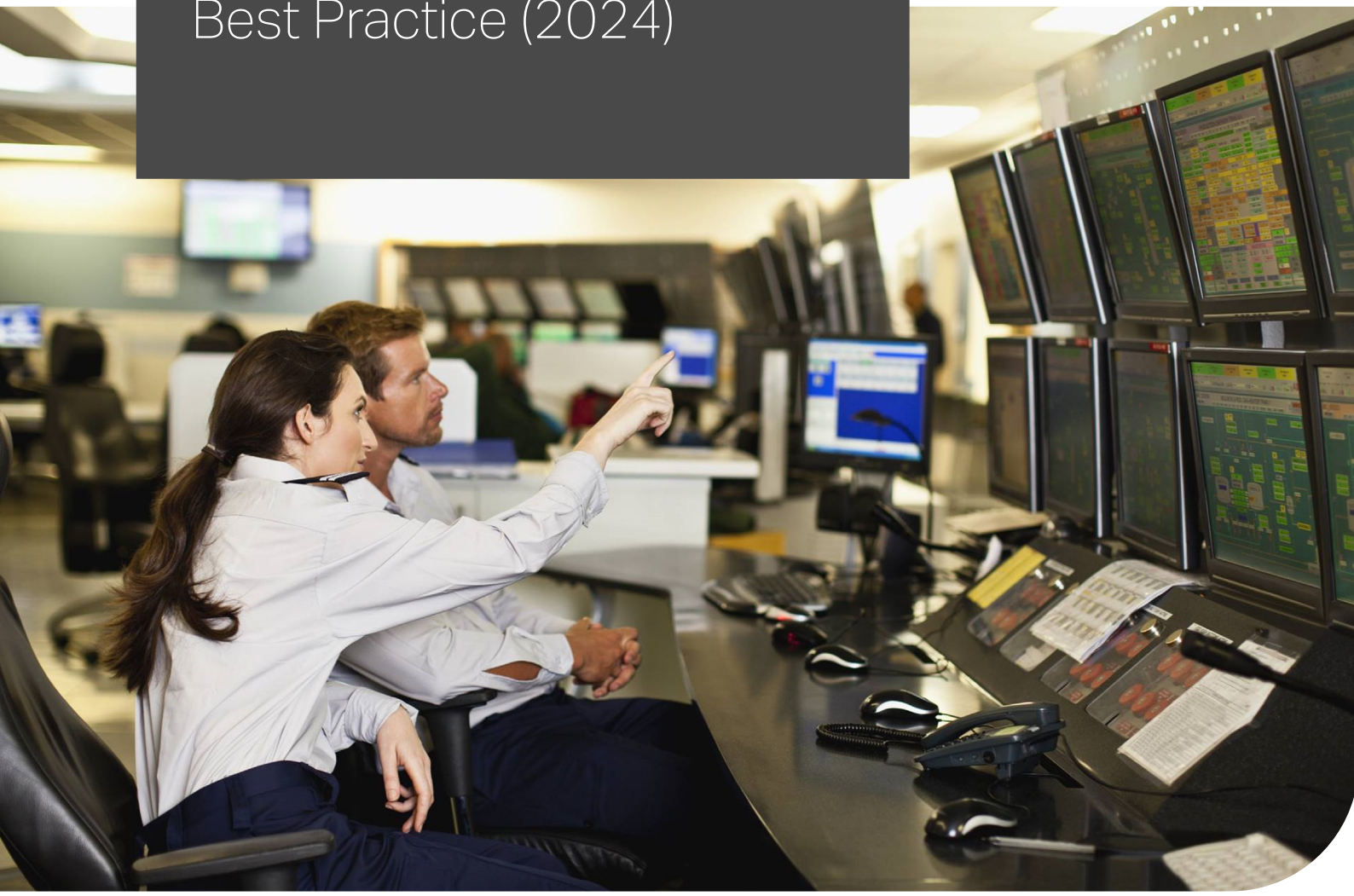
Interactive Advance Passenger Information (iAPI)

Best Practice (2024)



World Customs Organization

IATA

ICAO • OACI • ИКАО

国际民航组织 • منظمة الطيران المدني الدولي

wcoomd.org / iata.org / icao.int

Table of Contents

Acronyms

API	Advance Passenger Information
BGM	Beginning of Message
CAWG	Control Authorities Working Group (IATA)
CLNB	Close-Out Not-on-Board
CLOB	Close-Out On-Board
CUSRES	Customs Response
DCS	Departure Control System
EiT	Encryption in Transit
ERC	Application Error Information
ERP	Error Point Details
FTX	Free Text
iAPI	Interactive Advance Passenger Information
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
MQ	Message Queue
PAXLST	Passenger List Message
PAXLST WG	Passenger List Message Working Group (IATA)
PDSW	Passenger Data Single Window
PLF	Passenger Locator Form
PNR	Passenger Name Record
SARPs	Standards and Recommended Practices (ICAO)
UNSCR	United Nations Security Council Resolutions
UPRI	Unique Passenger Reference Identifier
VPN	Virtual Private Network
WCO	World Customs Organization

1.Introduction

1.1 Purpose

This Best Practice document is intended to provide guidance to States, aircraft operators, and system providers on the policy considerations and business requirements, for implementing and operating Interactive Advance Passenger Information (iAPI) systems.

Its content is the outcome of a collaboration between experts from the IATA Control Authorities Working Group (CAWG) and the IATA PAXLST Working Group and reviewed under the auspices of the World Customs Organization / International Air Transport Association / International Civil Aviation Organization (WCO/IATA/ICAO) API/PNR Contact Committee.

iAPI systems are technically complex, resource-intensive and time sensitive. Authorities planning to implement an iAPI system are invited to read this Best Practice guidance and seek assistance from other States, aircraft operators and system providers to ensure the sustainability and success of their program.

The iAPI Best Practice acts as a companion document to the WCO/IATA/ICAO Guidelines on API (2022) and is meant to be used in conjunction with other relevant guidance material, such as the PAXLST and CUSRES Message Implementation Guides. The PAXLST message is used by aircraft operators to provide API to States which have implemented legislation and the necessary systems to receive, process and analyze the data. The CUSRES message is used by States to provide a response message to aircraft operators.

This Best Practice should be considered as a living document and will be updated for any future requirements / principles as agreed by the Working Groups and the Contact Committee. The ICAO Standards and Recommended Practices (SARPs) referred to throughout the document (e.g., **Standard 9.7**) are those of Annex 9 – *Facilitation,* Sixteenth Edition (2022), to the Convention on International Civil Aviation (Chicago Convention, 1944).

1.2 Background and Overview

All API systems, whether in the batch or interactive mode, are subject to numerous ICAO Annex 9 SARPs, including **Standard 9.7** (requirement to establish an API system), 9.8 (requirement for an appropriate legal basis) and **Standard 9.10** (adherence to PAXLST message format and machine-readable data elements). While API systems are mandatory, States may choose between implementing batch and interactive modes of API. Over 20 States[1] have implemented iAPI as an advanced border control tool, and interest is growing in all geographic regions.

This Best Practice provides a source of information building on the international regulatory and technical frameworks. It provides insight for States to implement an iAPI system optimally based on

[1] At time of publication of this document.

best practices. By following international standards and specifications, in addition to the best practices and recommendations contained in this document, border control authorities can expect to reduce the costs and implementation times of their systems and best ensure adherence from industry stakeholders to their program.

Section 2 of this Best Practice provides an overview of the components and benefits of such systems, such as the two-way communication, pre-travel verification, and the expected input and output of this two-way communication.

In Section 3, the regulatory and legal frameworks surrounding iAPI, both at the international and national levels, are explained. Section 3 also addresses a number of policy considerations. Similar to API and Passenger Name Record (PNR) programs, the foundation for rolling out an iAPI system, is inter-agency cooperation and continuous collaboration with industry stakeholders, aircraft operators, and service providers alike.

Section 4 covers the technical and operational aspects of an iAPI system such as standard passenger data and the travel documents supported, the PAXLST message format, communication methods, transmission timings, CUSRES vetting results and recommendations for achieving greater harmonization, as well as outage and disruption procedures.

An overview of the main categories of costs that States, aircraft operators and service providers may incur is provided for reference further to some aspects of existing iAPI programs that are recognized as best practice.

For additional information on passenger data programs, detailed resources are available on the websites of the three organizations comprising the Contact Committee.

Note – This Best Practice covers iAPI systems compliant with international standards, i.e., those conforming with the specifications for UN/EDIFACT PAXLST messages found in the WCO/IATA/ICAO API Guidelines, as mandated by **Standard 9.10**.

2. What is an Interactive API System?

API provides border control authorities with data in advance of passengers' departure or arrival. These data were traditionally acquired upon each passenger's physical arrival and presentation at an immigration or border control point. iAPI enables an interaction between the aircraft operator and border control authority systems in real time prior to boarding a traveler, bringing significant benefits to authorities and aircraft operators.

This interaction provides greater control for border control authorities. It allows the authorities to issue a Board / Do Not Board response message to the aircraft operator, providing the authorities with the ability to resolve immigration-related issues and/or to prevent individuals from travelling to, entering or, when applicable, leaving their territory. Authorities use the information transmitted by aircraft operators to undertake advance screening of inbound passengers and, when applicable, of outbound passengers. This screening and targeting permits the identification of individuals who may warrant additional scrutiny (i.e., travelers who present the highest risk to border, aviation, or public safety) or are known to be inadmissible.

This interaction also benefits aircraft operators by decreasing the number of inadmissible passengers, and exposure to penalties, costs and responsibilities related to returning inadmissible passengers to their point of origin. Moreover, individuals presenting a threat to aviation security can be identified before boarding, avoiding potential security-related incidents within airport facilities or in aircraft cabins.

iAPI allows for improving travelers' facilitation and experience thanks to faster clearance of low-risk passengers. The use of technology and automated tools can lead to a reduction of the workload of aircraft operator staff and of border management officers and better allocation of resources, including reducing the need to deploy immigration liaison officers abroad.

Accordingly, iAPI can provide States and aircraft operators with tangible benefits in the identification of inadmissible passengers based on security and immigration purposes.

2.1 Two-Way Communication

Similar to an API message, the transmission of a traveler's travel document information by the aircraft operator to a State is central to an iAPI message. Yet the overarching concept of a robust iAPI system is the ability for two-way communication, where the State responds in real-time to aircraft operators on a per passenger basis. These interactive responses (also called CUSRES messages) provide aircraft operators with real-time messages from the State, for permitting or preventing boarding of individual passengers, or with specific instructions on how to proceed with each passenger (see Section 4.6 CUSRES Vetting Results). These message responses are based on applicable legislation and the scope of the iAPI program provided to aircraft operators and may take the form of directives or guidance. Authorities also have the capability to send unsolicited messages to the aircraft operators to update passenger status provided earlier (see Section 4.7 Unsolicited Messages).

These boarding response messages to the aircraft operator depend on the ability of a State to conduct checks against its databases. The State uses the travel document information as a pointer to conduct checks against multiple databases related to security and immigration. The vetting against immigration

and law enforcement records permits the identification of issues falling outside the remit of aircraft operators' pre-departure document checks.

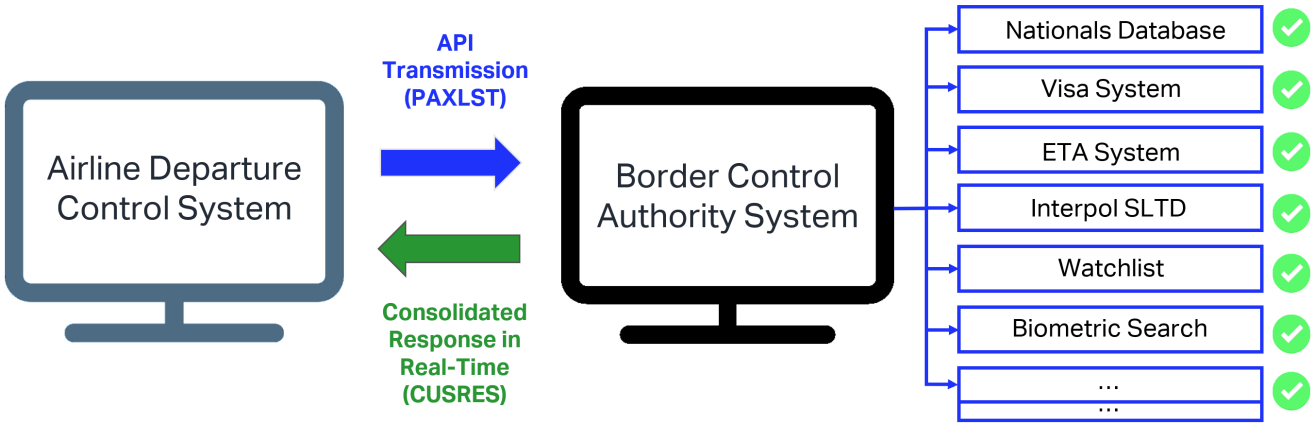
2.2 Pre-Travel Verification

As a best practice a State should integrate its iAPI system into two core areas:

- Security watch-listing of national and regional databases to identify known individuals who are a risk to national security or are otherwise inadmissible; and

- Immigration and travel document checks against databases of national travel documents, travel authorizations (visas and electronic travel authorities), permanent residents, entry/exit records and the INTERPOL Stolen and Lost Travel Documents (SLTD) database.

Relevant National and International Databases



With an iAPI system, States can extend their border control checks at the pre-travel phase, achieving significant benefits for border and aviation security. States can inhibit the issuance of boarding passes, passengers' journeys and even access to the sterile area of an airport.

For instance, when a State requires third-country nationals to obtain an online or electronic travel authorization, the passport data received via the iAPI message is used by the State to identify whether an individual's travel authorization is on file. The same identification process can verify a consular issued visa affixed to a traveler's passport. Moreover, iAPI systems do away with the need for passengers to present, and for aircraft operators to check, or even communicate, the travel authorization reference number, since the transfer of the passport details (primary travel document) will be used by the State as a pointer to the visa record.

However, iAPI systems should be able to accept and process additional documents such as visas and residence permits to resolve negative responses. For instance, if a valid visa is affixed to an expired passport, the communication of the valid primary travel document details would result in a negative result, since the State is not able to match the visa record with the transmitted primary travel document details. In order to generate a positive result, the State needs to locate the visa record. In this case, the

visa details are captured and transmitted by the aircraft operator in a subsequent message. The Recommended Practices for using an iAPI system to validate online travel authorizations to travel are outlined in Annex 9, Chapter 9, Section C – Electronic Travel Systems (ETS).

Health checks (prospective): With the unprecedented disruption to international civil aviation caused by the COVID-19 pandemic, considerations have been given to extend iAPI system capabilities to include health-related checks in addition to security and immigration checks. While limited experience has been gained with rolling out such capabilities, it remains a tool as part of a national preparedness plan for future public health emergencies of international concern.

To collect and verify public health-related information[2] required for entry prior to travel, States can set up a government digital health platform (**Recommended Practice 10.6**). A government digital health portal enables the verification that passengers have provided to the concerned authorities the required public health proofs and information[3].

Integration of the information collected through a government digital health platform into an iAPI architecture, can enable authorities to bind passengers' travel document details with this information. The verification of health-related information then results in a Board/Do Not Board to the aircraft operator as part of a combined iAPI response message (**Recommended Practice 10.7**).

Adding the health-related check result in an iAPI response would not change existing submission standards: the same travel document and flight information is transmitted from the operator to the destination government. It is to note that a passenger may not have fulfilled all health-related requirements prior to travel, but options are available to do so upon arrival. This will be reflected as a "Board" response message to the carrier.

2.3 Expected Input and Output

Several basic rules apply to all iAPI systems. These rules provide predictability with the input provided by aircraft operators to border control authorities, and the output from border control authorities to aircraft operators. This harmonization provides for interoperability between aircraft operator and border control authority systems. These basic expectations ease the implementation for aircraft operators that must connect their systems with multiple countries, and for States to connect with the systems of all aircraft operators operating in its territory. These principles should be considered from the onset of an iAPI program.

Input

- Provision of passengers' travel document data by aircraft operators to border control authorities is limited to data contained in the machine-readable zone (MRZ) of travel documents[4] (see ICAO Document 9303).

[2] For example, a State requires a vaccination or test certificate, a Passenger Locator Form (PLF) replete with contact tracing data from the traveler, as well as self-declaration form.
[3] For additional information, please refer to the IATA Best Practice for Government Digital Health Platforms (2023).
[4] As per the specifications contained in ICAO Doc 9303 Machine Readable Travel Documents, 2021

- All information required shall conform to the specifications for UN/EDIFACT PAXLST messages found in the WCO/IATA/ICAO API Guidelines as mandated by **Standard 9.10**. This Best Practice addresses only those systems compliant with this ICAO Standard.

- On the passenger-level, the data sets for batch API and iAPI messages are the same, i.e., travel document data, except that the iAPI message includes the Unique Passenger Reference Identifier (UPRI). The UPRI is used by States to provide passenger specific response messages and is also used by the aircraft operator for any required acknowledgements.

- Provision of travel document data is usually limited to a single transmission. However, additional transmissions of document data become necessary when qualified changes in travel document data occur. For instance, the initial transmission could be based on a web check-in platform, where the passengers can provide self-asserted travel document data. Manual entry of data often leads to errors and can mean inaccurate data is transmitted to border control authorities at this point. A second transmission is required for correcting the data with machine-assisted capture of the travel document by an aircraft operator's agent.

- iAPI messages at the passenger level contain check-in information and may include baggage and seating information if they have been collected at this point.

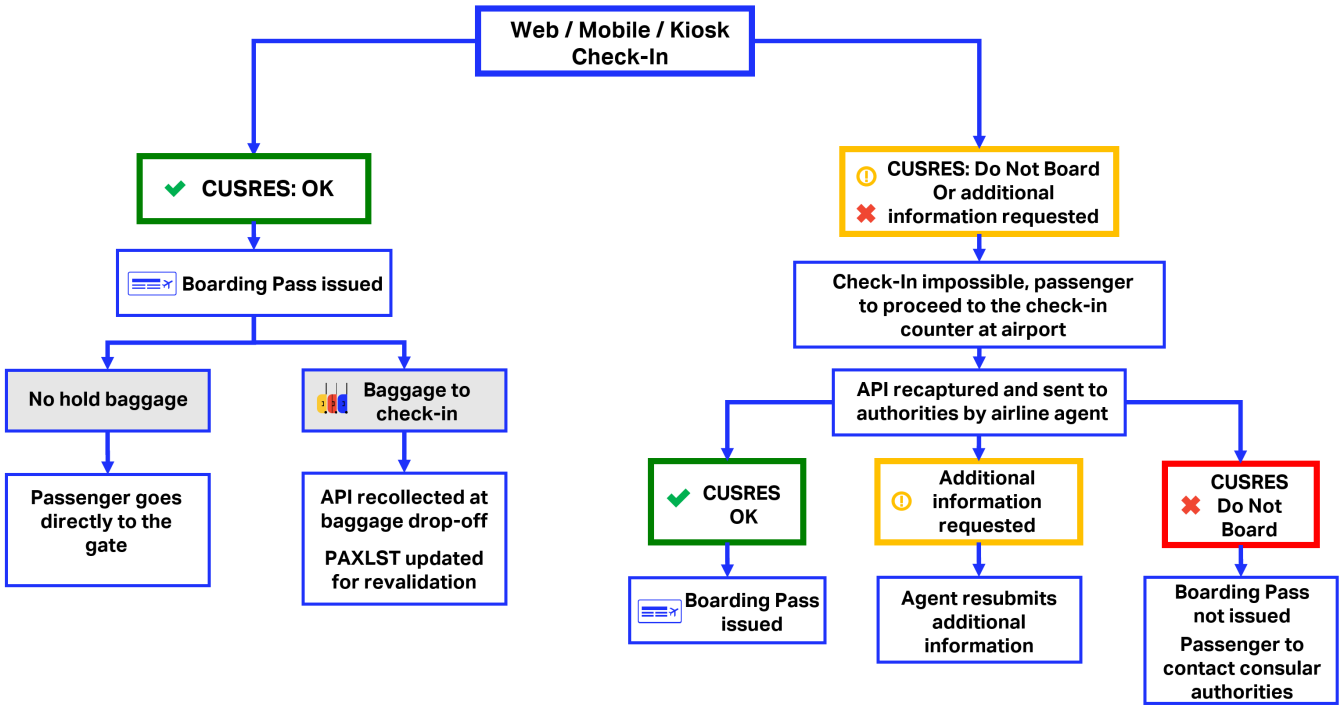
- Actions like change of seating and baggage information are not qualified changes and do not trigger a new interactive message as this information is not travel document data. If these additional check-in details are required, those may be found in a batch API message or within a PNR message.
- Batch API messages at the flight level contain passenger and flight information, including the number of passengers. Depending on the message version requested by the State this may contain baggage and seating information. In an iAPI system, the number of passengers on the flight is reported by the close-out message.

Output

- A primary feature of an iAPI system is to provide an immediate response, within a maximum of 4 seconds, to the aircraft operators within the normal check-in process times (see Section 4.5 Transmission Timings). To facilitate this, an iAPI system should be integrated into aircraft operator's Departure Control System (DCS) interfaces.

- iAPI systems should provide aircraft operator's check-in staff with real-time, unambiguous "Board/Do Not Board" response. In the case of a Do Not Board message, additional information may be provided to the operator whether the vetting result is immigration or security related. Further instructions on how to proceed may be provided. See Section 4.6 for the recommended codes to be used in CUSRES vetting results.

Generic Check-In Process with iAPI



3. Regulatory and Policy considerations

3.1 International Regulatory Framework

Passenger data programs including iAPI are subject to international regulations, principles, guidelines, and technical standards. The development and maintenance of this framework aim at facilitating the implementation of consistent and orderly passenger data programs by both border control authorities and industry to achieve costs and resources efficiencies.

SARPs and basic rules pertaining to passenger data programs are developed and maintained respectively in ICAO Annex 9 – *Facilitation* to the Convention on International Civil Aviation (Chicago Convention, 1944) and the International Convention on the Simplification and Harmonization of Customs Procedures (Revised Kyoto Convention) (WCO).

Moreover, a series of United Nations Security Council Resolutions (UNSCRs), such as UNSCR 2178 (2014), UNSCR 2309 (2016), UNSCR 2368 (2017) and UNSCR 2396 (2017) mandate Member States to receive and analyze API and develop the capabilities to receive and analyze PNR data.

The WCO/IATA/ICAO Guidelines on API (June 2022) establish internationally recognized standards to which border control authorities, aircraft operators and other passenger service operators implementing, and operating API systems should adhere to. The API Guidelines apply to both modes of API, batch and interactive.

Standard 9.7 mandates Contracting States to establish an API system, whether it be in batch or interactive mode. States not complying with this international obligation have to officially notify ICAO by filing a difference. The implementation of the API standard is verified through the ICAO Universal Security Audit Program (USAP). The implementation of an iAPI system is encouraged by Annex 9 **Recommended Practice 9.16**, therefore recognized as being a desirable practice, but is not mandated.

Standard 9.10 mandates that the data required conforms to the specifications of ICAO Doc 9303 and that the information required conforms to the specifications for UN/EDIFACT PAXLST messages found in the WCO/IATA/ICAO Guidelines on API.

The development of iAPI systems by States can as well be understood in the context of **Standard 1.4**, a general principle, which highlights that Contracting States shall develop effective information technology to increase the efficiency and effectiveness of their procedures at airports. Overarching Annex 9, Articles 13 and 22 of the Chicago Convention stipulate that States shall facilitate international air travel and that the aviation community must comply with the laws and regulations of States pertaining to entry, clearance, immigration, passports, customs, and quarantine. When well implemented, an iAPI system can improve operations and enhance security.

3.2 National Policies and Regulations

Each border control authority may have different processes for establishing their respective national legal authority for API, but it is a common process for a government to approve legislation that is

thereafter signed into law. While national legislation varies from country-to-country, there is a notable degree of commonality within the provisions of such legislation.

National Legislation

Aircraft operators do not systematically collect and retain travel document information from their passengers. They do not need this information in the normal course of their business, i.e., for operational and/or commercial purposes. It is therefore essential for States to provide a legal basis to aircraft operators to allow them to require this information from their customers, which falls outside the scope of the information necessary for the execution of the transport contract (as per general data protection principles).

States need to establish a clear legal framework (e.g., legislation, regulation, decree) before implementing API systems, as highlighted by **Standard 9.8**. The legal provisions must be clear for aircraft operators to collect, process and transmit API data to border control authorities, and do so in accordance with applicable national legislation. The legal framework must as well include rules for the collection, use, processing, and protection of data by authorities, along with measures to safeguard individuals' privacy.

To ensure clarity, just as in the case of API, legislation should be enacted to process the information at the pre-travel phase, understanding that this is the same information that authorities would process at the entry point upon presentation of travel documents by passengers. More information on the legal framework pertaining to API can be found in the WCO/IATA/ICAO Guidelines on API.

When specifically implementing an iAPI system, updates to the existing legal framework and technical specification documents adopted for batch API are required. The scope and purpose of the data collection should be expanded due to the interactive nature of the iAPI process. A key point to include in the regulatory framework is information on the vetting response providing aircraft operators with boarding instructions. The Passenger Data Single Window (PDSW) as outlined by Standard 9.1 is particularly relevant to the legal framework for iAPI by enabling the generation of a consolidated interactive response message.

The actions to be taken by aircraft operators for each vetting response need to be specified in the national legal and administrative instruments. Carriers will need a clear legal basis to deny boarding to passengers if a Do Not Board vetting response is received.

Data Protection and Privacy Considerations

Data privacy and data protection legislation has been enacted in many countries to protect individual rights to privacy and to allow individuals to exercise their rights relating to the use of their personal data. The nature of API (basic personal information that appears in an official travel document) leads to extensive discussions globally between border control authorities and aircraft operators to identify best practices and to ensure both aircraft operator and government systems are communicating properly, and to ensure the highest level of privacy protection. More information on these best practices is available in the WCO/IATA/ICAO Guidelines on API.

A great benefit of iAPI systems is that they can limit the handling by aircraft operators of personal information of passenger to what is contained in their travel documents. With pre-travel verification processes and systems, information required by authorities can be collected directly from passengers through the travel authorization process and as well through mobile apps or digital travel portals

(destination addresses, customs declaration, travel history, etc.) Based on the transmission of a traveler's travel document data by aircraft operators at check-in, authorities can take informed decisions based on the information collected in advance and on information readily available through national and international databases.

Solutions such as government digital health platforms already address the risks of proliferation of personal medical data through this interaction between authorities and passengers, removing aircraft operators as the data broker for data falling outside their remit. Prospectively, integration of government health digital portals with the iAPI system leads to even greater data protection and privacy. Airline staff do not need to verify health-related documentation.

Carriers' Liability and Penalties

With an iAPI system, States take the ownership of decisions to allow passengers to arrive at their borders. Several challenges faced by aircraft operators with batch API, or in the absence of an API system, are solved with the iAPI two-way communication.

Typically, aircraft operators have an obligation to take necessary precautions at the point of embarkation to ensure that persons are in possession of the travel documents prescribed by the State of transit or destination (Standard 3.33). Aircraft operators' staff are, in effect, responsible for determining if each passenger is adequately documented to travel. With an iAPI system, aircraft operators will be notified if a travel document belonging to a passenger is not recognized by border control authorities if a travel authorization or other immigration information is missing. In this way, aircraft operators' staff are not acting on behalf of border authority in determining the admissibility to travel of passengers.

In such settings, aircraft operators' exposure to sanction are significantly reduced if an OK to Board response was provided based on the pre-travel verification performed by authorities, and the passenger is found to be inadmissible upon arrival. Some States have reflected this principle in their legislation.

Where States have developed the ability to conduct checks against their databases, sanctions related to API data quality have decreased as well since resubmission of the travel document information by the aircraft operator can be requested. With iAPI, sanctions are typically limited only to cases where the data has not been sent, sent in the wrong format, at the wrong time, or if the aircraft operator did not comply with the vetting responses.

Fines and penalties should not be imposed on aircraft operators for any errors caused by a systems failure which may have resulted in the transmission of no, or corrupted, data being sent to authorities in accordance with API system requirements (**Recommended Practice 9.14**).

When it comes to passengers who hold and use multiple travel documents for one journey, an iAPI system may offer the possibility of solving travel document data discrepancies prior to departure, i.e., a travel document used by the passenger at check-in and its details provided for API purposes, and a second travel document presented by the passenger upon arrival at the border control point. Should the first travel document not be found in authorities' databases, the aircraft operator may prompt the passenger to provide a secondary travel document.

The liability towards aircraft operators' customers also changes with an iAPI system. In the case of Do Not Board responses, aircraft operators should not be held responsible or liable for any accommodation or transportation requested by the passenger as a compensation. National legislation should be clear in that regard.

3.3 Stakeholders Cooperation

The implementation of a national iAPI system requires cooperation and coordination among the main stakeholders: the border control agency and other relevant national agencies, aircraft operators operating to their territory and system providers. These stakeholders should be consulted before the development, change, adoption, and implementation of an iAPI system. International cooperation may be available from other country's border control authorities and international organizations such ICAO, other United Nations Agencies and IATA can offer assistance and support.

To ensure the best cooperation among the main stakeholders, attention must be paid to several key elements.

Any passenger data system that aligns with international standards and guidelines will ensure the support and cooperation of all stakeholders. This ensures faster and more economical implementation. Clearly written standard operating procedures and technical specifications for aircraft operators and service providers' systems to be programmed towards will increase this buy-in.

Aircraft operators must be free to select the system provider of their choice. Imposition of a specific provider by a State can mean an aircraft operator has to sign contracts with several service providers, with the inherent costs and burden that are multiplied by the number of destinations serviced by the aircraft operators. Authorities should allow more than one service provider for data transmission in their legislation and avoid sole sourcing.

To improve collaboration between border control authorities and aircraft operators, compliance monitoring and penalty frameworks are preferably based on periodic or trend-based enforcement, as opposed to a case-by-case basis. This enables reducing the burden of compliance monitoring as well as the monetary impact of penalties on aircraft operators. As part of their compliance framework, States should implement policies and procedures directed at improving aircraft operator compliance by providing strategic feedback on their performance.

When border control authorities provide aircraft operators with timely compliance monitoring information, it enables the aircraft operator to conduct internal investigations and implement corrective actions. The more information an aircraft operator can receive about non-compliance, the better able it will be to address the source of the challenge.[5]

iAPI systems should be capable of 24/7operation reflecting the 24/7 global particularity of air travel. As such, control authorities and aircraft operators should be able to communicate promptly in case of system outage and failure and provide the appropriate operational and technical support to return to

[5] More information on the importance of reporting non-compliance issues can be found in CAWG Considerations for Collaboratively Improving Advance Passenger Information Data Quality.

standard operations as soon as practicable (**Recommended Practice 9.2**). Control authorities should supplement these systems by providing aircraft operators with 24/7 technical and operational support. A support center is a key component of a successful iAPI program as well for mitigating check-in issues resulting from no board response. This collaboration relies on each stakeholder to provide the appropriate level of contact support (**Recommended Practice 9.4**).

Passenger Data Single Window

As highlighted in the Section 2.2. Pre-Travel Verification, with the effective use of iAPI, there is little need for an aircraft operator to communicate data which the State already has on file. However, locating the right records and required data within a State's border management infrastructure based on the travel document data requires strong inter-agency cooperation, including through the PDSW.

The overarching principle of the PDSW is to create efficiencies in data transmission and avoid duplication of costs and resources for both aircraft operators and States. It can also support data protection since the data is sent to one recipient.

Annex 9 defines a PDSW 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.[6] Requests for iAPI data and responses back to aircraft operators should originate from only one agency following the "single window concept". The single window applies to immigration related entry requirements and to aviation security measures.

The organizational framework and the cooperation arrangements within the PDSW should already be in place before implementing an iAPI system given the interactive nature of the communication with aircraft operators and the number of databases that may be checked in order to provide the CUSRES vetting result. Accordingly, States should share the content of API messages within their national border management framework, with all public authorities with a legal remit to use the data. The CUSRES result provided to aircraft operators has to be accurate to avoid cumbersome situations such as offloading a passenger following an unsolicited message.

Crew Members

The primary function of an iAPI system is to vet passengers' ability to travel. Crew members are out of scope for the purpose of an iAPI system.

Information about crew members is maintained in crew systems that are different from the aircraft operator's DCS. It is technically not feasible nor operationally manageable for aircraft operators to implement an iAPI process for their crew members. IAPI systems rely on a check-in transaction to trigger a CUSRES response, however there is no check-in system for crew. As such, crew data is never included in any iAPI message or in the close-out message. Crew data is being transmitted to control authorities in a batch API message and/or through the General Declaration (GenDec).

Additionally, the vetting of aircraft operators' crew is performed by most States before a crew member ID or certificate is issued. Routine vetting processes are in place for those States that issue

[6] For more information refer to Passenger Data Single Window Annex 9 Standard 9.1 and Recommended Practice 9.1.1.

Crew Member Certificates (CMC) even after issuance. In additional, carriers also continuously vet employees for employment purposes. The channels at borders used by crew upon arrival are usually not the same as for passengers.

It is to note that deadhead crew transported on Another Airline (OAL) flight will be reported as a passenger and therefore be subject to iAPI vetting because they are issued with a reservation. Additionally, some iAPI proprietary systems may offer some functionalities pertaining to crew members and transmission of data to border control authorities. These proprietary systems are not covered by this Best Practice that focusses on international standard-based systems.

Implementation Timeline

Implementing an iAPI program is technically complex, resource-intensive and a time sensitive undertaking. States wishing to implement an iAPI program should consult with aircraft operators, service providers, and local and international trade associations prior to implementing national laws and legislation to mandate the use of an iAPI program. Early consultation will ensure all stakeholders are setting achievable timelines for the introduction of national legislation, the writing of supporting guidance documents, for service providers and aircraft operators to make the required system changes and upgrades to their IT infrastructure, and finally for testing and certifying the system prior to activation of the iAPI program.

As a guide, it is recommended that States plan a period of 12 to 36 months for the implementation of a standardized iAPI program, in order to complete the necessary legislative and regulatory changes, IT development and system implementation. Timelines need to be extended when States try to implement measures in the iAPI program that differ from the WCO/IATA/ICAO Guidelines on API. Costs can be minimized when border control authorities choose a system provider that follows international iAPI standards to ensure interoperability of the systems. Non-standard solutions and proprietary products involve additional programming costs to accommodate different layouts and will extend implementation time.

It is recommended that authorities employ a progressive implementation plan, starting with a few aircraft operators and/or routes. This progressive implementation also allows for testing the robustness of the systems and procedures.

4. Functional Requirements

4.1 Standard Passenger Data and Supported Travel Documents

Provision of required iAPI data by aircraft operators to Control Authorities is limited to the data contained in the machine-readable zone of travel documents (see ICAO Document 9303) and shall conform with the specifications for UN/EDIFACT PAXLST and CUSRES messages found in the WCO/IATA/ICAO Message Implementation Guide (**Standard 9.10**).

iAPI systems should be able to accept and process secondary documents such as visas and residence permits to self-resolve negative responses. For example, a traveler has a relatively new Australian passport, but their United States Permanent Resident Card was issued and tied to their previous passport. In this scenario, the United States might return a Do Not Board response requiring the aircraft operator to enter a secondary document such as a permanent resident card to satisfy entry requirements. The same argument might apply to visas.

States are encouraged to have the ability to electronically link secondary documents to the primary one for reference and validation. Whenever authorities perform such a document validation process based on the transmitted primary travel document data, the additional transmission of secondary travel document data (visa or travel authorizations) becomes obsolete.

4.2 Passenger and Flight Messaging

iAPI messages are sent on both passenger and flight levels.

iAPI Passenger Level

At the passenger-level, the iAPI message can be transmitted one or multiple times, including:

- The time prior to departure when the aircraft operator is required to provide the information or when the border control authority is entitled to receive the data according to applicable legislation
- During the initial check-in transaction
- Each time already-transmitted data for the passenger is updated, including but not limited to travel document and itinerary information.

Furthermore, there are iAPI message options to indicate when a passenger's reservation for whom an initial iAPI message submitted has been cancelled, or that the reservation of one or more passengers in a group reservation has been split (divided) or cancelled.

Passenger level transmissions are focused on one or more specific passengers traveling together and should include flight details for any of the flights in their intended journey required by the receiving jurisdiction. For example, if two passengers in a single reservation are flying a connection from MSP-EWR-LHR operated by a US-based aircraft operator, that operator may include both passengers and the details of both flights in a single PAXLST message.

To meet service level objectives for response time of an interactive transaction, many States may limit the number of passengers included in a single interactive message, even when they are all in the same reservation and on the same itinerary.

iAPI Flight-Level

At the flight level, iAPI messages are submitted once the flight has departed. This is called the Close-out Message and is used to reconcile the actual passengers on board at departure. There are two options for construction of this message:

- Close-Out On-Board (CLOB) – lists the passengers on board at time of departure
- Close-Out Not-on-Board (CLNB) – lists the passengers for whom data has already been transmitted who were not on board at time of departure

The Close-out Message contains only two sets of data for the passengers:

- The PNR Record Locator; and
- The Unique Passenger Reference Identifier (UPRI) for each passenger.

Furthermore, there are iAPI message options to indicate that the flight has been cancelled or that the flight itinerary has been changed.

When baggage and seating information are required by the border control authorities, an iAPI program can be supported by a batch API message which is sent with additional data collected after check-in transaction has been performed (adding baggage, performing seat change).

4.3 Message Types and Format

Standard message formats such as UN/EDIFACT PAXLST and CUSRES should be used to avoid difficulties and the significant additional costs that would be caused by the introduction and use of bespoke national standards.

Full specifications for PAXLST and CUSRES messages can be found in the dedicated Message Implementation Guides, available in the IATA API PNR Toolkit:
https://www.iata.org/en/publications/api-pnr-toolkit

PAXLST Message

The core data elements other than message header and footer are:

- Flight details (aircraft operator, flight number and date)
- Passenger name and surname
- Passenger sex

- Passenger date of birth
- Passenger nationality
- Travel document type
- Travel document number
- Travel document expiry date
- Travel document issuing country (depending on the PAXLST version used)

Additional information, such as the UPRI, PNR locator, verified information indicator, contact, seat, and baggage information may also be present in a PAXLST message, depending on the message version and existence of the related information in the aircraft operator system.

Depending on the functional use-case, the BGM segment which acts as the beginning of the message, shall be used to provide the reason for message transmission: BGM+745' Indicates initial passenger data submission.

This segment also transports a message identification which shall be used as indication regarding the flight or passenger dynamics.

CUSRES Message

The purpose of the CUSRES response is to transmit the passenger status to the aircraft operator. This information is provided by the border control authorities following security and immigration checks.

The beginning of the message indicates what response type the client application should expect as follows:

BGM+962' Indicates response message
BGM+132' Unsolicited message
BGM+312' Acknowledgement message

Passenger status is provided in the ERC segment in Group 4 (Application Error Information). Border control authorities shall establish bilateral agreements for the values appearing in the data element within this segment (9321).

Border control authorities may provide special instructions or additional information on the response message within the FTX (Free Text) segment in Group 4. Border control authorities may establish bilateral agreements for the values appearing in data element 4440.

Examples:

FTX+AAP+++ CHECK-IN OK'
FTX+ AAP+++ERROR ON PAXLST – ITINERARY'

References to the flight or transaction may be provided within the RFF segment in Group 3, using different identifiers.

RFF+**AF**:OZ1234'	Air Carrier code (OZ) and Flight Number (1234)
RFF+**TN**:1234567890'	Transaction Reference Number (1234567890)

For Interactive PAXLST / CUSRES messaging, inclusion of RFF, Transaction Reference Number and its Revision Identifier may be declared as mandatory elements.

RFF segment in Group 4 on the other hand is used to indicate passenger reference type as follows:

RFF+**AVF**:WWHPDS'	Passenger reservation reference number
RFF+**ABO**:BA1321654987'	Unique Passenger Reference Identifier (UPRI)
RFF+**AEA**:123456789'	Border control authority reference number (Optionally issued by a State to facilitate entry)

Example of a query – response mapping and implementation suggestion

Query:

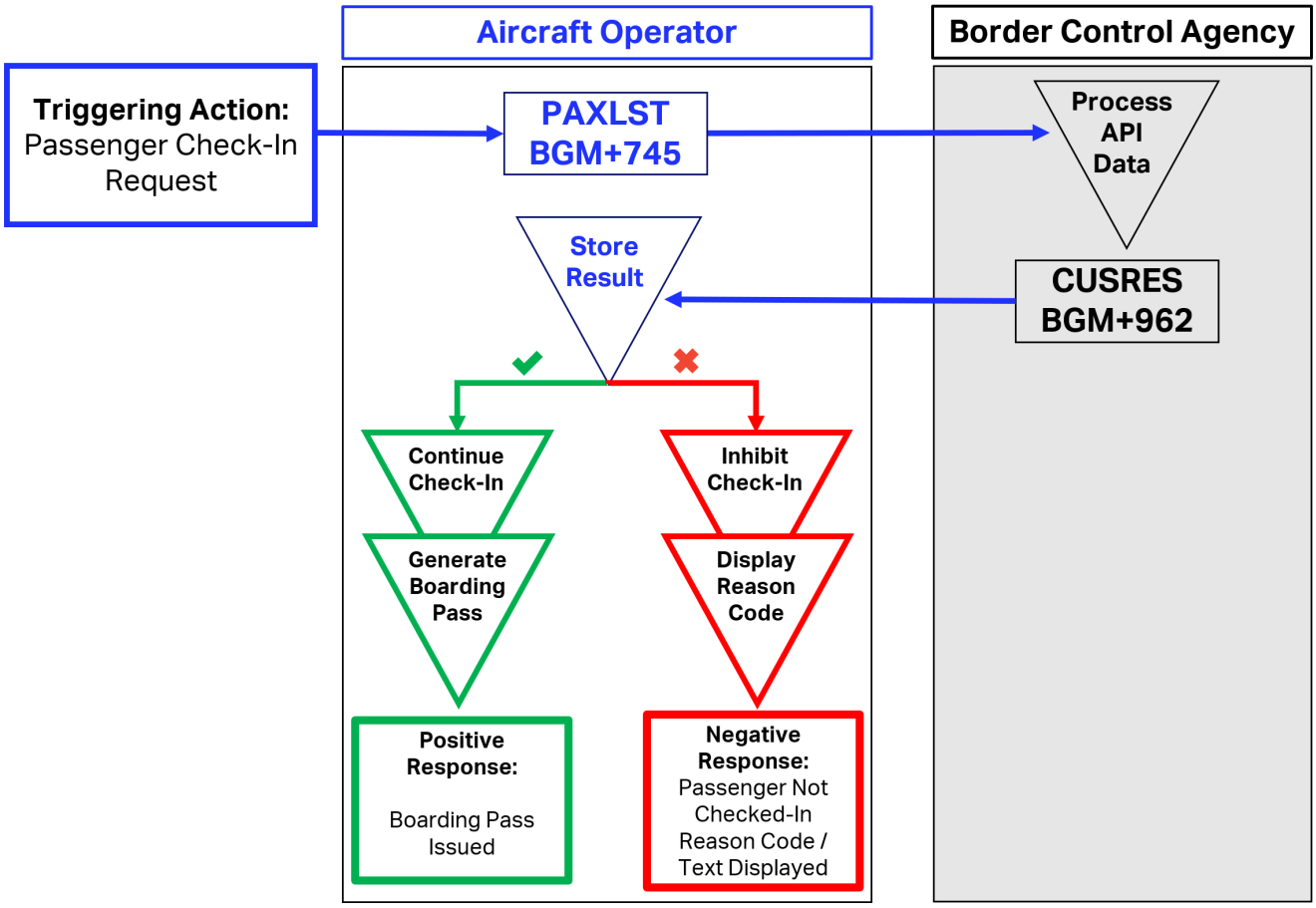
UNB+UNOA:4+API123+STATE+080708:0545+000000011' UNG+PAXLST+AIRLINE+STATE+080708:0545+11+UN+D:05B' UNH+PAX11+PAXLST:D:**05B**:UN:IATA' BGM+745' RFF+TN:**TRANSACTIONREFNB123**:::1' […] RFF+AVF:**WWHPDS**' RFF+ABO:**BA1321654987**' [...] UNZ+1+000000011'	 Message version 05B Transaction reference number Passenger reservation reference number Unique passenger reference identifier

Response:

UNB+UNOA:4+API123+STATE+080708:0545+000000011' UNG+CUSRES+AIRLINE+STATE+080708:0545+11+UN+D:05B' UNH+PAX11+CUSRES:D:05B:UN:IATA' BGM+962' RFF+TN:**TRANSACTIONREFNB123**:::1' [...] ERP+**2**' RFF+AVF:**WWHPDS**' RFF+ABO:**BA1321654987**' ERC+**X**' [...] UNZ+1+000000011'	 Transaction reference number Error Point – Detail Level Passenger reservation reference number Unique passenger reference identifier Application-Level Error (Response Code)

The diagram below illustrates the flow used during check-in, where API data is being sent for the first time for the passenger. The diagram combines the initial transmission and check-in processing.

Initial Transmission at the Time of Check-In



4.4 Communication Method

Secure and reliable exchange of API data and boarding response message using PAXLST and CUSRES messages is critically important. API data is classified as personally identifiable information and should be handled securely using commonly accepted encryption techniques.

The messages should also be exchanged using a reliable mechanism, which is particularly important for batch API as it is a one-way transmission for which there is no response. The aircraft operator and border control authority should be able to trust that messages generated and sent by the aircraft operator are not lost in transit and arrive in a timely manner to the border control authority. iAPI messages shift the focus toward timely delivery to meet service level objectives for response times, as the CUSRES indicates receipt of the PAXLST by the border control authority.

Whilst the border control authority and aircraft operator may implement any mutually acceptable communication method, a Message Queue (MQ) paradigm is well suited for the task. Commonly available MQ platforms facilitate asynchronous delivery while providing encryption in transit (e.g., Transport Layer Security – TLS). Message assurance / persistence and delivery acknowledgements are common features suited for batch API. Message correlation over paired sets of queues facilitate iAPI communication. MQ platforms are commonly used by aircraft operators.

Data Security

API data consists of sensitive personally identifiable information concerning passengers and therefore should be handled accordingly. Encryption in Transit (EiT) is encouraged whenever possible, including transmissions between aircraft operator and border control authority. Certificate-based encryption is commonly used and may be implemented directly in the MQ connection channel definitions of the MQ platform, or by encapsulation of that traffic in a sufficiently encrypted VPN tunnel. As MQ is inherently asynchronous in nature and supports message persistence, MQ platforms often write data to persistent storage. Data at rest in the persistent storage mechanism should also follow acceptable data security guidelines.

Transmission Exchange Pattern and Priority

API data in the form of PAXLST and CUSRES messages are exchanged between aircraft operator and border control authority using two basic patterns:

1. **Asynchronous Two-Way**

This pattern is used when both PAXLST and CUSRES messages are exchanged, but each message is processed independently as it is received. It is typically used in iAPI programs for lower priority business functions (those not requiring an immediate response). Examples include early or "pre-" transmission of API data prior to check-in, transmissions of larger messages, transmissions of messages for events more informational in nature, such as Reservation Cancellation, etc.

The aircraft operator generates and sends PAXLST messages to the border control authority triggered by the applicable business event, such as a time before departure, passenger check-in or boarding request, update of already transmitted passenger data, reduce number in party, etc. As the border control authority receives and processes the messages, it may (or may not as dictated by the use case) generate a CUSRES to be delivered back to the aircraft operator in order to acknowledge receipt of the PAXLST, provide an updated boarding response or both. The aircraft operator processes the CUSRES upon receipt.

2. **Synchronous Two-Way**

This pattern is used in high-priority use cases where a response is required in-line with handling the triggering business event. For example, the aircraft operator is processing a request to check-in a passenger and must transmit API data the border control authority in order to receive a required boarding response before continuing and completing the check-in process.

When an MQ platform is used, this pattern is accomplished through the use of a pair of queues/queue paths. The first queue path is used to asynchronously deliver messages from the aircraft operator to the border control authority. The second is used to deliver messages from the border control authority to the aircraft operator. Header fields from the MQ platform are used to correlate messages sent along the opposite path. The sender of the first message allocates a unique Correlation ID value and assigns it to the MQ header of the message before sending it to the recipient. The recipient is expected to copy the Correlation ID of a message it receives into any response that it generates and sends in the opposite direction. After sending the initial message, the sender waits until a message arrives using the same Correlation ID it used when sending the request, or a timeout period has elapsed.

iAPI programs use two possible message pairings:

PAXLST -> CUSRES is used for most transmissions, especially those originated by the aircraft operator

CUSRES -> CUSRES is used for the use case in which the border control authority sends an unsolicited message to the aircraft operator to provide a new boarding message. The aircraft operator is expected to confirm receipt of the unsolicited message and in some cases provide the disposition of the passenger and or their boarding pass (e.g., checked in, boarded or not) in a CUSRES returned to the border control authority.

It is generally accepted that all Synchronous Two-Way message exchanges should be considered ***High Priority*** whilst Asynchronous Two-Way messages are generally considered ***Low Priority*** and the term *batch* is used. Use of the term *batch* in this context is not to be confused with batch API. Rather it relates to the fact that the request and response messages are processed independently.

Batch API transmission takes place using Asynchronous One-Way pattern, where no CUSRES messages are used and there is no transmission path in the reverse direction from the border control authority to the aircraft operator. When an MQ platform is used, queue and message delivery need only be configured in one direction.

Best Practices for Communication Through an MQ Platform

Best practices for the exchange of Interactive API messages between aircraft operators and border control authorities can be summarized as follows:

- Select a MQ platform commonly supported by aircraft operators and border control authorities over use of another mechanism such as FTP or SFTP
- Configure the MQ platform to use Certificate-based TLS for communication channels with cipher and key management practices meeting the requirements of data security best practices. Ensure any data at rest used by the platform is also sufficiently encrypted and protected from unauthorized access.
- Create Queue and Transmission Channel definitions to facilitate message exchange for Asynchronous and Synchronous processing using four message delivery paths:
    - Asynchronous processing used when the aircraft operator system does not require an immediate response. It generates and transmits PAXLST messages when triggered to do so. It then processes CUSRES messages independently as they are received from the border control authority. For example, initial transmission of PAXLST information may be triggered at 48 hours prior to scheduled time of departure. When CUSRES responses are returned, the aircraft operator's system is updated.
        - Aircraft operator to border control authority– Low Priority
        - Border control authority to aircraft operator – Low Priority

    - Synchronous processing is used when the aircraft operator system must generate and send a PAXLST message then wait for a corresponding CUSRES message in order to continue. For example, when transmission is required at time of check-in, the generation and transmission of the PAXLST is initiated whilst processing the Check In request and cannot continue until the CUSRES has been received and processed.

        - Aircraft operator to border control authority– High Priority

        - Border control authority to aircraft operator – High Priority

- Use the MQ platform's **message persistence** capability for the Low Priority queues. This capability provided by many MQ platforms ensures that messages are stored on disk and not lost when the platform is restarted and is appropriate to help ensure that messages are not lost as they are delivered along their path between the aircraft operator and border control authority.

- Use the MQ platform's **message persistence** capability for the High Priority queues is also possible but isn't strictly necessary. Because the sender of a request is waiting for a response, they have the option to retransmit the request when a response isn't received in a timely fashion. The extra processing on the MQ platform to ensure message persistence is not necessary in this case. Because it may require more resources in the MQ platform to persist the message, a negative impact on response time may be observed. Therefore, each participant should determine what is appropriate for their environment.

- Use of a Correlation ID field is highly recommended for High Priority messages as it facilitates multiple simultaneous synchronous exchanges to be executed using a single pair of queues on most platforms. However, the platform architecture may vary. Use of Correlation ID for Low Priority messages is up to the discretion of the system architects.

- Leverage any message prioritization capabilities available in the MQ platform such that iAPI messages are handled with more priority than most or all other traffic on the platform in order to reduce transmission delays and increase chances of meeting service level objectives

- Ensure the MQ platform including any infrastructure used (including networking) is highly available/reliable in the environment. Outages in the network or the MQ platform can result in significant delays handling passengers, especially during critical airport functions such as Check-In and Boarding

- Ensure appropriate operational monitoring and alerting of MQ infrastructure is in place. The integrity and performance of MQ infrastructure is critical to the ability to handle processing of passengers and crew in airport use cases such as check-in, boarding and final preparation for departure. In order to minimize departure delays caused by the inability to obtain necessary boarding response messages, it is prudent to have the ability to quickly and proactively assess the status of the existing MQ infrastructure.

4.5 Transmission Timings

The iAPI message on a passenger level is sent during the check-in transaction once the passenger's travel document data has been collected, which is normally between 1-48 hours prior to departure. The check-in timeframe varies considerably in the case of connecting flights where the upline station communicates the data to the downline station, which transmits the iAPI data to the destination State, and then relays the response back to the upline station.

The legal and administrative framework may vary from State to State; however, it should be as harmonized as possible.

Time Constraints

iAPI messages are transmitted on a per passenger basis and require a real-time response message by the receiving State(s) to the aircraft operator, within a maximum of 4 seconds for high-priority messages listed below. Maintaining a maximum of 4 seconds response time is essential for aircraft operators because receiving the vetting results from border control authorities is only one part of check-in related transactions.

Several transactions need to be conducted during the time-sensitive check-in e.g., automated document check, positive ID check, basic verification of authenticity of the travel document, consultation of internal no-fly lists, assignment of a security number, seat assignment, a IATCI message (Inter-Airline Through Check-In), electronic ticket validity check, etc. If the transaction is via digital channels, the session time is also limited. If the defined time frame is not respected, then the check-in transaction will fail.

Additional time constraints arise when a passenger's itinerary involves multiple flights that need responses from multiple different iAPI programs. For example, for the routing LHR-AMS-YUL, the following iAPI programs are consulted: iAPI United Kingdom, EU EES (prospective), iAPI USA (due to territory overflight requirements) and iAPI Canada.

4.6 CUSRES Vetting Results

CUSRES results are generated by border control authorities and returned as responses to iAPI messages submitted by aircraft operators.

Response Types

The type of response returned in a CUSRES message can be classified into one of the following three categories:

- Response containing passenger status codes (security and immigration)
- Acknowledgment of receipt of a PAXLST message
- Error response

The combination of data elements C701/1049 and C901/9321 in ERP (Error Point Details) and ERC (Application Error Information) respectively determines the type of response.

Value in C701/1049 (ERP message segment)	Value in C901/9321 (ERC message segment)	Type
2		Passenger status codes
1	0	Acknowledgement
1	1	Error

Passenger status codes

Passenger status codes must be returned in the data element C901/9321 in the ERC message segment. Based on common practice by States readily using an iAPI system, such as Canada, United Kingdom and United States, the status code is composed of two characters, pertaining to security and immigration. For ease of implementation for new iAPI programs, it is recommended that States follow the common practice for a passenger status code returned in the format 'NA' where:

- First character 'N' is numeric, and it holds security or watchlist status code.
- Second character 'A' is alphabetic, and it holds immigration or travel document validation status code.

Acknowledgement

It is recommended that acknowledgment is returned to confirm the receipt of a PAXLST submission where passenger status is not relevant. Examples for such submission includes Cancel Reservation, Flight close-out, etc. The acknowledgement provides aircraft operators with the confirmation that the message was successfully received by border control authorities.

Error

An error response shall be returned when an error is encountered while processing the PAXLST. The error can be technical or functional in nature. An example of a technical error is a poorly formatted PAXLST message. An example of a functional error is an invalid date of birth. It is recommended that the transaction reference and flight details are returned, where possible, and the reason for the error is clearly stated in the FTX (Free Text) message segment.

Recommended Passenger Status Codes

Use of standard iAPI passengers' status codes by States has multiple benefits including increasing the predictability of the number of CUSRES codes to be programmed, the swift and efficient implementation of those programs by aircraft operators, the reduction of costs and training for all stakeholders, the easing of cooperation between States and aircraft operators, the facilitation of assistance and collaboration between States, the increasing of global interoperability and fostering the automation of passenger-related air transport processes.

The recommended passenger status codes presented in this Best Practice are based on common practice aimed at assisting States establishing a new iAPI program. The recommended codes cover the travel documents and travel authorizations that are in used in most jurisdictions.

Security or watchlist status codes

Code	Description	Explanation
0	OK to Board	Passenger is cleared to board
1	Do Not Board	Passenger is not cleared to board
2	OK to Board – Subject to security checks	Passenger is cleared to board subject to additional security checks (Selectee)
3	OK to Board – Known traveler	Passenger is cleared to board. Passenger is subject to reduced screening, for example as a member of a registered traveler scheme
4	Data Error	Passenger is not cleared to board. Data received in the PAXLST is not sufficient to make a decision or there is an error in the data

Immigration or travel document status codes

Immigration entry requirements and immigration national laws are very diverse in nature. The table represents the codes that can apply to most States. A number of additional codes are presented below for accounting for additional national specificities. From an aircraft operator point of view, the granularity of the status codes should enable them to better handle their customers and promptly advise them in case of a Do Not Board.

Code	Description	Explanation
A	Approved travel authorization on file	Passenger has a valid physical or non-physical authorization to travel
B	No electronic travel authorization on file	Passenger is eligible for electronic travel authorization (for example ESTA for the US, ETA for Canada, etc.) but there is no approved electronic travel authorization. Additional evaluation (e.g., correcting data entry error) is required to authorize travel
C	Electronic travel authorization denied	Passenger is eligible for electronic travel authorization, but the application was denied/revoked. Passenger is not cleared to board
D	No secondary document on file	Passenger does not have a valid secondary document, based on the primary document, e.g., visa or residence permit. Passenger is not cleared to board.
P	Decision pending	Decision on travel authorization is still pending. Recommend No Board until status resolved
R	Revoked	Passenger's travel authorization is revoked, recommend no board
T	Timeout	Response couldn't be provided within the stipulated time
X	Insufficient data	Missing mandatory data in PAXLST. Data insufficient to provide a clear result
Z	Travel authorization is not applicable	Passenger doesn't require or cannot obtain authorization for travel or is out of scope

Additional immigration and travel document codes that may be useful depending on the national circumstances include:

F	Invalid secondary document provided	Passenger does not have a valid secondary document (such as a visa in an old passport or residence permit). Passenger is not cleared to board.
I	Invalid primary document	Passenger does not have a valid travel document or data entry error. Passenger is not cleared to board
L	Issue with travel document	Adverse travel document issues, for example hit on the INTERPOL Stolen and Lost Travel Document (SLTD) database, recommend no board.

Health–related status codes

Although no countries have integrated health status codes in their iAPI system, this additional functionality is prospectively considered. Such status codes are recommended to be returned as a third component in the data element C901/9321 in the ERC message segment. For example, 'NAA' where:

- 'N' is numeric, and it holds the security or watchlist status code.
- 'A' is alphabetic and it holds the travel document validation status code.
- 'A' is alphabetic, and it holds the health status code.

The recommended health status codes are as follows:

Code	Description	Explanation
A	Health-related requirements met	OK To Board – Health-related requirements (vaccination, test, declaration, others) are met, not applicable, health exemption declared or can be resolved at any point after check-in
B	Health-related requirements not met	Do Not Board – Health-related requirements are not met

An example of a comprehensive Security, Immigration and Health CUSRES result, ERC+0BA would mean:

- Security status is OK to Board (0)
- Travel document validation status is No electronic travel authorization on file (B)
- Health status is Health-related requirements are met (A)

Segregation of Vetting Results

Although it is not prevalent, some iAPI systems use security status codes to convey both security and immigration vetting results and/or may provide the reason for denial of boarding as free text in the Free Text (FTX) segment. Such an approach is challenging for aircraft operators for several reasons and should be avoided.

Combining the security and immigration Do Not Board vetting result in one letter or digit, lacks the granularity needed to properly and promptly handle the passenger that may be denied boarding. Additionally, most aircraft operators' security Do Not Board results are handled by a specific

department, while Immigration Do Not Board results are handled by check-in or gate agents. Furthermore, when vetting results are combined, aircraft operator staff may have to contact border control authorities to understand the issue and instruct the passenger, which adds complexity and is time consuming.

It is recommended that a clear separation is maintained between security and immigration vetting results, using the recommended status code mentioned above. The use of FTX to report the Do Not Board result makes automation challenging, especially when the check-in transactions are performed via self-service channels. FTX is only recommended to be displayed to aircraft operator agents, which may contain advice for or instructions to be given to passengers.

4.7 Unsolicited Messages

Unsolicited messages are used by border control authorities to update a passenger status provided earlier. Airline systems process the message automatically and returns an acknowledgement confirming whether the update is successful or not. The CUSRES message is used for both the unsolicited message from the border control authority and its acknowledgement by the aircraft operator.

Two main reasons where a passenger status is updated are listed below:

1. To prevent a passenger from travelling if deemed a potential threat based on the latest risk sources.
2. To clear a passenger to travel after a manual or automated review by the border control authority.

It is recommended that the following guidelines are considered by border control authorities when implementing unsolicited messages:

- Boarding is the final step when a passenger with negative status can be intercepted. Passenger cannot be prevented from travelling if the unsolicited message is received after the passenger is boarded. Therefore, status update nearer to the departure time must be followed up with a phone call to the aircraft operator.

- Once the status is updated through an unsolicited message, any subsequent iAPI query on the passenger must result in the revised status being returned.

- If the security status and travel document verification status are managed by different entities, then an unsolicited message sent by one entity must also include the most recent status from the other entity.

- To meet the standard response time of 4-seconds, some border control authorities provide a default OK to Board response to an iAPI submission but send an unsolicited message (usually within few seconds) to revise the status if the passenger is deemed ineligible to travel. In such cases, an aircraft operator may issue the boarding pass based on the initial board response which allows an inadmissible individual access to the sterile area of the airport. To avoid such situation and the operational burden it imposes on aircraft operators, it is recommended that

border control authorities have powerful IT infrastructure to perform the evaluation within 4 seconds and not use unsolicited messages systematically to mitigate the lack of resources.

4.8 Outage Procedures

A border control authority may require that an explicit boarding response message be obtained by the aircraft operator through the exchange of PAXLST and CUSRES messages before certain actions may be taken. These actions may include, but are not limited to, passenger check-in, boarding pass issuance, passenger boarding.

Under normal IT operations, the aircraft operator's system constructs and transmits any necessary PAXLST messages, then waits to receive and subsequently process the CUSRES message from the border control authority during processing of requests for these actions. However, if the aircraft operator's system is unable to complete this exchange, airport operations should not be forced to immediately halt. Therefore, procedures for handling such an event should be defined.

System outages may be due to a variety of specific reasons, but fall into three main categories:

- The aircraft operator's system is unavailable
- The communications infrastructure between the aircraft operator's and border control authority systems is unavailable
- The border control authority system is unavailable

It is possible that more than one of the above is impacted concurrently.

Plans and Points of Contact

In any outage scenario, it is imperative that a clear procedure is defined for the aircraft operator and border control authority to communicate the nature of the event and to initiate alternative procedures. This is often known as the process of Declaring an Outage.

The aircraft operator and border control authority should ensure each other have current point of contact information to be used for this purpose, including names, telephone numbers and email addresses as appropriate.

Alternative Procedures

Alternative procedures for handling of passengers during an outage of one or more of the components listed above should be defined in order to facilitate continued handling of passengers at the airport and aircraft movements while making best reasonable effort to provide API data and honor boarding response messages. Acceptable alternative procedures may vary based on the nature or extent of the outage as well as the scope of the normal operating procedure.

When the aircraft operator's system is unavailable, the operator must handle passengers using an alternate process. It may be through the use of another departure control system, or it may involve a completely manual procedure. The aircraft operator may not have another system at its disposal to process API PAXLST or CUSRES messages. Any boarding response messages already received may also not be available.

When the communications infrastructure between the aircraft operator and border control authority systems is unavailable, each entity may have access to their own systems, however new or updated passenger information or boarding messages may not be exchanged between the systems. Data for some passengers on any given flight may have already been exchanged while for others it has not. Data already transmitted may be corrected in the aircraft operator system, but the correction may not be immediately available to the border control authority. Re-evaluated existing boarding messages may not immediately reach the aircraft operator system.

When the border control authority system is unavailable the aircraft operator may have transmitted API data which reaches the border control authority system but remains queued for processing and no response messages are returned. This may result in an increasing backlog of data to be dealt with upon restoration of the border control authority system, which may be after departure of the flight.

Outage procedures should consider how each of these situations are best handled considering the flow, availability and timeliness of data, the impact on the aircraft operator and the airport, the border control authority and processing areas and the passengers themselves.

Consideration of the following is highly recommended:

- Determine the criteria that must be met in order to constitute declaration of an outage and initiation of alternate procedures. This should include the scope and expected duration of the impacted system infrastructure. When an aircraft operator is unable to obtain a boarding response message from the border control authority:
    - What is a reasonable amount of time for the aircraft operator to wait for a response from the border control authority system? For normal operations requiring an interactive, synchronous exchange, the operational target should be less than 1 second, a response should be delivered within a maximum of 4 seconds. An upper limit should also be defined at which point the aircraft operator can consider the transaction a Timeout
    - What frequency of timed-out transactions warrants declaration of an outage?
    - Once declared, what conditions must be met in order to end the outage and return to normal operations?
- Consider implementation of redundant means of connection between systems. Multiple active and diverse connections may be justified. Or a back-up connection which can be quickly initiated may be appropriate.
- Consider the appropriateness of relaxed enforcement of normal rules. In this case, the aircraft operator system may be able to follow alternative flows once an outage has been declared in the system, minimizing delays to passenger handling during the outage.
- Consider the appropriateness and mechanics of falling back to non-interactive API when interactive boarding response messages are unavailable.
- Ensure all systems keep records of outage event details (especially timing) and include the context of outages during compliance audits and any resulting repercussions.

4.9 Override Processes / Mechanisms

Each State should make available real time 24x7, 365 days a year support for aircraft operator resolution and assistance. The support line should have sufficient resources to operate both when the system is functional and during an outage.

States should leverage unsolicited messages to modify a previous vetting result to an updated / most current result. In cases where transmission of an unsolicited message is not possible, aircraft operators should have the capability to override certain CUSRES responses in order to expedite customer processing.

The change in status should be persistent regardless of a change in itinerary, date and / or time. If the underlying requirements are still met (same origin/destination), the vetting response code in CUSRES should persist without reverting.

4.10 Disruption Procedures

It is important for every aircraft operator to have procedures in dealing with flight disruptions that may impact the delivery of iAPI, API and PNR data to each border control authority. Border control authorities and aircraft operators should have the resources to coordinate for the actions to be taken and avoid potential penalties being incurred by the aircraft operator.

The following common scenarios can be used as a guide in case of disruptions that allows both aircraft operators and border control authorities to agree on the next steps.

Flight Delays (resuming within the same day)

- Border control authorities receive the information about critical delays encountered in the flight operations through their own sources.

- Aircraft operators to ensure that all passengers in the current flight are in the iAPI data and accomplished during the check-in period to the border control authorities.

Flight Delays (resuming on a different day)

- Border control authorities receive the information about flight operations delayed to the next day through their own sources or should inform aircraft operators if they have specific procedures.

- Border control authorities may request for another iAPI check-in message to be accomplished by the aircraft operator. This is to maintain consistency by ensuring all current passengers are in the flight and for passengers that are no longer in the flight will not be included in the batch API at flight close-out.

Flight Cancellations

- Border control authorities may request iAPI cancellation message for all passengers if the flight is unable to continue. Aircraft operators must ensure that an iAPI cancellation message for all affected passengers are sent to the border control authorities.

- It is also recommended for the aircraft operators to contact the border control authorities and provide an update on the next flight availability. Affected passengers will perform another check-in and the aircraft operator will send another iAPI message at the time of check-in.

- Some passengers may board the next flight available with a different aircraft operator that may require them to perform another check-in process. The initial aircraft operator must ensure that the iAPI cancellation message of the affected passengers is sent to the border control authorities. The new aircraft operator must ensure that the iAPI check-in message of the affected passengers are sent to the border control authorities.

Flight Diversions

- In the event where the flight is unable to land in the original port of destination and the flight has been diverted to a different state that may require the aircraft operators to submit iAPI. Aircraft operators must contact the border control authorities to advise of the flight diversion and they may be required by the border control authority to send a batch API for the flight.

- Border control authorities may accommodate and authorize the temporary entry of passengers while the completion of necessary formalities is pending if the aircraft operator is unable to deliver the required information on time. Border control authorities must set an agreement with the aircraft operators to accomplish the pending information.

- Border control authorities should have the ability to accept non-scheduled flights from the aircraft operators once the flight diversion has been advised.

5. Costs and Resources

iAPI systems are more complex than batch API systems and have higher costs associated with their development, implementation, maintenance, and operations for both States and aircraft operators. The main costs for aircraft operators and border control authorities pertaining to batch API are detailed in the WCO/IATA/ICAO API Guidelines. The current Best Practice identifies categories of costs specific to iAPI for aircraft operators, border control authorities and service providers.

Regardless of the API mode, following international standards will lead to a faster and more economical implementation. Additionally, passenger data programs are an integral component of a country's national border control functions. These functions are a state responsibility and therefore the systems, processes, and resources for receiving, processing, and analyzing API data should be funded by the national budget, and not by aircraft operators and/or passengers through user fees, charges, and taxes.

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".[7]

5.1 Aircraft Operators

- System developments
  - Coding requirements for host system, including updates, testing
  - Updates and testing for other applications such web, mobile applications, self-service
  - Adjusting the existing system in case of diversion, to switch off the API requirements for a second transmission/mid-point
  - Availability of resources / technical expertise when facing simultaneous State implementations
  - Dependencies on timelines of providers

- Staffing
  - By moving from API to iAPI system, additional training of check-in staff is required to handle the different CUSRES vetting results and instructing passengers
  - Increase staffing at the support desk line for interactions with authorities
  - Additional workload at the gate in case of offload message

- Cost avoidance: At term, automation reducing the need for staff; and cost related to inadmissible passengers such as carriage back to origin, custody, and care (meals, accommodation), administrative costs, and fines and penalties.

[7] *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.

5.2 Border Control Authorities

- Considerations for selecting the vendors, setting up the contract (procurement process) or internal IT development costs.

- Aircraft operators may use systems provided by different service providers for different aspects of their business. It may be necessary to work with more than one service provider for any single aircraft operator.

- Elaborate a cost-benefit analysis prior to implementation to ensure appropriate funding for all the components of an iAPI systems, including set-up costs and recurring costs:
    - Set up costs:
        - Program and policy work
        - IT planning and system changes
        - Enhancements to IT infrastructure
        - Testing and certification of commercial aircraft operator / service providers
        - Project management
        - Corporate overhead (incl. employee benefits, office space, IT support, human resources, comptrollership, etc.)
        - Analysis tools development
    - Recurring costs:
        - Technical maintenance
        - Program management resources
        - Support center 24/7 and Liaison Network/Immigration Officer

- Cost avoidance: Automation reducing the need for staff; and costs related to inadmissible passengers

5.3 Service Providers

- Consistency in implementations is the most significant factor in cost to implement and operate IAPI functionality
    - For the business functionality required, follow established use of message construction and code sets. This is specifically true for the list of flight sectors which should be included in a message and the use of LOC codes for a given type of itinerary (e.g., International Inbound, International Outbound, Transit, Domestic, Overflight) and response codes.

    - Minimize or eliminate variance by aircraft operator or country from which they operate such that handling of several aircraft operators by a given system is consistent.

- Support standard MQ-compatible message delivery mechanisms which consider:
    - Handling of data for multiple aircraft operators on a single connection
    - Back-up/redundant alternative connectivity

- Unique or modified business requirements may require software changes to be designed, coded, tested, and implemented. Service providers must provide software that can address the needs of every border control authority that may be involved in any given flight, for any

of the aircraft operators to which they provide services. Several agencies may be involved in a given passenger's journey (departure, overflight, arrival jurisdictions), requiring any system to integrate each applicable mandate and determine a consolidated result. Increased variance in business process, or unique requirements add complexity to this process, which in turn impacts the time and cost required for implementation.

6. Best Practice Examples

The following best practice and lessons learned examples of specific aspects of current iAPI national programs is not intended to comprehensively present all existing best practices, but rather to highlight specific points that are commended by aircraft operators working with these national authorities.

6.1 Canada – Special Categories of Travelers for Electronic Travel Authorizations (eTA)

Foreign diplomats fall in the categories of travelers who are exempted from obtaining an electronic Travel Authorization (eTA) to enter Canada. However, when using the aircraft operator's self-service check-in applications, the CUSRES would indicate a no-board message, until the concerned passengers were able to present themselves to an aircraft operator agent for manual verification of their documents to confirm the exemption. This would result in an override or a not applicable indicator to the iAPI message. The Canadian authorities overcame this challenge by recording in a database all foreign diplomatic passports or by creating a database with all the passport codes of foreign diplomatic passports.

Another challenge faced in the onset of the iAPI system implementation were Canadian citizens with dual nationality who were travelling on their foreign passports and were not able to apply for an eTA, therefore having to obtain an emergency travel document if their Canadian passport was expired. A process was quickly developed for these dual nationals to apply for an electronic exemption that enabled an 'OK to board' message at check-in.

6.2 United Kingdom - Carrier Engagement Program

For each border control initiative, including their iAPI program, the UK authorities have engaged with industry stakeholders from the inception of new border programs or before proceeding with changes to existing programs. Engagement with aircraft operators has pursued the objectives of informing aircraft operators of the parameters of each new program, gathering recommendations and industry experience of other country's border control programs, further fostering a dialogue to obtain feedback on the impacts, challenges, and benefits for the industry.

This engagement with aircraft operators has among others taken the form of information pack, numerous webinars with Q&A sessions, sufficient timelines for industry to provide written comments, and providing specific contact details for follow up and questions by aircraft operators.

UK authorities have shared with stakeholders their future roadmap indicating which areas they will engage on, and which are government-led mandates.

6.3 United States – Document Validation Program

In 2013, the U.S. Customs and Border Protection (CBP) introduced the Document Validation Program (DocVal) to help prevent the use of fraudulent or invalid travel documents. DocVal allows CBP to use the Advance Passenger Information System (APIS) to check the validity of each travel document by comparing it to CBP's databases of valid U.S. passports, visas, Permanent Resident Cards, and travel authorization and Electronic Visa Update System enrolments.

Under DocVal, aircraft operators that voluntarily participate in the program receive a response message from CBP containing two elements: the first character indicating the security status of each passenger, while the second stating whether each passenger's travel document has been matched to an existing record in CBP's databases. Multiple aircraft operators have updated their systems to be able to receive the document validation message. DocVal has helped CBP to identify passengers using fraudulent travel documents more efficiently and to communicate that information to aircraft operators, preventing those passengers from boarding flights to or from the United States.

Examples from 2016 and 2017 demonstrate the effectiveness of the program. In one case, a participating aircraft operator received a response message indicating that seven passengers had travel documents that could not be validated. Later investigation revealed all seven were using lost or stolen visa numbers. In another case, a passenger was denied boarding because the date of birth on their visa did not match the information in CBP's databases, indicating an attempt to use a visa issued to someone else. There are a continued number of success stories in addition to these examples that highlight the importance of such a program.

U.S. Customs and Border Protection is in the final stages of publishing the Document Validation regulation which will require all carriers to electronically validate U.S. visas and other U.S. issued travel documents through APIS prior to boarding. This process will help governments and industry inhibit travelers without proper entry documents from boarding.

World Customs Organization

wcoomd.org / iata.org / icao.int