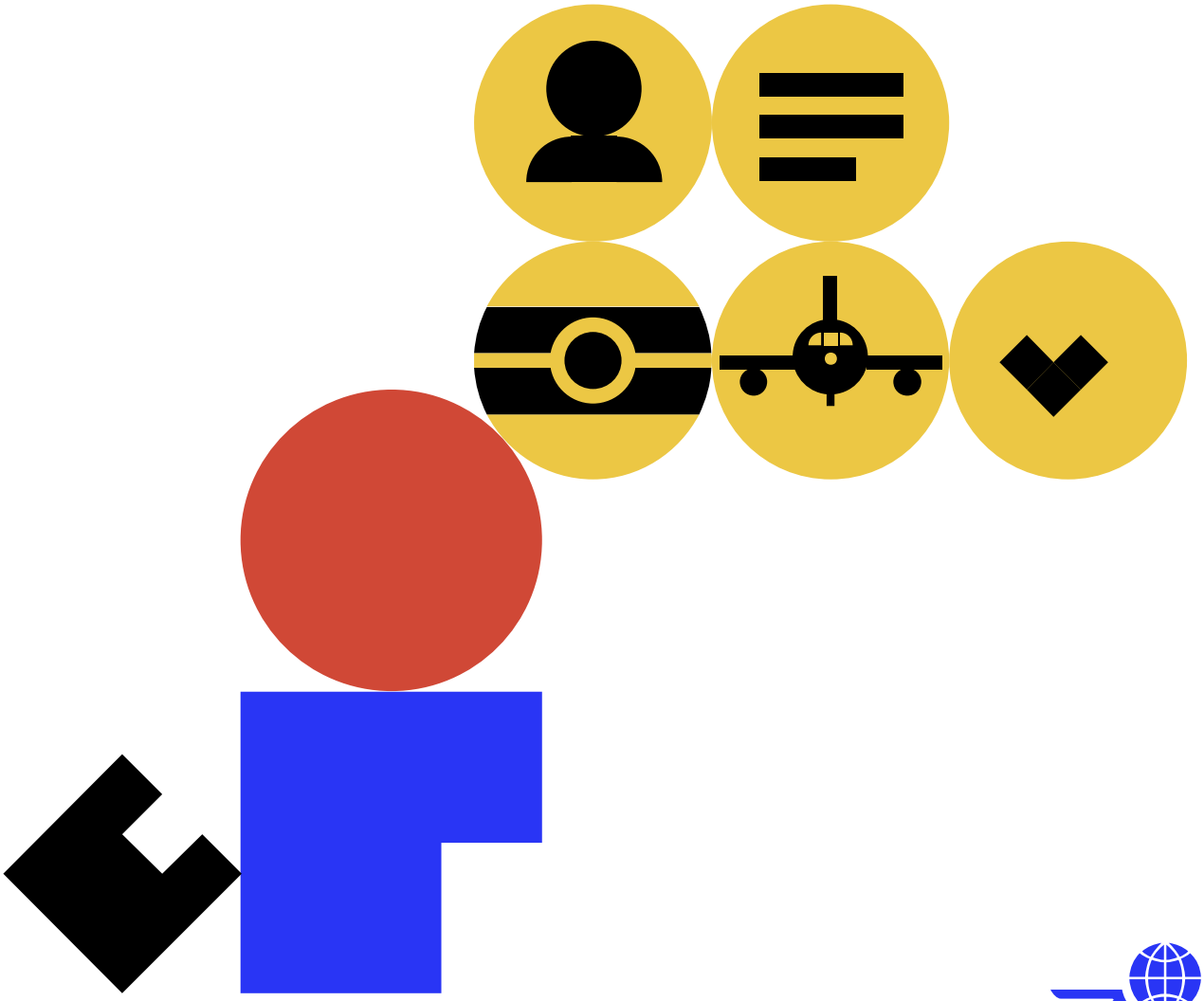
Effective 1 February 2021

Secured and Simplified Borders

Edition 1



IATA

NOTICE

DISCLAIMER. The information contained in this publication is subject to constant review in the light of changing government requirements and regulations. No subscriber or other reader should act on the basis of any such information without referring to applicable laws and regulations and/or without taking appropriate professional advice. Although every effort has been made to ensure accuracy, the International Air Transport Association shall not be held responsible for any loss or damage caused by errors, omissions, misprints or misinterpretation of the contents hereof. Furthermore, the International Air Transport Association expressly disclaims any and all liability to any person or entity, whether a purchaser of this publication or not, in respect of anything done or omitted, and the consequences of anything done or omitted, by any such person or entity in reliance on the contents of this publication.

Opinions expressed in advertisements appearing in this publication are the advertiser's opinions and do not necessarily reflect those of IATA. The mention of specific companies or products in advertisement does not imply that they are endorsed or recommended by IATA in preference to others of a similar nature which are not mentioned or advertised.

Senior Vice President
Airport, Passenger, Cargo and Security
International Air Transport Association
800 Place Victoria
P.O. Box 113
Montreal, Quebec
CANADA H4Z 1M1

Secured and Simplified Borders, 1st Edition
Material No.: 8971-01
ISBN 978-92-9264-245-7

Montreal—Geneva

Table of Contents

Foreword

The International Air Transport Association (IATA) is the trade association for the world's airlines, representing some 290 airlines or 82% of total air traffic. In its capacity, IATA represents, leads and serves the airline industry by advocating for the interests of airlines across the globe and improving the understanding of the benefits that aviation brings to national and global economies.

With its Open Border Strategy, IATA invites national authorities to enhancing border security while simplifying border crossing and removing unnecessary barriers to travel. The efficient use of border control technologies, principles and processes can help move toward a more open yet secure regime to boost travel, trade and tourism and thereby national economies.

The principles and programs detailed in the *IATA Secured and Simplified Borders Manual* will guide authorities in developing border control processes that integrate smoothly with air transport processes and do not impose an unnecessary burden on either the industry or travelers. The manual offers an opportunity for national authorities and international organizations to gain a greater understanding of the operational reality of airlines and how the latter can assist in increasing border security.

The context of the COVID-19 pandemic must be leveraged to rethink how border controls are performed and integrate them with health requirements and checks. Innovative solutions and partnerships between aviation authorities and industry stakeholders are crucial to working toward a more seamless and contactless travel journey.

Beyond the current context, I truly believe this manual will support much needed collaboration and provide authorities and stakeholders with a practical tool to support the implementation of efficient border security programs while facilitating greater freedom to travel.

Nick Careen

Senior Vice President for Airport, Passenger, Cargo and Security

Executive Summary

The unprecedented COVID-19 pandemic has highlighted more than ever that airlines, airports, governments and travelers share a common interest in ensuring that international air traffic is secure and predictable, while promoting greater connectivity. The *IATA Secured and Simplified Borders Manual* aims to provide a unique source of information for both governments and aviation stakeholders on how border control processes can be implemented in line with international standards and best practices.

The first section of the manual highlights the fundamental elements that should guide the development of border security programs for air travel. These consist of global harmonization, efficiency and cooperation:

- **Global harmonization** is the foundational element of air transport. The International Civil Aviation Organization (ICAO) has developed over the years a comprehensive set of standards and guidelines that member states are committed to abide by. The manual refers extensively to ICAO Standards and Recommended Practices (SARPs) contained in Annex 9–*Facilitation* of the Chicago Convention. Annex 9 is continuously evolving. The manual is based on Amendment 27 to Annex 9, applicable since February 2020.
- The second of these principles is **efficiency**. Prior to the outbreak of COVID-19, global air traffic was expected to double by 2035. This projection for growth constituted an important driver for airlines, airports and authorities to modernize border processes and rethink the passenger journey. With limited resources and infrastructure constraints, the industry and authorities were aiming to implement more efficient processes. This remains fully relevant today despite the drop in passenger numbers as health measures require more distancing and fewer passenger touchpoints. COVID-19 highlights the importance of most processes taking place off-airport, to accelerate the adoption of automated and touchless processes based on digital identities and to progressively remove manual and paper-based processes.
- The third principle of **cooperation** constituting a key message of this manual calls for a partnership approach in the development of border security measures. This cooperation should take place between aviation authorities and stakeholders, but also among governmental agencies for fostering synergies between the different processes.

The second section of the manual aims to help public authorities understand the different steps of the passenger journey and how airline systems work in the wider aviation ecosystem. This section will hopefully clarify some misperceptions and provide a more practical and operational view of the processes supporting the passenger's journey. Regulators often consider that airlines will simply adapt in a straightforward manner when adding a new data collection or control requirement. However, new requirements can have huge impacts on airline systems and/or passenger processing time. A couple of seconds per passenger can make the difference for a flight leaving on time or not.

The third section focuses on passenger data programs. More than any other border control program, passenger data requirements have a significant impact on airline systems and operations. The collection and transfer of travelers' information require airlines to change their processes and adapt their IT infrastructures. This section proposes a stepped approach to the implementation of passenger data programs, highlighting that states should carefully define theirs needs and resources available before engaging into complex programs. As such, IATA recommends states to focus first on the development of a robust advance passenger information (API) system that can support improved border management. To better fight illegal

trafficking and terrorist activities, API programs can be complemented by the collection of data from airlines' booking systems and passenger name records (PNR). This dataset can support the risk assessment performed by law enforcement authorities. As a final step, an interactive API (iAPI) system can bring significant benefits to authorities and airlines as it allows the identification of inadmissible passengers prior to boarding. This system is, however, complex and very time sensitive.

To ensure both authorities and stakeholders reap the full benefits of these programs, it is essential they be considered in the wider picture of border management tools and programs. The final section of the manual proposes a more holistic approach to border controls, leveraging passenger data in combination with travel authorizations, automated border control systems, travel documents and digital identity.

All these programs and tools will facilitate the introduction of more open border policies, which can ultimately help states to relax some of their entry conditions to facilitate travel, trade and tourism.

Acronyms

ABC: Automated Border Controls

ACI: Airport Council International

API: Advance Passenger Information

BAR: Board of Airline Representatives

CC: Contact Committee (WCO/IATA/ICAO)

CRS: Central Reservation System

CUPPS: Common Use Passenger Processing Systems

CUSRES: Customs Response

CUSS: Common Use Self-Service

CUTE: Common Use Terminal Equipment

DCS: Departure Control System

DMR: Data Maintenance Request (WCO)

DTC: Digital Travel Credential

eMRTD: Electronic Machine-Readable Travel Document

eTA: Electronic Travel Authorization

ETS: Electronic Travel System

EU: European Union

FSNC: Full-Service Network Carrier

FTF: Foreign Terrorist Fighters

GDS: Global Distribution System

iAPI: Interactive Advance Passenger Information

IATA: International Air Transport Association

IC: Integrated Circuit

ICAO: International Civil Aviation Organization

ID: Identity Document

ILO: Immigration Liaison Officer

INTERPOL: International Criminal Police Organization

IOM: International Organization for Migration

IT: Information Technology

KPI: Key Performance Indicator

LCC: Low-Cost Carrier

LoS: Level of Service

MCT: Minimum Connecting Time

MRTD: Machine-Readable Travel Document

MRZ: Machine-Readable Zone

NATFP: National Air Transport Facilitation Program

NDC: New Distribution Capability

NEXTT: New Experience Travel Technology

OCR: Optical Character Recognition

OSI: Other Service Information

PADIS: Passenger and Airport Data Interchange Standards

PKD: Public Key Directorate (ICAO)

PKI: Public Key Infrastructure

PNR: Passenger Name Record

PRL: Passenger Reconciliation List

PRM: Passenger with Reduced Mobility

RTPs: Registered Traveler Programs

SARPs: Standards and Recommended Practices (ICAO)

SLA: Service Level Agreement

SLTD: Stolen and Lost Travel Document (INTERPOL)

SSR: Special Service Request

TRIP: Traveler Identification Program (ICAO)

UN/CEFACT: United Nations Centre for Trade Facilitation and Electronic Business

UNECE: United Nations Economic Commission for Europe

UN/EDIFACT: United Nations Electronic Data Interchange for Administration, Commerce and Transport

UNOCT: United Nations Office of Counterterrorism

UNODC: United Nations Office on Drugs and Crime

UNSCR: United Nations Security Council Resolution

UNWTO: United Nations World Tourism Organization

USAP: Universal Security Audit Program (ICAO)

VIZ: Visual Inspection Zone

VUA: Visa Upon Arrival

WCO: World Customs Organization

WHO: World Health Organization

WTTC: World Travel and Tourism Council

Introduction: Shared Objectives and Interests

The last few years have been a tremendous time for openness and accessibility in air travel. In 2018, a record 4.4 billion passengers flew on scheduled flights. Had the COVID-19 pandemic not suddenly brought air traffic nearly to a halt in early 2020, forecasts were predicting that number would have nearly doubled to a staggering 8.2 billion by 2037[1]. Despite the fact that these forecasts are to be reviewed, the need for processing passengers more efficiently, in a more stringent global security context and with infrastructure expansion limitations, remains. In addition, the pandemic has further showed the pressing need to work toward increasingly processing passengers in a seamless and touchless way.

Air transport plays a crucial role in stimulating global economic growth and trade, reuniting families and friends, and facilitating tourism and cultural exchanges. While borders must remain secure, modern border control tools and technologies can help states and aviation stakeholders to reduce barriers to travel, increase countries' attractiveness and support the sustainable growth of international civil aviation.

The reduction in waiting times at the border and a more efficient use of the infrastructure needed to perform checks has a direct impact on passenger satisfaction. For example, industry studies have shown that improving the passenger experience results in higher retail revenues for airports[2]. Reduction of delays thanks to expedited border checks at departure or at transfer improves airline operational efficiencies, facilitating the journey of most travelers. Increased reliability in border control automation also allows authorities to manage a greater number of passengers by focusing resources on core security tasks and behavior analysis.

States can improve the attractiveness of their countries by reducing barriers to entry using modern border control tools.

Coupled with improved visa facilitation and the liberalization of entry requirements, improved border control and passenger facilitation can support countries' attractiveness.

Airline priorities remain the safety and security of their operations for their staff and passengers. The airline industry seeks to closely collaborate with public authorities to support these priorities and to maintain commercially viable operations. States also have vested interests to protect their air connectivity to support national interests. The aviation industry, including its indirect support to the tourism industry, accounts for 65.5 million jobs globally with a USD 2.7 trillion GDP impact[3].

---

1 *IATA Forecast Predicts 8.2 billion Air Travelers in 2037*, Press Release No 62, IATA, October 2018: https://www.iata.org/en/pressroom/pr/2018-10-24-02/.

2 *ACI releases new research paper analyzing the influence of customer service quality on airports' non-aeronautical revenue,* Media Release, ACI, August 2016: https://aci.aero/news/2016/08/08/aci-releases-new-research-paper-analyzing-the-influence-of-customer-service-quality-on-airports-non-aeronautical-revenue/.

3 *Facts & Figures*, Air Transport Action Group, January 2020: https://www.atag.org/facts-figures.

Overall, authorities and airlines share common objectives that should lead to a better understanding of respective needs and constraints in support of increased cooperation. This is particularly true when it comes to international security and border protection. Aviation remains a target for terrorist groups[4] and airlines and airports have been heavily impacted by recent terrorist attacks.

The threat posed by foreign terrorist fighters[5] also implies that civil aviation may not only be a target, but may also be a vector of international terrorism. Air transport can also be used for criminal activities such a human, drugs, weapons and wildlife trafficking. The airline industry recognizes that it can play an important role in helping to tackle transnational criminal activities.

As terrorist and organized criminal organizations increasingly use sophisticated methods to evade law enforcement, governments seek and benefit from the collaboration of airlines and airports. The transfer of passenger information from airlines to authorities can effectively facilitate timely identification of persons of interest while helping to detect illegal activities. The United Nations Security Council (UNSC) has adopted a number of Resolutions, notably *2178* (2014), *2396* (2017) and *2482* (2019), addressing threats to international peace and security and mandating states to receive and analyze API, develop capabilities to receive and analyze PNR, make full use of relevant watchlists and share information about foreign terrorist fighters (FTF) using commercial air transport within their jurisdiction and across jurisdictions. The collection and transfer of passenger data has become a cornerstone of the fight against terrorism and international crime.

Transfer of passenger data from airlines to authorities can support international efforts to fight against terrorism and protect civil aviation.

A return to the spirit of the Chicago Convention, whereby collaboration between authorities, airlines and airports is embraced, is key to the continued security and sustainability of international aviation. Article 22 of the Chicago Convention (1944) calls for Contracting States "*to adopt all practicable measures, through the issuance of special regulations or otherwise, to facilitate and expedite navigation by aircraft between the territories of contracting States, and to prevent unnecessary delays to aircraft, crews, passengers and cargo, especially in the administration of the laws relating to immigration, quarantine, customs and clearance*."[6] Cooperation between governments and air transport stakeholders is also a key principle in the SARPs of Annex 9–*Facilitation*[7] of the Chicago Convention.

This collaboration is also essential to the deployment of new facilitation processes and technologies such as travel authorizations and automated border control (ABC) gates, as well as in the overall approach aimed at performing checks away from the physical border itself, at earlier stages of the passenger's journey (e.g., upstream verification of travel documents and authorizations, identification of inadmissible passengers).

The aviation industry and authorities have a common interest in implementing efficient processes to enhance border security, therefore close consultation and a collaborative approach is needed.

---

4 *Threats to international peace and security caused by terrorist acts: Aviation security*, UNSCR 2309, 2016: http://unscr.com/en/resolutions/2309.

5 *Threats to international peace and security caused by terrorist* acts, UNSCR 2178, 2014: http://unscr.com/en/resolutions/2178.

6 *Convention on International Civil Aviation*, Doc 7300, ICAO, 2006: https://www.icao.int/publications/pages/doc7300.aspx.

7 *Annex 9–Facilitation*, 15th Edition, Amendment 27, February 2020: https://store.icao.int/en/annex-9-facilitation.

While its long-term impact on air transport remain uncertain, the COVID-19 pandemic could serve as an opportunity to rethink border control processes and technologies. It may prove easier to deploy new concepts and hardware in an operational environment facing fewer capacity constraints, as 2019 passenger levels are not expected to be regained until around 2024.[8]

[8] *Outlook for Air Transport and the Airline Industry*, IATA Annual General Meeting, November 2020: https://www.iata.org/en/iata-repository/pressroom/presentations/outlook/.

1. Key Principles

Governments and the air transport industry can work together to maintain the integrity of national borders while removing persisting inefficiencies in passenger checks. As such, a set of key principles should guide authorities and other stakeholders in the development of border control solutions for air travel: harmonization, efficiency and cooperation.

1.1 Harmonization

A harmonized approach to the implementation of border control processes and requirements is essential given international civil aviation's inherent cross-border and multi-stakeholder nature. Building on the SARPs of Annex 9–ICAO has set out rules and guidance material aimed at providing a framework within which governments, airports and airlines can cooperate to strengthen border security while facilitating the flow of passengers.

Annex 9 is continuously evolving. The manual is based on the SARPs contained in Amendment 27, applicable since February 2020. The difference between a Standard and a Recommended Practice is as follow:

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 recognized as desirable in the interests of safety, regularity or efficiency of international air navigation. States should endeavor to conform.

Adherence to internationally agreed upon standards for travel documents, passenger data messages, and technical specifications and methods for the transmission of this data is critical to ensure uniform, efficient and predictable management of border control processes that expedite the clearance of passengers. The use of technologies such as electronic Machine Readable Travel Documents (eMRTDs) or ABCs are recognized as further facilitating and improving air transport.

Adherence to internationally agreed upon standards facilitates swift and efficient implementation of border requirements, enhances interoperability and leverages the automation of passenger-related processes.

The ICAO Traveller Identification Program (TRIP) Strategy defines objectives and specifications for a global approach to traveller identification management. Key elements of TRIP include standards for evidence of identity, standardization of Machine Readable Travel Documents (MRTDs), standards for document issuance and control, guidance regarding inspection systems and tools for verification of MRTDs, and the development of globally interoperable applications for the linkage of MRTDs and relevant datasets (e.g., API, PNR, the International Criminal Police Organization (INTERPOL) Stolen and Lost Travel Documents (SLTD) database and the ICAO Public Key Directorate (PKD). In addition to an Implementation Roadmap for Contracting States, ICAO published detailed standards, guidance materials and technical reports for each of the key TRIP Strategy elements, including Doc 9303 on MRTDs.

Harmonization produces spillover effects on the overall management of border control requirements, allowing for quick implementation of reliable and robust systems.[9] Authorities should be aware that non-standard requirements will have an adverse effect on airlines, leading to significant delays in their implementation. For example, IATA assesses that the implementation of a non-standard API requirement can take more than 18 months for airlines to implement. An API program that is fully aligned with the WCO/IATA/ICAO standards and guidelines can be implemented within six months[10]. The adoption of standard dataset formats facilitates the automated capture of travel information from, for example, the Machine-Readable Zone (MRZ) of a passport which can be swiped or scanned. Information not included in the MRZ and requiring manual capture will likely be of lower quality and more difficult to use and cross-reference by authorities.

Non-standard requirements lead to lengthy and costly implementation processes for both authorities and operators.

International standards have also been developed to guide the protection of information and the systems processing passenger data. Authorities are, for instance, required to set up secure IT systems and communication channels when working with passenger data. The harmonized use of industry protocols for the transfer of data contributes to the overall security of border control systems. Requirements defined in ICAO Doc 9944 Guidelines on PNR Data[11] mandate Contracting States to develop data protection laws or regulations concerning the transfer and processing of PNR data. These ICAO requirements help Contracting States find the appropriate balance between passenger privacy and the need to process and share passenger data. The application of common principles and measures for the protection of personal data should not only provide privacy guarantees to passengers but also to other countries about the collection, processing and storage of the data of their citizens.

1.2 Efficiency

The international harmonization framework provided notably by ICAO leads to efficiency gains. The collection of API data upon entry and exit, for example, can replace entry and exit paper declaration cards, which are burdensome for border agents and airlines to store and manage. Such advance data collection systems, combined with ABC kiosks, can also automate entry declarations.

[9] *Challenges of Non-Adherence to Passenger Data Standards*, FALP/11-WP/4, ICAO, January 2020: https://www.icao.int/Meetings/FALP/Documents/FALP11-2020/FALP11.WP4.NON%20STD%20DATA.pdf.

[10] *API-PNR Toolkit*, IATA: https://www.iata.org/en/publications/api-pnr-toolkit/.

[11] *Guidelines on PNR Data*, Doc 9944, ICAO, 1st Edition, 2010: https://store.icao.int/en/guidelines-on-passenger-name-record-pnr-data-doc-9944.

1.2.1 Single Window

Regarding passenger data, a cornerstone of the efficiency principle is the implementation of the Passenger Data Single Window, which provides a coherent and unified framework for its transfer. A single window is a facility that allows airlines to submit standardized passenger data (i.e., API/iAPI and/or PNR) through a single data entry point within a state.

Recognizing the importance of the single window facility, its establishment was elevated from a Recommended Practice to a Standard applicable as of February 2020. As per ICAO Annex 9 Standard 9.1, states must create a single window for each data category or both categories combined. It is recommended that this facility be implemented to collect both categories combined.

While a single window facility reduces the operational impacts on airlines, it also prevents the duplication of work for authorities by establishing a single connection with each carrier for the transmission of both types of data. The national body responsible for collecting all the data from carriers transfers the data to the relevant and authorized authorities, as defined in the national law. A good practice that has been implemented in different regions of the world is for this national body to be composed of representatives from the different authorities that require the data. These representatives process the data based on the specific needs and rights of their respective agencies, but the sharing of facilities and data facilitates the necessary cross-agency collaboration for more efficient and rapid intelligence sharing.

Passenger data are required by an increasing number of states and are used for numerous purposes by different national agencies. The single window approach limits the costs and resources deployed by states and reduces the costs and impacts on airlines.

The data collected in accordance with a common framework should be used to cover the different processes managed by different agencies, such as:

- Identity verification
- Travel authorization verification
- Entry-Exit recording
- SLTD and watchlists vetting
- Aviation security risk assessment
- Immigration controls
- Customs controls

All agencies requiring access to passenger data (e.g., Immigration, Customs, Police, Intelligence) must clearly define the purpose of the collection, the data elements needed, and the ideal timing of transfer. Once established, a state is in a better position to propose a single set of requirements for passenger data transmission. To avoid duplicative or unnecessary data requests, authorities also need to clearly map the data that is already accessible in their own national systems (e.g., visa information, residence card numbers). States should refrain from adding these data elements to their passenger data requirements, as this leads to additional–often manual–data capture by carriers.

1.3 Cooperation

The global nature of civil aviation makes cooperation and collaboration between all stakeholders essential. While ICAO Standards are by design a product of international cooperation through rulemaking, Contracting States must transpose them into national legislation for the rules to be fully effective.

1.3.1 National Level

Collaboration between government agencies and transport stakeholders should be pursued before adopting a new legislation or rolling out a new program. Early collaboration helps ensure the new measures take into consideration the operational needs and constraints of the industry and limits negative impacts on operations and businesses. An open dialogue will foster the buy-in of the industry and help authorities make the best of these measures. By flying to multiple destinations and by interacting with multiple national authorities worldwide, airlines have gained extensive knowledge on best practices for border management, which can benefit many.

Close consultation with air carriers facilitate swift adoption and recognition of requirements.

National Air Transport Facilitation Program and Committee–Effective collaboration tools are the National Air Transport Facilitation Programs (NATFP) and Committee. A model of NATFP is provided in Appendix 12 of ICAO Annex 9. Guidance for establishing such a program that is prepared and managed by a National Air Transport Facilitation Committee, is available in ICAO Doc 10042. The purpose of the NATFP is to provide a framework to guide the improvement and optimization of aircraft, crew, passenger and cargo flows through airports and to improve customer service, while maintaining appropriate security requirements.

In the context of the COVID-19 pandemic, effective coordination is proving crucial, not only to facilitate an effective restart and recovery of aviation, but also to ensure a safe, secure, efficient and sustainable air transport system. Annex 9 Standard 8.19 mandates establishment of appropriate committees to provide a forum for consultation and information-sharing about facilitation matters among government stakeholders, government representatives of other air transport-related communities and the private sector.[12]

ICAO recommends that the national Civil Aviation Authority or the Department of Transport remain the party primarily responsible for the implementation and coordination of this program. It should also include the participation of relevant agencies (i.e., Customs, Immigration, the issuing authority for travel documents and visas, Public Health, Food and Agriculture Authority, Foreign Affairs, Tourism) as well as aircraft and airport operators.

[12] *Model National Air Transport Facilitation Programme*, Doc 10042, ICAO, First Edition, 2015: https://www.icao.int/WACAF/Documents/Meetings/2018/FAL-IMPLEMENTATION/DOC_10042_FULL_EN-EDENPROD-554135-v1.pdf.

Penalties–In the spirit of collaboration, given the complexities of dealing with passenger data, and to further promote collaboration and cooperation with air transport operators, states should consider a measured approach to sanctions against carriers in case of failure to implement specific provisions.

Carriers play a key role in the implementation of national border security strategies and should be considered as a partner. Punitive measures on carriers cooperating are discouraged.

Better outcomes are to be expected from collaboration than from sanction. Even where the source of the problem is known and identified, states include in their legal instruments the possibility to apply sanctions against operators for non-compliance. IATA strongly encourages authorities to adopt a stepped approach with carriers having difficulties complying with national requirements. Close cooperation and working toward fully understanding the operational and/or technical challenges emanating from the requirements is in the interest of both carriers and authorities. Carriers will be able to ensure they are implementing adequate mitigating measures to improve compliance and authorities will be able to facilitate a swifter implementation of their legislation, adapting requirements where possible based on discussions with carriers if they fail to implement a specific provision.

In the case of data quality issues or partial compliance, authorities are encouraged to first endeavor to provide airlines with a detailed analysis of the issues encountered and where they have occurred. This will help carriers to better define the source of the problem and identify what measures need to be taken to improve data quality or compliance. Such improvements could be linked, for instance, to IT system configurations, to the training of ground staff collecting the data at a specific station, or to the technical capabilities of check-in kiosks/desks in automatically capturing MRZ information from passports.

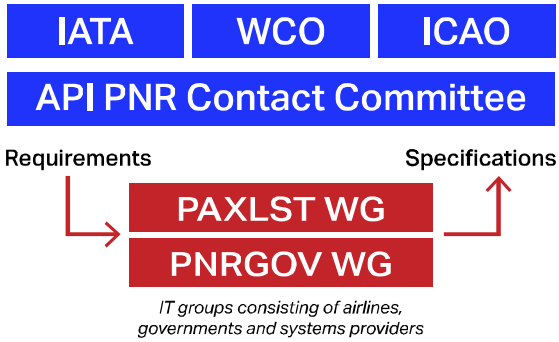
1.3.2 International Level

Cooperation is key for maintaining and developing new SARPs and technical specifications, notably within the ICAO Facilitation Panel and the Technical Advisory Group of the TRIP (TAG/TRIP). States, international organizations and industry associations participating in these forums are driving the modernization of border security tools and processes.

Regarding API and PNR, a committee was set up by the World Customs Organization (WCO), IATA and ICAO to maintain and develop international guidelines and reporting standards for passenger data. Any changes to the guidance and standards are also conducted within this forum. The extensive tools and materials developed by these three organizations are available to assist both authorities and operators in the implementation of passenger data systems.[13]

Modifications are controlled through the WCO/IATA/ICAO API-PNR Contact Committee (CC). The API-PNR CC reviews modification requests on an annual basis. Any changes to the standards have to be requested following the WCO Data Maintenance Request (DMR) procedure. Justified DMRs are reviewed by the API-PNR CC and as required, evaluated by the United Nations Centre for Trade Facilitation and Electronic Business (UN-CEFACT) for UN rules compliance. All approved changes will be included in the following PAXLST or PNRGOV version.

[13] *API Guidelines and PNR Reporting Standards*, ICAO: https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx.



Within the UN system, ICAO plays a leading role in border control and facilitation rulemaking. Nonetheless, several other UN agencies are key players in the implementation of effective border control systems. These include the UN Office of Counterterrorism (UNOCT), the UN Office on Drugs and Crime (UNODC), and the International Organization for Migration (IOM). The Organization for Security and Cooperation in Europe (OSCE), WCO and INTERPOL also play an active part in border control issues. All these organizations provide subject matter expertise and conduct extensive capacity building activities in support of national authorities on passenger data programs, among others.

In addition to this international framework, specific national or regional border requirements may be imposed. More stringent measures may also be put into place to address specific border and/or national security concerns. Initiatives of this sort that may stray from international standards and practices may not be in line with airlines' existing operational systems and processes. If carriers cannot comply with a specific legal requirement due to a conflicting law in another country, states should engage directly with the authorities of the country concerned instead of unduly sanctioning carriers. Diplomatic channels should be used to find a common agreement without harming air travel between the two countries or regions.

Moreover, whenever states impose specific inspection measures on passengers at their last point of departure to address targeted threats, coordination with the host country is essential to minimize the effect of such extra-territorial measures on the flow of passengers at airports, as well as to share valuable intelligence and threat assessments. Yet, as a principle, to reduce the burden on carriers, to ensure rapid compliance with border requirements, and to minimize the need for diplomatic intervention, authorities should avoid developing legislation that conflicts with international requirements or requires the industry to comply with competing, if not conflicting, legal bases.

1.3.3 Cooperation on Repatriation of Inadmissible Passengers

As per ICAO Annex 9, an inadmissible person is a person who is or will be refused admission to a state by its authorities. The airline terminology for a person who is refused admission to, or transit through the territory of a state is an “inadmissible passenger” or “INAD” or even “INADPAX”. Inadmissible passengers constitute a burden both to authorities, who have to dedicate extra resources to handle these passengers at the border, and to carriers that have to bear the cost of custody, care and removal of the individual to its initial point of embarkation, in addition to the penalties that may be applied by authorities. Based on the data collected by

IATA Timatic, the average fine imposed per inadmissible passenger is approximately 3500 USD. Fines can, however, reach up to 500 000 EUR[14].

INADs impose a significant operational and financial burden on both authorities and carriers.

The reasons for a passenger to be found inadmissible can broadly be classified under two categories:

1. Personal matters that a carrier could not be aware of (i.e., criminal record, record of previous overstay, doubts about the individual's intentions during their stay, lack of funds to sustain the stay).
2. Carrier has transported a passenger who is improperly documented. This includes:
    - Absent, invalid or expired visa.
    - Absence of onward or return ticket.
    - Travel document not valid (e.g., may appear expired, not belonging to the holder, false, altered, fraudulently obtained).
    - Travel document is inexistent, possibly destroyed during the trip.

Annex 9 Standard 5.9 clarifies that "*the aircraft operator shall be responsible for the cost of custody and care of an improperly documented person from the moment that person is found inadmissible and returned to the aircraft operator for removal from the State*". However, ICAO further draws a line between the responsibilities of airlines and authorities with regards to inadmissible passengers. As per Annex 9 Standard 5.9.1, the same responsibilities for the cost of custody and care of an improperly documented person until the removal fall within the remits of border authorities when the person is not admitted due to document problems beyond the expertise of the airline or for reasons other than improper documents.

To prevent upstream carriage of INADs, Annex 9 Standard 3.34 is addressed directly to airlines and highlights that necessary precautions should be taken by airlines at the point of embarkation to ensure persons are in possession of the documents prescribed by the states of transit and destination and meet all the conditions of entry. Airlines, therefore, verify, at varying touchpoints, that passengers are accurately documented, a process known as Document Check (see section 2.1.1). However, Annex 9 Standard 5.14 highlights that airlines should not be fined if a passenger is found improperly documented when the demonstration can be made that necessary precautions have been taken to ensure the passenger was compliant with the document requirements for entry.

When airlines cooperate to prevent the travel of INADs, authorities should mitigate (waive or reduce) any penalties if an INAD arrives on any of that airline's flights. A number of countries, including the US, Canada and the UK, have implemented such programs, which are intended to improve cooperation between the parties and enforce the adoption of appropriate best practices by carriers serving their territory.

The numerous burdens of INADs highlight the need for a real and effective collaboration between carriers and authorities. Airlines have a clear interest in ensuring that the traveler's documents are properly controlled before embarkation. Establishing the validity and authenticity of travel documents requires, however, a significant expertise that cannot be expected from air carrier agents. In line with Annex 9 Standard 3.32, it is,

[14] *Council Directive 2001/51/EC,* European Commission, June 2001: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0051&from=EN.

therefore, essential that states assist carriers in evaluating travel documents and ICAO Annex 9 Recommended Practice 3.33 promotes the deployment of immigration liaison officers (ILOs) at airports. The accurate identification of travelers enables border authorities to perform a more robust risk assessment. Automation and development of digital identity specifications can also offer a way for governments to validate and authenticate passenger identity ahead of travel. In the future, this should remove carrier obligation to perform document checks and the inherent liability.

Authorities should assist carriers in verifying the validity of travel documents prior to boarding.

The implementation of passenger data programs, combined with a strong national vetting and risk assessment capability, can also significantly contribute to the reduction in the number of inadmissible passengers and can reduce the need for the physical deployment of ILOs. Indeed, with a performant collection and processing of data in advance, authorities no longer rely solely on the capability of carriers to identify potential inadmissible passengers at departure. Risk assessment can be performed in advance based on pre-travel information collected from travelers and interactive data exchange can allow intervention before boarding. These capabilities allow governments to have direct control over who they allow to arrive at their border.

Passenger data programs can support efforts to reduce the number of INADs.

For airlines to avoid being penalized and prevent conflict with their customers, it is of utmost importance that states adopt clear and detailed rules providing a legal basis for airlines to refuse carriage to passengers who do not meet the conditions of entry into the country of transit or destination. The COVID-19 pandemic has dramatically highlighted the importance of this legal basis. Amid the crisis, new entry requirements were imposed and/or modify in an expedited way. The situation got unmanageable with the number of new and non-harmonized documents required and that airline staff did not have the competency to verify. Additionally, business processes did not have time to mature to take into consideration the new and ever-changing requirements. This led to an increased number of INADs, while corrective measures were close to impossible to implement by airlines.

The importance of close cooperation and collaboration between border authorities and air transport stakeholders cannot be overstated in all circumstances to minimize disruptions and avoid negative impacts on passengers and the air transport system generally.

2. Airline Systems and Operations Supporting Border Control Processes

This section covers touchpoints and processes within a passenger journey and their relevance to border security. Border control processes and passenger data requirements take place within the specific business and operational environments of air travel. These processes and requirements need to be designed in a way that allows their integration with the existing passenger journey. In providing details on the operational and commercial practices of airlines, this section intends to assist authorities in avoiding implementation of redundant requirements that are cumbersome for airlines, as well as understanding the time-sensitivity of each step in the journey.

2.1 Processes and Systems Supporting the Passenger Journey

Every step in the passenger journey is time sensitive and has a direct influence on the punctuality of flights and the ability of passengers to enjoy their journey. The variety of systems and stakeholders involved in each step can have a significant impact on how border security requirements may be implemented.

Authorities should consult with airports and airlines before imposing new measures that will impact booking, check-in or boarding processes.

2.1.1 Document Check

Before reviewing the various steps of the passenger journey, some key concepts around the process of Document Check are worth being clarified. There are often misperceptions surrounding the purposes of the passenger travel document verifications performed by air carriers at different steps in the journey, which often lead to misalignment with border security requirements.

Entry requirements–Passengers are responsible for holding the correct documentation to travel as stated per the conditions of carriage. Performing the checks to ensure each passenger is appropriately documented is a requirement of airlines. This requirement is enshrined in state legislation and in ICAO SARPs.

Under some circumstances, airlines failing to comply with the requirements could be subjected to fines imposed by the authority of the country where the passenger has been declared inadmissible (see section 1.3.3) and be responsible to repatriate the passenger at the airline's expense. Airlines perform document checks to verify that passengers meet the conditions to be admitted in the country(s) they are travelling to or transiting through.

These document checks, also referred to by the industry as DOC Check, generally consist of the following:

- Verifying that the passenger is the rightful owner of the travel documents. This positive ID check implies a face to passport comparison conducted manually or through automated means.
- Verifying the validity (e.g., expiration date) and authenticity of the passenger's travel documents.
- Verifying that the documents are accepted by the transit and/or destination country and are valid for the time period required by the transit and/or destination country.
- Verifying that each passenger meets all the necessary conditions for entry, such as:
    - Possession of relevant documents (e.g., passport, driver's license, residence card, refugee documents).
    - Travel authorization or visas.
    - Other documents (e.g., vaccination, parental authorization for minors, valid return ticket).

Given the complexity of travel rules, IATA has developed Timatic Solutions[15] to support the industry. For over 50 years, Timatic has been maintaining a travel regulation database to support air carrier and travel agent staff in verifying that passengers are properly documented based on each passenger's nationality, passport, visas, destination, transit points, etc. Many airlines have integrated Timatic Solutions in their reservation or Departure Control System (DCS) to help automate the verification.

These controls by airlines were until recently performed visually at the time of check-in. With the increasing proportion of passengers using online and mobile check-in options, these controls are occurring at various points of the journey, including at the boarding gate. Depending on the flight destination and risk profile, airlines will adapt their measures to ensure such checks are done appropriately; for instance, by disabling the possibility to use web check-in or by adding specially trained agents at the gate to focus on the DOC Check process.

The vast majority of documents verified by airlines are subject to international harmonization, through standards and specifications issued mainly by ICAO, World Health Organization (WHO) and IATA, which ease visual verification and automated processing. It is essential that any new health-related documents that will be required in response to COVID-19 be subject to this same harmonization.

Despite the current harmonization, the controls remain very resource-intensive and time-consuming and airlines are keen on developing automated solutions to alleviate this burden on their operations. Indeed, the uptake on digital and biometric solutions will help reduce the number of manual verifications and touchpoints as we know them today.

[15] *Timatic Solutions*, IATA: https://www.iata.org/en/publications/timatic/.

The development of the specifications for digital identities, such as the digital travel credential-DTC (see section 4.2.3) and the digital travel authorization undertaken by ICAO, contributes to making travel journeys increasingly seamless and touchless.

Immigration liaison officers–Despite the solutions described above and the due diligence airlines apply to ensure only legitimate passengers are transported, airline staff are not expected to possess the same level of expertise in detecting fraudulent documents or impostors as border officers or ILOs. Annex 9 Standard 3.32 mandates states to assist airlines with this task and Recommended Practice 3.33 highlights that states should consider making arrangements with other states to permit the positioning of ILOs at the point of departure to assist airlines in establishing the authenticity and validity of travel documents.

ID check–In several jurisdictions, aviation security regulations require airlines to conduct a reconciliation between the passenger ticket and passenger identity at the time of baggage drop off and at the gate. This requirement relates to the Standard 4.5.3 of ICAO Annex 17–*Aviation Security* for ensuring that each baggage loaded into the aircraft hold corresponds to a passenger on board. This is a deterrent measure aimed at preventing for instance potential criminals from checking in a bag filled with explosives without boarding the flight themselves. The systematic screening of bags loaded on board an aircraft with sophisticated equipment, however, may remove the need for this measure in the future.

It should be highlighted that the various purposes for ID checks will largely depend on local regulations as well as airline operational and commercial practices. In all these cases, however, the ID check is limited to a visual verification that the name of the passenger indicated on the travel document corresponds to the name displayed on the boarding pass in addition to a face to passport check. These ID checks are not used to verify the authenticity of the travel document.

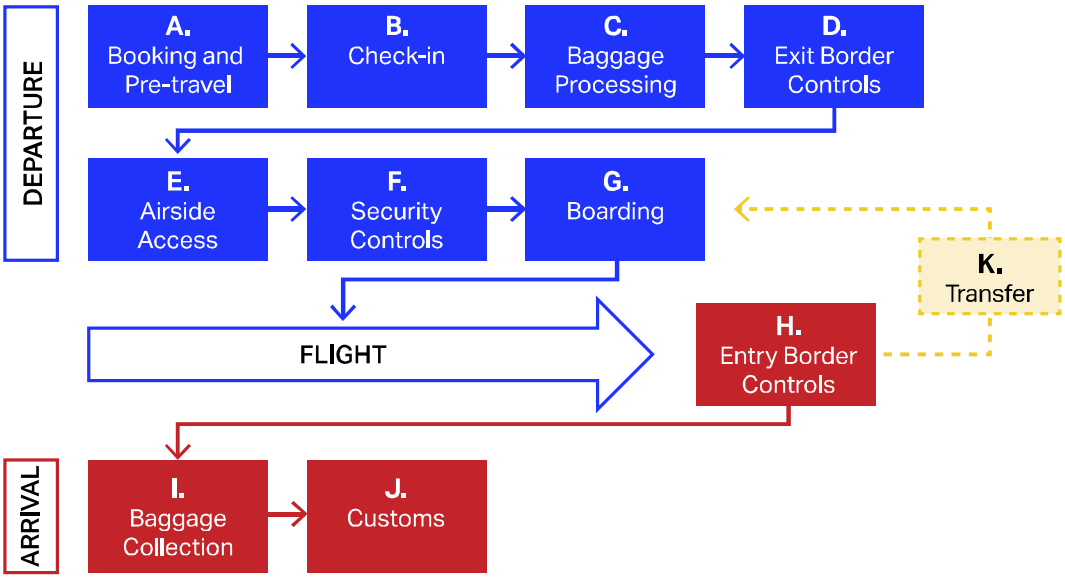
As the ID check requirement is present at different stages of the passenger journey and considering the extra resources necessary to perform these controls, airlines and border authority agencies are increasingly moving from manual processing toward automated solutions. Modern collaborative arrangements, such as those promoted by IATA One ID (see section 4.4.2), will allow the validation of the identity of passengers and their authorizations at one touchpoint of the journey, alleviating the need for redundant verifications.

2.1.2 Understanding the Key Processes in the Passenger Journey

Each touchpoint in the passenger journey supports both commercial and operational activities as well as regulatory requirements. This section aims to clarify the purposes of each step as well as their interdependencies in the overall journey.

Depending on the airport and national requirements, the touchpoint sequence may vary; for instance, in some locations, the Airside Access and Security Controls are combined, and some legislations may not require Exit Border Controls. Today's flow of touchpoints can be represented as follows:

Representation of Today's Flow of Touchpoints



Recognizing that some of the processes and requirements in today's travel continuum may be inefficient and duplicative, aviation stakeholders are working on modernizing the touchpoint flow toward a seamless journey to benefit border security and the facilitation of travel across borders as well as to improve the passenger experience. The current processes are discussed in this section and their modernization, including the combination of touchpoints, are discussed in the section 5.

A. Booking and Pre-Travel

Booking–Depending on each airline's commercial arrangements, booking can be done either directly on the airline's website or through Customer Service (in which case, the information captured is stored directly in the airline's reservation system), via an accredited travel agent, or via another partner airline (in the case of interlining arrangements). When booking is done via a travel agent or another partner airline, the operating airline might only receive the data strictly necessary to deliver the relevant transportation service; for instance, it might exclude passenger contact information, full fare details, other travel segments, etc. This information is typically not shared with airlines for commercial reasons. The latter means account for about 50% of bookings, which influences the amount of information contained in the PNR.

Depending on the booking channel, the PNR can include very few elements or complete information. Therefore, airlines cannot operationally provide a specific dataset.

During booking, a customer intending to travel will provide necessary information for the execution of a contract related to an air transportation service, and possibly in combination with other services (e.g., car

rental, train ticket, hotel reservation). To fulfill the contract, a passenger typically needs to provide the following information:

- An indicative name to serve as a reference in the booking.
- An itinerary: point of departure, point of destination, intended date to travel, single or return journey.
- Other services required, if relevant: additional baggage (will vary depending on the baggage allowance policy of the airline and fare chosen), travel class (economy, business, etc.), special requests for meals, special assistance needed.
- Fare information: price of the service. If different fares apply, additional information may also be collected; for instance, for child fares, the age of the child would be captured in the booking (but not necessarily the date of birth). For military fares or complementary travel, other information might be captured as part of the booking.
- Contact information: this could be limited to an email, with no obligation to collect address or phone information. This will depend on the airline's commercial practices or the booking channel.

At the time of booking, seat and baggage information is not necessarily available, but when it is some airlines offer the possibility to travelers to preselect their seat. Seating and baggage information will otherwise become available at the time of check-in.

Pre-travel authorization and travel documentation requirements–At the time of booking, depending on the booking channel, passengers could also be informed about specific conditions to be admitted to the country(ies) they are travelling to or transiting through. The ways passengers are informed vary greatly depending on the airline's distribution channels. However, the conditions of carriage accepted by passengers at the time of booking stipulate that it is the direct responsibility of the passenger to ensure they have in their possession all relevant travel documents for their travel.

Passengers can get information on the required travel documents from the country of destination's embassy or official websites. The travel agents or tour operators could also inform their passengers at the time of booking. IATA also makes freely available to the general public its Travel Centre where individuals can determine whether they possess sufficient travel documents and satisfy the health requirements based on their identification document and itinerary[16].

B. Check-in

For the last 20 years, to accommodate traffic growth and given airports' infrastructure constraints, airlines have focused their efforts on automating the check-in process through web or mobile check-in. Bringing this process off-airport reduces waiting time for passengers, avoids the installation of additional check-in desks and helps manage airport congestion. The check-in is a very time-sensitive process and its automation is a key element of the airlines' strategy.

When authorities are planning new processes or new entry requirements, prior consultations should take place with airports and airlines to understand the impacts on passenger processing at check-in.

[16] *Travel Centre*, IATA: https://www.iatatravelcentre.com/.

Indeed, manually processing passengers at airport desks is lengthy, particularly when travel documents other than identity documents are required. For example, some states require airlines to check the validity of a travel authorization at check-in by accessing a government website. If the requirement applies to 50% of the passengers on a wide-body aircraft flight (200 to 850 passengers), a verification process taking an additional 30 seconds or more per passenger would lead to an increase of 1.5 hour of work to check-in passengers. As a further complication, check-in facilities are often not connected to the Internet.

Any manual check required by authorities has a tremendous impact on the time-sensitive check-in process, defeating the modernization the industry is working toward.

The check-in process is used to confirm each passenger's intention to travel with the airline, ensure they are properly documented (see section 2.1.1) and process hold baggage, allowing information on final load and baggage weights to be refined. This is one of the reasons why check-in happens shortly before the flight, between 24 hours to 40 minutes prior to flight departure.

The check-in process used to be entirely performed at the airline's desk at the airport, but technology allows this process to be increasingly done off-airport. The number of platforms available to passengers to complete their check-in has diversified:

- Prior to arrival at the airport: through the airline website, a dedicated airline mobile app or automated check-in for frequent flyers on certain routes.
- At the airport: at a self-service kiosk (CUSS) or by an agent at the company's desk (CUTE, CUPPS).

At the time of check-in, passengers are prompted to provide their travel document details. When done online, the airline may allow passengers to take a picture of the front page of their passport to automatically extract the information and prepopulate the check-in page. This is usually supported by optical character recognition (OCR) technology. This method enhances the quality of the data captured. At this time, passengers can still change their seating arrangement and/or baggage services. In the case of disruption or change of passenger preferences, the passenger names and itinerary can also be changed.

For international flights, check-in typically includes the phase where airlines collect passenger information contained in the MRZ of their travel document for API transmission purposes (see section 3.1). The diversification of check-in platforms means that each passenger is not processed in a homogeneous way, including for the purposes of API data collection and verification. Moreover, when passengers have not purchased their ticket directly from the airlines, check-in often represents the first interaction between the passenger and the carrier operating the flight.

The main outcome of the check-in process is the issuance of the boarding pass, which will be the token used by the passenger to allow entry into the airside section of the airport and board the aircraft. The image below displays the standard information captured on a boarding pass for visual verification. The same information is nowadays captured in a QR code for increased verification automation. A boarding pass does not, however, contain personal information and notably excludes travel document information. Therefore, it is impossible for ground staff to verify the accuracy of the API data collected based on the cross-examination of the boarding pass and of the passenger's travel document. The accuracy of API data can only be verified through the capture of the MRZ.

Example of a Boarding Pass

C. Baggage Processing

Commonly, the check-in process would be coupled with the registration and acceptance of passenger hold baggage at the check-in desks. With the increased use of web/mobile check-in and self-service kiosks at the airport, the issuance of the boarding pass and the check-in of hold baggage have been dissociated at some airports. Where self-service bag drop kiosks have be set up, passengers first get a boarding pass (e.g., from a self-service kiosk), then drop their hold baggage at a self-service bag drop.

If there is an API transmission requirement in place, the initial API data captured during online check-in might be revalidated and recaptured at the time of baggage drop, either by the airline agent scanning the MRZ of the travel document or an automatic capture of the information by the self-service kiosk.

D. Exit Border Controls

Some countries performed exit border controls. The main purpose of these controls is to reconcile the arrival and departure records which in turn allows a travel history to be established and available for analysis[17]. These exit controls also enable the application of national and international watchlists and to identify overstayers. These controls are not aimed at verifying whether the passenger fulfils entry conditions for the transit or destination country.

To enhance the effectiveness of exit border checkpoints or to fill the gap left by the absence of such checkpoints, an increasing number of states require passenger data at departure. The collection of API data on departure is also a requirement on states included in the United Nations Security Council Resolution (UNSCR) 2178 (2014).

[17] *ICAO TRIP Guide on Border Control Management*, Version 1, F. Entry and Exit Databases, ICAO, 2018: https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Guide%20BCM%20Part%201-Guidance.pdf.

E. Airside Access

In accordance with ICAO Annex 17, access to airside should be restricted to persons with a valid authorisation. For passengers, airside access is granted based on the verification of the validity of the boarding pass, either with a visual check by the relevant airport agent, or by reading of the boarding pass barcode. Some countries might also require coupling this check with a verification of the passenger ID. However, agents in charge of this control do not have access to airline departure systems and therefore cannot verify the accuracy of the information in the airline systems against passenger IDs.

F. Security Controls

Passenger security controls at airports are typically carried out under the supervision of the aviation security authorities, either directly by a government agency or by a subcontractor of the airport or government. Similar to the airside access touchpoint, security controls are aviation security controls and not directly contributing to border security. Matching of passenger IDs and boarding passes might be performed at security controls also, especially in cases where the authorities mandate different screening requirements based on a per-passenger risk assessment.

G. Boarding

Gate occupancy time is a major factor in airline operational efficiency. Each airline is seeking to minimize the time aircraft spend on the ground and maximize flight time. The duration of the boarding process is, therefore, an important key performance indicator (KPI) that airlines seek to minimize. As such, airlines are investing in biometric self-boarding gates and are exploring solutions based on the IATA One ID concept where passengers arrive at the airport ready-to-fly (see Section 4.4.2) and their biometrics is use at each touchpoints.

In the meantime, with the increased use of web and mobile check-in, the boarding gate is often the first place where an airline will see the passenger in person. In this context, the legal obligations imposed on the airlines to perform the DOC Check and reconcile the boarding pass with the identity of the passenger can only be performed at the boarding gate.

H. Entry Border Controls

As per Annex 9 Standard 3.44: "*The aircraft operator shall be responsible for the custody and care of disembarking passengers and crew members from the time they leave the aircraft until they are accepted for examination* [by public authorities]". In conjunction with the gate occupancy KPI mentioned above, it is in the interest of airlines to ensure there is a swift disembarking process and that passengers pass efficiently through immigration controls.

Annex 9 Recommended Practice 3.40 emphasizes the goal of reducing the amount of time passengers spend passing through immigration controls: "*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*."

In addition to gate occupancy and passenger experience, there are two other main issues at stake for airlines in the way immigration controls are performed: securing a minimum connecting time (MCT) to transfer passengers and managing inadmissible passengers (see section 1.3.3).

I. Baggage Collection

The established indicative industry target for moving passengers from the aircraft door to the taxi stand is 30 minutes. The efficiency of baggage collection and customs controls is key in meeting this objective.

J. Customs

Customs authorities have been among the first law enforcement authorities to use passenger data to feed their risk assessment, in particular, PNR as it reveals an itinerary and the number of traveling companions under the same reservation. This data allows officials to target controls at passengers of interest instead of implementing systematic controls on every passenger upon arrival. Efficient use and distribution of PNR data is achieved through implementation of the Single Window facility (see section 1.2.1). The implementation of biometric recognition at customs may be very useful to identify persons whose biometric data have been collected in the context of law enforcement exercises.

Customs' role is critical to prevent aviation from being used as a mode of transport to carry dangerous and illegal goods between two countries. Their analysis is used to identify and dismantle networks of traffickers involved in human, drugs, weapons or animal trafficking/smuggling. National customs authorities are supported by the WCO to implement best practices in the matter.

To facilitate the process, a number of authorities are relying on passengers to self-declare the goods they carry with them and that might be in excess of the authorized limits. This was commonly done through paper-based declarations that are progressively evolving toward electronic declarations. Other countries have opted for green and red lanes to segregate passengers who have goods to declare.

K. Transfer

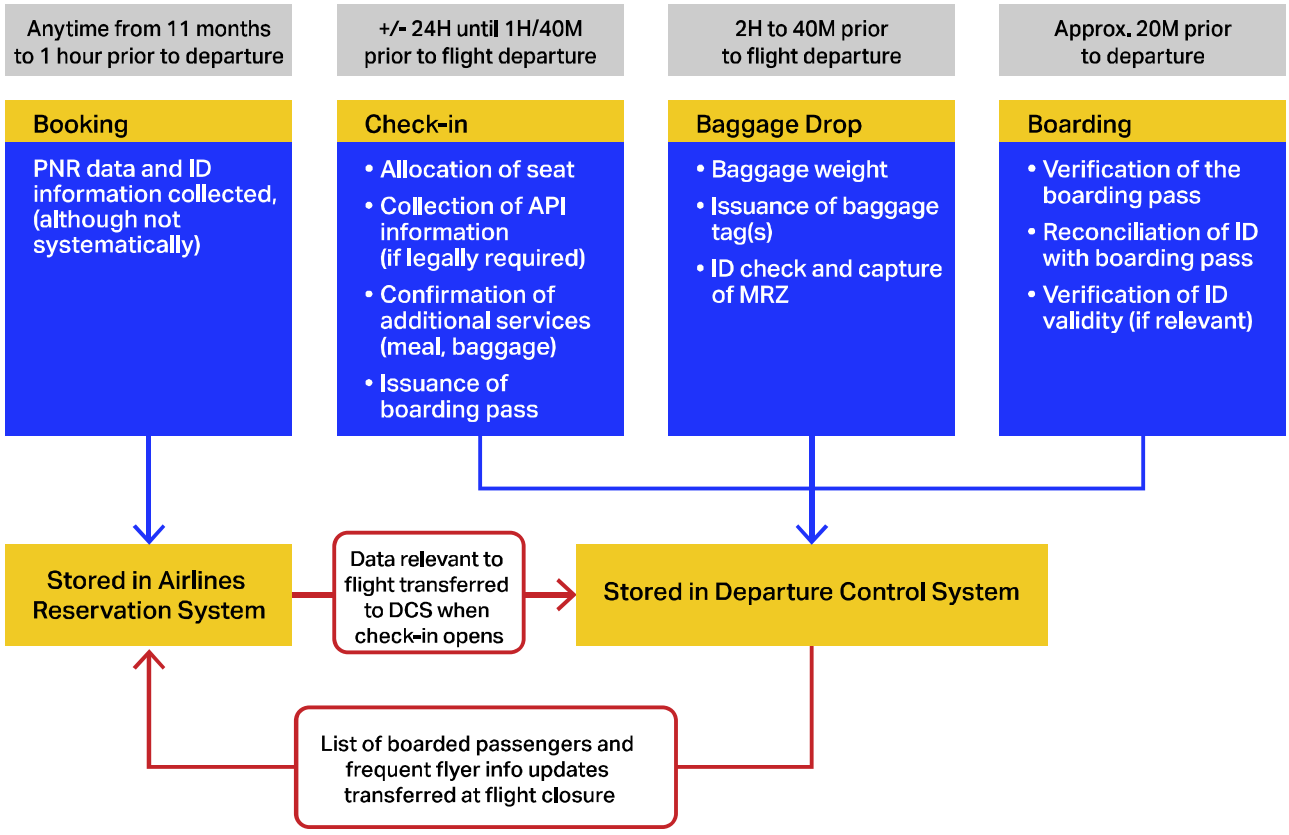
Connectivity is a key element of airline competitiveness and attractiveness. Connectivity is measured by an airline's ability to offer customers a wider range of routes in the shortest time possible. Therefore, the efficiency of the airline's duty station and its ability to guarantee a MCT between two flights is essential to the sustainability of any hub carrier.

Today, airlines strive to guarantee a MCT of about one hour between two flights, but in some cases the MCT can be as short as 40 minutes. Within these time windows, passengers will have to potentially clear immigration and security controls and make their way to their boarding gate. MCT is part of the service level agreement (SLA) signed between airlines and airport operators and meeting these targets requires close coordination between all the actors involved.

2.1.3 Data Flow and Systems Supporting the Different Steps in the Passenger Journey

Based on the processes and legal contexts described in the previous sections, the following diagram provides a high-level description of the data flow and supporting systems used in the course of the passenger journey.

High-Level Data Flow and Supporting Systems



Central Reservation Systems–Booking information is typically captured in airline central reservation systems (CRS) where the passenger record is created. Airlines generally have one reservation system at the global level. Many airlines have subcontracted this function to a global distribution system (GDS). The PNR data message is created from the CRS with the information it contains, which may vary depending on how the ticket has been booked and the commercial model or offer of the airline (see section 2.2).

When flights open for check-in, typically between 24 to 48 hours prior to departure, the information necessary for the operation of the flight and delivery of the requested services will be transferred to the DCS of the airline.

Specific data elements will not be collected in the airline's system before check-in starts. The timing set by authorities for their data transfer requirements should consider that passenger data becomes richer after the check-in process.

Departure Control Systems–Data collected in the DCS constitute a subset of the data collected in the CRS. Agents having access to the DCS at airports (e.g., the check-in and gate agents) do not have access to the full information included in the PNR registered in the CRS and they are not trained to operate such systems. It is, therefore, impossible for a gate agent to modify or update passenger information in the PNR (e.g., insert a name or correct a spelling mistake in the name).

DCSs support all airline operations at the airport and can be used for the check-in process (e.g., issuance of boarding pass, capture of API data, baggage acceptance), for boarding, and for aircraft load control (weight and balance). The API data message (PAXLST) will generally be created and transferred from the DCS prior to the aircraft departure, once the flight is closed (implying that no passenger can enter or leave the aircraft). The DCS will generate a final close-out message providing the list of boarded passengers or the list of passengers who did not board. This message is sent to the CRS mainly for accounting purposes and mileage accrual management.

Airlines can use different DCSs depending on the airport they operate from. An airline can, for example, use more than 20 different DCSs, each of which must be individually programmed and adapted to transfer API data to authorities. Considering that an airline can fly out from multiple countries, a state's non-standard request would significantly influence the airline's ability to comply.

The airlines' IT environment often relies on legacy systems that have been adapted over the years. It is often a very lengthy and costly process to modify them. These systems were developed in the 1970s as unique systems used only by the airline industry. They do not rely on web connections or applications and use proprietary standards[18] to format the data. The information exchange originally relied on the use of teletype standards, which evolved to use the United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT) data formats[19], maintained by the United Nations Economic Commission for Europe (UNECE). The use of XML format is seen as the next evolution, but industry adoption in the area of passenger services systems remains rather low (in contrast to the cargo area).

Airport operators can also connect to the DCS for the purpose of validating the boarding pass presented by passengers upon entry into the airside. This process only confirms that the boarding pass is valid, but does not give access to the information contained in the system.

[18] Specifications for hardware or software that are not available through open sources and generally controlled by one company.

[19] *Introducing UN/EDIFACT,* UNECE : https://www.unece.org/cefact/edifact/welcome.html.

2.2 Factors Influencing the Ability of Airlines to Share Passenger Data

The operational processes and IT infrastructure described above can significantly influence the way and type of passenger data that airlines will be able to share with border authorities.

The following factors contribute to the ease or limitations faced by airlines in complying with passenger data requirements:

- Airline operating model: network carrier, charter, low-cost, cargo, general aviation.
- Distribution channels used by the airline: tickets booked directly on the airline's website or through a travel agent.
- Airline IT infrastructure: integration or segregation of the CRS and DCS, crew management system, integration of load management systems into the DCS, etc.

2.2.1 Airline Operating Models

Understanding the profile of airlines operating at national airports is an essential step in setting up a successful passenger data exchange program. This will allow authorities to define risk profiles and priorities in processing the data, but also to understand which type of data will be sent by carriers. The following models are generally used to describe airline operating models:

Full-Service Network Carriers (FSNCs)–FSNCs are generally former or current national airlines that connect their home country to the rest of the world. They fly internationally and offer a large range of destinations, either directly or via a connecting flight. They generally have interlining agreements[20] with other carriers and are part of airline alliances. These airlines typically offer a full range of services to their customers with different travel classes, meal choices, routing options and frequent flyer programs.

For these airlines, the efficiency of their hub airport and the ability to offer a large range of connecting flights within a MCT is a key component of their commercial strategy. These airlines have a direct interest in ensuring that border controls, especially at transfers between domestic and international flights, are as efficient as possible and offer the best passenger experience possible.

Note: *The PNR data elements listed in ICAO Doc 9944 were defined based on the usual data collected by FSNCs upon booking and during their operations.*

Low Cost Carriers (LCC)–LCCs have developed significantly since the 1990s and have become, in certain regions, the major carriers in terms of number of passengers carried. LCCs offer point-to-point flights with no connections and with a limited number of services. As a result, the amount of data collected will often be limited. In the past, many LCCs relied on proprietary systems and IT infrastructures that made it difficult for them to provide PNR data. However, for the transmission of passenger data to governments, they are increasingly using standards and protocols similar to those employed by FSNCs.

[20] Interline is a relationship between airlines that allows one airline to sell services to a customer that are provided by another airline. Airlines use interlining to sell itineraries that they would otherwise not be able to service.

Charter Airlines–Charter airlines mainly operate regular or *ad hoc* flights to holiday destinations. They do not have direct sales channels, as the booking is managed entirely by a third party (i.e., tour operators). Therefore, they generally do not have a traditional reservation system from which PNR on individual passengers can be extracted. The airline will receive minimal information from the travel agency or tour operator to allow for the issuance of tickets and boarding passes and for the delivery of the requested service. These carriers also rely heavily on contracted staff and systems at airports where they operate. The training of the subcontracted staff on any specific requirements regarding ID checks might be a challenge for these operators. A progressive implementation, destination by destination, as well as a close dialogue between the authorities and the operators is recommended for this type of carrier.

Regional Airlines–Regional airlines operate mainly short- to medium-haul flights, connecting smaller regional airports to international hubs. Their operating procedures and systems are similar to those used by FSNCs, and they depend primarily on their ability to offer a swift connection to international flights at main airports to remain competitive. Like FSNCs, the efficiency of border controls and their impact on transfers between domestic and international flights is an important element of their competitiveness.

Cargo Airlines–Cargo airlines do not carry paying passengers and do not have booking systems. Therefore, cargo airlines should naturally be excluded from the scope of PNR requirements. However, these airlines may carry passengers who are not crew. These passengers can be airline staff, off-duty crew, mechanics, or persons required to accompany specific shipments (e.g., during the transportation of live animals like racing horses).

General Aviation–General aviation can be defined as flights that are not operated by commercial airlines. Aircraft can have a single owner or be used by companies for the carriage of passengers or goods as an aid to the conduct of their business (described in this case as business aviation). These operators do not have booking systems for individual passengers and will generally not have IT capabilities allowing the transfer of API data in UN/EDIFACT formats. For these operators, specific transfer protocols are necessary, such as uploading information directly on a secured web portal.

2.2.2 Distribution Channels

The amount of data available in the airline system will depend largely on which channel was used to book the ticket. When the ticket was purchased directly from the airline (either via the website or airline agents), the PNR contains information (including contact details) provided directly by the passenger or their representative.

When the ticket is booked via a travel agent (in person or online), airlines generally receive a subset of the information provided by the passenger. Typically, for commercial reasons, the travel agent will not transfer the entire contact details of the passenger to the airlines. Price, payment forms, as well as information on other travel segments might not be provided to the airlines.

Similar to the challenge presented by charter airlines for the collection of PNR data, a number of seats in flights operated by FNSCs might be blocked by travel operators. For these bookings, airlines have limited information on the associated passengers. If the booking was completed as a group, the information may not even be attached to a name, instead being listed under a group title (e.g., “national football team”). The

names and identities of group passengers will, in these cases, not be known until the time they arrive at the airport.

Beyond the specificities of each airline operating model, the amount of data collected on each passenger might differ significantly depending on how the seats have been booked.

The variety of airline operations is wide. Given the complexity of airline systems, authorities are encouraged to adopt a stepped approach in their implementation, starting with the airlines that already have experience in implementing border security requirements and progressively expand the scope of implementation to other categories of carriers. Not all airlines will be able to transfer both API and PNR data, since some airlines do not have paying passengers using a reservation system. International Standards developed by ICAO set a common framework for the development of border security programs. However, for a successful implementation of these programs, states need to ensure the requirements cover the different models of operation and capabilities of all the airlines impacted.

2.2.3 Airline IT Infrastructure

Another factor influencing the capability of airlines to collect or transfer data is the IT infrastructure of the airline.

Integration or Segregation of CRS and DSC–The integration of the CRS and DCS implies that the information collected at the time of check-in (e.g., seat information) can be updated in the CRS and included in the PNRGOV message that is generated from the reservation system.

As a consequence of CRS and DCS integration, some airlines might have load management systems that are not integrated into their DCSs. These airlines might have difficulties transferring information on baggage as part of the PNR to the API, as this information will not be captured in their reservation systems.

On the contrary, airlines operating segregated CRS and DCS might have difficulties transferring seat and baggage information from their CRS, as this information will only be captured in the DCS. In a segregated environment, the CRS would transfer to the DCS the information necessary for the operation of the flight once check-in opens (generally 48 to 24 hours prior to flight departure). From this point on, the information collected in the DCS will not be transferred back to the CRS. The only exchange of data between the DCS and the CRS will happen at flight closure to update the CRS on which passengers boarded the flight as well as frequent flyer information.

Authorities need to enquire about the IT configurations used by airlines flying to/from their country to understand which types of data can be sent as part of the PNR or API message.

At global level, half of airlines operate with integrated CRS and DCS whereas the other half have segregated CRS and DCS. This variation happens both between and within regions. In the US, most of the airlines operate integrated systems whereas in Europe, most airlines operate segregated systems.

Crew Management Systems–Airlines have different types of crew management systems. Depending on the configuration, the system will allow airlines to either transfer API data for crew as part of the general PAXLST message or via a different message. Since crew management systems are not linked to a check-in trigger, it is generally difficult for airlines to implement interactive API for crew. Therefore, batch API will be the preferred option for the transfer of crew data.

Note: *As operating crew do not book their seat on board, they are not recorded in the booking system and authorities cannot, therefore, require PNR data for operating crew.*

Storage of payment information–Depending on local legal requirements and the controls put in place in line with Payment Card Industry Data Security Standards, airlines might store payment information details on different systems from the CRS and exclude this information from the PNR. This implies that, for many airlines, it might be difficult for authorities to receive complete information on payment form as part of the PNRGOV message.

3. Implementing Efficient Passenger Data Programs

Historically, authorities have been performing both the identification and risk assessment of travelers only once they reach the border itself. This practice has become increasingly obsolete as governments can now refine their risk assessment for each traveler notably by using passenger data transmitted by carriers prior to arrival and other information collected in advance[21].

This section describes the three passenger data programs that have become a key pillar of ICAO Annex 9: API, PNR and iAPI. These programs require airlines to adapt both their IT systems and their operations in order to collect and transfer these data. Communication and engagement with airlines as early as the scope definition phase will smooth the implementation process for both airlines and authorities (see section 1.3).

Considering the significant impact these passenger data programs have on airlines, IATA, together with its member airlines, is closely involved in the development of standards and best practices, allowing for a smoother implementation of these requirements. IATA's goal is to build greater awareness in the international community on what these data are, where they can be found, how and when they can be transferred to authorities, as well as how these data, in combination with innovative technologies, can be better leveraged for efficient border controls and passenger processing.

Considering the complexity and costs of setting up these systems, governments are encouraged to adopt a progressive approach that allows for establishing a solid framework for the collection and processing of data, ensuring the efficient use of each dataset and a smoother integration with airlines' systems.

Airlines invest significant resources in heavy IT infrastructures to collect and format passenger data for its transmission to national authorities. Despite these investments, some states impose additional charges and costs on carriers to finance their own border control activities.

Passenger data programs are an integral component of national border control functions, which are a state responsibility. Receiving, processing and analyzing API/PNR data is a state's duty and should be funded by the national budget, similarly to other border control functions, and not by airlines and/or passengers through user fees, charges and taxes.[22] ICAO's policies state that: "*Civil aviation should not be charged for any costs that would be incurred for more general security functions performed by States, such as general policing, intelligence gathering and national security*".[23]

---

[21] *ICAO TRIP Guide on Border Control Management*, Version 1, 2.3 Identification of Travellers and Risk Assessment, ICAO, 2018: https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Guide%20BCM%20Part%201-Guidance.pdf.

[22] *Tackling Passenger Data Charges*, IATA: https://www.iata.org/contentassets/4eae6e82b7b948b58370eb6413bd8d88/passenger-data-charges.pdf.

[23] *ICAO's Policies on Charges for Airports and Air Navigation Services,* Doc 9082, 9th Edition, Section II paragraph 7 iv) and Section III paragraph 3. v), ICAO, 2012: https://www.icao.int/publications/pages/publication.aspx?docnum=9082.

3.1 Advance Passenger Information

API programs, introduced in the 1990s, were the first type of passenger data exchange program to be implemented. At the time, the routine examination of all passengers upon arrival at the border was no longer a sustainable way for border officers to work. Increased passenger volumes combined with the rise in international terrorism and serious crime led to the need for border officers to execute passenger checks and risk assessment more efficiently.

3.1.1 Value and Purpose

The transfer of passenger passport information prior to arriving at the border gives authorities more time to process and analyze passenger data. This enables the conduct a first assessment before passengers present themselves to a border officer, allowing individuals identified as low risk to be quickly processed while those raising concerns undergo more focused scrutiny.

Given the border control efficiency improvements made possible by API, the programs have, from the outset, been considered as facilitation tools. API programs are also proving to be an attractive passenger vetting tool, especially considering evolving data privacy requirements. API data is considered less sensitive because border officers would otherwise have access to this information when inspecting passengers' travel documents at the. This is a key difference with PNR data, which would not necessarily be requested or obtained from the passenger by border guards at immigration controls.

Originally, API was meant to send in advance the information that the border officers would have access to when travelers present themselves at the border.

API is typically composed of two types of data: information on the passenger's identity found in travel documents and information on the flight.

These are important elements used by border authorities to establish the risk profile of the flight, and to assess the number and types of passengers who will present themselves at the border (e.g., national citizens, passengers requiring a visa, visa-exempt passengers). This allows authorities to more precisely plan the staffing of their control booths and adapt the deployment of agents; for instance, between national citizen channels and foreigner channels.

API programs have been used for different purposes by authorities:

- **Facilitating immigration:** advance transfer of travel document information allows risk analysis and watchlist vetting to be performed before passengers present themselves at the border.
- **Simplifying entry and exit processes:** collecting API data for inbound and outbound flights allows authorities to eliminate entry/exit cards. This not only simplifies entry/exit procedures for passengers, but also relieves border authorities of the storage and management burdens associated with paper forms.
- **Exit border controls:** for countries that do not have such controls, the introduction of API programs, which provide a list of all passengers on outbound flights, allows authorities to reconcile entry and exit databases, perform watchlist checks and identify overstayers.

- **Security and customs controls:** transfer in advance of traveler identity information allows different agencies, through the Single Window facility (see section 1.2.1), to have access to the data prior to passengers arriving at the border. Sharing this information enables all concerned agencies to perform their risk assessment against their own databases and submit the passengers to relevant controls upon arrival. This could include the full range of law enforcement agencies, not just immigration. Contrary to traveler information collected through travel authorizations, API data is collected for ALL passengers on a given flight. This allows authorities to have an overview of all border crossing activities, not just with respect to foreigners but also their own citizens.

The wide variety of potential uses of API programs illustrates the importance of clearly defining the purpose of the program and which authorities will need to have access to the data. It is equally important that the outcome of the advance processing is passed back down to frontline border officers so they are better equipped to perform their tasks.

Start with a strong API program as the foundation of passenger data requirements:

- The data elements that can be transferred as part of the PAXLST message are sufficiently detailed to support different border security, immigration and law enforcement purposes. Authorities are strongly encouraged to start implementing a solid API program before moving to other types of passenger data programs.
- Airlines do not collect API for their operational and commercial purposes. Authorities should provide a clear legal basis to allow airlines to collect this data from their passengers.

3.1.2 International Standards

Since February 2018, ICAO mandates its Contracting States to establish an API system, as per Annex 9 Standard 9.5. States that do not complying with this measure need to officially file a difference with ICAO. The implementation of the API standard is verified through the ICAO Universal Security Audit Program (USAP).[24]

Definition–"*An electronic communications system whereby required data elements are collected and transmitted to border control agencies prior to flight departure or arrival and made available on the primary line at the airport of entry*." (ICAO Annex 9)

As per this definition, API information must be transferred electronically (eliminating the need for a paper manifest). This definition also stresses the fact that, unlike for PNR data elements, the authorities are requiring the transfer of specific data elements. Therefore, a legal basis is necessary to define which data elements should be collected and transmitted by carriers. It is important to stress that in the absence of such legal mandate, airlines will not systematically collect and retain travel document information from their passengers, since they do not need this information in the normal course of their business (unlike PNR data). States, therefore, need to establish a clear legal framework before implementing API systems, as highlighted by Annex 9 Standard 9.6.

[24] *The Universal Security Audit Programme Continuous Monitoring Approach (USAP-CMA) and its Objective*, ICAO: https://www.icao.int/security/usap/pages/default.aspx.

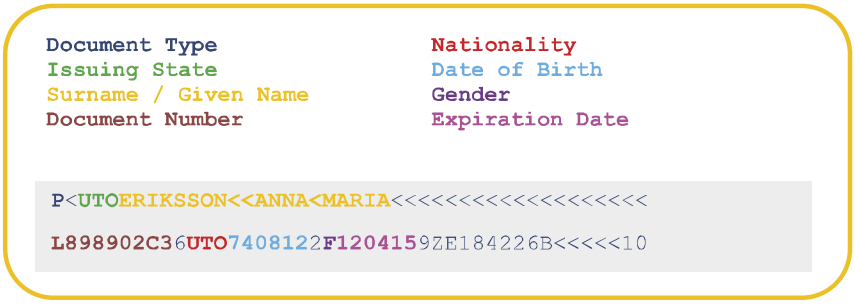
Data Elements–API is made up of two different datasets:

- Information related to the identity of the passenger: eight data elements
- Information related to the flight: nine data elements

Flight Information	Passenger Information
1. Flight Identification	1. Surname/Given Names
2. Scheduled Departure Date	2. Nationality
3. Scheduled Departure Time	3. Date of Birth
4. Scheduled Arrival Date	4. Gender
5. Scheduled Arrival Time	5. Official Travel Document Number
6. Last Place/Port of Call of Aircraft	6. Issuing State or Organization of the Official Travel Document
7. Place/Port of Aircraft Initial Arrival	7. Travel Document Type
8. Subsequent Place/Port of Call within the country	8. Expiration Date of Travel Document
9. Number of Passengers	

For the information related to each passenger's identity, Annex 9 Standard 9.8 limits the data to be transferred to those included in the MRZ of the travel document as defined in ICAO Doc 9303 Machine Readable Travel Documents[25].

ICAO Doc 9303 Machine Readable Zone Specifications



It is possible to include additional data elements related to passengers in API requirements. However, a distinction needs to be made between additional API data that can normally be found in airline systems and data that are not normally found in airline systems, which require additional resources for the airlines to collect.

[25] *Machine Readable Travel Documents*, Doc 9303, Seventh Edition, Part 3: Specifications Common to all MRTDs, ICAO, 2015: https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf.

Additional API Data Normally Found in Airline Systems

- Seating Information
- Baggage Information
- Traveler's Status
- PNR Number/Identifier
- Port of Embarkation
- Port of Clearance
- Port of Onward Destination

These data might be included in the airline's DCS, from which the API message is sent. Because of airline IT system IT Infrastructure, airlines have noticed, when implementing PNR programs, that many airlines (about half of the airlines worldwide) with a segregated CRS and DCS (see section 2.2) were not able to send seat and baggage information as part of their PNR message. This information was only available in their DCS and not in their CRS. As a result, the API message has been modified to include other data elements that can be found in the airline's DCS. This allows states requiring both PNR and API data to receive a more complete dataset from the airlines.

API data elements should be limited to the data collectable from the passport's MRZ and to data already present in airline systems. Any additional data elements to collect constitute a burden on the airlines and can disrupt operations significantly.

It should be stressed, however, that each airline will have slightly different arrangements regarding which data is included in their CRS or DCS. It is, therefore, essential for governments to collaborate closely with each airline when connecting them to the API or PNR systems to arrive at a common understanding of where the different data elements are in the airline IT systems.

Additional API Data NOT Normally Found in Airline Systems

- Place of Birth
- Visa Information
  - Visa Number
  - Issue Date of Visa
  - Place of Issuance of Visa
- Other Document Used for Travel
  - Document Type
  - Document Number
- Primary Residence
  - Country of Primary Residence
  - Address
  - City
  - State/Province/Country
  - Postal Code
- Destination Address
  - Address
  - City
  - State/Province/Country
  - Postal Code

While some of these data elements might be present in a travel document, they are not included in the MRZ and therefore cannot be captured automatically. Capturing these data elements requires a manual input, either by the passengers themselves or by airline agents. Manual data entry generally leads to mistakes and causes poor data quality. In addition, when it comes to capturing addresses, this information is purely declarative and cannot be verified by the airline. Finally, in keeping with the principle of efficiency, visa information is already available in national databases and should be searchable based on MRZ data. Requiring the capture of this information by airlines is duplicative.

API Data for Crew–API data can also be requested for crew. Data elements for crew are typically extracted from the airline's master crew list and include the following:

- Full name (last, first and middle if available)
- Gender
- Date of birth
- Place of birth (city, state if applicable, and country)
- Citizenship
- Country of residence
- Address of permanent residence
- Passport number if passport required
- Passport country of issuance if passport required
- Passport expiration date if passport required
- Pilot certificate number and country of issuance, if applicable
- Status on board the aircraft

Airlines can transfer API data for crew as part of the same PAXLST message sent for all persons on the flight or as a separate PAXLST message specifically for the crew. The choice of which PAXLST message to send depends on the airline's IT infrastructure. Authorities wishing to receive biographical information on crew members must specify the requirement in their programs. When receiving crew API, authorities could consider removing their requirement for a paper-based General Declaration (Appendix 1 of Annex 9).

API Data Format–As per Annex 9 Standard 9.8, all information required under API data exchange programs shall conform to the specifications of the UN/EDIFACT PAXLST messages. These specifications are detailed in Appendix IIA of the WCO/IATA/ICAO API Guidelines[26]. This document provides the message structure and segment details of the PAXLST message. These rules are maintained and approved by UNECE. They provide agreed standards and guidelines for the electronic interchange of structured data between independent computerized information systems. It is important to stress that the UN/EDIFACT PAXLST standard is a specific format used in the airline industry, as opposed to the widely used XML electronic format. Authorities need to make sure that their systems can receive and parse different data formats.

ICAO Standards mandate states to use the UN/EDIFACT PAXLST message for the transfer of API. Other solutions can be offered, such as XML PAXLST or web applications to accommodate all airline systems. However, airlines should remain free to choose which format they use.

[26] *Advance Passenger Information Guidelines*, Appendix IIA, WCO/IATA/ICAO, 2016: https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/appendix-iia-paxlst-message-implementation-guide-2016.pdf.

PAXLST Message Versions–In line with Annex 9 Standard 9.9, states must adhere to the PAXLST format. Should they wish to request any additional data element not covered in the existing guidelines, they shall follow the WCO's DMR. The DMR should be submitted through the API/PNR Contact Committee managed by WCO, in close collaboration with ICAO and IATA.

Several versions of the PAXLST message exist as a result of the DMR process. The original version of the message (D02b), adopted in 2003, did not include segments on seat and baggage information. At the time, API programs were mainly implemented to expedite immigration controls, and this information was not necessary for that function.

In 2010, in the aftermath of several deadly terrorist attacks, more states have been implementing PNR programs for security purposes. Seat and baggage information have become important data elements for risk assessment. The information is used to help identify international trafficking and criminal networks. About half of the world's airlines could not share these data elements as part of their PNR message issued from their CRS, forcing governments to seek a solution.

Several states submitted DMRs through the WCO process to ensure seat and baggage information was included in version D05b of the PAXLST message, adopted in 2010. The PAXLST message was subsequently enhanced, in 2013, with version D12b. This version includes baggage weight (in addition to the number of checked bags), and covers new elements linked to the implementation of interactive API programs. Further versions, D14b, adopted in 2014, and D15b, adopted in 2016, are also available.

The PAXLST version programmed in airline systems has a direct impact on the ability of the airlines to transfer certain data elements. For example, airlines that are still operating under a PAXLST D02b version will not be able to send seat and baggage information as part of their PAXLST message. In this case, airlines may have to send a separate passenger reconciliation list (PRL) from their DCS to the authorities. Additional information transfers of this type need to be specifically agreed and arranged between airlines and authorities.

Transfer of PAXLST Message–Due to the nature of API data elements, the PAXLST message has a rather condensed size. Unlike PNRGOV messages, which contain many more segments and can contain unstructured information as well as free text, PAXLST messages can be easily transferred over teletype systems, such as Type B. Type B has, however, limitations in terms of size, allowing only 60 lines of 63 characters for each message, and characters used. This implies that several messages may need to be sent to cover all the passengers on a single flight. To receive these messages using the Type B transfer protocol, authorities will have to connect through one of the telecommunication networks specifically used in the aviation industry.

Airlines do not necessarily have access to the same transfer channels. Direct connection to their systems might be a preferred option for some airlines. For smaller operations (such as general or business aviation), operators will not be able to use the UN/EDIFACT format. These operators may find it necessary to transfer the necessary information through a web portal or other alternative means, such as an email attachment, however, this is not considered to be a best practice that guarantees a secure transfer of data. As a result, states will have to work with each airline to define the possible and preferable methods of transfer.

Example of PAXLST Message Structure (One Passenger)[27]

```
UNB+UNOA:4+ZZAIRLINE+CUSTOMS+130620:0900+000000001'
UNG+PAXLST+ZZAIRLINE+CUSTOMS+130620:0900+000000001
+UN+D:15B'
UNH+PAX001+PAXLST:D:15B:UN:IATA'
BGM+745'
RFF+TN:1234567890'
NAD+MS+++DAVIDSON:ROBERT'
COM+202 628 9292:TE+202 628 4998:FX+NONAME.AT.
IATA.ORG:EM'
TDT+20+ZZ123+++ZZ'
LOC+125+SYD'
DTM+189:1306210900:201'
LOC+87+HNL'
DTM+232: 1306212200:201'
NAD+FL+++WILLIAMS:JOHN:DONALD+235 WESTERN ROAD
SUITE 203+SLEAFORD+:::LINCS+PE224T5+GBR'
ATT+2++M'
DTM+329:720907'
MEA+CT++:2'
GEI+4+174'
FTX+BAG+++ZZ012345:3'
LOC+22+HNL'
LOC+174+GBR'
LOC+178+SYD'
LOC+179+HNL'
LOC+180+:::AMBER HILL GBR'
COM+44 188 84 14151:TE'
NAT+2+GBR'
RFF+AVF:TYR123'
RFF+ABO:ABC123'
DOC+P+MB140241'
DTM+36:151231'
LOC+91+GBR'
CNT+42:160'
UNT+30+PAX001'
UNE+1+000000001'
UNZ+1+000000001'
```

Timing of Transfer–Considering that the purpose of API data programs was originally to provide advance information to border guards on who was going to arrive at their border, API data is sent in one batch at flight closure, after the aircraft doors have been closed. This is why API programs are also called batch API (in contrast to interactive API programs described in the Section 3.3).

The timing of the data transfer allows users to ascertain exactly who has boarded the flight, taking into account all last-minute changes. Therefore, the PAXLST message is complete with the information of all passengers and/or crew on board.

International best practice for batch API programs foresees the transfer of one single PAXLST message at flight closure. Depending on the program, “at flight closure” can be defined as 15 to 30 minutes after the aircraft doors have been closed. It should be stressed that flight closure is a manual process conducted by airline agents. The PAXLST message is generated automatically from the DCS once the flight is closed. This manual intervention might sometimes cause delays in the transfer of the message.

In some cases, however, some states might require sending API data one hour prior to departure. This could be the case for international short-haul flights, where authorities would not have enough time between flight departure and arrival to process the data and perform their risk assessment. This could also be the case if states want to identify potential inadmissible passengers before they board the aircraft. However, at one hour

[27] For other samples of PAXLST messages, refer to the *Advance Passenger Information Guidelines*, Appendix IIA, WCO/IATA/ICAO, 2016: https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/appendix-iia-paxlst-message-implementation-guide-2016.pdf.

before departure, check-in might not be fully completed (some airlines allow check-in until 40 minutes prior to departure). Both passenger and crew lists can change up until the last minute. States requesting API data an hour prior to departure for advance analysis should also have the capability to contact the airlines to prevent a passenger from boarding. A clear legal basis providing authority to the airline agents to prevent a passenger from boarding might also be necessary.

Multiple transfers of API data can be inefficient for authorities and costly for the airlines. Any additional transfers need to be justified based on a clear purpose and where the data is effectively used and acted upon prior to flight closure.

ICAO recommends that the number of times API data is transmitted for a single flight be limited (Recommended Practice 9.10). The number of transfers should be proportionate and relevant to the purpose of the data collection and processing.

3.1.3 Operational Impacts

Unlike PNR, the collection of API data has a direct operational impact on passengers and airlines. Data beyond was is necessary for the delivery of the transport service have to be collected from passengers and verified by airline staff.

As discussed in section 2, prior to implementing API systems, states should understand how airlines are capturing data (the different check-in options), how the airline systems are organized (segregated CRS/DCS, separate crew management or baggage handling systems) and the flight profile. A long-haul flight where most passengers are holiday makers (where the majority goes through check-in desks) and a medium-haul flight with a majority of business or frequent travelers (where the majority checks in online) might present different profiles in terms of data quality.

The quality of the data captured also largely depends on the training of the airline agents on the ground. Therefore, airlines need sufficient time, when a new API data requirement is introduced by a state, to inform and train their staff at the impacted stations.

To reduce the number of false positives in their initial risk assessment, authorities will also have to ensure their databases are enriched; for instance, in cases of names with different spellings (based on the alphabet used) or regarding individuals with several nationalities (this is particularly important when matching entry and exit records, in the event that different passports are used).

3.1.4 Implementation Considerations

ICAO provides a useful checklist for governments implementing API programs[28]. IATA also lists key elements for states when establishing a passenger data program[29]. To summarize, the key steps for the implementation of an API program are the following:

Establish Legislation–Establish national legislation that clearly defines the purpose for processing API data (e.g., immigration, law enforcement) and the appropriate authorities to receive and process the data. In line with the Single Window principle (see section 1.2.1), a single agency is to be in charge of collecting the data from the carriers.

The legislation should also specify the scope of the requirement (i.e., for all flights or a limited number of flights, inbound only, outbound only). It is also useful to define whether the requirements apply to passengers and crew or passengers only and which types of airline operations should be covered (i.e., only commercial aviation, cargo operators, business aviation).

Based on the purpose of the requirement, authorities need to list the data elements to be collected and transferred by carriers and mandate a precise timing for the transfer. As highlighted previously, carriers do not generally collect travel document information in the normal course of their business. Therefore, it is important to provide a legal basis to carriers for them to be allowed to request this information, which falls outside the scope of the information necessary for the execution of the transport contract (as per general data protection principles).

Provide a Detailed Implementation Guide–The first step for airlines to start programming their systems to send API data to a country is the provision of a detailed implementation guide, on the model of the one provided in Appendix IIA of the WCO/IATA/ICAO API Guidelines. This guide is the basis for airlines to start programming their systems. It should include the following information:

- Reference to the legal basis on which the API data request is based.
- Contact of the Single Window unit.
- List of data requirements (including specific formats/types of flights/scope).
- List of accepted travel documents (this is especially important in some regions where passengers might be allowed to travel regionally with identification documents other than the ones defined by ICAO Doc 9303).
- Definition of transmission protocols, including testing procedures and contingency measures in case of unavailability of the system (both on the side of the agency and of the carriers).
- Transmission format.
- Message structure. This must be adapted depending on the specific features of the national program.

[28] *The Implementation Steps of Advance Passenger Information (API) System*, ICAO: https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20API%20Brochure_2018_web.pdf.

[29] *Checklist, How to set up a passenger data exchange program*, IATA, 2013: https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/passenger_data_program_checklist.pdf.

Communication with Airlines–Airlines will only be able to start preparing their systems to transfer API information once the two following conditions are met:

1. A clear legal basis mandating the API data collection and transfer is enacted.
2. A detailed implementation guide has been communicated to the airlines, including the testing and production address.

To communicate with the airlines, states can use different channels. It is recommended to use several of the following channels to ensure all airlines are well informed:

- **At the national level**:
  - Airline Operators Committees.
  - National Board of Airline Representatives (BAR).
  - National Facilitation Committee (see section 1.3.1).
  - Any other consultative body that has been set up by the Civil Aviation Authority to communicate with the carriers operating in the country.
- **At the international level**: IATA provides all member airlines and governments access to its API/PNR World Tracker on IATA's Facilitation Extranet[30]. States are encouraged to provide IATA with a fact sheet and a copy of the implementation guide to ensure all airlines flying to their country are informed. This information is also a useful reference for airlines that are starting new routes to a country.

Timeline–Authorities should allow enough time for carrier compliance and for their own units to test and connect to each airline's systems. It can take between three to six months from the moment the airline receives the implementing guide for it to comply with a standard API requirement, provided it is fully aligned with international standards and best practices. In the case of a non-standard requirement, the delay for compliance can be from 24 to 36 months. Connecting each airline can be a long and cumbersome process for the authorities, depending on the set-up and complexity of each airline's IT systems and operation network. Therefore, it is recommended that authorities employ a progressive implementation plan, starting with a few airlines and/or routes. This progressive implementation also allows the authorities to test the robustness of its own systems and procedures.

3.1.5 Use of API Data to Secure and Simplify Border Controls

A well-conceived and thoroughly implemented API program is a powerful tool to support a state's immigration and national security policies. Providing accurate advance information on persons entering or leaving the territory allows states to:

- Remove paper-based processes such as passenger manifests and entry/exit cards.
- Plan the staffing of their border checkpoints efficiently (by receiving an accurate number of persons on the flight).
- Speed up border controls by performing watchlist vetting and database consultations before passengers present themselves in front of a border officer.

[30] Access to the IATA API/PNR World Tracker can be requested to passengerdata@iata.org.

- Expedite the controls on low risk passengers and focus resources on travelers raising concerns.
- More accurately identify over-stayers.
- Identify potential terrorists, human traffickers and other transnational criminals by checks made against watchlists and through the collection of additional data elements such as routing, seat and baggage information.

Before implementing additional border control measures or requesting additional passenger data, authorities should establish whether all the potential benefits brought by API data processing have been realized and fully implemented to avoid duplication.

3.2 Passenger Name Record

API programs provide a powerful tool to improve border management processes. However, for law enforcement purposes, when authorities are looking at identifying potential trends and patterns for illegal trafficking, criminal activities or terrorist movements, API data can only provide a partial picture. The use of the booking information captured by airlines is used by law enforcement authorities for risk assessment purposes and for matching against risk profiles and/or indicators, even if the traveler is not already known to the authorities.

3.2.1 Value and Purpose

Unlike API, PNR is not a dataset originating from a legal requirement. PNR is the name given to the file created by the airlines whenever a person books a flight. This file is the repository of all the relevant information provided by the persons who purchased an air travel service. It is a business record. Whereas API is a useful tool to establish and verify the identity of the persons travelling, PNR provides indications of travel intention, itinerary, date and time, relationship between persons travelling together, and services requested (e.g., extra luggage, special meals, travel class, seating arrangements, special assistance).

PNR information is provided by individuals. It is declarative and the information contained in the PNR can change up to the last minute of the planned trip, making the information's accuracy difficult to verify. The data is simply a transcript of the service requested to be delivered by the carrier.

PNR data helps authorities perform risk assessment on travelers that are not known to them and do not appear on any watchlist. The risk assessment is done based on specific criteria and risk profiles established by the authorities.

PNR data was initially used by customs authorities at airports. Analyzing this data on both inbound and outbound flights allowed customs officers to better target their checks. A complete inspection of hold luggage by customs authorities is not feasible. In the aftermath of terrorist attacks in the 2000s, PNR data has also increasingly been used by Ministries of Interior, immigration services, intelligence services and law enforcement authorities to identify international trafficking networks as well as potential terrorist and foreign terrorist fighter movements.

Whereas API data is usually kept only for the time necessary to perform watchlist matching (unless API is used to record entry and exit), the analysis of PNR over a period of time can help establish useful traveler patterns/profiles and detect international trafficking networks, even if the persons involved are not initially known to the authorities. To be fully useful, PNR data needs to be kept and analyzed from an historical perspective (generally five years or more in the case of a specific suspicion). This implies that, when implementing PNR programs, states should also develop such risk-assessment and analysis capabilities.

PNR programs to be used for law enforcement:

- PNR programs will have limited benefits for border management purposes since the information is not verified against the travelers' identity documents. However, PNR data will provide essential information to law enforcement agencies to detect potential illegal trafficking or terrorist activities.
- For law enforcement purposes, as PNR data can be located in different airline systems, authorities should consider combining their API and PNR data programs, so the PAXLST message sent from the airline DCS can complement the information in the PNRGOV message sent from the airline CRS.

The information provided by passengers to the airline or its agents is not information they would typically expect to provide to authorities at the border. Some elements in the PNR message, or the combination of different elements in the PNR, can in some cases reveal information on the race, ethnicity, religion (in the case of meal preference), political views, trade union affiliations, marital status or sexual orientation (in the case of a group PNR). PNR is, therefore, considered sensitive personal data and must be adequately protected by specific conditions in its collection and processing by authorities.

PNR data elements are more sensitive than API data elements and need to be subjected to appropriate privacy and data protection safeguards. The transfer of these data can be subjected to specific conditions depending on the data protection regime applicable in the flight's country of origin.

Note: *Airlines can legitimately collect this information, as it is voluntarily provided by the passenger and directly linked to the execution of the services requested (e.g., special meal, seating arrangement, special medical assistance) as part of the contract (the ticket) established between the passenger and the airline.*

ICAO Doc 9944 sets out the general principles to be applied for the processing, filtering, storage and general protection of PNR data.

3.2.2 International Standards

Amendment 28 to Annex 9 contains a new Standard to the effect that states shall develop a capability to collect, use, process and protect PNR data. This new Standard is applicable as of February 2021.

Definition–"*A Passenger Name Record (PNR) is the generic name given to records created by aircraft operators or their authorized agents for each journey booked by or on behalf of any passenger. The data is used by operators for their own commercial and operational purposes in providing air transportation services.*" (ICAO Doc 9944).

As per this definition, PNR data will provide information not just on one flight segment (like for API), but on the whole passenger journey. This will help identify the routing of the passenger, which can be an important element of the risk assessment performed by law enforcement agencies.

The definition also stresses the fact that PNR data is collected by airlines in the normal course of their business, for the purpose of providing air transport services. This implies that the amount and type of data contained in the PNR will vary significantly from one airline to another and even from one passenger to another. As a result, it does not make sense for states to mandate the collection and transfer of specific PNR data elements, as airlines do not offer all the same services or have the same commercial offering (see section 2.2). There is no such thing as an incomplete PNR message or inaccurate PNR data, as the data transferred is simply based on the information airlines have collected in their systems. For these reasons, amid the COVID-19 pandemic, PNR has not proven to be an efficient tool for authorities to collect contact tracing information. Contact tracing and other health-related information are better collected directly from passengers by authorities. Contact tracing and health-related information do not serve any business or operational purposes. Authorities may set up web portals to fulfil their needs for such data.

PNR data is collected in the normal course of airline business. Airlines are providing these data to support law enforcement activities but cannot be requested to collect or verify specific information.

PNR Data Elements–Appendix 1 of ICAO Doc 9944 defines a list of 19 categories of possible data that can be found in a PNR message:

1. PNR locator code	10. Travel agency
2. Date of reservation/issue of ticket	11. Code share PNR info
3. Date(s) of intended travel	12 Split/divided PNR info
4. Name(s) on the PNR	13. Travel status of passenger
5. Frequent flyer info	14. Ticketing info
6. Other names on PNR, incl. number of passengers on PNR	15. All baggage info
7. All available contact info	16. All seat info
8. Form of payment info	17. General remarks including other service information (OSI) and special service request (SSR) info
9. Travel itinerary for specific PNR	18. Any API data collected
	19. All historical changes to PNR

Some of these data elements are normally found only in the airline's DCS (i.e., seat or baggage information). The ability of the airlines to transfer these data elements as part of the PNR message will depend on their IT infrastructure and whether their CRS and DCS are integrated.

It is also an accepted principle that airlines will only provide information that is stored in their systems. If some of the data elements listed above are stored in different systems (e.g., payment information), airlines are not obliged to transfer them as part of the PNR message.

Data format–All the data elements listed above are accounted for in the PNRGOV message structure. The functional and business principles that govern the use of PNRGOV can be found in a guidance document developed by IATA[31]. The message structure and the format to be used for the transfer of PNR data are defined in the PNRGOV EDIFACT Message Implementation Guide as well as in the PNRGOV XML EDIFACT Message Implementation Guide[32]. It should be highlighted that the PNRGOV message format is managed directly by IATA, in collaboration with ICAO and WCO. It remains an industry standard, developed to ensure a common format to be used across airlines as well as travel agents to capture bookings. The Passenger and Airport Data Interchange Standards (PADIS) board is in charge of maintaining this standard.

PNRGOV provides an indicative list and message structure for the data elements that could be available in airline systems. However, it does not mandate the transfer of specific data elements.

While an XML version of the PNRGOV message has been developed, it is not yet widely used by the airlines. The vast majority of airlines are still using the EDIFACT version of the PNRGOV message, making it necessary for authorities to develop the capability to receive and parse this specific data format.

Transfer Protocols–The **push method** is the method used by all states and carriers in the implementation of PNR programs. With this method, airlines transfer the available set of data to the Single Window facility.

The first PNR programs implemented by customs authorities in the 1990s were based on the **pull method** whereby states have access directly and copy to the data from airlines systems. This method is considered contrary to data protection principles. Nowadays, it is only used by a limited number of countries and in exceptional circumstances (i.e., emergency landing, technical problems).

Considering the size of the PNR message, which is much longer than an API PAXLST message, airlines have implemented the IBM MQ protocol. Type B messaging could still be used by some airlines; however, the size limitations of this protocol render its use rather expensive and burdensome. Direct connection and file upload directly on a secured web platform provided by the authorities are also possible. To be able to connect the maximum number of air carriers, authorities must offer several options for data submission.

[31] *Functional and Business Principles PNRGOV*, Version 17.1, IATA, 2017: https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/pnrgov20principles2017201.pdf.

[32] For all the versions of the Guide: https://www.iata.org/en/publications/api-pnr-toolkit/#tab-3.

Example of PNRGOV Message Structure (One PNR Including One Adult and One Infant)[33]

```
UNA:+.?*'
UNB+IATA:1+AM+MXPNRGOV+130522:1540+13052210400995+PNRGOV'
UNG+PNRGOV+AM+MXPNRGOV+130522:1540+13052210400995+IA+11:1'
UNH+13052210400995+PNRGOV:11:1:IA+AM498/230513/1142'
MSG+:22'
ORG+AM'
TVL+230513:1039:230513:1142+MTY+LAS+AM+498'
EQN+1'
SRC'
RCI+AM:XXXYET::300413:115500'
SSR+OTHS:::::::: ADV TKT NUMBER BY 03MAY13 1800CO OR WILL CANCEL'
SSR+OTHS:::::::: IF THE FARE RULE TL DIFFERS FROM THE AUTOMATIC'
SSR+OTHS:::::::: TL THE MOST RESTRICTIVE TL WILL APPLY'
DAT+700:180513:1502'
ORG+AM:BOG'
TIF+TESTSURNAMEONE+TESTNAMEONE MRS:A:1.1:1'
SSR+INFT:NN:1:AM::::TESTSURNAMETWO/TESTNAMETWO/10AUG11+::1.1'
SSR+INFT:NN:1:AM::::TESTSURNAMETWO/TESTNAMETWO/10AUG11+::1.1'
SSR+TKNE:HK:1:AM:::MEX:CUN:1392178947000C2+::1.1'
SSR+TKNE:HK:1:AM:::CUN:BOG:1392178947000C3+::1.1'
SSR+TKNE:HK:1:AM:::MEX:CUN:INF1392178947000C2+::1.1'
SSR+TKNE:HK:1:AM:::CUN:BOG:INF1392178947000C3+::1.1'
SSR+DOCS:HK:1:AM::::/P/CO/52263000/CO/30MAY76/F/31OCT15/TESTSURNAMEONE/TESTNAMEONE
MRS+::1.1'
TIF+TESTSURNAMETWO+TESTNAMETWO:IN:2.1'
IFT+4:28+AM INF'
SSR+DOCS:HK:1:AM::::/P/COL/AO234000/COL/10AUG11/FI/21DEC22/TESTSURNAMETWO/TESTNAMETWO+::2.1'
TVL+150513:0105:150513:0557+BOG+MEX+AM+709:R'
RPI+1+YG'
APD+737'
RCI+AM:XXXYET::300413:115500'
TVL+190513:1500:190513:1710+MEX+CUN+AM+445:S'
RPI+1+HK'
APD+738'
SSR+INFT:NN:1:AM::::TESTSURNAMETWO/TESTNAMETWO/10AUG11'
SSR+TKNE:HK:1:AM:::MEX:CUN:1392178947000C2'
SSR+TKNE:HK:1:AM:::MEX:CUN:INF1392178947000C2'
RCI+AM:XXXYET::300413:115500'
TVL+230513:0135:230513:0500+CUN+BOG+AM+718:Q'
RPI+1+HK'
APD+737'
SSR+INFT:NN:1:AM::::TESTSURNAMETWO/TESTNAMETWO/10AUG11'
SSR+TKNE:HK:1:AM:::CUN:BOG:1392178947000C3'
SSR+TKNE:HK:1:AM:::CUN:BOG:INF1392178947000C3'
RCI+AM:XXXYET::300413:115500'
UNT+42+13052210400995'
UNE+1+13052210400995'
UNZ+1+13052210400995'
```

Timing of data transfer–ICAO Doc 9944 encourages states to limit the timing and frequency of PNR data transfers to what is relevant to the purpose of the data collection. Limitations and capabilities of airline systems should also be taken into account. In practice, authorities traditionally request two transfers of PNR data:

- Once between 72 to 24 hours prior to flight departure
- Once at flight closure

[33] For other PNRGOV message examples, refer to the *Passenger and Airport Data Interchange Standards EDIFACT Implementation Guide–PNRGOV*, 2017: https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/pnrgov20edifact20implementation20guide2017_1.pdf.

This timing allows authorities to perform a first risk assessment prior to the flight and identify potential individuals of interests. This first risk assessment, especially when conducted on outbound flights, will allow authorities to better target their controls at the airport. The first push is, however, unlikely to include seat and baggage information. It will only provide the authorities with information on passenger itineraries and some indications on the profile of travelers who intend to travel on the flight. It should be stressed again that the name indicated on the PNR is not verified against any official travel document. The name provided is only of the person who booked the ticket (who might be a third party). It can contain spelling mistakes or just provide a reference for a group booking. For example, the PNR name could be “National Football Team”, including 22 seats booked, but not necessarily knowing at the time of booking all the names of the players and coaches who will be flying.

The second PNR push at flight closure will provide updated information on which passengers have boarded the flight and, if the airline's systems allow, updated information based on the data collected in the DCS (e.g., seat, baggage, frequent flyer, API information).

Some states request additional pushes in between these two timeframes to receive information whenever there is an update to the PNR information. The proportionality of such requests is questionable. Requesting too many pushes of PNR messages will lead to a significant volume of potentially duplicative information. Duplicate information means that authorities have to dedicate additional resources and time in reconciling the different messages, while imposing additional burdens and costs on airlines. For inbound flights, the updated PNR information sent at flight closure should be sufficient to perform risk assessment and plan targeted controls upon arrival. For outbound flights, authorities requesting multiple pushes will need to develop the capability to reconcile the different versions of the messages and perform real-time risk assessment. In the absence of such capability, requesting multiple PNR updates has limited value and only represents an unnecessary burden on both the carriers and the Single Window unit collecting the data.

In the case of multiple data pushes, air carriers should always have the possibility to send updates rather than resubmitting the complete set of PNR data for the whole flight. This helps minimize the volume of data transferred and facilitates reconciliation between the different messages.

3.2.3 Operational Impacts

When PNR data transfer is implemented in accordance with international standards and practices, this limits the impact on both air carrier operations and passengers. No additional information should be collected from passengers by carriers and carriers will only have to push the data they have in their systems.

Deviation from international standards and best practices can lead to significant impact and delay the implementation of PNR requirements by airlines. Depending on their contractual arrangements with service providers and on which transfer protocol is used, each push of data per PNR file might incur direct costs to the airlines. Therefore, a disproportionate request for numerous PNR data transfers might impose high costs on the airlines and be contrary to the principle of efficiency.

As seen previously, PNR consists of declarative data collected from the passenger at the time of booking. As such, the information may not match exactly the information contained in the passenger's travel document. For example, a ticket can be booked under the name Mr. and Mrs. Smith, but the travel document of Mrs. Smith might only show her maiden name. In this context, correcting PNR data does not fulfil any airline operational or commercial purpose. If authorities want to receive accurate information on passenger identity, they should introduce an API requirement.

Sanctioning airlines for inaccuracy or incompleteness of PNR data is unjustifiable. Airlines only send what they have in their systems for the purpose of delivering the requested air transport service. If some information is missing from the PNR, such as baggage information, this is linked to the fact that this information is stored in different systems than the CRS and cannot be aggregated in the PNR. If authorities want to receive this information, they will have to discuss with the airlines possible options to receive data in a separate message or under a separate program, such as an API data requirement that includes seat and baggage information collected in the DCS.

PNR data is understandably limited to commercial airlines carrying passengers. Cargo carriers and business aviation operations do not have any PNR data. However, they can provide API data for their crew and other persons on board.

Due to the sensitivity of PNR data, some countries might forbid carriers from transferring this data to foreign countries in the absence of a bilateral agreement guaranteeing data privacy and protection in the collection and processing of PNR data. This is the case for the European Union (EU). The EU forbids the transfer of PNR data to foreign countries in the absence of a specific PNR agreement[34]. States wanting to receive PNR data for flights originating in the EU will have to negotiate a bilateral agreement directly with the European Commission.

Note: *This prohibition is applicable to any flight from the EU territory, not just for EU carriers.*

Under some national data protection regulations, the processing of certain data elements contained in the PNR message may be forbidden in some states. It is the responsibility of these authorities to conduct the filtering of the data they receive. Airlines should not be required to filter data. This practice ensures that authorities remain in control of defining, depending on national legislation, what data elements they need to receive and what should be filtered out, while also alleviating airlines flying to different countries of the burden of programming different message versions.

[34] *On the global approach to transfers of Passenger Name Record (PNR) data to third countries*, COM (2010), European Commission, September 2010: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0492:FIN:EN:PDF.

3.2.4 Implementation Considerations

WCO provides useful guidance on PNR program implementation[35] and a checklist to guide them in the collection and processing of PNRGOV messages[36]. The IATA checklist[37] also provides the key steps to be followed.

Establish a legislation–Establish national legislation to define the purpose of the data collection, the appropriate authorities, the scope of the requirement (inbound/outbound and impacted carriers), the data elements and transfer timing. Due to the sensitivity of PNR data, and to encourage international acceptance, specific provisions regarding the protection of PNR data, in line with the measures recommended in ICAO Doc 9944, should be included in the national legislation. The law should also reflect that, for PNR, sanction for noncompliance shall only apply in the event that carriers do not transfer any PNR data. Unlike for API, carriers cannot be sanctioned for inaccuracy or incompleteness of transmitted data.

For authorities, PNR data processing is more complex and burdensome than API data, which can be limited to a simple watchlist matching. The analysis of PNR data requires states to develop sophisticated risk assessment capabilities. Procedures for data anonymization, minimization and retention also need to be established.

The volume of PNR data is significantly larger than for API. The Single Window facility will have to set up an IT infrastructure with sufficient bandwidth to handle all the messages received.

In light of this complexity, states should allow enough time in their implementation plan to set up IT infrastructure as well as recruit and train necessary staff. For example, the European Commission recommends a minimum of 12 months between the start of the project and implementation deadline[38]. Several international organizations can also support authorities with dedicated projects (see section 1.3.2).

Implementation Guide–In addition to a clear legal basis, air carriers will need to receive a detailed implementation guide outlining specific national requirements before programming their systems to send PNR data. IATA provides a model Implementation Guide for PNRGOV, both in the EDIFACT[39] and XML format[40].

---

[35] *WCO Guidance for Customs Administration, How to Build an Advance Passenger Information (API)/Passenger Name Record (PNR) Programme*, WCO, July 2017: http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/api-guidelines-and-pnr-doc/guidance-for-customs-administrations-on-how-to-build-an-api-pnr-programme.pdf?la=en.

[36] *PNR lessons learnt high level checklist,* Version 1.1, WCO, May 2016: http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/api-guidelines-and-pnr-doc/pnrgov-lessons-learnt-high-level-checklist-en.pdf?la=en.

[37] *IATA Checklist, How to set up a passenger data exchange program*, IATA, 2013: https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/passenger_data_program_checklist.pdf.

[38] *Commission Staff Working Document* , SWD(2016) 426 final, European Commission, November 2016: https://ec.europa.eu/transparency/regdoc/rep/10102/2016/EN/SWD-2016-426-F1-EN-MAIN.PDF.

[39] *Passenger Data and Interchange Standards, EDIFACT Implementation Guide*, Version 17.1, IATA, 2017: https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/pnrgov20edifact20implementation20guide2017_1.pdf.

[40] *Passenger Data and Interchange Standards, XML Implementation Guide*, Version 16.1, IATA, 2016: https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/pnrgov20xml20implementation20guide2016_1.pdf.

Implementation guides should include the following elements:

- Reference to the legislation on which the PNR request is based and, if relevant, the sanction regime in case of noncompliance.
- Contact of the Single Window unit.
- Scope of the requirement and, where relevant, how the API and PNR requirements are combined.
- List of data, timing and format of transfer.
- Fall-back procedures in case of system unavailability, special cases or flight configurations.
- Accreditation/certification process for the airlines to connect to the Single Window facility.
- Message structure must be adapted depending on the specific features of the national program.

Communication–The same communication process as described in the API section (see section 3.1.4) should be applied in the implementation of a PNR program. PNR programs are, however, more complex to implement and authorities will have to invest time to understand how each airline IT infrastructure is set up (segregated or integrated CRS). During this process, authorities might also have to interact directly with airline service providers who control the CRS. The certification/connectivity testing process will be more complex than for API.

For PNR programs, states should also provide clear information to passengers on the purpose of data collection and processing, as well as on possible data access and redress procedures. An example of a standard communication to passengers is provided in Appendix 2 of ICAO Doc 9944.

Timeline–PNR programs are much more complex than API programs to implement. Authorities should, therefore, allow enough time to first set up their own systems and then connect all the airlines in the scope of the program. If the PNR requirements are aligned with international standards, airlines will need between six and 12 months to comply from the time they have received the detailed implementation guide. In the case of non-standard requirements, the implementation period can be much longer. Bearing these timelines in mind, authorities are encouraged to consider a progressive implementation of requirements, connecting airlines in batches, depending on IT system configurations, service providers, or number of routes into the country. This approach will also allow the authorities to develop and test their risk profiles and criteria using test data from a limited number of air carriers.

The use of PNR data requires authorities to develop a robust risk analysis capability, with risk indicators and profiles. If authorities do not have these capabilities, the use of API data is probably more beneficial, as it allows for a simple check against existing databases or watchlists.

3.2.5 Combining API and PNR Requirements

To achieve maximum efficiency, states often combine API and PNR to achieve the following benefits:

- PNR can be collected between 72 to 24 hours prior to the flight, allowing enough time for the authorities to perform a preliminary risk assessment on the passengers booked on the flight.
- API data collected at flight closure (or sometime during the hour prior to departure) will confirm the identity of the passengers, allowing for a more accurate watchlist/database verification.

- Seat and baggage information will be transferred, either as part of the PNR messages or as part of the API message, depending on the capability of the airline systems.
- API information will also include information on crew.

The combination of both passenger data programs allows authorities to receive a more complete set of data at different stages of the passenger journey.

3.3 Interactive API

iAPI is the most advanced among passenger data programs. To be successfully implemented, it needs to rely on robust procedures and a mature use of API and PNR data. The benefits of iAPI are numerous for all stakeholders, including passengers. However, this is a very time-sensitive system, which can significantly impact carrier operations if not implemented correctly.

3.3.1 Value and Purpose

Batch API data allows states to perform identity verification and watchlist matching on passengers before they arrive at the border. iAPI programs rely on the same dataset and principles as batch API programs, but the data is sent immediately to authorities when the passenger checks in. This allows the authorities to inform the airlines on the status of a passenger before they board the flight.

The benefits of iAPI are significant for both the authorities and carriers. Authorities will be able to identify individuals of concern at the time of check-in and advise airlines of any necessary action (e.g., refuse boarding, provide additional information, perform additional controls), thereby reducing the need to deploy ILOs. For airlines, iAPI should significantly reduce the number of inadmissible passengers they have to manage, and the related fines and penalties.

The advance notice and interactive features provided by iAPI can also support different border control and law enforcement programs, such as:

- **Border security:** instead of relying on airline staff to determine the admissibility of passengers prior to departure, authorities can have the direct control on which passengers they allow to arrive at their border through checks performed on relevant databases, including national travel documents and other national ID, travel authorizations, national and international watchlists, and the INTERPOL SLTD.
- **Aviation security risk assessment:** based on an initial risk assessment using a combination of PNR data received 72 to 24 hours prior to the flight and the API data received at the time of check-in, authorities can mandate airlines or entities in charge of passenger screening to subject specific passengers to additional targeted screening measures.
- **Exit checks:** in countries where there are no exit border controls, iAPI programs can give authorities the information and time necessary to prevent an individual from leaving the country.

While iAPI provides significant value, it is a complex and costly system for both authorities and airlines. It is also a very time-sensitive process that can have a significant impact on both passengers and air carrier operations in case of system failure. The implementation of iAPI programs needs to be considered in the light of a state's capability to provide a Customs Response (CUSRES) message to carriers within 3-4 seconds as well as to support a very reliable IT system on a 24/7 basis.

Building a robust iAPI as the next step after API/PNR programs:

- iAPI programs can bring significant benefits for border management and law enforcement. However, iAPI is a very complex and costly system to implement. States should first implement batch API and PNR programs as per their international obligations to fine tune their data processing methodologies and tools.
- When rolling out an iAPI system, authorities should ensure a single and aggregated response is provided to the airline (CUSRES message) for each passenger. Such an aggregated response includes checks against all relevant databases, including national travel documents and other national ID, travel authorizations, national and international watchlists and the INTERPOL SLTD.

3.3.2 International Standards

Definition–"*An electronic system that transmits, during check-in, API data elements collected by the aircraft operator to public authorities who, within existing business processing times for passenger check-in, return to the operator a response message for each passenger and/or crew member*". (ICAO Annex 9).

As mentioned above, iAPI relies on the same data elements as API. The data is sent on a per-passenger basis at the time of check-in. Authorities respond in an automated way to the carrier, in four seconds or less. The response will depend on the programs and/or legal requirements iAPI is supporting. This response will generally condition the issuance of the boarding pass by the carriers.

iAPI systems rely on the same dataset as API, but the data is sent per passenger at the time of check-in, providing the opportunity for authorities to communicate a response on each traveler's status.

Data Elements–The data elements sent by carriers are identical to those of batch API (see section 3.1), combining both biographical data from the passenger and information on the flight. The data elements sent back by the authorities to the airline include the following:

- Control information: reference to the PAXLST message to which the response relates.
- Flight information: as included in the original PAXLST message sent by carriers.
- Message status indicators.
- Data relating to each individual passenger, including indication on the status of the passenger and result of the data analysis.

Data Format–The data format of the message sent by the airlines remains the PAXLST message, structured according to Appendix IIA of WCO/ICAO/IATA Guidelines on API. The format of the message to be used by authorities to respond to carrier API messages is the UN/EDIFACT CUSRES as defined in Appendix IIB of the same API guidelines.

Transfer Protocols–The same protocols used in batch API programs can be used. The systems used by the airlines will vary and authorities will need to be able to work with the different transfer protocols used by carriers. However, iAPI relies on more robust network protocols to allow for the immediate response to carriers.

Timing of Data Transfers–Data is sent at the time of check-in on a per-passenger basis. Check-in timing is generally linked to the transfer of the data from the CRS to the DCS, which for most airlines occurs between 72 to 24 hours prior to the flight, and until approximately 1 hour to 40 minutes prior to the flight departure. The data transfer timing varies depending on airline systems and practices. Authorities need to define check-in timing with each airline to understand the timeframe within which they will be receiving data for each flight.

Authorities should respond to data transfer in less than four seconds. In an iAPI program, airline DCSs are programmed to issue boarding passes based on the information included in the CUSRES message received from authorities.

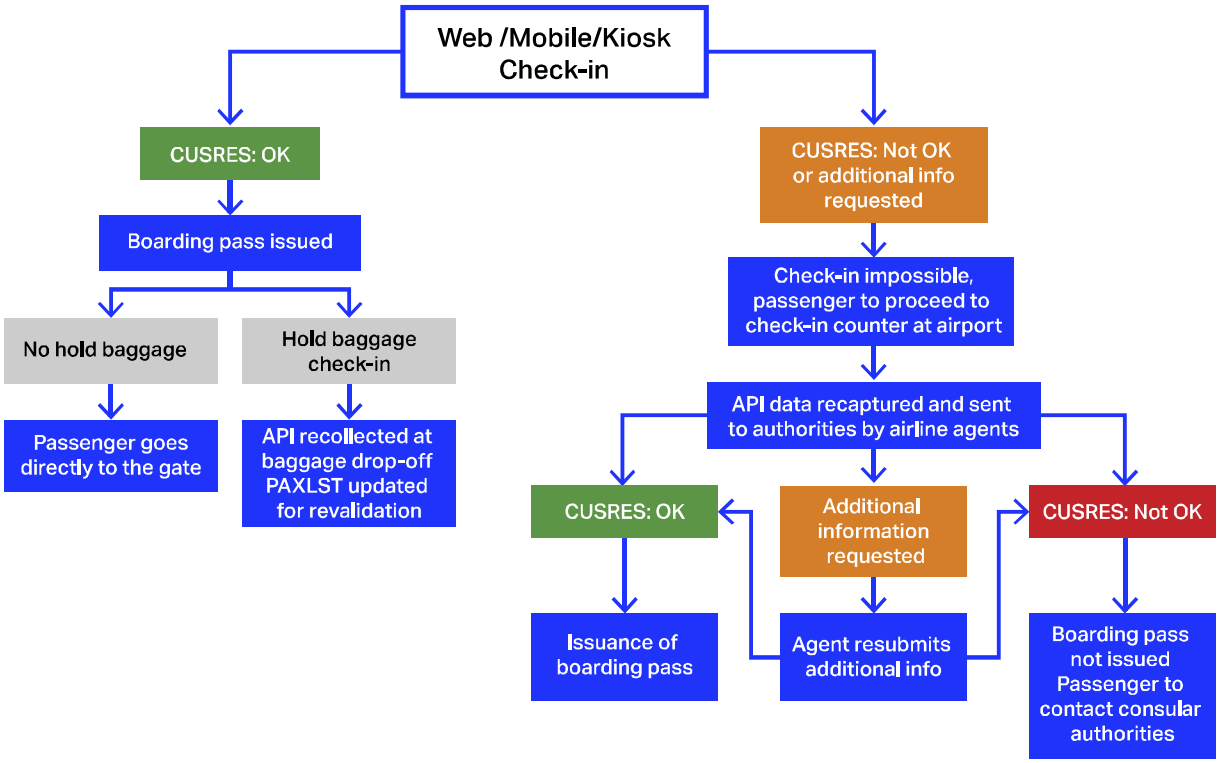
3.3.3 Operational Impacts

iAPI is closely linked to the check-in process, which is a key step in air carrier operations and in the passenger journey. This makes the provision and verification of iAPI a highly sensitive process that can, in the case of system failure or malfunction, paralyze airline operations. Therefore, the following conditions need to be met by states implementing iAPI programs:

- The system needs to guarantee a high level of availability and reliability. In the case of failures, a clear and detailed fallback procedure needs to be established and agreed with the airlines to allow the issuance of boarding passes.
- The CUSRES message sent by the authorities needs to be accurate the first time. The airlines will issue the boarding pass based on the information received in the CUSRES message. Once the boarding pass is issued, the airlines will only be able to interact with the passenger (e.g., deny boarding or request additional information) at the boarding gate.
- Providing a 24/7 help desk support to airlines.

The quality of the response sent by the authorities will have a direct impact on the resources carriers allocate to the check-in process.

Generic Check-in Process with iAPI



Data Quality–iAPI provides a great tool to enhance the quality of the API data submitted to authorities. By receiving the data at the time of check-in, the authorities can send a message back to the carrier if the information is wrong or incomplete. This allows the carrier to revalidate the data through an automated capture of the travel document at the airport. Sanctions in case of inaccurate API data should, therefore, be significantly reduced with iAPI programs.

iAPI systems can be an effective tool to improve data quality, providing the opportunity for authorities to validate the information or ask for additional information at the time of check-in.

In the case of a hit in a database, authorities can also request additional information, which the carriers can collect from the passenger (e.g., resident card number, redress number).

Responses from Authorities–To minimize the operational impact of iAPI programs on carriers and passengers, the CUSRES response provided by authorities will have to be clear, include granularity beyond the OK/Not OK to board, and be accompanied by adequate procedures to handle the different possible responses.

Impact on Passenger Rights–In the case of a “not OK” or “no fly” response, the authorities will also have to provide a contact point and additional information that the carriers' agents can communicate to the impacted passengers. National laws should be clear to the effect that passengers denied boarding following a government's notification via the iAPI process are not eligible for compensation under passenger rights regulations.

3.3.4 Implementation Considerations

When implementing an iAPI system, updates to the existing legal framework and technical specification documents that have been adopted for batch API would be required.

For the regulatory framework, the scope and purpose of the data collection can be expanded due to the interactive nature of the iAPI process. A key point to include in the regulatory framework is the information on the vetting response. Carriers will need a clear legal basis to deny boarding to passengers if a “not OK” or “no fly” vetting response is received. The actions to be taken by carriers for each vetting response need to be specified in the national legal instruments.

With iAPI, states take back the ownership of the decision to allow or not passengers to arrive at their borders. Therefore, airlines should not be exposed to sanctions in the case of inadmissible passengers. Similarly, sanctions related to API data quality should no longer apply since authorities have the possibility to request resubmission of the travel document information. Under iAPI programs, sanctions should be limited only to cases where the data has not been sent, sent in the wrong format, at the wrong time, or if the carrier did not comply with the vetting responses.

Where iAPI systems are in place, no sanctions for API data quality or for inadmissible passengers should be imposed.

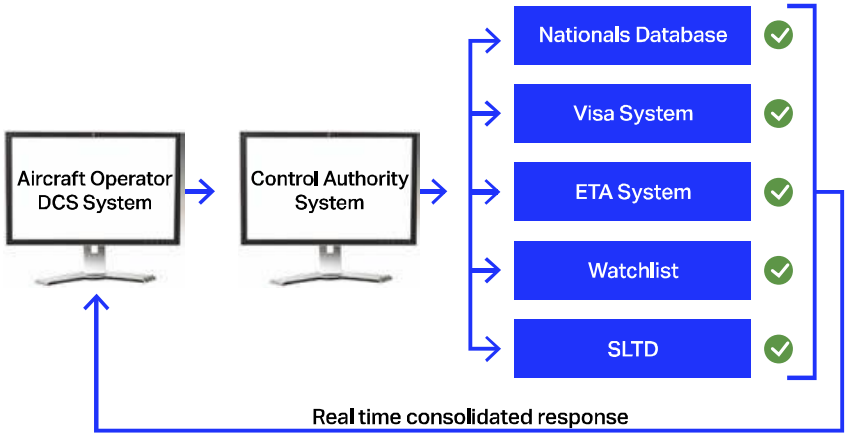
Implementation Guide–The guide developed for the batch API program will have to be amended to include specifications for the format and transfer protocols for the CUSRES message. WCO/IATA/ICAO API Guidelines Appendix IIB provides an example of an implementation guide for the CUSRES message.

Outages Procedures–To avoid paralyzing the airline's check-in process, authorities need to establish in advance, together with the airline, clear procedures in the case of an outage of the system, either on the side of the authorities or on the side of the airlines. Authorities also need to implement a robust IT infrastructure with possible redundancies to ensure continuous availability of their systems.

Connection to Relevant Databases–To guarantee the accuracy of the response provided per passenger through the CUSRES message, checks against all relevant databases should take place in the systems of the authorities. The consolidated response to the carrier would include a vetting process for each type of passenger, whether national, resident or foreign national requiring or not a travel authorization.

For all passengers, checks would include national and international watchlists in addition to the INTERPOL SLTD. For nationals and residents, the national ID and/or passport and/or residence permit databases should be checked to validate the existence of the travel document used. For foreign nationals, when a travel authorization is required, checks against these databases serve to confirm that the passenger is in possession of a valid authorization.

Querying the different databases should be done based on the passport information transmitted by the airline, thereby removing the need to transmit information such as the visa number, as it is readily available in the authority's systems. The following graphic illustrates the different components in authorities' systems to be queried to provide a consolidated CUSRES message:



Timing for Implementation and Communication to Carriers–iAPI systems are more complex to implement both for authorities and carriers, as they need to upgrade their IT infrastructure and adapt some of their operational procedures. A minimum of 12 months should be considered between the adoption of the iAPI requirements by the authorities and the live implementation by carriers.

3.3.5 Impact of iAPI on Other Passenger Data Programs

iAPI programs will provide authorities with passenger travel document information at the time of check-in, which will allow for the vetting of the passengers before they board the aircraft. However, some data elements that are typically included in the PAXLST message will be missing, such as the total number of passengers on board, the passengers who did not board, or possibly the baggage information. As stated above, iAPI systems are also difficult to use for crew, where a batch message might be preferable to take into account last-minute crew changes.

iAPI programs are, therefore, often implemented in conjunction with either batch API programs or requirements to send at the time of flight closure (typically 15 to 30 minutes after flight departure) an additional close-out message confirming the total number of passengers and the list of passengers who boarded or did not board.

For optimal use, the different passenger data programs could be combined as follows:

Timing	-72H/-24H	-24H/-40m	-1H	Flight Closure
Data	PNR	iAPI	Crew API	Close-out message PNR

This approach allows to perform a first assessment of the passengers with the first PNR message, which can also inform the vetting response provided through the iAPI process. Crew can also be vetted through a message sent shortly before departure. A final close-out message, including passengers on board, together with the last PNR push will provide updated information.

4. Path to Modern Border Security

The passenger data programs described in the previous section provide authorities with tools to vet passengers before their arrive at their borders. To ensure both authorities and aviation stakeholders reap the full benefits from these programs, it is essential that they be considered within the wider context of border management tools and programs.

This section covers the different facilitation tools and processes (e.g., travel authorizations, travel documents, airport processes, innovation, digital identity), which, in addition to passenger data programs, can lead to the removal of barriers to travel while increasing border security.

4.1 Modernizing Travel Authorizations

IATA and other international organizations such as ICAO, United Nations World Tourism Organization (UNWTO)[41] and World Travel and Tourism Council (WTTC), among others, promote the removal of barriers to travel to unlock its social and economic benefits. A study by WTTC indicates that a relaxation of visa requirements can lead to an average 16.6% growth in travel demand. Other improvements, such as the introduction of eVisas, result in an 8.1% increase in travel demand.[42]

There are several modern facilitation tools and processes that can perform some of the functions of travel authorizations. Tools and processes available to vet and identify travelers include API/iAPI, registered traveler programs (RTPs), ePassports, digital wallet, electronic declaration, ABC, and biometrics. IATA encourages states to make the best use of these tools and processes to relax their travel authorization requirements to increase their country's attractiveness and competitiveness.

IATA encourages states to make the best use of modern facilitation technologies, principles and processes to relax their visa requirements.

In a complex international security environment, travel authorizations aim to collect information on passengers and perform risk assessment prior to their travel. It remains the sovereign decision of states to impose travel authorizations or not.

Types of Travel Authorizations–When a country imposes visa requirements for specific nationalities or decides that additional information on visa-free nationalities is required, electronic travel systems (ETS) for the issuance of eVisas and electronic travel authorizations (eTAs) are more efficient, from a facilitation and border control perspective, than traditional counterfoil or stamp visas. However, ETS imply the roll out of an iAPI system, which is complex and costly. Online application and/or issuance facilitate the obtention of a visa, but they present challenges for their verification. Lastly, issuance of a visa upon arrival (VUA) undermines the passenger experience and border security, though it might prove useful when visas upon departure are difficult to obtain. The five types of travel authorizations presented in this section are generic and national variations do exist.

[41] *Travel Facilitation*, UNWTO: https://www.unwto.org/sustainable-development/travel-facilitation.

[42] *Visa Facilitation–Enabling Travel & Job Creation through Secure and Seamless Cross-Border Travel*, WTTC, August 2019: https://www.wttc.org/priorities/security-and-travel-facilitation/visa-facilitation/.

Leveraging Travel Authorizations:

- IATA and other international organizations invite states to consider removing barriers to travel such as travel authorizations to unlock the social, political and economic benefits of travel.
- The efficient use of border security and facilitation tools such as API, RTPs, ePassports, ABCs and biometrics can eliminate the need for travel authorizations.
- When travel authorizations are required, an ETS can have more security and facilitation benefits than traditional visas, online visas or VUA, in addition to enhancing a country's attractiveness.
- When implementing modern travel authorizations, consideration should be given to their integration with a contactless travel environment.

Adopting the Right Solution–Countries are increasingly moving away from conventional visas and adopting electronic solutions such as online application/issuance and the more complex ETS. There are three broad processes associated with travel authorizations:

- Lodgement (or application)
- Acceptance (or issuance)
- Verification

While application and issuance are transactions taking place between passengers and authorities, the verification is also of concern to airlines, which have to verify that passengers are properly documented to be admitted to the country(ies) they are travelling to or transiting through (see section 2.1.1). These three processes are either performed manually, semi-automated or fully automated depending on the type of travel authorization.

Each jurisdiction has a different travel authorization regime, which can variably be composed of visa-free for certain nationalities, visa required for others, and increasingly eTA for nationalities that are visa-free. The decision to not impose, remove or to require a travel authorization for specific foreign nationalities mainly depends on external relations, national facilitation, and security objectives. Other drivers for this decision include:

- Tax collection and/or statistical purposes.
- Whether or not the information required in advance can be obtained through existing mechanisms.
- Bilateral arrangements.
- Regional free movement zones.
- Whether or not the cost of the travel authorization reduces the attractiveness of a country and impacts tourism.

Authorities are, however, increasingly applying a 100% travel authorization regime where all foreign nationals–generally excluding those that possess residency rights–must obtain a form of travel authorization prior to travelling. This is notably the case of Australia, Canada, the United States and, shortly, countries of the Schengen Area.

Each type of travel authorization carries different benefits and challenges for countries, airlines and passengers. These benefits and challenges can be looked at from different angles: passenger facilitation, border security, operations, resources and costs, and their possible integration with seamless and contactless solutions.

4.1.1 Visa-Free Regime

A visa-free regime is the most favorable to the free movement of people, trade, travel and tourism, and is applied to nationals from countries that are considered low risk. These arrangements are usually taken on a bilateral or regional basis and consider factors such as diplomatic relations, historical and economic ties, low-risk nationals as well as tourism and business.

Passenger Facilitation–Travelers can freely move across borders without the need to undertake steps to comply with entry requirements of the transit or destination countries. The process at the airport is fast, smooth and hassle-free.

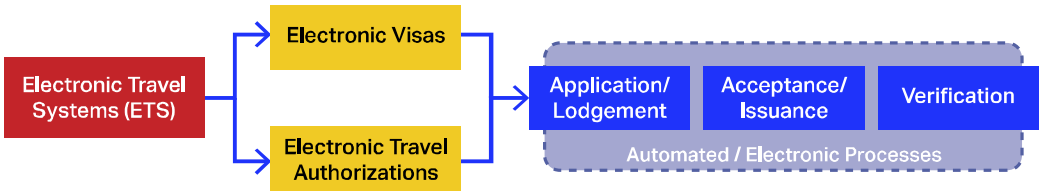
Border Security–Although no travel authorization is required, the country may use other tools to identify travelers and perform their risk assessment. API, PNR and RTPs data enable this identification and risk assessment prior to arrival. Enhanced identification of travelers can be achieved using ABC gates and biometrics upon arrival.

Operations, Resources and Costs–Resource needs and costs mainly emanate from the collection of passenger data and the modernization of entry controls, such as ABCs. From an airline's perspective, no additional controls or verifications are needed on passengers and the use of online/mobile/self-service check-in can be fully leveraged. Processing these passengers requires minimal resources.

Contactless–Visa free travelers could use contactless processes and tools.

4.1.2 Electronic Travel Systems

ETS are integrated systems used for the application, acceptance and verification of eVisas and eTA. ETS expedite the pre-vetting and acceptance of passengers into a country, while providing a secure method for applicants, governments and airlines to confirm authorization for travel. A section in Chapter 9 of ICAO Annex 9 is dedicated to ETS. The definition stipulates that the three processes related to travel authorizations must be automated.



Although the objectives sought with eVisa and eTA are different, key considerations for their application and verification processes are similar.

- **eVisas** expedite the risk assessment and acceptance of passengers. A passenger who requires an eVisa is not eligible to an eTA. eVisa programs are a direct replacement for traditional paper visas. Although the application process is simplified with the online application and issuance, the vetting of the application is conducted by a government official.
- **eTAs** expedite the pre-vetting of visa-free foreign nationals. Processing eTA applications does not usually require the intervention of government officials. The vetting is performed automatically by the country's border control system according to a set of watchlist rules. For some countries, the response can be delivered to the passenger in a few minutes.

While the application and issuance are performed relatively easily online, the automation of the verification process is performed through an iAPI system (Annex 9 Recommended Practice 9.17). The automation of the three processes unlocks tremendous facilitation and border security benefits for states, passengers and carriers. However, iAPI systems are extremely complex and quite expensive to set up and maintain (see section 3.3). There are currently fewer than 10 countries worldwide that have rolled out an ETS with iAPI integration.

Passenger Facilitation–Travelers apply online (up to a few hours prior to their departure in the case of eTA) and receive the notification electronically. The facilitation benefits are tremendous compared to a traditional visa that must be applied for in person at an embassy, a consulate or by postal mail. Travelers do not need to carry any proof of possession of the authorization given that its presence in the transit or destination authority's database is confirmed automatically through iAPI upon check-in.

eTAs apply to visa waiver foreign nationals; therefore, to persons who were previously traveling without a travel authorization. Introducing a new travel requirement necessitates building public awareness, prior to its effective date, with a clear and comprehensive communication campaign.

Border Security–With an iAPI system, the travel authorization database of the destination or transit countries are queried at check-in, and the instant board/no board message sent to the carrier confirms that each passenger requiring travel authorization has been granted such authorization. This query process is made on national travel authorization databases along with other databases such as national watchlists, international watchlists, INTERPOL SLTD, etc. States are, therefore, in complete control of determining the identity and eligibility of each passenger.

Operations–The iAPI CUSRES response should provide more granularity than a simple OK/NOT OK to board message to enable airlines to troubleshoot with their customers. Authorities should introduce a 24/7 support line that helps airlines in cases of boarding issues as well as a dedicated 24/7 hotline to assist passengers with their application.

Resources–The application and issuance processes for eVisa and eTA are cheaper for states than traditional visas where a diplomatic network abroad must be maintained. Despite the complexities and costs related to iAPI for both airlines and authorities, significant border control and security benefits can be achieved as it reduces close to nil the instances where inadmissible passengers are transported. However, the expertise and cost of setting up and maintaining the iAPI system are significant. This advanced border control tool is not advisable for all states.

Contactless–Given that all the processes of an ETS are performed automatically and electronically, this solution is readily contactless. ETS can be easily integrated in off-airport processes and self-service options within the airport environment. Interventions of border security and carrier staff is required only in the case of a NOT OK to board CUSRES message.

4.1.3 Online Application and/or Issuance of Travel Authorization

Not all states have the resources and expertise to roll out an iAPI system. Instead, to modernize their travel authorization regime, over 40 states have implemented a travel authorization system where the application and/or issuance are performed online. Passengers are required to travel with a printout of their travel authorization. While this mix of electronic and manual processes can facilitate the obtention of visas, the verification process by airline staff is cumbersome.

Passenger Facilitation–Similarly to ETS, travelers apply online and/or receive the notification electronically; therefore, the in-person process at a diplomatic representation can be avoided. Visa issuance can take a few days. Travelers are also required to travel with their visa printout. Because airline staff have to visually verify a printout, travelers cannot use self-service check-in kiosks or online/mobile check-in options. Passengers who do not carry their printout need to find a facility nearby to get their document printed. This requires time and explanation from airline agents who have to deal with upset passengers.

Border Security–Airline staff perform a visual verification of the printout. Border authorities verify this same printout and, where they have access to their government's database, they may retrieve the electronic record of the submission. Holders of such travel authorizations are already known to border authorities given the risk assessment that has been performed to issue the authorization.

Operations–Visual verification of the printout by airline staff at the airport check-in extends this time-sensitive process. The aviation industry is working toward the removal of staffed check-in desks at airports. This type of travel authorization in its current form does not readily integrate with self-service facilities and modern processes.

While IATA fully supports the implementation of systems that enable electronic authorization to travel, authorities should not introduce noninteroperable solutions.

Due to the absence of reliable means to verify printouts, carriers cannot be held liable for any passenger who is found inadmissible for an absent or invalid visa printout (these can be easily forged). Airline staff can only apply due diligence in verifying that the printout seems to belong to the passenger and that it is apparently valid for travelling.

To address this verification challenge, some countries have proposed solutions for carriers to make a query on a web-based portal for each passenger who must hold such an authorization. This solution is neither sustainable nor viable in an airline operating environment. Most carriers' check-in counters are not equipped with Internet access. In the rare event where such a connection exists, making a web-based query for each authorization holder would stretch the time-sensitive check-in process beyond what is available.

Resources–Similarly to ETS, the online travel authorization application/issuance enables governments to save costs related to maintaining a diplomatic network abroad. However, the absence of reliable verification means that airlines may potentially carry improperly documented travelers and have to deal with inadmissible persons upon arrival, which is a burden for both authorities and airlines because of incurred costs and additional resources. ETS and traditional visas provide a higher level of confidence that the passenger's authorization has been appropriately vetted.

Contactless–This type of travel authorization prevents the use of mobile or self-service check-in. With the new reality of COVID-19, long queues at airport and exchange of documents between persons must be reduced. The manual processing that occurs at airports with the visa printout, traditional visas and VUA calls for these type of travel authorization to be modernized and automated to address health risks.

4.1.4 Traditional Visas

Traditional visas are the most cumbersome processes for passengers, and they induce the most barriers to trade, travel and tourism. They are generally required for the following reasons:

- Nationals of countries considered high risk
- Where travel documents may be more easily forged
- Implemented as part of a reciprocity policy

The application and issuance of traditional visas are performed in person at an embassy, consulate or by postal mail. The verification is performed visually by airline staff or semi-automated through a swipe. The technical specifications for machine-readable visas are set forth in ICAO Doc 9303 MRTDs.

Passenger Facilitation–The time, cost and effort involved in obtaining traditional visas can deter travelers from visiting certain countries. IATA strongly encourages states to reconsider the necessity of imposing traditional visas since verified information on passengers is increasingly becoming available early in the journey with API and PNR assists for the risk assessment.

API and PNR already contain an important number of datasets that, when efficiently used, may reduce the need for travel authorizations.

Passenger processing is increasingly automated. Manually checking a counterfoil or stamp visa or swiping a visa's MRZ interrupts this flow, decreases the passenger experience, and prevents the use of online and self-service applications. On the other hand, technology is now supporting the electronic capture of the information through optical character recognition (OCR) for ICAO-compliant visas.

Border Security–When the risk is considered high, traditional visas allow additional screening measures such as face-to-face interviews.

Operations–While there is a wide variety of security features available to protect visas, a counterfoil or stamped visa can still be forged, which can result in transporting an improperly documented traveler.

Resources–For passengers, the application for a visa is time-consuming and difficult to obtain, especially when diplomatic representation or a third-party visa application center are not available locally. For countries, maintaining a diplomatic network abroad is resource-intensive (i.e., infrastructure, resources, personnel).

Contactless–Traditional visas are an entirely manual process or can be semi-automated (swipe of the visa's MRZ). As government portals and digital identity wallets develop, OCR technology should be used to extract the information contained on the visa and simplify the verification process for airlines and border authorities.

4.1.5 Visas Upon Arrival

VUA are less and less common and are not effective from a facilitation and security standpoint. States may consider other means to meet their objectives sought with VUA.

Passenger Facilitation–In an era when the focus is on providing a seamless experience for passengers, queuing to obtain their visa at arrival hampers their experience. Nevertheless, this process has value where the process on arrival is effective. The obtention of the visa is also less cumbersome than when traditional visas are required, although passengers should be well informed of the documents required.

Border Security–Information collected while the passenger is already at the border does not allow for a risk assessment comparable to a visa obtained in advance. This is particularly true when an API system is not in place.

Operations and Resources–Just like for visa-free passengers, from an airline's perspective, no additional controls are needed on passengers and the use of online/mobile/self-service check-in can be leveraged. Processing these passengers requires minimal resources. However, more border staff is needed at the entry point to deliver the visas.

Contactless–VUA are manual processes and require an exchange of paper documents between passengers and the border authorities. Therefore, this type of travel authorization is less appropriate where health considerations are of primary importance.

4.2 Leveraging the Modernization of Travel Documents

All programs covered in this manual rely on the accuracy of biographic and biometric information which travel documents contain. The most widely accepted forms of identity documents used for international travel are MRTDs and eMRTDs (commonly referred to as ePassports). ICAO sets the technical specifications in ICAO Doc 9303[43], which enable the standardization of travel documents, increase their security and lay the foundation for system interoperability.

The biographic and biometric data contained in passports are the inputs for many authority and aviation stakeholder processes: API, PNR, RTPs, travel authorizations, watchlist screening, manual and automated border controls, airport security access, among others.

A secure and trustworthy travel document provides border authorities with reliable identity information. However, these travel documents can only be as secure as the underlying processes for their application and issuance. Additionally, the physical and electronic security features that a travel document contains build the trust that countries and aviation stakeholders will place in them. A robust national travel document and the efficient use of the data it contains can lead to the elimination of manual and duplicative processes.

Leveraging Travel Documents:

- Robust national identification management and issuance processes of travel documents as well as security features and interoperability of these documents increase the trust and facilitate travel for the country's citizens.
- eMRTDs or ePassports are the most robust travel documents and they can leverage the possibilities for biometric innovation and seamless travel.
- Elimination of manual and redundant processes becomes possible with secure and reliable travel documents.

4.2.1 National Identification Management and Travel Document Issuance Process

The security of travel documents starts with the processes to establish and verify a person's identity, which will be reflected in the travel document. Robust national identity management gives the assurance that the authenticity of the identity of each national can be established. Uniquely identifying individuals is central to the ICAO TRIP Strategy and guidance is made available for states to assess their evidence of identity context.[44]

[43] *Machine Readable Travel Documents*, Doc 9303, Seventh Edition, ICAO, 2015: https://www.icao.int/publications/pages/publication.aspx?docnum=9303.

[44] *ICAO TRIP Guide on Evidence of Identity*, Version 5.3, ICAO, May 2018: https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20Guidance%20on%20Evidence%20of%20Identity.pdf.

Nowadays, travel document security features have reached levels that make them difficult to forge or falsify. Enrollment and issuance processes, therefore, remain the soft target that can lead to obtaining genuine travel documents illegally. ICAO provides guidance for states to strengthen these processes.[45]

A country having the reputation of rightfully delivering breeder documents (i.e., a document that serves as a basis to obtain other identification documents, such as a birth certificate) and securely handling and issuing its travel documents will gain international trust in the integrity of its national documents. The nationals from such jurisdictions can expect more facilitation measures when crossing borders, such as being exempted from visas and entitled to use ABC, thereby improving their traveling experience and enabling the industry to guarantee minimum border crossing times.

On the other hand, a jurisdiction that struggles to identify its nationals will negatively impact the trust placed by other jurisdictions in its national travel documents. Third countries may decide to impose additional measures and controls on these nationals, such as a stringent visa application process, restrictions on the purpose and length of the stay or transit, or additional screenings at arrival.

4.2.2 Interoperability of Passports and Security Features

The automation of processes and the interoperability of the systems used by all stakeholders in the travel continuum depend on the compliance of travel documents with the technical specifications of ICAO Doc 9303. Such conformance makes it possible to capture the data fields by electronic means (e.g., machine reader, keyboard swipe, kiosk, mobile application) without the need for manual interventions.

Facilitation–The electronic capture of data has led to great improvements in efficiently processing passengers over the years, and governments around the world and the industry continue to improve with further automated, touchless, biometrically-enabled and self-service processes. All these processes use travel documents as their main token and rely on their capability to be machine-readable or for the data to be extracted from the integrated circuit (IC) chip in ePassports.

Secure and interoperable travel documents are a pillar of border security.

Problems swiping the MRZ, reading the full data page or extracting the data from the IC chip of ePassports trigger manual interventions. Manually typing the data from the travel document lengthens passenger processing and inevitably leads to errors and typos. Additionally, this can deteriorate the identity information provided by the airlines to border authorities through API, which can lead to penalties for carriers. Erroneous identity information, in turn, weakens the risk assessment performed by border authorities when watchlists and databases are checked.

Verification and Authentication of Travel Documents–Physical security features are found throughout travel documents. Basic security features enable the manual and visual inspection of travel documents, without specialized equipment. Upon receiving a basic training, different stakeholders, including airline staff, are able to verify the authenticity of travel documents and identify impostors. This verification is part of the DOC Check responsibility of carriers (see section 2.1) and contributes to identifying improperly documented passengers.

[45] *Guide for Assessing Security of Handling and Issuance of Travel Documents*, ICAO, 2016: https://www.icao.int/Security/FAL/TRIP/Documents/Guide%20Part%201%2c%202%20and%203.%202016NA.pdf.

The inspection of more advanced physical security features is typically performed by border authorities. It requires equipment that ranges from basic (i.e., optical-electronic readers used by frontline officers) up to forensic, in the case of suspected fraud investigations. This equipment, coupled with a deeper training, enable border authority staff to authenticate a travel document and make the determination whether or not to admit a traveler.

Another tool at the disposal of border authorities to enhance their risk assessment is the use of the INTERPOL SLTD that compiles travel documents reported as stolen, blank, lost and/or revoked. Border authorities screen this database, using the passport type and number sent through the API message, along with national and international watchlists, to enhance the risk assessment of each traveler in advance of their arrival.

Despite the availability of an interface for airlines to access the INTERPOL SLTD, the I-Checkit, the solution has had no uptake. The risk assessment performed on travelers is the responsibility of border authorities and asking carriers to check this database is duplicative and goes beyond their responsibility. The liability of carriers toward a passenger whose travel document receives a positive hit on the INTERPOL SLTD could be put at risk. Denying boarding to a passenger based on such a failure or hit without further analysis could damage the carrier's reputation.

Airlines are in the business of securely, safely and efficiently transporting people. They cannot substitute authorities responsible for assessing the risks of travelers or establishing the validity of travel documents presented.

The detection of fraudulent or tampered with documents and impostors is increasingly performed automatically, particularly with the important uptake of ePassports in the past 20 years.

4.2.3 ePassports

While great efficiencies were gained with MRTDs, both for border security and traveler facilitation, the introduction of eMRTD contributes to the removal of the need to manually inspect travel documents. The digitized traveler's biographic and biometric data (the facial image being the primary biometric identifier) is stored in an IC chip embedded in the booklet. The data and facial image stored have a better quality that those printed on the visual inspection zone (VIZ), helping both the industry and border authorities implement biometric and contactless solutions with a higher level of trust throughout the traveler's journey. There are currently 140 countries that claim to be issuing ePassports[46].

The biographic information contained in the IC chip of ePassport enables carriers and their partners to obtain identity information of greater quality at check-in when a mobile application is used or at off-airport or at the airport's self-service kiosks. This enables a higher level of API data quality for transit/destination authorities to proceed with the identification of travelers.

[46] *Development of an ePassport Standard Roadmap*, Working Paper/11, 11th Meeting of the Facilitation Panel, ICAO, 2020: https://www.icao.int/Meetings/FALP/Documents/FALP11-2020/FALP11.WP11.ePassport%20Roadmap.pdf.

Authentication of ePassports–The most significant advantage of ePassports is that it can be digitally authenticated, enabling the biographic and biometric data read from the chip to be relied on in processes that automate document and identity verification. For border authorities, an ePassport is the most secure identity document. With the right authentication architecture, the Public Key Infrastructure (PKI), fraudulent documents or documents that have been tampered with can be more easily detected. The process to determine the authenticity and integrity of an ePassport is by verifying the digital signature on the IC chip. The authentication of ePassports is ensured through publicly available digital signature master lists or through the ICAO Public Key Directorate (PKD). The ICAO PKD facilitates the sharing of these certificates between states.[47]

As stakeholders worldwide are making a shift from the traditional means for identifying individuals toward digital means, ID management service providers are on the rise, helping governments and airlines manage digital identities. There is increasing recognition that extending the ICAO PKD for commercial use could add value in securing the travel continuum through more robust advance risk assessment and intercepting inadmissible passengers early. Indeed, multi-stakeholder partnerships and process streamlining are part of the framework for modern facilitation and border security arrangements such as the one proposed by One ID (see section 4.4).

Biometric Touchpoints–The better quality of the image in ePassports eases the deployment of automated touchpoints by both the industry and border authorities. ABC can be used without the need to obtain images for 1:1 biometric matching elsewhere than the ePassport itself (which is not possible with MRTDs only). The efficient use of API data and the authentication of ePassports through notably the ICAO PKD can contribute to extend the use of ABC gates beyond the national population. Indeed, when an ePassport is authenticated, the facial image stored in the eMRTD can be trusted to match a live captured biometric of the passenger. This helps reach the arrival processing KPI (see section 2.1.2), which benefits airlines, airports, travelers and border authorities.

The combination of API and authentication of ePassports can lead to extending the use of ABC beyond the national population.

Digital Travel Credential–More efficient exchange of biographic and biometric data across many stakeholders, in accordance with data privacy and consent principles, will be possible with the next generation of travel documents, the DTC. The DTC is a digital representation of the traveler's identity that is meant to substitute a conventional passport temporarily or permanently. It will contain the same data as the ePassport's IC chip and will be as secure.

The first type of DTC is bound to the eMRTD and will be derived from an existing document. The first set of technical specifications[48] for this DTC was endorsed by ICAO Member States in 2020.

With the digitalization of ePassport data, holders will be able to send their information in advance into the travel ecosystem, which will enable authorities to perform their risk assessment based on a verified identity much earlier than the current process. As such, a DTC could be used even at the time of booking or when

[47] *ePassport Basics*, ICAO: https://www.icao.int/Security/FAL/PKD/Pages/ePassportBasics.aspx.

[48] *Guiding Core Principles for the Development of Digital Travel Credential (DTC)*, ICAO, October 2020: https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Guiding%20core%20principles%20for%20the%20development%20of%20a%20Digital%20Travel%20Credential%20%20%28DTC%29.PDF.

applying for a travel authorization. The DTC will further ease the implementation of touchless processes and will enable the development of truly seamless travel frameworks, such as proposed by the IATA One ID program (see section 4.4).

4.3 Path to Modern Airport Processes

Historically, border controls at the airport relied on manual processes involving border officers performing their duties at checkpoint desks. In this legacy process, each passenger is processed sequentially and depending on the sub-processes needed to enforce the level of border security required by the regulator (e.g., travel document verification, interviews, biometric acquisition and/or verification), the processing time for each passenger could be significant.

To limit the waiting times at the border in such deployment, the only option available is to increase the number of desks and border officers. However, this solution is limited by the increased staffing cost and footprint that can be allocated to border control processes in the airport premises. Additionally, adding staff may be inefficient overall if the peak times are very limited throughout the day. The features of modern processes enable a rethink of how border controls are currently implemented at airports and to focus on improving their effectiveness and efficiency, while enhancing the passenger experience.

Automation of routine manual processes allows border officers to focus on more added-value tasks. Automation is achieved with tools such as ABC gates, kiosks for data collection/biometric collection, and web-based solutions/apps for early data collection. When automated processes are in place, the eligibility criteria to use them should be expanded to as many passengers as possible. Advance processing of passenger information allows the pre-vetting of passengers and allow them to use automated processes if they are identified as low risk. Deployment of automated solutions at the airport should be made through careful planning, cost benefit analysis and use of existing best practices.

4.3.1 Implementation of Automated Processes

Passenger data programs enable data to be collected and analyzed by border and security authorities ahead of the passenger's arrival at the border, which opens the possibility of clearing the border formalities using automated processes instead of a resource-intensive manual process for each passenger. ABC tools perform similar tasks as those of a manual control, ensuring at least that travelers are carrying a genuine and valid travel document, that this document belongs to them by verifying their identity biometrically, and that they are allowed to cross the border based on a predefined logic.

The introduction ABC systems is a Recommended Practice of ICAO to facilitate and expedite the clearance of persons entering or departing by air (Annex 9 Recommended Practice 3.34.4). The European Border and Coast Guard Agency (Frontex) has also published best practice guidelines for technical considerations and options for deployment of ABC systems[49].

[49] *Best Practice Operational Guidelines for Automated Border Control (ABC) Systems*, Frontex, 2016: https://frontex.europa.eu/publications/best-practice-operational-guidelines-for-automated-border-control-abc-systems-WJLwNL.

Introducing Modern Airport Processes:

- The collection of passenger information in advance allows for the pre-vetting of passengers and should lead to the deployment of ABC processes to facilitate the border crossing for identified low-risk passengers.
- Eligibility to use ABC processes should be extended beyond the country's nationals to maximize the efficiency of controls at airports.
- Biometric-enabled touchpoints enable higher trust in determining passengers' identity while enabling a more seamless process for passengers who normally must present different travel documents to multiple stakeholders.

ABC tools could be implemented in the form of hardware deployed at the border checkpoint (e.g., kiosks, gates). They could also consist of nonhardware processes (i.e., web-based solutions, mobile apps) that allow passengers to begin the process of crossing the border before they reach the checkpoint itself.

Other Automated Processes–As technology evolves, mobile solutions can be used to facilitate the crossing of borders and streamline the flow of travelers. Solutions such as Mobile Passport Control in the US, for instance, allow arriving passengers to use apps on their smartphone or tablet to submit their passport information and answer inspection-related questions prior to the border check. By successfully using such apps, passengers no longer have to fill in a paper-based form or use kiosks upon arrival. This enables authorities to perform several checks against relevant databases ahead of the passenger's arrival at the border checkpoint (manual or ABC), thereby speeding up the overall process.

App-based solutions also provide an additional layer of flexibility to authorities who may easily update interfaces to adapt questionnaires to specific needs. This may be particularly useful, for instance, when requiring passengers to provide information on their travel history and/or contact details for during their stay.

4.3.2 Eligibility Criteria

Experience from deployment of ABC processes around the world reveals that authorities tend to restrict the usage of these processes to a limited subset of the traveler population (e.g., their nationals). To maximize the benefits of ABC tools, IATA invites authorities to include as much of the traveling public possible into the pool of eligible passengers.

While authorities are ultimately responsible for enforcing the required security level at their border, limiting the volume of passengers eligible for the ABC process limits the associated benefits (e.g., more efficient use of border staff, passenger experience, capacity improvement, cost reduction). Maintaining an adequate border security level while pursuing the objective of expanding the eligible pool of passengers could be achieved by leveraging the biometric data contained in eMRTDs' IC chip for matching with the biometrics captured at the gate/kiosk and/or performing early risk assessment through the use of API and PNR data as well as information obtained via eTA.

To maximize the facilitation benefits and improve the business case for ABC process implementation, authorities should consider expanding the pool of the eligible population.

Early Risk Assessment–States are encouraged to incorporate the results of the risk assessment performed based on passenger information received in advance in the border controls performed at the airport. Often, different authorities are processing this passenger data, without communicating the outcome of their assessment to border authorities. Building greater synergies between national agencies triggers more efficient controls upon arrival at the destination airport.

The results of the processing of passenger data in advance should be efficiently used to adapt the controls performed on passengers at the border control points.

The result of this pre-vetting could help guide the passengers to different lanes and help better manage queuing at the border control points. The use of mobile apps or preregistration kiosks can be used to that effect.

4.3.3 Deployment at the Airport

While airports may not be at the forefront of the development of border security measures, they still have an important role to play and should be closely consulted, together with airline stakeholders, to ensure a smooth implementation of new requirements.

As discussed in section 2, MCT is a key factor in the commercial strategies of network carriers. Successful strategies attract international connecting traffic, which directly benefits both the hub carrier and the airport. Additionally, time spent by passengers in the departure gate area has been proven to translate into increased nonaeronautical revenue for the airport. As a result, facilitating passenger flows throughout the airport terminal has become a priority for airports and strongly influences the way airports are organizing and adapting their infrastructure.

In this context, IATA encourages airports to adopt level of service (LoS) best practices[50] as a basic airport planning tool. The LoS framework provides key metrics in terms of space, maximum waiting time, and seating or occupancy in the following areas:

- Public departure hall.
- Check-in area, including self-service kiosks, bag drop desks/units and traditional check-in desks.
- Security control.
- Emigration control.
- Gate hold rooms and departure lounges.
- Immigration control.
- Baggage reclaim.
- Customs control.
- Public arrival hall.

[50] *Level of Service (LoS) Best Practice,* IATA: https://www.iata.org/contentassets/d1d4d535bf1c4ba695f43e9beff8294f/airport-development-level-service-best-practice.pdf.

Border and customs authorities are also invited to take these guidelines into consideration when developing and implementing control areas at airports. In addition to employing planning tools like LoS, airports, airlines and authorities sharing the airport facilities are also encouraged to adopt service level agreements (SLAs)[51]. An SLA provides a framework defining key performance measurements and service standards to be delivered by the airports. SLAs typically define acceptable waiting times at security and border controls. Failure to meet the requirements and/or standards outlined in an SLA may result in financial penalties being levied against the airport.

It is, therefore, in the interest of airports to ensure border controls remain efficient and that the infrastructure provided is sufficient for the types of controls required. The implementation of new equipment and/or infrastructure, such as pre-enrollment kiosks or automated border gates, needs to be done in collaboration with the airports. Similarly, changes to border control processes need to be discussed in advance with the airport community to facilitate necessary planning, infrastructure restructuring, and passenger flow management adjustments.

Airports, airlines and border authorities should negotiate SLAs to ensure border controls do not constitute a bottleneck in airport operations.

It is also of utmost importance to ensure the deployment program can deliver the benefits that are envisioned. Any airport deployment of modern border control capacities should be based on a strong business case incorporating the input from the different stakeholders.

4.3.4 Registered Traveler Programs

RTPs are voluntary programs, generally aimed at frequent travelers, that allow individuals to be pre-vetted before arriving at the border. This preassessment, via a thorough background check against relevant databases as well as the advance collection and verification of nationals and in some instance foreigners' biographic and biometric data. RTPs can help expanding the population eligible to use ABCs beyond the country's citizens.

RTPs require some additional resources from authorities, as they need to set up registration and preassessment facilities, either at the airport or in their consulate. However, in countries with high numbers of cross-border commuters and/or frequent business travelers, these programs can be very beneficial in speeding up border checks for visa-exempt foreign nationals.

API and PNR data should also be used for the continuous vetting of RTP members to enhance the security of these programs.

RTPs are generally granted for a duration of several years. To maintain the integrity of this program, in addition to the initial background check, authorities will also need to perform continuous vetting of the members to identify any change in the security profile of the individual. API and PNR data can usefully support this continuous vetting process. The collection of API data whenever the passenger travels allows for a regular matching against the relevant databases and the analysis of PNR data can feed the continuous risk assessment.

[51] *Airport Service Level Agreement (SLA)–Best Practice*, IATA: https://www.iata.org/contentassets/4eae6e82b7b948b58370eb6413bd8d88/airport-service-level-agreement.pdf.

4.4 Innovative Processes and Digital Identity

The industry is currently advocating for more innovation in the area of border controls and passenger facilitation. Innovation is needed as traffic volumes pick up again but also to support new health requirements. The planned transformation of air transport processes will be increasingly digital and rely on advanced technologies. States, airlines and airports should take into account these future evolutions to design future-proof border control processes.

In particular, the use of a trusted digital identity will not only facilitate progress in terms of speed and ease of identity authentication and verification, it will also allow passengers to assert their identity online early in their travel journey. This opens the possibility of moving more processes off-airport and having passengers arrive at the airport ready to fly. Ideally, travel authorizations will be associated with the digital identity, removing in the longer term the need for passengers to carry physical ID and travel documents with them.

The digital identity could be stored on a cloud-based digital platform or on a mobile device or physical token. The availability of biometric sensors on customer mobile devices could present an opportunity to make use of these smart devices instead of expensive, static airport infrastructure.

IATA encourages governments to provide DTC (see section 4.2.3) to their citizens as this would enable passengers to provide validated identity information at the time of booking, check-in or whenever required.

4.4.1 New Experience Travel Technologies

Increased industry innovation is reflected in the industry-wide vision, jointly developed by IATA and ACI, reflecting best use of New Experience Travel Technologies (NEXTT). This initiative aims to:

- Create industry-level consensus on the concepts for future airports.
- Determine research and development, standardization and/or regulatory development needs.
- Roll out work streams to facilitate making concepts a reality.

To support these efforts, NEXTT investigates how passengers, cargo, baggage, and aircraft move through the entire journey, with a focus on three emerging themes:[52]

1. **Off-Airport Activities:** NEXTT explores the possibilities of transferring onsite processes off-site, such as security processing and baggage check and drop off, to streamline the airport experience.
2. **Advanced Processing Technology:** NEXTT investigates how advanced processing technology, such as tracking and identification technology, automation and robotics, can improve safety, security, the customer experience and operational efficiency.
3. **Interactive Decision-Making:** NEXTT promotes the better use of data, predictive modelling and artificial intelligence to facilitate real-time decision-making, a key element in improving the passenger experience and optimizing operational efficiency.

[52] *NEXTT Let's Build the Journey of the Future*, IATA: https://nextt.iata.org/en_GB/.

These three emerging themes are key to unlocking the full capacity of existing aviation infrastructure. This industry transformation will produce benefits in terms of a reduction in the need for infrastructure investment, resulting in the generation of tangible cost savings. It will also address the need for improvement in operational efficiency for processing passengers. This translates into increased throughput and more visibility of both the baggage and passenger journeys, which in turn could also support states to control their borders more effectively and efficiently.

In addition to operational benefits, off-airport baggage processing will generate richer passenger baggage data earlier in the process, increasing the quality of authorities' risk assessment. Practical steps have already been taken in the implementation of the NEXTT baggage journey, notably with the development of Baggage XML.[53] Baggage XML is a modern baggage messaging standard being developed by IATA. The implementation of this new standard is an important step toward the key principle of harmonization (see section 1.1) and is also necessary to support system integration and innovation. It would allow authorities to perform better assessment in advance and improve cooperation with their counterparts in the detection of illegal trafficking, while facilitating customs controls at transit or destination.

Off-airport processes will allow authorities to receive more complete data at an earlier point of the passenger's journey.

The passenger journey envisaged by NEXTT will allow airports, airlines, and governments to have an earlier access and improved information exchange relevant to their respective processes. Early collection and analysis of passenger data allows airlines to confirm directly with governments that passengers have the required travel authorization and are approved for travel on a specific day/trip. iAPI programs (see section 3.3) are an important step in this direction. Deployment of biometric technology across the passenger journey promises to further increase the effectiveness and efficiency of identity confirmation, walking-pace processing and passenger tracking throughout the journey. The IATA One ID program is a cornerstone of the NEXTT vision for the passenger journey.

4.4.2 One ID

The IATA One ID program seeks to alleviate one of the greatest points of friction along the passenger journey: the need to produce travel tokens (e.g., passports, boarding passes, travel authorizations, health credentials) multiple times to satisfy the requirements of different stakeholders (e.g., airports, airlines, border control and immigration authorities). Information is not typically shared among these stakeholders, which leads to repeated requests and verifications of travel tokens. The timing and type of travel token required can also differ significantly from airport to airport, further complicating the issue.

From an operational point of view, presentation and verification of travel tokens are time consuming and resource intensive in terms of both staffing and footprint required to run the process. The current fragmented approach will rapidly become unsustainable as traffic volumes pick up again and new and reinforced health measures will call for an increasingly touchless passenger journey.

[53] *Modern Baggage Messaging*, IATA: https://www.iata.org/en/programs/ops-infra/baggage/baggagemessaging/.

The One ID program generates specific benefits related to border processes:

- Verified identity information on passengers will be available at the time of booking, or shortly afterward, allowing for early transmission of data to authorities.
- Increased data quality will make risk assessment more robust and reduce the risk of fines imposed on airlines due to incomplete or incorrect information.
- Early verification of the traveler's credentials will allow passengers to arrive at the airport ready to fly, without having to go through additional checks.
- Creation of accurate biometric exit and entry records, which could potentially eliminate the need for exit border checks.

One ID is bringing substantial benefits to governments, one of them being the enhancement to the quality of the data collected at an earlier phase of the journey.

The concept of having passengers arrive at the airport ready to fly encompasses the following steps:

- The passenger's border control formalities have been cleared by the appropriate authorities of the requiring state(s).
- The passenger has confirmed intent to travel on a specific flight on a specific date and time, with or without bags, and has obtained acceptance status from the airline.
- The passenger's identity has been authenticated.
- The authenticity of the passenger's identity document/credential has been validated.
- The passenger has submitted biometrics such that the passenger can be biometrically recognized at subsequent touchpoints.
- The information is secured and can be trusted by border authorities and/or other government agencies.

The cornerstone of One ID program is the introduction of a robust, integrated identity management process implemented across an end-to-end biometric passenger journey. It relies on the following four elements to ensure it is effective, efficient and secure[54]:

- **Trusted Digital Identity:** ascertaining that the passenger is who they say they are and requiring 1-to-1 matching of the passenger against a verifiable source.
- **Identity Management System:** a service that manages the identity information needed for the facilitation of passengers throughout their journey, such as on-airport control points where biometric identification and/or access authorization is required.
- **Identification through Biometric Recognition:** 1-to-n (1 to few, e.g. a gallery) biometric capture and matching for instant identification, thereby removing the need to physically present documents and credentials at every touchpoint.

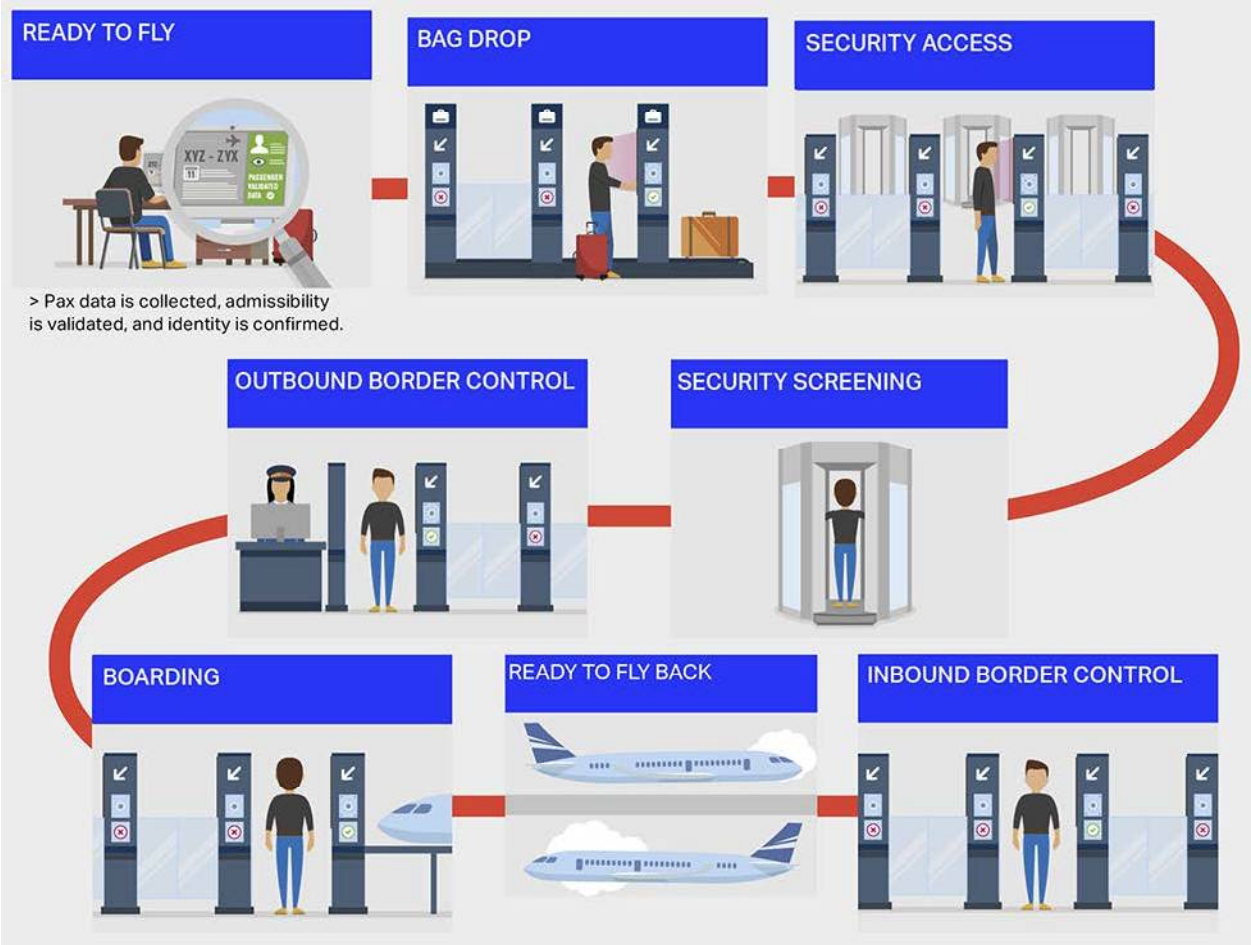
[54] *One ID*, IATA: https://www.iata.org/en/programs/passenger/one-id/#tab-1.

- **Operational Framework (also commonly known as trust framework):** set of specifications, rules, and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a community of participants, and bound by a common set of requirements.

Reaping the Benefits of Digital Identity:

- The use of digital identity as early as the time of booking allows passengers to arrive at the airport ready to fly, with all necessary checks and verifications performed in advance.
- Enhanced data quality, including verified passenger biographic and biometric data as well as information related to baggage and booking, will not only help the aviation industry to introduce more efficient processes, but also allow authorities to perform early and more robust risk assessment on travelers.
- Airlines, airports and authorities need to closely cooperate to allow the implementation of a truly touchless journey, where the passenger's biometric information can be used as a token throughout the different steps of the journey.

One ID: A collaborative identity management solution spanning across all stakeholders using biometric recognition



Compared to the processes described in section 2.1, One ID will simplify the touchpoints through the use of biometrics while enabling some touchpoints to be combined:

- **API:** today's programs require that the data is not only correctly captured from the travel document, but also accompanied by a reconciliation between the person presenting the document and the document itself. This process requires a specific touchpoint at the airport, referred as DOC Check (see section 2.1.1). With One ID, authenticated passenger biometric and identity data will be provided directly by passengers directly ahead of their arrival at the airport.
- **Bag Drop:** the passenger is recognized at bag drop, where applicable, through biometric recognition against the information contained in the passenger data. The bag tag and license plate is also validated to match the passenger data.
- **Security Access:** the passenger is biometrically recognized and matched against the passenger data.
- **Exit Border Controls:** can be performed before or after security access and/or combined with another process. For instance, systematic exit checks can be eliminated and replaced by a combination of vetting of each passenger in advance and the biometric identification of the passenger accessing airside and at the boarding gate. Exit border controls should not require passengers to stop unless they are selected for a secondary inspection by border officers.
- **Boarding:** the passenger is biometrically recognized and matched against the passenger data (boarding is enabled or not). Visual inspection of the ID document will no longer be needed. Positive ID check will be done automatically during the boarding process.

One ID requires a change to the current data exchange model where multiple transborder schemes may co-exist depending on the trust frameworks in place. Harmonization of requirements and interoperability of solutions are crucial for the success of such schemes. A key role for One ID is the creation of standards that would enable interoperability among different transborder programs, allowing a truly end-to-end process where all industry and regulatory requirements are met with touchless controls.

5. Ask the Expert–Questions and Answers

You did not have time to read the whole manual Secured and Simplified Borders or you still have questions? Here are quick elements of response to questions you may have.

What is the difference between API and PNR?

API are biographic data collected from the passenger's travel document. The accuracy of the data is verifiable on the basis of check against the traveler's travel document. PNR data are collected from the passenger's booking. These are declarative data that indicate an intention to travel and cannot be verified. There is no such thing as verified or accurate PNR data. Airlines will only send what is in their systems.

For authorities, if they want to ascertain the identity of passengers and to perform watchlist matching, they will have to use API data. PNR data, which is not verified information, will only help authorities to establish patterns or identify risk profiles, but not to validate the identity of the person.

For more information on API and PNR data, see the section 3. Implementing Efficient Passenger Data Programs and consult the IATA API-PNR Toolkit: https://www.iata.org/en/publications/api-pnr-toolkit/#tab-1

Can a document check be performed to increase the accuracy of PNR?

PNR information is declarative data provided by the passenger at the time of booking. Even the name of the passenger can often have spelling mistakes or incomplete information (like using Bob instead of Robert). Mandating airlines to verify passenger travel documents for the purpose of verifying the accuracy of PNR data does not make sense.

If authorities want to validate the identity of the passenger, they need to require API data.

For more information on PNR, see section 3.2.

Where can I find baggage information in the airline's system?

Baggage information generally only becomes available at the time of baggage drop-off shortly before departure. This information is stored in the airline's DCS. If the airline has the capability to integrated DCS information into its reservation system, the PNRGOV message should include baggage information. However, if the airline operates segregated DCS and reservation systems, the baggage information will not be included in the PNRGOV message. These airlines might, however, be able to include the baggage and seat information in the PAXLST message sent at flight closure as per the API requirement.

For more information on integrated and segregated DCS and CRS, see section 2.2.3. Airline IT Infrastructure.

When should PNR data be sent? Could PNR data be required one week before the flight?

PNR data is collected from the booking information of passengers. However, even if tickets can be booked up to a year in advance, the booking information can be changed up to departure. To optimize the transfer of information and minimize the volume of data sent, the international best practice is to send the first message

with PNR information between 72 and 24 hours prior to departure. This allows for the transfer of the most updated information on passengers who intend to travel.

Requiring PNR data prior to that time will mean that authorities receive data that might not be up-to-date and will need to be reconciled with subsequent PNRGOV messages reflecting the changes made in the passenger's booking. This can be a burdensome and costly process, which might not have much added value for the authorities' risk assessment.

For more information on PNR data timing transfer, see section 3.2.2 International Standards.

Why can't the airline comply with a PNR request within a month?

Airline systems differ greatly and authorities will have to cooperate with each airline individually to establish the adequate connection to the airline's systems. Airlines need time to adapt their IT systems to ensure they can correctly extract the PNRGOV message from their systems in line with the government's requirements.

For more information on PNR implementation, see section 3.2.4. Implementation Considerations.

Can API data quality be checked on the basis of the boarding pass?

API information is generally saved in the airline's DCS. It is not captured on the boarding pass. Airline staff performing travel document and boarding pass checks at the gate do not have visibility of the API data captured in the DCS when performing these visual controls. Therefore, the document check performed at the gate does not necessarily help with improving API data quality.

For more information on Document Check and on the boarding pass, see section 2.1.1. Document Check and Check-in under section 2.1.2. Understanding the key processes in the passenger's journey.

Is an iAPI system mandatory if I want to issue an eVisa?

iAPI are complex and costly systems, which not all states can support. However, if authorities want airlines to ensure passengers are adequately documented prior to boarding, they will need to provide interoperable solutions for airlines to automatically verify the status of passengers. Today, the solution supported by international standards and industry best practices remains iAPI systems.

If a state cannot support the use of an iAPI system for the verification of eVisas, it cannot expect airlines to be reliably verify the visa printout presented by the traveler. Although airline staff will apply due diligence in verifying the printout, sanctions should not be imposed on airlines if the travel authorization is non-valid or fraudulent.

For more information on travel authorizations, see section 4.1.2. Electronic Travel Systems and 4.1.3 On-line Application and/or Issuance of Travel Authorization.

Can passenger data programs (API/PNR) be used to comply with public health requirements?

PNR can provide contact details for passengers. However, these contact details are often missing (for instance, if the ticket was booked via a separate distribution channel) or can be inaccurate. PNR is a simple business record.

The collection of passenger contact and/or other health-related information should be a transaction taking place between passengers and authorities. For electronic collection, it is best for authorities to set up web portals on which passengers can directly provide their information. Health information is sensitive from a data privacy perspective and it is not the role of airlines to collect this information from their passengers.

If allowed by national legislation, PNR can be useful for disease control authorities as it provides information on the passenger's journey and can help identify travelers coming from higher risk countries.

For more information, refer to section 3.2.2 on PNR and International Standards.

Where can details about each national passenger data programs be found?

To help airlines comply with the different national requirements, IATA maintains the API/PNR World Tracker that provides detailed information on each national program. States can have access to this tracker and are encouraged to provide IATA with the necessary documentation explaining their national requirements (preferably in English).

For accessing the IATA API/PNR World Tracker, communicate with: passengerdata@iata.org

Who deploys ABC systems? Do airports or airlines have a say in how border controls are performed?

Even if ABC systems are used for border control purposes, they can be partially or fully financed by the airport operator or the airlines. Investment in ABC systems should be the outcome of a consultation process between the airports, airlines and authorities to improve the quality and speed of border controls. Airport operators generally have an important role to play as they are providing the infrastructure necessary for the deployment of the systems.

For more information on ABC systems, see the section 4.3.

How can the use of ABC be expanded beyond the national population?

With API, PNR, RTP and ETS programs, states can perform assessments in advance of travelers to determine whether a passenger is deemed high or low risk. With the introduction of more secure travel documents, together with the implementation of enhanced border management tools, authorities should be able to expand the use of ABC systems to nonnationals, without diminishing the security of their border.

For more information on ABC systems, see the section 4.3.

Under the IATA One ID, how will passenger data be used?

One ID relies on secure and lawful sharing of data amongst stakeholders. One ID supports the principle that data should be processed transparently, lawfully and fairly.

Following the principle of data minimization, only strictly necessary personal data shall be collected and only for the express purpose for which it is collected; passengers shall be properly informed and where stakeholders wish to use data for additional purposes, they should define those purposes and seek the appropriate legal grounds and passenger consent.

Importantly, the quality, accuracy, integrity and overall security standards of the personal data should be set high to protect the privacy of the passenger.

It is important to note that API data that is currently transferred in international air travel from carriers to governments is mandatory under ICAO Annex 9 and UNSCR 2178 (2014) and 2396 (2017). While One ID will not remove the requirement for API transfer, it could provide opportunities to minimize the amount of personal data managed by industry while facilitating this exchange.

For more information on One ID, see section 4.4.2 and consult the One ID webpage: https://www.iata.org/en/programs/passenger/one-id/#tab-1.

International Air Transport Association
ISBN 978-92-9264-245-7
Customer service: www.iata.org/cs
+1 800 716 6326

iata.org/publishing