 See: *Topics E - National Watchlists* and *L - INTERPOL Database of Stolen and Lost Travel Documents*
56 See: *Topics C - Biometric Identity Verification* and *K - eMRTD Biometric Identity Verification*
57 See: *Topic E - Entry and Exit Databases*

RISKS AND COST MITIGATION

ABC is an expensive investment, and care should be taken to produce a sensible, persuasive cost-benefit analysis and 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 adoption of necessary regulations, development of the national ABC programme concept, acquisition of necessary software and hardware[58], IT system linkage, development of program enrolment capability, and training of relevant staff.

ABC may be viewed negatively by staff, who feels that the system may put their jobs at risk and reduce the need for a high level of skill and experience. This may lead to demotivation, and possible lack of care in checking passengers rejected by the eGates. Comprehensive training and agreement on working conditions 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 are able to be monitored by border agency staff. This monitoring can include Closed Circuit Television (CCTV) 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 reference sample in a one-to-one (1:1) biometric verification of identity. However, there are many eGate solutions that:

- Do not use eMRTDs as the token; or
- 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 also use a biometric reference sample obtained elsewhere (e.g. from a trusted traveller enrolment, or a visa or Electronic Travel System (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 databases.

Data protection, privacy standards and legislation must be in place and adhered to. Litigation against border agencies is likely if traveller personal data is disclosed or used in an unauthorised or unlawful way.

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 staff) to ensure that the border can continue to function.

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.

A full cost-benefit analysis, including long-term support and maintenance implications, should be conducted to avoid costly and operationally unnecessary projects.

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, light level, humidity etc.

To allow supervision of the eGates, monitoring stations should be provided which are near enough to allow staff to observe travellers' behaviour and, if necessary, to intervene.

Coordination between agencies responsible for travel document issuance and BCM may be needed to ensure that ABCs have integrated access to, or are equipped with, the most recent PKI certificates, watchlist and other data required to securely facilitate passenger processing.

Appropriate legislation and measures to adhere to data protection standards ('privacy by design') should be in place.

Staff should be adequately trained, and working conditions amended to promote healthy working and motivation. Staff monitoring an ABC system should be rotated regularly to other duties, to maintain their effectiveness.

Port management should be encouraged to provide adequate signage and assistance to travellers using an ABC system.

58 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

Extract from ICAO Annex 9 – *Facilitation*, Chapter 3 - Entry and departure of persons and their baggage[59]:

"...

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

Reference

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

States seeking to set up ABC systems at their international airports are referred to the following Guide intended for project managers in charge of implementing ABC solutions: *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

FRONTEX sets out the basic blueprint of an ABC system: *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

59 *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

5

Interoperable Applications

The interoperable applications developed by ICAO, the World Customs Organization (WCO), International Air Transport Association (IATA) and INTERPOL support the automation of travel document inspection, with benefits for improved security and facilitation of travel. They play a crucial role in delivering data created or obtained from outside a State integrated with national inspection systems and tools in the receiving State's national BCS.

Information about travellers obtained from airline systems can be used by States to supplement national data sources to inform traveller identification and risk assessment.

International watchlists assist States in meeting their international obligations to combat terrorism and other transnational crime by identifying risk targets for border interventions.

Authenticated traveller identity data is available through visa systems and from border control systems at entry and departure controls – the ICAO PKD extends and strengthens this authentication. Unverified 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 the PNR. When combined with verified identity data and intelligence from national sources, airline data (API and PNR) can be analysed to support traveller identification and risk assessment.

In best practice jurisdictions, international watchlists - including the CUNSCSL and INTERPOL Red Notices, and the INTERPOL database of SLTD database, are integrated with border control systems to prevent or to disrupt travel.

TRIP Strategy Element: Interoperable Applications	
Purpose	Share data about travellers
Objective	To assess risk to prevent travel and to disrupt travel throughout the journey.
Where	National, Regional and International
Who	Data about travellers is used by multiple border agencies and by international organizations and airlines
Topics in the Guide	H. Advance Passenger Information and Interactive Advance Passenger Information I. Passenger Name Record J. ICAO Public Key Directory K. eMRTD Biometric Identity Verification Solutions L. INTERPOL's Database of Stolen and Lost Travel Documents M. International Watchlists

H. ADVANCE PASSENGER INFORMATION AND INTERACTIVE ADVANCE PASSENGER INFORMATION

***Interoperable Application for Traveller Identification & Risk Assessment** - by providing border agencies advance notice from airlines of travel, provides additional time to complete a more detailed traveller identification and risk assessment. 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

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

OVERVIEW

Advance Passenger Information (API) is an electronic communication system whereby required data elements are collected and transmitted to border control agencies at check-in prior to flight departure, including for joining travellers at points of transit, and made available to border control systems 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 those items of data that currently appear on machine readable passports and other official travel documents

A standard electronic message, called the UN Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) Passenger List Message (PAXLST) or the UN/EDIFACT PAXLST message, was developed specifically to handle such passenger manifest transmissions. The basic concept of the PAXLST message is that there is *one* message (a "legacy" or "batch" transmission) for all passengers on the specified flight, and a *second* message 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 interactive API (iAPI). iAPI is an electronic system that transmits API data elements collected by the aircraft operator during check-in directly to relevant public authorities. While the traveller is at passenger check-in, public authorities return a response message to the airline operator for each passenger and/or crew member. The message either confirms that the traveller is "OK to board", or denies boarding authority and directs the carrier to "refer to national authorities".

The World Customs Organization (WCO), the International Air Transport Association (IATA) and ICAO have jointly agreed on the maximum set of API data that should be incorporated in the PAXLST message for the transmission of such data from carriers to border control agencies at the destination. With respect to the message format for API data transmissions, ICAO mandates (through Annex 9 — *Facilitation* to the Convention on International Civil Aviation) 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 agencies via a single and globally interoperable message structure and format avoids the unnecessary complexity in systems needed to support multiple data exchange processes.

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, particularly where it relates to trade in goods and services between independent, computerized information systems.

WCO, IATA and ICAO provide complete guidelines on API[60], and a toolkit outlining the basics on passenger data exchange[61].

HOW IT WORKS – BORDER AGENCIES

API can be used for risk-based targeting and to complete watchlist checks – either manually or automatically – since it contains the full names (except where the full name contains

60 *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

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

more than the available number of characters in the first line of the Machine Readable Zone (MRZ)), dates of birth and nationalities of all passengers and crew on a flight.

Watchlist responses will either be negative, possible or positive. Care should be taken to ensure name matching in watchlist systems are configured to search variations in name-order, the number of names and alternative spelling and transliteration. Variations in spelling may be a result of transliteration from other alphabets, issuance errors or attempts to avoid detection. The application of watchlists is discussed further in *Topics E - National Watchlists* and *M - International Watchlists*. This is a complicated subject and professional help may be required.

Typical API messages for passengers consist of the following data elements:

- Full name (as it appears on the MRTD)
- Date of birth
- MRTD number
- State or organization issuing the MRTD
- MRTD expiry date
- Nationality
- Sex
- Data relating to the flight containing, inter alia, flight number, departure/entry date and time and airport of origin and destination

Some States require additional API data elements from airlines.

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 travellers.

HOW IT WORKS – AIRLINES

Biographic data for API is typically captured either from travel documents or, as is becoming more common, from declarations made by passengers themselves when making reservations or checking in online via the internet. In the latter case, the data is confirmed by the airline when the passenger arrives to take the flight. 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 those 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 up to 72 hours in advance of travel until the check-in, depending on the relevant border agency's demands and the airline's own system capability.

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

BENEFITS AND OPPORTUNITIES

Implementing API is an ICAO Standard effective as of 23 February 2018 and will assist compliance with UN Security Council Resolutions 2178 (2014)[62] and 2309 (2016)[63].

API/iAPI implementation addresses several issues. Provided the API data is timely and accurate, it improves facilitation and reduces bottlenecks in border processing by enabling pre-clearance or partial pre-clearance of flights. It also enables States to use border security resources more effectively and efficiently.

API data can be used by border agencies to search MRTD document numbers which have been reported as lost or stolen, to check their expiry date, to search watchlists to identify suspect travellers, and to profile traveller attributes according to risk. iAPI makes it possible to prevent travel, and thus enhances aviation security and border control processes.

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 air travellers.

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

API can be used to restrict the use of automated border control (ABC) kiosks or eGates to passengers previously risk-assessed by the national border inspection authorities.

62 *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/

63 *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/

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 (servers, switches, etc.), IT system linkage, testing, and training. Costs will also depend on whether a State decides to set up a simple stand-alone programme, or something more sophisticated. If a "Passenger Data Single Window" is used when developing API systems, costs can be reduced significantly. API should be received at a single point, and seamlessly distributed by the receiving agency to the other border agencies that require it.

This Passenger Data Single Window is a facility that allows parties involved to lodge API, iAPI and/or PNR information through a single data entry point to fulfil all regulatory requirements relating to the entry and/or departure of passengers that may be imposed by various agencies of the contracting State. The Passenger Data Single Window facility to support API/iAPI transmissions does not necessarily need to be the same facility used to support PNR data exchange.

API relies on standardized, interoperable interfaces between airline and border agency systems. Several Information and Communication Technology (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, especially if other vendors are available.

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 agencies to ensure single window collection.
- ✓ Handling of personal information from API to meet national privacy and data protection legislation.
- ✓ ICT integration of border control system to receive and interface with API data.
- ✓ Reliable, continuous supply of electricity and connectivity at 24/7 operations centre.

RISKS AND COST MITIGATION

Particularly in the case of travellers that do not require a visa, API data collected and transmitted by airlines is the first instance border agencies are informed of the intent of a traveller to travel. A good relationship between border agencies and each airline, supported by a clear legal framework and effective operating protocols, is required.

Airlines are responsible for collecting and transmitting API since they manage the first process in the travel chain.

Border 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 agency, at risk of litigation, especially if data is lost or disclosed in an unauthorised or illegal manner.

Border agencies should carefully consider how API is delivered and by whom. There may well be transaction charges for each API message received. There is always a cost in information transfer and processing, and the fees could be significant if the contracts are not managed well.

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 codes of practice) needs to be in place to manage the everyday use of API. The 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 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 business.

API should be *used*: the system of advance warning of potential threats can be called into question if the data is not exploited fully and in a timely fashion.

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 in order to extend access to API to States who 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 of the service to which the API relates.

Alerts raised as a result of possible matches should be assessed for accuracy and relevance before dissemination to border staff at primary inspection and/or regional partners.

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 Systems[64]:

"...

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.

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.

64 *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 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 to 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 presented 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/CBP%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

Interoperable Application for Traveller Risk Assessment*- by obtaining from airline reservation systems, for analysis, prior to travel commencing, 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 agencies for the purpose of targeting certain individuals by pre-travel behaviour.
- ✓ 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 from airline reservation systems collected at the time that flight bookings are made. Because the reservation systems of each airline and their associated global distribution systems need to communicate with each other, the 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 which, 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 it will be used and in what form, and for how long it 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 flightpaths 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 Data[65]. Foreign airlines will, in general, only provide PNR to a State in which they are operating if Memoranda of Understanding (MOU) or other inter-governmental agreements are in effect.

PNR data can also include Advanced Passenger Information (API) data elements. This is achieved by the airline booking system requiring travel document details corresponding to the data elements in the Machine Readable Zone (MRZ) of Machine Readable Travel Documents (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 threat[66].

The World Customs Organization (WCO), the International Airline Transport Association (IATA) and ICAO provide complete guidelines on API[67] and a toolkit that provides the basics on passenger data exchange[68].

65 *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

66 See *Topic H – Advance Passenger Information and Interactive Advance Passenger Information*

67 *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

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

HOW IT WORKS – BORDER AGENCIES

Depending on both local legislation and the legislative obligations of operating airlines to other States, border 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 agency's system via airline telecommunications systems.

There are commercially available systems which offer PNR access, coupled 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, 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 particular combinations of data elements. However, these profiles need to be checked for effectiveness and continually updated and tuned as known patterns 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 Standards and Recommended Practices, it is important that border 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 generally 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 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 interdictions.

The analysis of PNR data can link travellers to organized criminal activity, for example by identifying commonalities with 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 such as tickets booked at short notice and paid for in cash, indirect travel routings, and short stays following long haul travel.

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 border control systems, 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 agencies to look for patterns which indicate to them that traveller behaviour is outside statistical norms or matches characteristics identified in intelligence analysis.

The logical search rules which allow such automatic triggers need to be developed as a hypothesis and established in the PNR data analysis system, either by the solution provider or by national border agency staff, 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 Information and Communication Technology (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 is consistent with ICAO Standards and Recommended Practices (SARPS), meets their needs, and is 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 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 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 agency prior to the entry of the traveller. Joint targeting centres help ensure that Border Control Management (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 Systems[69]:

"...

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..."*

69 *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 has issued the State Letter "Adoption of Amendment 26 to Annex 9", Ref.: EC 6/3-17/88, 14 July 2017 to inform States that the Amendment 26 to the *International Standards and Recommended Practices Facilitation* (Annex 9 to the *Convention on International Civil Aviation*) was adopted by the Council at the seventh meeting of its 211th Session on 16 June 2017.

> "Amendment 26 relates to, inter alia, issues such as Machine Readable Travel Documents (MRTDs), the transport of minors by air, the passenger manifest, Automated Border Control (ABC) systems, and passenger data exchange systems."
>
> "Amendment 26 to Annex 9 is intended, inter alia, to: [...] c) mandate the establishment of Advance Passenger Information (API) Systems, and promote the use of interactive API (iAPI), to enhance security and facilitation; d) support adherence to content, format and transmission standards to mitigate non-compliant PNR data requests, in response to the growth in PNR programmes; e) standardize Electronic Travel Systems (ETS)-related terminology and describe its functions in a policy and regulatory framework within Annex 9; ..."

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

Adoption of Amendment 26 to Annex 9, ICAO State Letter No. EC 6/3-17/88, 14 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.

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

***Interoperable Application supporting Traveller Identification** - by assurance that the data read from the IC chip in the eMRTD is unaltered, and was written to the chip by a genuine issuing authority, allows the data read from the eMRTD to be relied on in other business processes.*

KEY MESSAGES

- ✓ The authentication and verification of passport data held in the chip components of eMRTDs using digital certificates.
- ✓ Adds an additional layer of assurance of the validity and accuracy of a travel eMRTD
- ✓ ICAO's PKD reduces the distribution burden on State authorities responsible for eMRTD issuance, and the collection burden on States undertaking eMRTD PKI authentication at border inspection.
- ✓ Utilization requires the development of a NPKD

OVERVIEW

The technical specifications of ICAO for global interoperability of electronic Machine Readable Travel Documents (eMRTDs) ensure that data can be accurately read from the Integrated Circuit (IC) chip of properly configured eMRTDs by properly configured document readers. The interoperability standards for eMRTDs are published in ICAO Document 9303[70].

Public Key Infrastructure (PKI) cryptography is used to secure eMRTDs to ensure that only ICAO compliant eMRTDs issued by recognized issuing authorities are accepted at border inspection.

PKI is a cryptography-based system in which private "keys" (also referred to as digital certificates) are generated and held in a central repository, and used to create and distribute public keys for system users, as a means of verification or authentication. PKI cryptography is asymmetric, i.e. the public keys can be distributed, shared and verified without revealing the private key. PKI is also used in many countries to securely deliver online services to citizens.

The application of PKI in eMRTD issuance, and the exchange of digital certificates, is how States determine that an eMRTD presented by a traveller:

- has been issued by a genuine authority;
- contains data which is unaltered; and
- has not been revoked.

The arrangements for PKI authentication of eMRTDs rely on the global distribution of keys and revocation lists from passport issuers to border inspection agencies between States. In the absence of more efficient alternatives, this distribution would require the bilateral exchange of these certificates. While theoretically possible, individual bilateral exchange would be too difficult to achieve in a timely or sustainable way.

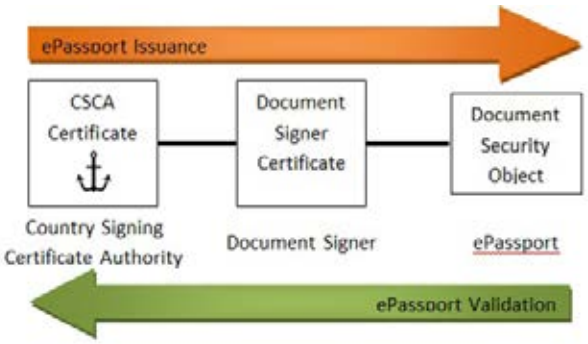
ICAO maintains the Public Key Directory (PKD) in order to reduce the distribution burden on State authorities responsible for eMRTD issuance, and the collection burden on undertaking PKI authentication at border inspection.

PKI 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 national passports issued in booklet format. The term ePassports is used throughout the rest of this Topic given it is the most common travel document used with PKI authentication.

The ICAO PKD is the global repository of all relevant 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 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 basic ePassport PKI authentication 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 level of basic access. For PKD members, downloads are available in an easier to use, transaction ready, format.

70 *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

To assure business continuity, the PKD has extensive system redundancy and backup. Given global travel volumes, the PKD operates offline in batch processes and is not designed to support individual authentication transactions. Instead, States download certificates and revocation lists from the ICAO PKD[71] to their National Public Key Directorate (NPKD). State NPKD is the national reference database containing the certificates and revocation lists downloaded from the ICAO PKD, and obtained by bilateral exchange. The State NPKD can then be accessed by border control systems.

An NPKD needs to be separate from the national PKI infrastructure which supports ePassport issuance and uploads to the ICAO PKD. Establishing and operating a NPKD is a significant, ongoing administrative and technical commitment independent of ePassport issuance and ICAO PKD uploads.

HOW IT WORKS – BORDER AGENCIES

Travellers present their ePassport to a border inspection official, or place their document onto an eGate interface.

The Machine Readable Zone (MRZ) of the ePassport is read optically by a machine reader[72]. The data read from the MRZ initiates a transaction to access the data from the IC chip, and a privacy protection protocol that relies on data read from the MRZ is completed.

Data is retrieved from the IC chip of the ePassport.

A comparison is made between the digital certificates retrieved from the ePassport with the DSC and CSCA Master List or link certificates downloaded from the NPKD. Certificate matches confirm that the ePassport was genuinely issued and is unaltered. A further check against the most recent revocation list obtained from the ICAO PKD confirms that the certificates remain trusted by the issuing authority.

The PKI authentication checks in the certificate trust chain are fully automated, typically taking just a few seconds. As a result, PKI ePassport authentication is completed in the background without delaying the traveller.[73]

The PKI authentication of ePassports at border inspection does not require States to issue ePassports. However, States issuing ePassports 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 or intending to issue ePassports. Membership requires application and payment of a one-off joining fee and an ongoing annual fee[74]. New members of the PKD have up to 15 months in which to commence the uploads of certificates for their ePassports, and start 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.

Presently, some of the certificates available from the PKD have unusual conformance characteristics or do not fully meet technical specifications. It is intended that in future, PKD members will have access to defect lists which identify

71 For downloading the certificates and revocation lists: *ICAO PKD data download*, ICAO, Montreal, https://pkddownloadsg.icao.int/
72 See: *Topic B - Document Readers*
73 More information on the fundamentals of ePassport are found at *ePassport Basics*, ICAO, Montreal, https://www.icao.int/Security/FAL/PKD/Pages/ePassportBasics.aspx
74 The latest PKD fee are available in the folder PKDFinanceDocuments: *Publications*, ICAO, Montreal, https://www.icao.int/Security/FAL/PKD/Pages/Publications.aspx

any non-conformance, and provide border inspection work-around solutions.

Membership to the PKD is continuously growing and the list of participants is available at: https://www.icao.int/Security/FAL/PKD/Pages/ICAO-PKDParticipants.aspx

HOW IT WORKS – AIRLINES

PKI authentication of ePassports is a State responsibility. However, there is no technical obstacle to airlines downloading digital certificates and revocation lists from the ICAO PKD, and undertaking PKI authentication of ePassports. In the future, it is possible that operating partnerships may emerge that include all electronic travel documents, and that eMRTD authentication may be undertaken by airlines or other commercial entities, where this brings advantages to their operations.

BENEFITS AND OPPORTUNITIES

The ICAO PKD provides an efficient, secure and sustainable means to obtain the certificates and revocation lists necessary to undertake PKI authentication of ePassports.

PKI authentication of ePassports means that the document can be used with confidence as the identity token in Automated Border Control (ABC) systems. When PKI certificates fail to authenticate, eGates can be configured to refer travellers for human inspection and clearance.

PKI authentication of ePassports provides a reliable, automated mechanism to determine the integrity of the travel document presented by the traveller.

TECHNICAL ISSUES

PKI authentication of ePassports 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 border inspection needs to maintain systems which can read ePassports both optically and electronically. The electronic interface must access the up-to-date digital certificates obtained from all States issuing ePassports, so that the necessary PKI 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 commercial ePassport readers include functionality to present the necessary data to a border control system. The border control system must include functionality for PKI authentication and for referring "fail to authenticate" instances to border agency staff.

RISKS AND COST MITIGATION

PKI authentication of ePassports at border inspection relies on an extensive technical infrastructure, and adherence to demanding administrative protocols and practices[75]. The document readers deployed at border inspection need to be capable of handling ePassports. 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 inspection. Certificates and revocation lists must be regularly updated, and earlier certificates need to be retained for as long as the travel documents they authenticate remain valid. A border control system which does not authenticate against up to date certificates and revocation lists has the potential to falsely reject good documents and falsely accept compromised documents.

States intending to undertake PKI authentication of ePassports 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) protocol. The certificates required for EAC are not available from the ICAO PKD and must instead be obtained bilaterally from ePassport issuers.

A careful appraisal of administrative capacity and capability, sufficient to sustain effective ePassport PKI certificate handling arrangements, should precede consideration of the implementation of ePassport PKI authentication.

75 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

RELATED REQUIREMENTS

- ✓ National legislation authorising creation of a NPKD, downloads from the ICAO PKD and eMRTD PKI authentication at border control.
- ✓ 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 border control systems and document readers to access the certificates and revocation lists necessary to complete ePassport 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 PKI authenticated at the Australian border.

Membership of the ICAO PKD should be managed by a designated position within the border 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.

All ePassport readers should be checked regularly to ensure that they are accessing up to date certificates from the NPKD.

Where ePassports 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.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Extracts from ICAO Annex 9 – *Facilitation* Chapter 3. Entry and departure of persons and their baggage[76]:

"...

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 include 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."

76 *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

Publications, PKDFinanceDocuments, ICAO, Montreal, available at: https://www.icao.int/Security/FAL/PKD/Pages/Publications.aspx

Other Sources

Guideline on requirements for inspection on machine readable (electronic) identity and travel documents produce 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_htm.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

***Interoperable Applications for Traveller Identification** - by providing States with a universal, mandatory, standardised, globally interoperable, biometric verification option (face images) and optional alternatives (fingerprints and iris images)*

KEY MESSAGES

- ✓ Comparison of live biometric samples (face, fingerprint or iris) from a traveller with biometric templates held within the chip in eMRTDs.
- ✓ State MRTD issuers can determine which optional biometric data to include in an eMRTD chip, and control access at border control to this sensitive information.
- ✓ Where integrated with eGates, kiosks and airline check-in processing, provides efficiency, security and facilitation benefits.

OVERVIEW

States able to undertake the electronic Machine Readable Travel Document (eMRTD) Public Key Infrastructure (PKI) authentication at border inspection[77] can rely on the biometric images[78] available in eMRTDs as being genuine and unaltered.

States wishing to undertake eMRTD biometric identity verification at border inspection 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 Integrated Circuit (IC) chip in each eMRTD[79].

States may be able to access the optional fingerprint or iris images stored in DG 3 or 4 in those eMRTDs where they have been included. Most States that include the optional, additional fingerprint or iris images in their eMRTDs restrict access to this sensitive personal information. The mechanism most commonly used to achieve this restricted access is the Extended Access Control (EAC) protocol. EAC allows the eMRTD issuing authority to determine which document readers at which airports and other border locations 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 eGates[80], or can be used to support human inspection. 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 at eGates or human inspection of travel documents.

HOW IT WORKS – BORDER 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.

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[81].

Templates are created from both biometric images by the biometric software engine. The templates are compared and a result is returned to the border control system. 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:

77 See: *Topic J* - Public Key Infrastructure and the ICAO Public Key Directory

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

79 *Machine Readable Travel Documents,* Doc 9303, 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

80 See: *Topic G - Automated Border Controls*

81 See: *Topic J* - Public Key Infrastructure and the ICAO Public Key Directory

- 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 can only inform 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 border control systems 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 which is a feature of all Information and Communication Technology (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 which 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 in this manner outside ABC to confirm that an individual is the genuine holder of an eMRTD.

Using biometric identity verification through eMRTDs 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 ICAO Doc 9303 Part 11 – Security Mechanisms for MRTDs[82] 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 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 can be expensive and require adequate computing power and network cabling. As for ABC systems, it is important that vendor independent, solution neutral advice informs consideration of options prior to committing to solutions or biometric modalities[83].

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

83 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

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 National Public Key Directory (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 border control system with biometric capture and an eMRTD Public Key Infrastructure 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. In these national solutions:

- Australia, Finland, Germany, New Zealand, Portugal and the United Kingdom, amongst other States, use facial images; and
- France, Hong Kong, Malaysia and Singapore, amongst other States, use fingerprint images.

The United Kingdom uses a standalone facial image matching system at its primary line whenever there is doubt about the identity of the holder of an eMRTD. The traveller might be referred there by a border officer at the conventional control, or the traveller might have been rejected by the ABC system. This provides officers with additional objective information which can help to resolve the situation.

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.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Extracts from ICAO Annex 9 – *Facilitation,* Chapter 3. Entry and departure of persons and their baggage[84]:

"...

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

84 *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 DATABASE OF STOLEN AND LOST TRAVEL DOCUMENTS

***Interoperable Application supporting 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 over 76 million records of stolen, stolen blank, lost and revoked travel documents as reported by the 75 Member States of INTERPOL.
- ✓ Accessible by both border agencies and airlines, via multiple INTERPOL technical solutions (FIND, MIND and I-Checkit)
- ✓ Supplements the use of national watchlists at border inspection.

OVERVIEW

The international police organization (INTERPOL), enables police in 190 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.[85]

INTERPOL operates from its General Secretariat in Lyon, France, 24 hours a day, 365 days a year. It also has seven regional offices worldwide, and representative offices at the United Nations in New York and at the European Union in Brussels. Each INTERPOL member country maintains a National Central Bureau (NCB) staffed by its own highly trained law enforcement officials.

The Integrated Border Management Task Force (IBMTF) is the central point of contact and coordination for international border security activities at INTERPOL.[86]

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.

The IBMTF draws upon expertise across departments within INTERPOL as well as from international partners. INTERPOL also offers a range of policing capabilities which can help States to enhance their own border security procedures, and to integrate their efforts with those of their neighbours.

INTERPOL's Stolen and Lost Travel Documents (SLTD) database enables INTERPOL, NCBs and other authorized law enforcement entities – including border 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 United States, to help States secure their borders and protect their citizens from terrorists and other dangerous criminals using 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

85 *INTERPOL*, https://www.interpol.int/
86 *Border management*, INTERPOL, https://www.interpol.int/INTERPOL-expertise/Border-management

these documents to INTERPOL headquarters for inclusion in the SLTD database.

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. Passports 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 – 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 officials 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 through I-Checkit, a system interface specially developed for them.

HOW IT WORKS – BORDER AGENCIES

The exchange of SLTD information is a key strategy to strengthen border controls and mitigate the impact of identity theft and immigration fraud. The ICAO Doc 9303 Part 2: Specifications for the Security and Design, Manufacture and Issuance of MRTDs[87], 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 verify documents against INTERPOL databases systematically at primary inspection; and
- Install checks to determine whether a holder is presenting a stolen, lost or revoked document at a border crossing.

When border agency staff receives an SLTD alert via their border control system 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 obtain a replacement travel document. If the travel document is in being presented by a person other than the person to whom the travel document 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 and law enforcement agencies via INTERPOL's I-24/7 secure global police communications system. Only the State which 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 that states be proactive in submitting notice of such documents to INTERPOL.

Law enforcement officials at INTERPOL NCBs and other locations with access to INTERPOL's databases through the I-24/7 system – such as airports and border crossings – can query the documents of individuals travelling internationally against the SLTD, and immediately determine if the document has been reported as stolen, stolen blank, lost or revoked so they can take necessary action. Once an alert is raised, it must be resolved by contacting directly the State of issuance that has reported the document.

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,

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

including border agency officials responsible for the identification of travellers.

For access to its SLTD databases, INTERPOL offers real time and batch update interfaces. Either can be integrated with national border control system for primary and/or secondary processing of travellers.

SLTD can also be implemented as a separate, additional screening check to support secondary examination, where more time can be dedicated to such checks. However, when fully integrated with national border control systems, the INTERPOL SLTD greatly enhances the capacities for identification of travellers at primary processing.

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 admission. 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 and electronic contents to determine whether any unauthorised change has taken place, and if so whether any observed forgery or counterfeiting techniques should be circulated to front line staff, INTERPOL and the original issuer.

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-Checkit[88]. 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 a screening solution that complements and enhances national border security systems. It allows airlines and cruise ship operators to conduct advanced passenger checks in real-time, in collaboration with national border and law enforcement agencies. However, I-Checkit is only fully effective when border 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 which can be readily accessed by police and border 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 irregularly) 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 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 can be initiated when the MRTD is placed on the document reader without any other processing input from border agency staff. 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.

88 *I-Checkit*, INTERPOL, https://www.interpol.int/INTERPOL-expertise/I-Checkit

TECHNICAL ISSUES

Border agencies have two main methods for accessing the SLTD.

In 2005, INTERPOL introduced two networks, the Mobile INTERPOL Network Database (MIND) and the Fixed INTERPOL Network Database (FIND). MIND and FIND facilitate searches by border agencies of SLTDs, people, and even stolen motor vehicles, at international border control points. 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, while MIND does not contain this personal data.

The application of FIND to supplement national watchlist searches of the biographic details of travellers is discussed in *Topic N - International Watchlists*.

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 this list in the course of their duties.

RELATED REQUIREMENTS

- ✓ National legislation for Border Control Management (BCM) agencies to access and act on SLTD matches is an INTERPOL requirement for the implementation of MIND/FIND.
- ✓ Protocols and business processes for the resolution of SLTD matches.
- ✓ 24/7/365 operational support for contacting the passport issuing agencies of other States (via their NCBs) to resolve SLTD matches.
- ✓ ICT integration of border control system with INTERPOL MIND/FIND.
- ✓ Reliable, continuous supply of electricity and connectivity.

RISKS AND COST MITIGATION

Primary processing or joint targeting centre access to the SLTD will require upgrades and integration with information and communication technology (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 agencies should consider covering air borders by means of advance passenger information (API) details being run through the SLTD via a central system before the passenger concerned embarks; other airports or ports with low volume or mixed traffic (including maritime) should have local access to the SLTD.

BEST PRACTICE EXAMPLES

Establish a good working relationship with the local INTERPOL NCB to allow for quick searches of INTERPOL resources, and timely responses on database matches.

Where infrastructure and finances allow, install or upgrade primary line and targeting centre links to INTERPOL's SLTD system 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 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 as soon as possible.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Annex 9 – *Facilitation*, Chapter 3. Entry and departure of persons and their baggage[89]:

"...

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. ...*"

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."

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, INTERPOL Database Management Unit: databasemanagement@interpol.int

89 *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

M. INTERNATIONAL WATCHLISTS

Interoperable Applications for Risk Assessment *- by supplementing 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 transnational 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 exit or entry, and facilitate information-sharing between States concerning potentially high-risk travellers.
- ✓ In best practice, should be integrated into national watchlist systems for simultaneous consultation during visa, ETS, ABC and primary line queries.

OVERVIEW

Member States of the United Nations (UN) have obligations and responsibilities which include the enforcement of UN imposed sanctions. To support the enforcement of its sanctions, the UN publishes the Consolidated United Nations Security Council Sanctions List (CUNSCSL), which includes all individuals and entities subject to sanction measures imposed by the Security Council.[90] 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 Security Council resolutions on counter-terrorism request States to prevent the mobility of terrorists and the travel of Foreign Terrorist Fighters (FTFs), whether or not they are listed under CUNSCSL.

Additionally, INTERPOL member States 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 border control management.[91] These Notices are published by INTERPOL's General Secretariat at the request of National Central Bureaus (NCBs) and other authorized entities.

The different types of Notices include:

Red 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.

Blue Notices – A request to collect additional information about a person's identity, location or activities in relation to a crime.

Green Notices – Issued to provide warnings and/or intelligence about persons who have committed criminal offences and might repeat these crimes in other countries.

Yellow Notices – A request to help locate missing persons, often minors, or to help identify persons who are unable to identify themselves.

Orange Notices – Issued to warn of an event, a person, an object or a process that represents a serious and imminent threat to public safety.

In the case of Red Notices, the specified persons are wanted[92] 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 United Nations, international criminal tribunals and the International Criminal Court to seek persons wanted for committing crimes within their

90 *Consolidated United Nations Security Council Sanctions List*, United Nations Security Council, https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list
91 *Notices*, INTERPOL, https://www.interpol.int/INTERPOL-expertise/Notices
92 *View Red Notices*, INTERPOL, https://www.interpol.int/notice/search/wanted

jurisdiction; notably genocide, war crimes, and crimes against humanity.

INTERPOL also leverages its network and established arrangements for publishing and distributing INTERPOL-United Nations Security Council 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.[93]

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 border control systems.

HOW IT WORKS – BORDER AGENCIES

In best practice jurisdictions, international watchlists should be integrated into national watchlist systems so that they are consulted at the same time as visa, Electronic Travel System (ETS), Automated Border Control (ABC) and primary line queries, at both the central level as well as by frontline officers.

This integration is facilitated by:

- (In the case of the UN sanctions list) publication or the watchlists in standardised, downloadable .xml, .html and .pdf formats; and
- (In the case of INTERPOL Notices) interfaces with existing national border/law enforcement systems through the INTERPOL FIND solution.

HOW IT WORKS – AIRLINES

The purpose of watchlists is to trigger an intervention from a responsible State authority to more closely examine the risk posted 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.

Some international watchlist datasets – such as the CUNSCSL and INTERPOL Red Notices – are publicly available, and it is technically feasible for airlines to check passenger information against these datasets. However, this requires a framework for State authorities to provide support to airlines when matches occur. In the absence of such a framework, it may be inadvisable and ineffective for airlines to assume this role.

BENEFITS AND OPPORTUNITIES

States that incorporate searches of international watch lists into their systems are helping to combat terrorism and other transnational crime in collaboration with the United Nations, INTERPOL, and regional and other entities. Additionally, States 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. However, UNSC Resolution 2322 (2016) calls upon States to share biometric and biographic information on FTFs and individual terrorists, and to provide such information to frontline screeners. Indeed, international biometric watchlists are growing, and models are emerging for managing the related privacy and data protection issues.

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 future.

TECHNICAL ISSUES

INTERPOL's Criminal Information System is available to the National Central Bureaus (NCBs) of its member countries 24 hours a day, 7 days a week. For border agencies and frontline screeners, 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 facilitation. Some level of integration with national border control systems desirable for effective implementation.

93 *Special Notices, INTERPOL – United Nations Security Council Special Notice,* INTERPOL, https://www.interpol.int/INTERPOL-expertise/Notices/Special-Notices

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. But name matching can be a challenging and error prone task. 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).

Matching is less likely if the details included in the watchlist record do not match the details included in the Machine Readable Travel Document (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 border control systems. 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 such a person's 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 which meet national data quality standards are included;
- Listings include clear advice on the action required from border agency staff;
- Listings are subject to regular review;
- 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.

As noted previously, 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 which attempt to participate without mature capability to sustain effective watchlist management are susceptible to failure. The reputational risk of integrating international watchlists into national border control systems prematurely or incorrectly should be carefully evaluated.

RELATED REQUIREMENTS

- ✓ National legislation for Border Control Management (BCM) 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.
- ✓ Information and Communication Technology (ICT) integration of border control system 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)[94] from the Asia-Pacific region is an example of a regional biometric watchlist application, and is intended to

94 *Regional Biometric Data Exchange Solution (RBDES)*, The Bali Process, http://www.baliprocess.net/regional-support-office/regional-biometric-data-exchange-solution/

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 which 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; members can opt in and opt out of the RBDES at any time, and endorsement of the RBDES by Bali Process members does not commit any member to using it.

The significance of the RBDES arrangement is that 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 national legislation and privacy and data protection protocols within 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/

6 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 staff 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 do indeed assist in making faster and more accurate 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 determinates of the effectiveness and efficiency of those efforts.

Where doubts arise about traveller identity or risk, the authentication of travel documents may need to be supplemented by:

- Closer, forensic inspection of MRTDs and any other identity documents the traveller may hold (something they "have");
- Interviews with travellers to establish their true circumstances ("continuity" and what they "know"; and/or
- Alternative or additional biometric comparisons (who they "are").

6.1 Primary and Secondary Examination of Travellers

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, etc.)? Does the traveller qualify for admission 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 watch list entry or intelligence assessment?

If any of the points above are in doubt, an officer may decide to carry out more thorough questioning, and to request that the traveller produce evidence to support their statements. Adverse information available to the border officer may be put to the traveller where it does not prejudice intelligence or law enforcement operations and the response of the traveller 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 is unable to be read should alert border officers to the possibility that the holder may be an impostor.

Attempts by travellers to bribe or intimidate a border officer at primary examination should be reported to management.

SECONDARY EXAMINATION, DETENTION AND REMOVAL

Standard Operating Procedures (SOPs) for interventions at secondary examination should be published and accessible to and understood by border staff. 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. Border control systems should include modules to record and manage the resolution of referrals at secondary examination.

SOPs should highlight to border agency staff 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, people smuggling and other abuses of human rights. Where detention is required, the conditions should preserve the dignity of travellers, and 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 and in conformity with international law, and based on the evidence presented by the traveller, as well as any background information available to the border officer(s) conducting the examination. Travellers should be informed of adverse decisions, in writing, and informed of any appeal procedures.

If a decision is made to deny entry, ideally the traveller should be removed in accordance with national legislation and the SARPs of Chapter 5. Inadmissible Persons and Deportees of Annex 9 - *Facilitation*[95].

PHYSICAL ARRANGEMENTS FOR TRAVELLER AND DOCUMENT INSPECTION

The full benefit of the verification of traveller identity to help prevent and deter the travel of terrorists and other trans-national criminals can only be achieved when *all* travellers are subject to border controls. For effective BCM it is essential that international airports have adequate layout and reliable access controls at all times, in particular to prevent travellers and crew from circumventing departure and entry controls.

This can happen when travellers are assisted in avoiding border control inspection points, when entries and departures are not recorded or processed in border control systems, 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 the trust and confidence among BCM agencies and personnel, other national authorities, airport stakeholders, and travellers.

Implementing some simple measures can reduce the risk of border control evasion and related conspiracies to facilitate irregular migration at control points. The introduction of snake queues at counters can help disrupt conspiracies involving facilitators, corrupt officials and airline check-in staff. Ensuring that travellers are randomly presented to airline and border staff makes it difficult for a traveller 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 staff 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 officials to be on duty at a time and place coordinated with travellers attempting irregular migration.

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. The key to enforcing a "no mobile phone" policy is the installation of lockable storage cabinets in which front line border staff can leave their phones during their shift. When border staff 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 Documents[96]

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 country 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 in the form of document readers is invaluable but the need for human inspection of MRTDs remains. All front-line border officials should be trained in basic document inspection and verification techniques, including the identification of fraudulent or altered documents and imposters.

95 *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

96 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.

The ICAO training package "Control of the Authenticity and Validity of Travel Documents at Airport Borders - Level 1"[97] 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)[98] and UNODC[99], various States as part of their bilateral cooperation programme, and the private sector. A good practice is for basic frontline inspection to be supported by forensic specialists at secondary inspection.

Another 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 for limited use at primary examination, and more extensive use at secondary examination, that can be part of the personal equipment of each frontline officer.

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. Ultraviolet light sources can be used at secondary examination to expose altered or counterfeit text, or disturbance to areas of printing or the paper or other substrate, that may indicate document abuse. Whatever equipment is deployed, it is necessary to provide training on their use.

Border agencies should be expert in inspecting and verifying the security features of their own country's travel documents, as well as those of other States' travel documents which are commonly encountered on their border[100]. Relevant training to achieve this expertise should be a high priority for border agencies.

Some systems, such as the **E**lectronic **D**ocumentation **I**nformation **S**ystem **O**n **N**etwork (EDISON TD) image library[101] contains descriptions and security features of genuine travel and identity documents issued by countries and international organizations. Another useful product is the EU database False and Authentic Documents Online (FADO) for EU law-enforcement agencies only and its public version Public Register of Authentic travel and identity Documents Online (PRADO)[102] which displays travel documents and their security features. In addition, INTERPOL has developed a database that contains information related to forged and counterfeited travel document. The Digital INTERPOL Alert Library-Documents Database (Dial-Doc) was created in order 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 secure cloud I-24/7[103]. Other commercially available publications and image databases show genuine examples of travel documents, with specifications and explanations of their security features.

WORKING WITH AIRLINES, AIRPORT MANAGEMENT AND OTHER BORDER AGENCIES

Although not yet universal, 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 travel identification process.

BCM authorities should keep airline staff operating in their border space informed about trends in irregular migration (including specific examples of travel document fraud) and travellers known to present a risk, so that airline staff can be more effective in contributing to confirmation of traveller identity.

In major embarkation and transit airports, airline check-in and boarding gate staff are assisted by LOs, State officials seconded to airlines to help ensure that only properly documented travellers commence or continue their journey.

Border control authorities should also collaborate with airport operators and airlines in influencing the design

97 *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

98 *Passport Examination Procedure Manual (Second Edition)*, IOM, 2016, to make an order: https://publications.iom.int/books/passport-examination-procedure-manual-second-edition

99 *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

100 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

101 *EDISON Travel Documents*, available at: http://www.edisontd.net/

102 *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

103 *Databases*, INTERPOL, available at: https://www.interpol.int/INTERPOL-expertise/Databases

and operation of access control arrangements[104]. Airlines or airport staff 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, and these areas should also be secured with appropriate access controls. Depending on a State's national legislation and the policy of the border 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 staff.

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Extracts from ICAO Annex 9 – *Facilitation* Chapter 3. Entry and departure of persons and their baggage[105]:

"...

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. ..."

"...

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.*

..."

104 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

105 *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

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 multi-channel 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.

..."

7 Human Resource Considerations in Border Control Management

Sections 4 and 5 of this Guide describe, respectively, National Border Inspection Systems and Tools, and Interoperable Applications, and thus deal primarily with the application of technology in traveller identification and risk assessment in BCM. While the use of these technical solutions can contribute significantly to effective and efficient BCM and identification of travellers, they are not the only contributing factors in achieving these outcomes.

The importance of the human resource in ensuring the integrity of border controls cannot be overstated; irrespective of the tools and applications used, no border is secure or efficient without effective leadership and management, a competent and motivated workforce, clear prioritization of efforts and resources, and an overarching policy framework that is robust and adaptive.

7.1 Personnel

This section addresses key principles and practices relating to the human resource of BCM including appropriate staffing levels, training, career opportunity, adequate remuneration, recognition and utilization of staff skills and experience and clear and attainable objectives, standards and values

RECRUITMENT AND RETENTION

Persons working in border management have an important role to play, in both traveller facilitation and on the national and international security fronts. Given their important responsibility, border officers should be carefully 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. BCM cannot be secure if not enough officers are deployed to carry out the processes and use the tools and applications described in sections 4 and 5. Sufficient staff 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. 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 staff and promoting compliance with departmental 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 staff alert and fresh. Shifts should be structured so that staff are not on duty for too long, and that breaks are built into the schedule.

Staff should be rotated through front-line and back office duties, to broaden their experience and keep them up to date with any 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 staff can carry out the widest possible range of duties relevant to their operational environment.

Staff 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.

Staff appraisals provide an opportunity to identify, understand, and address sub-standard performance, as well as to identify career development opportunities. Appraisals should be impartial and unbiased, aligned with published agency standards and objectives.

PROFESSIONAL STANDARDS

The senior management of BCM authorities should set clear and attainable objectives, standards and values for the agency. These should be formal, published, and easily accessible for all staff. While they can be expressed as vision statements and/or objectives, it is also important that they be sufficiently concrete and concise to be understood by all staff.

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 border control systems can assist in monitoring and auditing staff activity, including in recording individual officers' actions and decisions.

Measurable performance indicators should be identified to assess the performance and standards of border agencies. These might include transaction times and queuing times at entry and departure. Performance reporting should be analysed to identify staff shortages, misaligned work priorities, and ineffective processing methods. One technique is the "mystery shopper", where a trusted person is placed in the traveller queue to observe the border process and staff performance.

Good practice is for border agencies to have a professional standards unit, and/or to have regular external inspection and auditing. External review is an important means of maintaining the confidence of other border agencies, citizens and travellers in the efficiency and integrity of border officers.

Staff should be encouraged to make suggestions as to how to improve their jobs and the overall performance of BCM. Staff who report unprofessional practices of any sort should be protected, and their concerns investigated.

HUMAN FACTOR

Appropriate attention to human factors in BCM allows border control staffs 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 is multidisciplinary in nature and impacts 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 ;
  - Efficiency ;
- Well-being of operational personnel.

For example, motivated individuals perform with greater effectiveness than unmotivated individuals. Some of the many factors which may influence the well-being of operational personnel working 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 BCM 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 BCM personnel. This ensures that all border services officers are clearly identifiable by travellers, making them more accountable for performing their duties in a consistent and professional way. In jurisdictions where border agency staff 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 staff in headquarters and in operational / traveller contact positions.

Having a functional and accessible system for travellers / customers to report complaints, or simply to provide feedback on their entry or exit experience can also convey transparency and help to maintain good governance in BCM

Having all BCM staff 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 border control systems typically include session and transaction audit features. However, for these to be effective, clear and strictly enforced protocols need to be developed and enforced. Whenever a frontline border control 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, log-in credentials and passwords should be unique to each authorized officer. The sharing of log-in 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 staff, as well as for ensuring, first, that the entry of all travellers and crew are processed by the border control system at primary inspection or control; and second, that all referrals to secondary processing are recorded in, and managed by, the border control system.

In scenarios where a traveller cannot be processed through the border control system, 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 staff, or as supporting evidence in an investigation or a case of complaint.

Taken together, the transaction audit functionality of a border control system can be used in conjunction with log-in and log-off timestamping and CCTV recordings to perform transaction pattern analysis of the work of front line border inspection officials, yielding useful information about BCM performance.

Finally, a customary practice in many BCM 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.

8 Assistance to States

ICAO works with its 191 Member States, international and regional organizations and industry groups to maintain and develop the SARPs related to Annex 9 – *Facilitation* and its programmes, including the TRIP Strategy, to reflect current priorities, opportunities and challenges.

In addition to its core civil aviation standards and policy work, ICAO also provides guidance and assistance to States to help them as they work to implement the ICAO requirements.

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 remains committed to assisting Member States in the development and maintenance of a NATFP[106] 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. The ICAO TRIP Platform, a one-stop source of facilitation-related information, is aimed at the dissemination of expertise and information of a sensitive nature through restricted and controlled access. Upon nominating their National Focal Point and Alternate Focal Point for Facilitation matters, States are granted access to the platform[107].

For the implementation of the ICAO TRIP Strategy at the national level, a structured action plan was developed by the ICAO Secretariat to provide guidance to the relevant entities[108]. 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. The national focal point for facilitation matters is to coordinate the implementation of the roadmap[109] by the National Air Transport Facilitation Committee and Programme.

The actions related to the two TRIP elements related to BCM, Inspection Systems and Tools and Interoperable Applications, are to be implemented mainly by border control authorities and airlines and include the use of the PKD, facial recognition comparison capabilities of ePassports, inspection of travel documents using ABCs, checking passports against the INTERPOL SLTD, implementing API and PNR, and using watchlists and other mechanisms for information sharing. These implementation mechanisms are described in the 13 technical Topics in Section 4 and 5 of this Guide. The ICAO resources on the TRIP elements currently available, including technical guidelines, the TRIP Magazine published twice a year and the new TRIP Compendium can be found at: https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx

In addition to all these materials and guides, 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.

Every year, the Secretariat organizes the ICAO TRIP Symposium and Exhibition in Montreal. The Symposium enables the exchange of information on all aspects of traveller identification management and the ICAO TRIP Strategy while also providing decision makers and technical experts with insights on key current and emerging issues. The accompanying technical exhibition showcases a broad range of products and services related to travel document security applications, border control and automated border control systems, and identity management.

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 while fostering engagement with international experts and the sharing of experience and best practices. Information on past and upcoming events is available at: https://www.icao.int/Security/FAL/TRIP/Pages/Events.aspx.

---

106 See: *Section 3.3 Border Control Management Agencies and Stakeholders*

107 *Nomination of a National Focal Point for Facilitation,* ICAO State Letter No. EC 6/1-16/106, 14 December 2016. 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.

108 *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

109 *ICAO TRIP Implementation Roadmap for Member States*, ICAO State Letter No. EC 6/3-17/96, 11 August 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.

Additionally, States and selected international organizations 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 the task of developing policy, recommendations and proposals for the implementation of the ICAO TRIP Strategy, including the development and maintenance of MRTD standards and specifications[110].

States are invited to nominate qualified and experienced experts in evidence of identity, MRTDs, document issuance and control, inspection systems and tools, and interoperable applications to participate in the TAG/TRIP: https://www.icao.int/Security/FAL/TRIP/Pages/TAG-TRIP-Membership.aspx . Alternatively, agenda and discussion papers and a meeting report are available for download: 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 or by contacting the ICAO Facilitation Section at FAL@icao.int.

Through the network of ICAO Regional Offices, the Secretariat provides direct assistance to States[111]. 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, enabling them to effectively implement the ICAO SARPs and the TRIP roadmap.

In terms of coordinated policy development and assistance to States, ICAO works with numerous international organizations.

The efforts of ICAO complement 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 their implementation of the United Nations Security Council Resolutions[112] related to counter-terrorism such as:

- Resolution 1373 (2001) – A wide-ranging counter-terrorism resolution adopted following the 11 September terrorist attacks on the United States;
- Resolution 2178 (2014) – Addressing the threat of terrorism by stemming the flow of foreign terrorist fighters (FTFs); and
- Resolution 2309 (2016) – Calling on Member States to work with ICAO to ensure that its international security standards are reviewed, adapted and implemented to effectively address threats to aviation security.

Outside ICAO, representatives of BCM agencies from many States meet their airline partners in the IATA Control Authorities Working Group (IATA/CAWG)[113], a forum for ongoing dialogue between airlines and Immigration officials in respect of the control of illegal migration.

For operational implementation of API and PNR[114], ICAO relies on partnerships with the WCO and IATA. The importance of these sources of passenger data continues to grow and this is reflected in the UN Security Council Resolutions and the SARPs in Annex 9.

ICAO and INTERPOL work closely together to help States integrate their border control systems with the mechanisms of INTERPOL, including the SLTD[115]. Another important partnership for assisting States with their BCM is taking place under the memorandum of understanding signed by ICAO and IOM in 2016. 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 projects[116]. IOM is well placed to deliver strategic and operational advices and support to States, wishing to develop and enhance their BCM.

Engaging with these organizations, committees and panels, and reviewing their publications, can provide deep insights into contemporary best practice, and therefore inform strategic national policy development and implementation.

110 *Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP)*, ICAO, available at: https://www.icao.int/Security/FAL/TRIP/Pages/Panels.aspx
111 *ICAO's Regional Presences*, ICAO, available at: https://www.icao.int/secretariat/RegionalOffice/Pages/default.aspx
112 *Security Council Resolutions*, United Nations Security Council, available at: http://www.un.org/en/sc/documents/resolutions/
113 IATA/Control Authorities Working Group (IATA/CAWG) , IATA, available at: http://www.iata.org/whatwedo/workgroups/Pages/icawg.aspx
114 See: *Topics H*- Advance Passenger Information and Interactive Advance Passenger Information and *I – Passenger Name Record*
115 See: *Topic L – INTERPOL SLTD Databases*
116 *Immigration and Border Management*, International Organization for Migration, 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

Manual on Notification and Publication of Differences, Doc 10055, ICAO, Montreal, YYYY, available at: TO BE PUBLISHED.

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 information

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 Presences, 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

Publications, PKDFinanceDocuments, 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

UN 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/

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/

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/

UN Strategy

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

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

Immigration and Border Management, International Organization for Migration, available at : https://www.iom.int/

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,

http://www.baliprocess.net/regional-support-office/regional-biometric-data-exchange-solution/

5. National

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