Chapter 9

PASSENGER DATA EXCHANGE SYSTEMS

9.1 INTRODUCTION

Advance Passenger Information and Passenger Name Record

9.1.1 The transfer of Advance Passenger Information (API) and Passenger Name Record (PNR) data by aircraft operators to States allows public authorities to check watchlists, conduct analysis and take operational decisions. The availability of such pre-travel and pre-arrival passenger data allows the application of appropriate risk management techniques by States to expedite clearance processes at border control points and focus resources on travellers assessed to pose higher risk.

9.1.2 Practice has shown that the processing of API and PNR data by public authorities is necessary for border control and law enforcement purposes. Ideally, these stakeholders cooperate within the framework of a Passenger Data Single Window to facilitate inter-agency processing of passenger data, as well as international data sharing. These agencies cooperate within structures that are often called multi-agency targeting centres or Passenger Information Units (PIU).

9.1.3 Article 22 of the Chicago Convention requires States to facilitate international air navigation and adopt all practical measures to prevent unnecessary delays. Article 13 requires the aviation community to comply with a State's laws and regulations "... relating to entry, clearance, immigration, passports, customs, and quarantine ...". In operational terms, a new procedure connected with the arrival or departure of a flight should serve to improve productivity of operations. API systems can effectively resolve national security problems, unacceptably long delays in passenger processing and the deterioration of facilitation efforts due to availability of personnel resources.

9.1.4 An API message contains passengers' biographic and document details from their passport or other travel document, as well as flight details and other information collected during check-in. Depending on the availability of data in aircraft operator systems, the API message may also include information on the passenger's connecting flights. Some States require API for passengers and crew, and some for passengers only.

9.1.5 There are two modes of API:

a) Batch API is data covering all passengers and, in many cases, crew members on board a specific flight, which is collected during the check-in process and transmitted in a single message for each (one batch message for passengers and a separate batch message for crew members). Batch API messages are typically ready for transmission only after check-in has closed, and in some cases only after aircraft departure. In that sense, Batch API was originally designed for the control of arriving passengers and traditionally sent to the Destination State only as pre-arrival information. Consequently, Batch API messages are of limited use to the Departing State since a passenger would likely already have cleared outbound border control, or even departed, by the time the message is transmitted to the Departing or Destination State.

b) Interactive API (iAPI), as an alternative to Batch API, is transmitted in real time on a passenger-by-passenger basis. This pre-departure information enables State authorities to process the data during check-in and provide a response message also in real time to the aircraft operator. The iAPI mode is of value to the Departing State and the Destination State, allowing both States to undertake border-related and aviation security controls before the passenger is granted a boarding pass and allowed access to the sterile area of an airport. As such, iAPI enables States to operate pre-departure checks and "no fly" schemes. In addition, a flight close-out message after the aircraft doors have closed can confirm the passengers that have boarded (and not boarded) the flight. States requiring iAPI may also maintain a Batch API message requirement either as a back-up capability or to receive details not normally collected during web check-in.

9.1.6 PNR data, in the air transport industry, 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. Such reservation data are collected and created at the time of booking for commercial and operational purposes and may be modified until departure. When required to transfer PNR data to States, it is provided as a PNRGOV message sent by, or on behalf of, aircraft operators typically from 72 or 48 hours before Scheduled Departure Time (SDT). This is well before verified travel document data collected during check-in in the form of machine-read API data will be received. While a PNRGOV message may transmit travel document data (including name, nationality, sex, date of birth, etc.) for some booked passengers on a given flight, it should be noted that "Any collected API data" contained in PNR will likely be self-asserted and unverified information.

9.1.7 States are encouraged to use their National Air Transport Facilitation Committee (NATFC) to support and coordinate the development of API and PNR systems.

Passenger Data Single Window

9.1.8 A Passenger Data Single Window is defined in Annex 9 as "a facility that allows parties involved in passenger transport by air to lodge standardized passenger information (i.e. API, iAPI and/or PNR) through a single data entry point to fulfil all regulatory requirements relating to the entry and/or exit of passengers that may be imposed by various agencies of the Contracting State".

9.1.9 The Passenger Data Single Window Standard means aircraft operators need to transfer required API and PNR data to a single facility within any State. All public authorities with a legal remit to make use of the data should do so within the context of their national border framework. The overarching principle of the Single Window is to create efficiencies in data transmission and avoid duplication of costs and resources for both aircraft operators and States. From a border integrity perspective, the Single Window can lead to significant improvements in collaboration and cooperation among State agencies. At a minimum, the Single Window Standard means that States shall require only one entry point for the respective API and PNR messages. This would mean, for example, that API/iAPI messages could be sent to one single window facility, while PNR data could be sent to a separate single window facility (Standard 9.1).

9.1.10 Facilitation benefits can be derived from the processing of API and PNR data in combination with each other. PNR messages have traditionally been required by States to flag otherwise unknown individuals in the fight against terrorism and serious crime, while API messages are used to identify known individuals and travel document data from watchlists. Some States have chosen to process both API/iAPI and PNR messages using one Single Window facility (Recommended Practice 9.1.1).

Operational support

9.1.11 API and PNR data are transferred by or on behalf of aircraft operators to States using telecommunication systems, which may be subject to outages. In the event of a system outage or failure, the State or the aircraft operator should have access to a 24/7 contact (such as a monitored group mailbox, call centre or designated individuals or teams). This contact should be able to address any operational or technical issues and answer general procedural questions (Recommended Practices 9.2, 9.3 and 9.4).

9.1.12 Providing notification of scheduled maintenance allows all parties to plan for and implement necessary contingencies. In the event of an outage, failure(s) or scheduled maintenance, it is the responsibility of either the State or an aircraft operator to have notification and recovery procedures in place to ensure all parties are aware of the need to implement appropriate operational actions to continue processing passengers, while minimizing potential negative impacts to security and facilitation.

Standardized data elements

9.1.13 The message specifications, including the data elements for API and PNR data, are set out in their respective guidelines; WCO, IATA and ICAO *Guidelines on Advance Passenger Information (API)* (hereafter referred to as the "API Guidelines") and ICAO *Guidelines on Passenger Name Record (PNR) Data* (Doc 9944) (hereafter referred to as the "PNR Guidelines"). Adherence to the respective API and PNR guidelines is essential to enable aircraft operators to comply with the requirements of multiple States in a consistent way and to support the successful implementation of passenger data programmes worldwide.

9.1.14 Standard 9.5 reaffirms that States shall not require aircraft operators to provide non-standard data elements as part of API, iAPI and/or PNR provisions. Standards 9.8, 9.10, 9.24(b) and 9.30 also require compliance with international standard data formats.

World Customs Organization Data Maintenance Request

9.1.15 The WCO/IATA/ICAO Contact Committee on API and PNR Data (hereafter referred to as the "API-PNR Contact Committee") was established by the three aforementioned organizations to develop the API Guidelines and to manage and maintain other initiatives relating to both API and PNR data. The PNR Guidelines are managed and maintained by ICAO while the PNRGOV message implementation guidance materials are published and updated by WCO and endorsed by ICAO and IATA.

9.1.16 The WCO DMR process is managed and overseen by the API-PNR Contact Committee, as the official inter-governmental process which considers the addition of non-standard data elements into the existing API and PNR Guidelines. States considering data requirements that deviate from the standard data elements as defined in the API and PNR Guidelines shall, according to Standard 9.6, follow the WCO DMR process before any deviation is requested from the aircraft operator. In the case of a DMR process change to PNR data elements, it should be recalled that aircraft operators will only collect this (new) data element if it is part of their business operating procedure (Standard 9.30).

9.1.17 The API-PNR Contact Committee uses the WCO DMR process to ensure that any modification to the existing standardized data elements, including addition, deletion or update to any data element is undertaken based on sufficient business needs and other rationale, bearing in mind the objective to maintain the simplicity of the standards and the efficiency of API and PNR data transfer.

9.1.18 Maintaining and modifying the message specifications should be undertaken in the respective IATA PAXLST and PNRGOV Working Groups, which work in accordance with the WCO DMR process and report to the API-PNR Contact Committee.

9.2 ADVANCE PASSENGER INFORMATION

The Standards and Recommended Practices of Annex 9, Chapter 9, Section B: Advance Passenger Information (API)

Baseline requirement

9.2.1 Annex 9 stipulates that States shall establish an API system supported by appropriate legal authority (such as, *inter alia*, legislation, regulation or decree) and be consistent with internationally recognized standards for API as jointly agreed by the API Guidelines. API message construction is based on the United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT), with API data content and format being defined by the UN/EDIFACT Passenger List (PAXLST) Message. This format is required to ensure global interoperability and connection of API systems between States and aircraft operator systems. When implementing an API programme, only those data elements defined in the UN/EDIFACT PAXLST message shall be included (Standards 9.7, 9.8 and 9.10).

9.2.2 The legal basis for API should be coordinated to meet the needs of all involved agencies and enable the Single Window facility. States should consider nominating a lead agency to guide the inter-agency development of an API system (Recommended Practice 9.9).

9.2.3 Annex 9 requirements for API arose from United Nations Security Council Resolution 2178 (2014), which called upon States to require aircraft operators to provide API, *inter alia*, to detect the departure or attempted entry into or transit through their territories by means of civil aircraft of individuals designated as foreign terrorist fighters by the United Nations Counter-Terrorism Committee. In this context it is important to note that API data, as such, does not identify otherwise unknown foreign terrorist fighters but is a tool that can be used to identify known individuals designated as such by the United Nations or by States. Accordingly, States should take appropriate measures and share information with each other, and with INTERPOL, based on legal agreements and with mutual assurances regarding the safeguarding of information.

Advance Passenger Information description

9.2.4 An API system involves the following steps:

For aircraft operators:

1) capturing certain travel document information ideally through the Machine Readable Zone (MRZ) prior to departure of the persons and complementing it with particular flight and check-in data;

2) transmitting the above information by electronic means to the relevant public authorities;

3) ensuring the information transmitted is complete, correct and valid (data quality);

4) confirming the number and identities of passengers and crew onboard the aircraft; and

For States:

5) effectively processing such data for targeting, analysing (risk assessment) and determining the control process to be applied when the passenger and crew arrives.

Advance Passenger Information benefits

9.2.5 The primary value of API is the improvement in facilitation, security and passenger clearance procedures in terms of efficiency, effectivity and preventing unnecessary delays at border controls. Statistically, the vast majority of passengers and crew do not pose any threat and should be subject to standard checks only. One of the main benefits of processing API is to enable screening travel document data against watchlists, searching for “hits” in databases thereby identifying wanted individuals or travel documents that are suspicious or associated with illegal intentions (known threats).

9.2.6 API is a facilitation measure, but it is also acknowledged as a security tool since watchlist subjects of interest and travel documents of interest may be identified in advance of arrival, thereby enhancing law enforcement and security. The application of API to border control should be a strong motivation for a State to allocate the resources necessary to improve and/or automate aspects of its inspection processes. The success of an API programme should be measured by its law enforcement and security outcomes, by the increase in operational efficiency and the reduction in airport congestion at border controls.

Advance Passenger Information data quality

9.2.7 Many States are automating border clearance processes, with a view to enhance facilitation. API, and in particular, travel document data, received in advance of passenger arrival (Batch mode), or in some cases in advance of passenger departure (iAPI mode), assists with clearance procedures. A critical element of the API message consists of the data contained in MRZ of a Machine Readable Travel Document (MRTD). In this context, Standard 9.10 establishes that when requiring identifying information on passengers, this data shall be limited to the travel document MRZ.
The Standard also underlines the concept of pursuing standardized data elements only and notes that API data requests shall conform with the agreed data requirements as defined by the API Guidelines.

9.2.8 In many cases travel document data in the API message is collected by aircraft operators or their agents from a travel document’s MRZ. Traditionally, this data was collected at the airport check-in desk, but, with the increased prevalence of web check-in, the passenger typically enters this data manually. All States rely on high-quality travel-document data to perform their border control functions based on API and aircraft operators are required to conduct a document check at the latest before boarding, a swipe of the travel document MRZ at the airport is still usually employed, also with a view to enhancing API travel document data quality.

9.2.9 Enhanced automated solutions for travel document data capture that address data quality during web check-in are already employed and will grow in importance in the coming years.

9.2.10 Doc 9303 specifies that MRZ is a cornerstone of global interoperability for a multitude of actors, from travel document issuing authorities to aircraft operators and immigration authorities. The document reading device is an important tool for minimizing check-in, boarding and border clearance times. Automated capture of data has two main benefits:

a) faster data capture; and

b) enhanced data accuracy.

9.2.11 Manual data collection and entry of other personal details during check-in, such as contact details, whether through web check-in or at the airport, negates the efficiencies and time savings achieved by using the MRZ. Additionally, there is no ability to guarantee the accuracy of the contact details provided, despite the effort and cost involved. States that are considering the collection of contact details should refer to the API Guidelines.

9.2.12 In addition to the MRZ data capture, multiple factors can affect the aircraft operator's ability to transmit accurate data in the API message. Many such challenges can be addressed through collaboration and communication between aircraft operators and authorities. Guidance on how States and aircraft operators can collaboratively work together to improve API data quality is available in the IATA Control Authorities Working Group (CAWG) Guidelines for Collaboratively Improving API Data Quality, which may be found at https://www.iata.org/en/programs/passenger/passenger-facilitation/facilitation-policy/.

Multiple travel documents

9.2.13 Passengers can legitimately travel with multiple travel documents. Some common examples include dual nationals, who possess passports of both the State of departure and arrival, or passengers employing a laissez-passer for entry and/or visa facilitation purposes.

9.2.14 Nonetheless, the fact that passengers travel with multiple travel documents, beginning the journey using one passport and then entering a destination State with another document for ease of entry presents challenges to the aircraft operator and the State. This is particularly the case when the API data at time of check-in does not match with the travel document data being presented to immigration. The complexity rises when the aircraft operator is required to send API data in an interactive mode to both the State of departure and arrival. The intent of the Standard 9.11 is to relieve the aircraft operator from liability or penalties when a passenger uses multiple travel documents during one journey.

9.2.15 When confronted with a mismatch between the data provided in API and the travel document information captured at border control, it is recommended that States establish mechanisms in their entry-exit and border control management systems to reconcile such differences by comparing key biographical data, such as name, date of birth and sex, as opposed to travel document details.

Importance of adherence to Doc 9303

9.2.16 As identified in Annex 9, Chapter 3, Standard 3.11, all passports shall be machine readable in accordance with the specifications of Doc 9303, Part 4. Those specifications ensure the efficient reading of the data and enable the automated collection and transmission of API data from the MRZ and the interoperability of systems.

9.2.17 However, non-compliant MRTDs continue to be issued and other inconsistencies in travel documents issued by States have resulted in different approaches by aircraft operators and States on how to collect, transmit and process API information. The vast majority of States implementing API programmes require aircraft operators to ensure that the data available from the travel document MRZ is correctly transmitted in the API message.

9.2.18 A key aspect of API data is the passenger's name as represented by the travel document. According to Doc 9303, in MRTDs, the surname is the MRZ "primary identifier", while the given name is the "secondary identifier". Doc 9303, Part 4 mandates that the MRZ secondary identifier field (i.e. given name) be filled in except "where the holder's name has only predominant component(s), this data field shall be left blank". Essentially, if a citizen only has a surname or one-word name, this must be used as the MRZ primary identifier. MRTDs issued without a MRZ primary identifier are not aligned with ICAO specifications.

9.2.19 Some States insist on receiving first and last names in an API message, although in some cultures no given name is assigned, and thus it is not reflected in a travel document. When passengers have no given names and MRTDs are correctly issued with MRZ primary identifiers only, a State needs to recognize that Doc 9303 specifications, embedded in the UN/EDIFACT PAXLST message format, supersede a requirement for "full name" consisting of both surname and given names in the API message. When a State requests full passenger name and the passenger only has a primary identifier (compliant MRTD), or has only a secondary identifier (non-compliant MRTD), the aircraft operator in practice will transmit FNU (for "First Name Unknown") to indicate that a name identifier is blank in the travel document. This, however, represents a manual entry.

Operational considerations

9.2.20 Recommended Practice 9.12 advises States to minimize the number of times API data are transmitted for a specific flight (i.e. multiple requests for data for any one individual flight should be avoided), since multiple transmissions of the Batch message will likely provide identical data and each transmission of data incurs some cost to operators.

9.2.21 The purpose of an API Batch message is to transmit complete details of all passengers and, where required, crew members on board the flight. A Batch message is essentially only ready for transmission when check-in has closed and no additional passengers can board the flight. If a Batch API message is required by a State before aircraft departure, essentially between the end of check-in and the closing of the aircraft doors, then a State could request a final close-out message, which gives assurance as to which checked-in passengers (whose details were already transmitted on the Batch message) actually boarded the aircraft.

9.2.22 API systems should work with existing data collections and boarding processes. When implementing an API system, it is essential to involve all relevant authorities in the planning and development stages to prevent the non-participation of one of the agencies, thereby negating the productivity gains for the others. API systems, to be successful, require the cooperation of all parties involved in the passenger inspection process. Since participation in an API system involves costs to the operators, their cooperation is most effectively obtained through engagement at an early stage.

9.2.23 It is essential that the requirements associated with the API systems are determined with consideration of the potential impact to the aircraft operators as they are responsible for providing the required passenger data to the authority. Standard 9.13 requires limiting operational and administrative burdens on aircraft operators to the greatest extent possible – this includes the amount and timings of transmissions required, emergency protocols for outages, maintaining a cooperative dialogue with aircraft operators on data quality, as well as other issues.

9.2.24 When an aircraft operator makes a valid attempt to transmit API data required by State(s), the State(s) should take into consideration the circumstances surrounding the noncompliance before penalizing aircraft operators. State(s) should work with the aircraft operator (providing feedback, examples, etc.) to analyse and assess the issue that caused the system failure and identify solutions to minimize the potential for reoccurrence (Recommended Practice 9.14).

9.2.25 Standard 9.15 provides that when an API system is in place, aircraft operators shall not be required to provide a passenger manifest in paper form.

Interactive Advance Passenger Information

9.2.26 Recommended Practice 9.16, advises that States should consider the introduction of an iAPI system.

9.2.27 An iAPI system enables States to process incoming API data, scan their border control system instantaneously and provide a response message to the aircraft operator in real-time. Using iAPI, States are able to vet watchlists, compare border control records, query visa databases and other information related to entry requirements in real-time and provide a board/do not board message to the aircraft operator before the flight departs. This way, States are able to extend their border control measures to pre-departure, thereby achieving significant border integrity benefits, such as by identifying inadmissible passengers before a boarding pass is issued.

9.2.28 In addition to the major border control benefits it provides, an iAPI system also enhances aviation security since a boarding pass cannot be issued until a State provides an “OK TO BOARD” directive to the airline system, thereby prohibiting access to the aircraft itself, and even to the sterile area of an airport for a particular passenger.

9.2.29 The use of iAPI should lead to a considerable decrease in inadmissible passengers and penalties as the iAPI response message will provide aircraft operators with real-time directives from the State, for approval or denial to board or messages with specific instructions on each passenger. As an example, iAPI allows States to conduct systems-based checks on travel documents during check-in meaning that admission refusals related to information contained in the State's border control database can be determined before travel to that State.

9.2.30 When States implement an iAPI system, they should consult with other States and aircraft operators in advance to identify lessons learned and best practices to smoothen implementation and to minimize the impact on the aircraft operator systems. In deploying iAPI requirements, States should work with aircraft operators to integrate State systems with aircraft operator Departure Control Systems (DCS) based on existing interfaces. The specifications for iAPI messages are contained in the API Guidelines, in particular Appendix IIA – WCO/IATA/ICAO Passenger List Message (PAXLST) Implementation Guide and Appendix IIB – WCO/IATA/ICAO API Response Message (CUSRES) Implementation Guide (Recommended Practice 9.17).

9.2.31 Since travel can begin in any time zone, API systems need to receive and process data 24 hours a day, seven days a week. Likewise, contingency measures have worked effectively for both States and aircraft operators in situations where iAPI systems have been temporarily unavailable. Experience suggests that contingency measures are more effective when resilience plans are prepared and communicated in advance by both States and aircraft operators (Recommended Practice 9.18).

9.2.32 Additionally, iAPI provides avenues for the increased automation of border control clearance. The development of CUSRES response codes will grow in importance.

9.2.33 States should be aware of Standards 9.1, 9.7 and 9.24, which oblige States to establish a Passenger Data Single Window facility, an API system and develop a capability to collect, use, process and protect PNR data. The sequence of which passenger data regime (API or PNR) should be implemented first needs to be based on each States priorities, operational objectives and risk profile. When considering the implementation of iAPI or transitioning from Batch API to iAPI, States should measure the potential benefits afforded by the interactive component and applicability to their aviation environment. For States with particularly low traffic volumes, an additional critical factor to assess is the cost proposition of iAPI.

9.3 ELECTRONIC TRAVEL SYSTEMS

The Standards and Recommended Practices of Annex 9, Chapter 9, Section C: Electronic Travel Systems (ETS)

9.3.1 Increasingly, States are requiring passengers intending to travel to their territory to apply or register online prior to travel. These countries are using varying terminology such as "electronic visa", "electronic travel authority" or "visa on arrival" to describe their online programmes. As States establish non-standardized authorizations to travel, traditional document validation techniques adopted by aircraft operators for physical visas will not be effective.

Electronic travel systems and interactive advance passenger information

9.3.2 The purpose for implementing an Electronic Travel System (ETS) is to undertake and expedite pre-travel vetting and acceptance of low-risk passengers into a country, while providing a secure method for States and aircraft operators to verify the existence of a passenger's electronic authority to travel using interactive API. Electronic authorities to travel are designed for low-risk nationals who do not require a visa, but for whom there is a requirement to provide information online prior to travel, essentially seeking authorization to travel. Typically, the data required during such applications are comparable, but usually less than required for visa applications. The issuance of such authorization also takes less time and can be applied for usually between three and seven days prior to travel.

9.3.3 The use of an iAPI system ensures that aircraft operators are informed of the existence of a passenger's electronic authority to travel. With the corresponding CUSRES response message, aircraft operators receive a verification that the traveller is in possession of a travel authorization. When there is no iAPI in place, the authority to travel programme is not fully automated and does not qualify as an ETS programme as set out in Annex 9, Chapter 9, Section C.

9.3.4 ETS makes use of the iAPI message, allowing States to match their existing records based on standard travel document data, typically contained in the travel document MRZ. Since the electronic authority to travel is linked to a specific travel document, the passenger must travel with the same travel document for the aircraft operator to obtain an "OK TO BOARD" CUSRES iAPI response message.

9.3.5 From a cost-benefit perspective, all States with iAPI already in place could capitalize on this investment by developing an electronic authority to travel programme to make use of the pre-departure verification benefits provided by iAPI. Consequently, Recommended Practice 9.19 urges States seeking to establish ETS for pre-travel verification to combine this with an iAPI system. This will allow States to integrate their system with the DCS using data messaging standards in accordance with international guidelines to provide a real-time response to the aircraft operator to verify the authenticity of a passenger's authorization during check-in.

Electronic travel system programme description

9.3.6 Essentially, there are three distinct automated processes with ETS:

a) lodgement (or application);

b) acceptance (or issuance); and

c) verification.

9.3.7 With traditional visas, these three processes are entirely manual or semi-automated, such as verification through the swiping of the visa MRZ. The automation of the ETS processes unlock tremendous facilitation and border security benefits for States, passengers and aircraft operators. Further guidance relating to Recommended Practices 9.20, 9.21, 9.22 and 9.23 on implementing an ETS programme is provided by the IATA CAWG Best Practice for ETS:
https://www.iata.org/contentassets/67e015cf3db1410392cd5b5bb5961a16/iata-cawg-best-practice-for-ets-2016.pdf.

Challenges associated with non-standardized authorizations to travel

9.3.8 A number of States have introduced non-standardized, non-physical authorizations to travel. Without the support of iAPI, the aircraft operator faces numerous challenges in verifying whether these travel authorizations are valid, such as:

a) **Paper printout**: States that have a non-physical authorization to travel without an iAPI system often require passengers to travel with a paper printout as a proof of possession of their authorization to travel. Aircraft operators are required to verify this printout, which may include a two-dimensional (2D) barcode without any form of standardization in place. Although aircraft operators can perform due diligence in verifying that the printout seemingly belongs to the passenger and that it is apparently valid for travelling, these printouts can easily be falsified; they do not contain any basic security features like traditional visas. Furthermore, the layout and data fields of the printouts vary extensively among countries.

b) **Web portals**: To address the verification challenge, some countries have proposed solutions for aircraft operators to query a web-based portal to determine if in-scope passengers hold an authorization to travel. This solution is neither sustainable nor viable in the industry environment and, where deployed, is a cause of delays. Most airline counters are not equipped with internet access. In the rare event where such a connection exists, making a web-based query for each in-scope passenger would stretch the time sensitive check-in process.

c) **Self-services**: A further limitation of non-standardized authorizations to travel is that they prevent passengers from using self-service (check-in, bag drop, etc.) by reintroducing manual check-in by an agent at the counter at the airport. States and industry are looking at solutions for efficiently and seamlessly processing travellers.

Digital Travel Authorizations

9.3.9 As a response to the challenges mentioned above, ICAO developed the technical specifications for the Digital Travel Authorization (DTA) which standardizes the layout, data content and verifiable security feature for electronic (or non-physical) authorities to travel. While ETS functions only with an iAPI system in place to conduct a systems-based check of the authorization to travel, DTA can be deployed as a verifiable credential in a situation where there is no iAPI system in place, or as a backup solution in case of an iAPI system outage or failure.

9.3.10 The DTA specification provides a step-by-step framework for issuing an electronic notification containing a harmonized 2D barcode that can be easily read and verified, enabling both data capture and verification of integrity in one transaction. DTA can be used in both digital and physical formats, meaning it can be presented on a smart device or on a printed piece of paper with the same security and results. Importantly, DTA standardizes the data set that is collected for each passenger, regardless of the issuing State. This provides a critical advantage to the aircraft operator since it can harmonize its method of verifying DTA barcodes. DTA makes use of the Visible Digital Seal for Non-constrained Environments (VDS-NC) and can greatly assist aircraft operators to verify the passenger's acceptance for travel.

9.3.11 Doc 9303, Part 7 defines the specifications for MRVs, which allow compatibility and global interchange using both visual (eye readable) and machine readable means. Part 7 is now augmented with the DTA Technical Report, which allows for the needed standardization of electronically issued travel authorizations.

9.4 PASSENGER NAME RECORD DATA

The Standards and Recommended Practices of Annex 9, Chapter 9, Section D: Passenger Name Record (PNR) Data

Collect, use, process and protect passenger name record data

9.4.1 Annex 9 stipulates that States shall develop a capability to collect, use, process and protect PNR data. Standard 9.24 sets the baseline commitment for States to introduce PNR programme capability supported by an appropriate legal and administrative framework, which shall be consistent with the PNR standards in this section of Annex 9. This Standard also requires alignment with the PNR Guidelines, as well as the PNRGOV message format as specified by the implementation guidance materials published and updated by WCO and endorsed by ICAO and IATA.

9.4.2 Standard 9.24 should be interpreted as a requirement that all States without a PNR system should initiate the development of a PNR capability. While the development of a capability to collect, use, process and protect PNR data can be initiated quite quickly, its full and effective operation may take much longer, including up to 2–5 years. The initial steps in developing a PNR programme should focus on the creation of the appropriate legal and administrative framework consistent with all the Standards contained in this section of Annex 9.

9.4.3 By indicating that a State's PNR legislative and administrative framework shall be consistent with all PNR Standards in Section D, Standard 9.24 outlines the concept that the PNR standards are intended to provide a global framework for PNR data transfer, not only in technical terms but also regarding mutual recognition of data privacy and protection. The concept of Annex 9 functioning as a global framework for PNR data transfer is further described in Standards 9.35, 9.36 and 9.37.

9.4.4 Since its inception, PNR data transfer and processing has raised data protection and privacy concerns. Historically, this has resulted in some States requiring bilateral agreements to permit PNR data transfer subject to legally binding appropriate safeguards. Unfortunately, not many agreements have been signed to date, and over time conflicts of laws have arisen in which States were implementing PNR programmes but not receiving data from certain aircraft operators because these operators were prohibited or inhibited from transferring PNR data by those States requiring bilateral agreements.

9.4.5 Just as with API, the legal authority for PNR should be coordinated to meet the needs of all involved agencies, also with a view to strengthening the Single Window facility, border integrity and overall facilitation measures. Often, States will nominate an agency to lead the inter-agency development of a PNR system, including ensuring that all concerned agencies agree to process PNR in the same message type, with the same message construction standards, and through one data point so aircraft operators are not duplicating efforts (Standard 9.1).

9.4.6 The adoption of a new suite of PNR Standards of Annex 9 was a consequence of United Nations Security Council Resolution 2396 (2017), which at paragraph 12, "[decides] that Member States shall develop the capability to collect, process and analyse, in furtherance of ICAO [SARPs], [PNR] data and to ensure PNR data is used by and shared with all their competent national authorities, with full respect for human rights and fundamental freedoms, for the purpose of preventing, detecting and investigating terrorist offences and related travel" and also "urges ICAO to work with its Member States to establish a standard for the collection, use, processing and protection of PNR data."

Passenger name record description

9.4.7 PNR data is airline booking information recorded by reservation systems for each journey booked by or on behalf of any passenger. PNR data are used by airlines for their own commercial and operational purposes in providing air transportation services and provide a mechanism for all the different parties within the aviation industry (including travel agents, aircraft operators and handling agents at airports) to recognize each passenger in a common format, and have access to all relevant information related to the passenger's journey; departure and return flights, connecting flights (if any) and special service requests on board the flight.

9.4.8 PNR data contains only as much as the aircraft operator or booking agency collects in the process of creating and managing its travel bookings. Accordingly, the amount and the nature of the information in a PNR varies from aircraft operator to aircraft operator, and from passenger to passenger on the same flight, often depending on how and by whom the reservation was made. States shall not require aircraft operators to collect PNR data not required as part of their normal business operating procedures (Standard 9.30(a)).

9.4.9 PNR data for an individual passenger may contain as little information as a name, contact information, itinerary, ticketing information and form of payment. Alternatively, a PNR may contain full address, contact details, travel document information and payment information and all other data relating to the booking. The airline industry cannot guarantee the accuracy of information contained in PNR data, as reservation data includes unverified data collected for commercial purposes.

9.4.10 Reservations may be created by various marketing organizations, with only pertinent details of the PNR data then transmitted to the operating carrier(s), who in turn transmit the details to States. At the same time, airline industry systems are programmed to transfer the entire contents of a PNR they have in their systems to States. States shall not require operators to filter data prior to transmission (Standard 9.30(a)), including personal data which may be considered sensitive. To prevent the processing by States of PNR data they consider to be sensitive, States need to set up their own data filtering and protection systems to deal with such data.

9.4.11 A detailed description of PNR can be found in Doc 9944.

Segregated and integrated systems

9.4.12 Some DCS systems are programmed such that certain information created at the point of check-in can be overlaid into the existing PNR for each passenger, thereby complementing the original booking data collected during the reservation process. However, this can only take place when an integrated system is in place or where the aircraft operator's system allows for communication between the reservation systems and DCS. Around 40 per cent of aircraft operator's systems support such an integrated data flow. In a segregated system, check-in data is not fed back into PNR. States need to accommodate both integrated and segregated systems.

9.4.13 Additional PNR data elements that might be collected during check-in and added to a PNRGOV message are indicated in the PNR Guidelines, Appendix I, PNR Data Elements with an asterisk: "These elements are contained in the DCS and are not available prior to departure", such as seat assignment and/or baggage information.

9.4.14 In the case that an integrated system exists, the PNR data content collected by DCS would only be contained in the PNRGOV close-out message sent after aircraft departure, and not beforehand. In requesting such data a State should remain cognizant that the combined use of both API and PNR data will provide (through the API PAXLST message) essentially the same information to a State as analysing any check-in data that might be contained in a post-departure PNRGOV close-out message.

Passenger name record benefits

9.4.15 PNR data can be sent to States in a PNRGOV message to fulfil border control and national security purposes. PNR was traditionally used by customs authorities to help identify contraband and smuggling routes. Today PNR is being used for a wide range of law enforcement measures, including the fight against terrorism and organized crime.

9.4.16 PNR plays an important role in risk assessment and analysis and helps States to identify previously unknown people who should be subject to additional checks. PNR data can help States identify trends they were not previously aware of based on the analysis of travel reservations, including payment, associated travellers, arrangement of flight legs, etc. Analysis of PNR data requires strong analytical computing tools to identify unknown travel routes and connections among individuals (including non-travellers), as well as between individuals and entities.

9.4.17 Processing of PNR data has become necessary to public authorities for examining travel patterns or certain behaviours that may indicate criminal activity. This includes (but is not limited to) the examination of payment details (such as paying by cash or purchase of a ticket at the last minute before travel), repeated no-shows or association with known criminals.

9.4.18 However, by its very nature, PNR data is limited in that it cannot be guaranteed in completeness or accuracy, as the aircraft operator has no control over the data provided by the passenger. There is, for example, no Annex 9 requirement for a carrier to collect a home address for a passenger, or for a passenger to provide proof of address. This highlights the reason why PNR data is optimally used in conjunction with other data sets collected with greater certainty of accuracy, including API.

Purpose limitation

9.4.19 The proper use of PNR data has long been a key point of discussion in aligning legal requirements regarding PNR data processing. Therefore, Standard 9.25 is designed to limit the scope of PNR data use, including by specifying that the purposes for which PNR data may be used should be no wider than necessary in view of the aims to be achieved, including border security purposes to fight terrorism and serious crime. This Standard emphasizes that processing and use of PNR data be done with full respect for human rights and fundamental freedoms.

9.4.20 Standard 9.25(a) specifies that States shall clearly identify in their legal and administrative framework the PNR data to be included in their PNR processing. This does not mean that States are able to mandate the collection of certain PNR data elements by aircraft operators (Standard 9.30(a)). Instead, States shall clarify if they will process all or parts of a PNR data set for their purposes, keeping in mind that some States consider some data to be too sensitive to apply to their operations. This essentially means that a State could choose, in its legal and administrative framework, to decide not to use certain PNR data it considers sensitive or otherwise deems unnecessary. Some States replicate all the “PNR Data Elements” listed in Appendix 1 to the PNR Guidelines as being in scope, allowing them more latitude in their operations. In either case, the principles of commercial data collection, non-filtering and use of sensitive data delineated in Standard 9.30 apply equally.

9.4.21 Standard 9.25(b) requires States to clearly set the purposes for which PNR data may be used, for example for purposes related to border security, fighting terrorism and serious crime.

9.4.22 Concerning purpose limitation, Standard 9.25(c) also places a restriction on domestic and international data sharing and limits the disclosure to other entities, based on the criteria of comparable purpose and data protection. This means the receiving entity must use the data for similar purposes as those outlined in line with Standard 9.25(b), such as law enforcement and border security purposes, as well as to employ similar data protection measures as the disclosing authority, which are those measures that are consistent with Section D.

Safeguards and redress mechanisms

9.4.23 Standard 9.26 defines several specific data protection and privacy measures which can generally be considered safeguards and redress mechanisms.

9.4.24 Standard 9.26(a) specifies that States shall adopt a legal framework that includes measures for preventing unauthorized access, disclosure and use of PNR data held within State systems, as well as providing for penalties for misuse, unauthorized access and unauthorized disclosure.

9.4.25 One of the main purposes of PNR data processing is to find otherwise unknown subjects of interest. That requires disaggregation of data based on pre-defined rules to identify threats, eventually resulting in lawful differentiation between individuals. Such a differentiated approach needs to be lawful, meaning that any rule-based targeting of PNR data or continued investigation into an individual based on information gained from PNR data needs to be based on law.

9.4.26 Standard 9.26(b) provides that States shall ensure that the safeguards applied to their collection, use, processing and protection of PNR data are applied equally to all individuals, without unlawful differentiation. Without unlawful differentiation denotes that States are nonetheless allowed to apply lawful differentiation as the result of analysing PNR data. This may also result in differentiated screening of passengers at airports.

9.4.27 Standards 9.26(c) and 9.26(d) are related to informing individuals about the transfer of PNR data. These points require measures by aircraft operators to inform their passengers that their reservation data will be transferred to requesting States, as well as measures by States to ensure that individuals are informed of the collection, use, processing and protection of PNR data and related privacy standards. An aircraft operator would typically inform the customer about the transfer of PNR data during the booking process. A State could take measures to inform the broader public about its PNR programme as the legal and administrative framework is being developed, or after its adoption.

9.4.28 Standards 9.26(e) and 9.26(f) provide for redress and correction mechanisms, enabling individuals to seek a remedy if public authorities unlawfully processed their PNR data, as well as providing mechanisms for individuals to obtain access to their PNR data and to request, if necessary, corrections, deletions or notations.

Automated processing

9.4.29 Effective processing of PNR data can only be achieved in an automated fashion employing modern technology allowing for data disaggregation. At the same time, Standard 9.28(a) provides that States shall base automated PNR data processing on objective, precise and reliable criteria without unlawful differentiation and, as Standard 9.28(b), that States shall not make decisions that produce significant adverse actions affecting the legal interests of individuals based solely on the automated processing of PNR data. Such decisions shall therefore take place under human supervision and control, especially regarding enforcement measures taken based on information gained from PNR data. Law enforcement use of PNR data involves the insertion of rule-based information into automated targeting systems to identify risks and trends. The identification of risks and trends will occur based on both human analysis and machine generated knowledge. Consequently, human supervision and validation of disaggregation and selector criteria becomes even more important.

9.4.30 Standard 9.28(b) requires States not to base decisions that result in significant adverse actions affecting legal interests of individuals based solely on automated processing of PNR data. In other words, when the analysis of PNR data leads to significant adverse actions towards a person’s legal interests the decision-making process coming to that determination must be accompanied by human oversight.

Independent oversight

9.4.31 Standard 9.29 requires States to define in their legal and administrative frameworks, one or more authorities with the power to perform independent oversight of their PNR programme. The standard takes into consideration that States around the world have different approaches to oversight and thus does not specifically require that the oversight function be external to the authority that processes PNR data, stressing instead the concept of independent oversight.

9.4.32 The standard allows for oversight functions and control mechanisms to be performed either internally or externally to the public authority processing PNR data. Since multiple entities might be named to perform independent oversight the standard allows for a layered and diversified approach. In any case, PNR data programmes require oversight to ensure protection of PNR data and to determine whether PNR data are being collected, used, processed and protected with full respect for human rights and fundamental freedoms.

Data content, non-filtering and sensitive data

9.4.33 Standard 9.30 underscores the concept that PNR data is commercial self-asserted data that is collected differently by every entity according to its business requirements. Standard 9.30(a) specifies that States shall not require aircraft operators to collect PNR data elements that are not required as part of their normal business operating procedures, a long-standing principle of PNR data collection and transfer.

9.4.34 Standard 9.30(a) also defines the concept of non-filtering of PNR data by aircraft operators. States shall not require aircraft operators to filter any data the State considers to be sensitive personal data, even if it has, pursuant to Standard 9.25(a), declared that it will not use a certain data set that the State considers sensitive.

9.4.35 Standard 9.30(b) denotes that States must not use PNR data that is sensitive personal data and must delete such data as soon as practical.

Data retention and depersonalization

9.4.36 How long PNR data may be retained is an issue on which States have differing perspectives. Some States contend that data should be kept for an extended period of years, while others elect to maintain much stricter data retention schedules. While Standard 9.31 does not set a specific period for which PNR data shall be retained, the standard does stipulate that States shall set defined periods for data retention in Standard 9.31(a) and depersonalization in Standard 9.31(b), and provide for deletion or anonymization in their legal and administrative framework, as well as set the grounds for re-personalization of data. The PNR data retention period shall be necessary and proportionate for the purposes of the PNR programme, which is outlined in the legal and administrative framework per Standard 9.25 on purpose limitation.

9.4.37 Standard 9.31(b) requires States to depersonalize retained PNR data after set periods defined in national laws and policies. Depersonalization is the masking of information that would enable direct identification of an individual. Depersonalization does not hinder law enforcement use of PNR data, it is simply an additional safeguard reflecting the data protection and privacy concerns over the use of PNR for law enforcement purposes. Under Standard 9.31(d), States shall delete or anonymize PNR data at the end of the retention period, also in accordance with set periods defined in national laws and policies. Instead of deleting data, some States choose to anonymize PNR data, which is the permanent removal of identity information of a person from the PNR record, which is permissible under the Standard.

9.4.38 Standard 9.31(d) makes clear that data does not need to be depersonalized, deleted or anonymized if it is currently being used for law enforcement purposes as defined in a State's legal and administrative framework per Standard 9.25(b). Similarly, a State shall only re-personalize PNR data if the data is used in connection with the purposes outlined in Standard 9.25(b).

9.4.39 Recommended Practice 9.32 suggests a recommended maximum data retention period of five years for States after the transfer of PNR data, with extensions to the retention period allowed if the data is required to be used in an investigation, prosecution or court proceeding. Similarly, Recommended Practice 9.33 recommends that States should depersonalize PNR data within six months of, and no later than, two years after the transfer of PNR data.

Operational considerations

9.4.40 Standard 9.34 provides several measures that are designed as operational considerations conducive to aircraft operators.

9.4.41 Standard 9.34(a) denotes that States shall, as a rule, acquire PNR data using the "push" method, as opposed to accessing aircraft operator systems using the "pull" method. The "push" method allows aircraft operators to remain in control of their systems. The "push" method is aligned with the use of the PNRGOV message format for airline-to-government PNR data transferal as specified in Standard 9.24. The "pull" method allows public authorities from the State requiring the data to reach into ("access") the aircraft operator's system and extract ("pull") a copy of the required data from its systems.

9.4.42 Standard 9.34(b) provides that States shall seek, to the greatest extent possible, to limit the operational and administrative burdens on aircraft operators, while also enhancing the facilitation of passengers.

9.4.43 Standard 9.34(c) requires States not to fine or penalize aircraft operators when no data or corrupted data is transferred due to an unavoidable transmission system failure.

9.4.44 Standard 9.34(d) mandates that States minimize the number of times they request the same PNR data be transmitted for a specific flight. Typically, States request PNR data for a flight two to three times, at 72 and 24 hours before departure, and once at time of departure. States should not require additional messages apart from the agreed upon transmission schedule, except in cases of duly valid urgency, and ideally only for those records which have been created or updated since the last transmission.

Global passenger name record framework

9.4.45 Standards 9.35, 9.36 and 9.37 address means to resolve the conflict of laws surrounding PNR data transfer. As outlined in Standard 9.24, the suite of PNR standards is meant to be implemented as a package, such that a State's legal and administrative framework shall be consistent with all the PNR standards in Annex 9, Chapter 9, Section D.
The PNR Standards have also been designed to function as a global PNR framework governing the collection, use, processing and protection of PNR data, which all States should adopt without difference.

9.4.46 In accordance with Standard 9.35(a) States shall not inhibit or prevent the transfer of PNR data by aircraft operators to a certain State, when that State has implemented the PNR standards in this section. This essentially allows States to establish their individual PNR systems and facilitate data exchanges through a set of baseline requirements as stipulated by Annex 9. This will reduce the need for States to establish bilateral agreements between one another in order to implement an effective PNR system.

9.4.47 Equally, in accordance with Standard 9.35(b), States retain the ability to introduce or maintain higher levels of PNR data protection in accordance with their legal and administrative framework and to enter additional arrangements that go beyond the measures outlined by this suite of PNR Standards, provided that these arrangements do not conflict with the PNR Standards of Annex 9.

9.4.48 Taken as a whole, even if a State requires a higher level of PNR data protection (Standard 9.35(b)), that State shall not inhibit or prevent PNR data transfer to another State which has implemented the suite of PNR Standards in this section (Standard 9.35 (a)).

9.4.49 Whether a State is compliant with the PNR Standards is an important consideration. Standard 9.36 requires States to demonstrate their level of compliance with the standards contained in Annex 9, Chapter 9, Section D to any other State requesting that information. States are to cooperate in this process in good faith, with the goal of ascertaining compliance as quickly as possible to avoid uncertainties and to safeguard the predictability that is essential to the aviation system to operate effectively and economically. Demonstration of compliance can take place through bilateral consultations, as well as the ICAO Compliance Checklist for Annex 9, which contains information on the implementation level of SARPs.

9.4.50 Standard 9.37 outlines that if States must inhibit, prevent or obstruct the transfer of PNR data by aircraft operators to other States, they shall be transparent about their reasons for doing so, including by referencing the implementation level of PNR SARPs. Moreover, States shall take such actions with the intent of resolving the situation that resulted in the prevention or suspension of PNR data transfer in the first place, without making aircraft operators the proxy of such disputes.

9.4.51 The global PNR framework standards are complemented by Recommended Practices 9.36.1 and 9.39 that provide additional guidance to States when determining the compliance of other States with PNR Standards. States should allow other States, which have already shown compliance with PNR Standards, to continue to receive PNR data, at least provisionally, while engaging in consultations regarding demonstration of compliance (Recommended Practice 9.36.1) and States should not fine or penalize aircraft operators when attempting to resolve disputes about PNR data transfer as this would not resolve the situation nor the bilateral conflict (Recommended Practice 9.39).

9.4.52 Finally, States should proactively inform other States when they are preparing a PNR requirement or are making significant changes to an existing PNR programme, with the goal of informing other States of their compliance with PNR SARPs. Moreover, early notification would also allow ample time for States to consult each other on making determinations about compliance (Recommended Practice 9.38).