



IATA/CONTROL Authorities Working Group

Guidelines
For Document Check & Carrier Liability

Original 27 October 2016

THE IATA/CONTROL AUTHORITIES WORKING GROUP (IATA/CAWG)

The IATA/Control Authorities Working Group (IATA/CAWG) was established as an IATA initiative in 1987. The main goal was to bring Control Authorities and Aircraft Operators together in an informal setting to develop mutually acceptable working arrangements, recognizing the needs and limitations of the two parties.

Members of IATA/CAWG are the National Aircraft Operators and Immigration Departments (sometimes supplemented by Civil Aviation and Border Police) of Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Japan, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, the United Kingdom, the United Arab Emirates and the United States. The Airlines for America (A4A), the National Airlines Council of Canada (NACC), and the Association of Asia Pacific Airlines (AAPA) are also represented.

The IATA/CAWG Vision Statement is: "An expert forum of Airlines and Government officials to work collaboratively to recommend solutions and establish best practices for border management that contribute to the facilitation of legitimate travellers whilst ensuring a secure border".

GUIDELINES FOR DOCUMENT CHECKS AND CARRIER LIABILITY

1 INTRODUCTION

- 1.1 Within this document, Governments are referred to as States, Immigration Authorities as Control Authorities and Airlines as Carriers.
- 1.2 The aim of this document is to present best practice guidelines for the conducting of document checks and to define the liabilities of Carriers.

- 1.3 When defining the liabilities of Carriers, IATA/CAWG recognizes that there is also significant importance in effective cooperation and swift communication between Carriers and Control Authorities, to enable Carriers to recognize passengers holding insufficient or fraudulent documents. Therefore the guidelines also touch upon the responsibilities of Control Authorities.
- 1.4 New methods of both border management and check-in are changing the traditional way of checking travel documents; therefore a short reflection on these new methods is included in the guidelines.
- 1.5 The aim of these guidelines is to supplement the IATA/CAWG document: **GUIDELINES RELATING TO PERSONS IDENTIFIED AS HOLDING FRAUDULENT OR FALSIFIED DOCUMENTS.**
- 1.6 Carrier liabilities in the handling and removal of inadmissible passengers are reflected in a separate IATA/CAWG document: **GUIDELINES FOR THE REMOVAL OF INADMISSIBLE PERSONS.**
- 1.7 Nothing in this document is to be construed as to contradict national legislation, regulations or court decisions.

2 DEFINITIONS

For the purposes of this document, the following definitions from Chapter 1, Section A of the latest edition of International Civil Aviation Organization (ICAO) Annex 9, will apply unless otherwise indicated.

- 2.1 **"ADVANCE PASSENGER INFORMATION (API) SYSTEM".** An electronic communications system whereby required data elements are collected and transmitted to border control agencies prior to flight departure or arrival, and made available on

the primary line at the airport of entry.

- 2.2 **"AUTOMATED BORDER CONTROL (ABC)".** An automated system which supports the border control process. The system authenticates the electronic machine readable travel document or token, establishes that the passenger is the rightful holder of the document or token, queries border control records, then determines eligibility for border crossing according to pre-defined rules.
- 2.3 **"IMPOSTOR".** A person who impersonates the rightful holder of a genuine travel document.
- 2.4 **"INADMISSIBLE PERSON".** A person who is or will be refused admission to a State by its authorities.
- 2.5 **"INTERACTIVE API (iAPI)".** An electronic system that transmits, during check-in, API data elements collected by the aircraft operator to public authorities who, within existing business processing times for passenger check-in, return to the operator a response message for each passenger.
- 2.6 **"PASSENGER NAME RECORD (PNR)".** PNR 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. The data is used by operators for their own commercial and operational purposes in providing air transportation services. Industry standards related to PNR creation are detailed in IATA's Passenger Services Conference Resolutions Manual and in the A4A/IATA Reservations Interline Message Procedures — Passenger (AIRIMP). A PNR is built up from data that have been supplied by or on behalf of the passenger concerning all the flight

segments of a journey. This data may be modified by the operator or his authorized agent, for example, changes to requested seating, special meals and additional services requested ¹

- 2.7 **"TRAVEL DOCUMENT".** Official document issued by a State or organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) and machine-readable data.
- 2.8 **"NECESSARY PRECAUTIONS".** Verifications carried out by adequately trained aircraft operator or staff members of the company operating on behalf of the aircraft operator, at the point of embarkation, in order to ensure that every person holds a valid travel document and, where applicable, the visa or residence permit required to enter the receiving State. These verifications are designed to ensure that any reasonably apparent document alteration or document use by an impostor is detected.

3 NEW METHODS OF BORDER MANAGEMENT

- 3.1 Automated Border Control (ABC) clearance has been introduced at airports in many countries and makes immigration clearance both more efficient and effective. Detecting fraudulent documents and impostors is also effective through ABC channels. In the case of electronic passports, ABC gates can validate the authenticity of the travel document through a Public Key Infrastructure (PKI) check. On that basis the identity of the passenger can be verified through a one-to-one biometric match between the travel document and the passenger.
- 3.2 Making use of API- and PNR-data, transmitted by Carriers to Control Authorities, serves as an added

¹ ICAO Doc 9944 Definition

tool in detecting fraudulent documents, in combatting transnational crime and in preventing illegal travel.

3.3 Pre-registered traveler schemes, where passengers provide specific data to the Control Authorities at time of registration, for performance of background checks on the applicant, expedite immigration clearance for enrolled members while enabling Control Authorities to focus on unknown passengers.

3.4 The use of an iAPI system, when connected to the visa database of the destination country, should reduce the number of inadmissible cases. For example, if a passenger, who needs a visa or an electronic travel authorization, is not in possession of either, the Carrier would not receive an “authority to carry” response from the Control Authority. Stolen blank documents and other documents reported stolen or lost by the holders, can in many cases be detected through the use of iAPI, In addition persons considered to be a threat or security risk can be denied authority to travel through the use of an iAPI system.

4 CHECK - IN METHODS

4.1 Check in methods like kiosk, internet and mobile apps have become the norm for many Carriers and are introducing new challenges to conducting travel document checks.

4.2 Interline (through-checked) passengers (checked from one Carrier to another via EDIFACT) pose a particular challenge to Carriers. The passengers hold boarding passes for the complete route, printed by the originating Carrier, and travel document checks should have been performed by the originating Carrier. However, the transporting Carrier across borders is responsible for any immigration fines, should the passenger not be

adequately documented. Due to the nature of interline traffic connecting passengers may show up at the gate of their connecting flight close to departure time, therefore reducing the time which dedicated to a travel document check.

4.3 Automated bag check-in enables fast and efficient baggage handling. In some instances, this can be accomplished without document checks at the baggage drop-off point. In other cases regulations in effect require such checks before baggage acceptance, and may represent an opportunity for airline validation.

4.4 Document checks may take place at any stage of the passenger process. The increased use of automated passenger processes give fewer opportunities and may limit time for agents to check travel documents.

5 CONTROL AUTHORITY RESPONSIBILITY

5.1 Control Authorities should assist Carriers in the evaluation of travel documents presented by passengers, in order to detect and deter fraud and abuse as well as avoid insufficiently documented passengers from being transported.

5.2 Illegal travel trends change frequently; therefore Control Authorities should keep Carriers informed about these trends in a timely fashion.

5.3 Control Authorities should consider coordinating amongst each other, where possible, to develop training and offer such training on a regular basis or as the need arises.

5.4 Control Authorities should consider sending out alerts to Carriers, which highlight any new security features introduced in travel documents and information concerning trends in fraud.

- 5.5 Control Authorities could also consider entering into cooperative arrangements, such as a Memoranda of Understanding (MoU) with Carriers providing international services to and from their countries. An MoU could, among other things, specify the frequencies of training to be provided to the Carrier by the Control Authority, require the Control Authority to share alerts with the Carrier, outline certain measures expected from the Carrier and require the Carrier to share information on detected cases. Fulfilling the requirements included in the MoU would allow for some benefits to the Carrier, e.g. in the form of mitigated immigration fines.
- 5.6 Control Authorities should consider making arrangements with other States to permit the positioning of Liaison Officers at airports, in order to assist Carriers in establishing the validity, sufficiency and authenticity of the travel documents of embarking passengers.
- 5.7 In cases where a passenger arrives undocumented, with a fraudulent document or as an impostor, the Control Authorities should consider accepting API-data, as evidence that the passenger was documented when accepted for travel by the Carrier.
- 5.8 Control Authorities should also consider vetting iAPI data against external watch lists, including Interpol's Stolen and Lost Travel Document (SLTD) database, in order to minimize the transport of persons using suspect documents of identity by transmitting denial of authority to board to the Carrier.
- 6 CARRIER LIABILITY**
- 6.1 Carriers should take the necessary precautions to ensure that passengers are in possession of the required travel documents before travel.
- 6.2 Carriers should work in close cooperation with Liaison Officers and Control Authorities to prevent travel by insufficiently and/or improperly documented passengers.
- 6.3 Where possible, Carriers should consider sharing, with Control Authorities, information on fraud and abuse that they have detected. Control Authorities should on their part share this information with other authorities and Carriers, as deemed appropriate, to prevent further illegal travel attempts from a specific region.
- 6.4 Carriers should conduct basic travel document training. However, Carrier staff and their agents should not be expected to possess the same level of expertise in detecting fraudulent documents or impostors as border control officers or liaison officers.
- 6.5 Carriers should not be required to use specialized equipment when checking documents, unless separately agreed to between the Control Authority and the Carrier (e.g. in an MOU).
- 7 CONTENTS OF DOCUMENT CHECKS**
- 7.1 Document checks should consist of at least the following:
- 7.1.1 Verifying the authenticity of the document by visual means.
- 7.1.2 Verifying that the document is recognized as a valid travel document in the receiving and/or transit State(s).
- 7.1.3 Verifying that the presenter of the document matches the photograph in the document (identity check).
- 7.1.4 Verifying that the document is valid;
- 7.1.4.1 Verifying that a passport is valid for the time period as required by

the transit and/or destination country.

- 7.1.5 Verifying whether a visa is required, and if so ensuring at least the following:
 - 7.1.5.1 Verifying that travel takes place within the validity dates indicated on the visa (not before or after).
 - 7.1.5.2 Verifying that a single- or double-entry visa has not been exhausted on previous visits.
 - 7.1.5.3 Verifying that the visa covers all passengers in the passport.
 - 7.1.5.4 Verifying that a minor travels together with the person(s) indicated in the visa, if specified.
- 7.1.6 Verifying that, if a visa is required, but none is presented, the passenger holds a valid residence permit that is recognized by the receiving and/or transit State;
- 7.1.7 Verifying whether an e-visa/electronic travel authority is required and then ensuring approval to board is received from the Control Authority via an iAPI system.