

First edition
2015-03-15

Corrected version
2016-06-01

Traveller processes for biometric recognition in automated border control systems

*Processus relatifs au voyageur pour la reconnaissance biométrique
par les systèmes de contrôle aux frontières automatisées*



Reference number
ISO/IEC TR 29195:2015(E)

AVA Documents
Document Sharing Hub
© ISO/IEC 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword	iv
1 Scope	1
2 Terms and definitions	1
3 Key drivers	2
4 Overview of automated border control system	2
4.1 General	2
4.2 The biometric process at the border	2
4.3 The processing steps	3
5 Key Success Factors	4
5.1 Operational considerations	4
5.1.1 Traveller considerations	4
5.1.2 Traveller processing	5
5.1.3 Operational environment	5
5.1.4 Border stakeholder engagement	5
5.1.5 System management	6
5.1.6 Vulnerabilities	6
5.2 Technical considerations	7
5.2.1 Security/Privacy	8
5.3 Standards for interoperability	8
5.4 Enrolment for automated border control systems	8
5.5 Privacy background for ABC systems	8
6 Guidance relating to specific modalities	9
6.1 Face	9
6.1.1 Presentation of subject to camera	9
6.1.2 Other factors	9
6.2 Vascular (vein)	9
6.2.1 General	9
6.2.2 Presentation of subject to vein sensors	10
6.2.3 Other factors	10
6.3 Fingerprint	10
6.3.1 General	10
6.3.2 Enrolment	11
6.3.3 Verification	11
6.4 Iris	12
6.4.1 Presentation of subject to camera	12
Annex A (informative) Different types of ABC systems	13
Annex B (informative) Examples of automated border control systems	14
Annex C (informative) Malaysia Autogate System	15
Annex D (informative) Nexus iris recognition system	18
Annex E (informative) United Kingdom	19
Annex F (informative) Global Entry	22
Annex G (informative) Examples of Signage used in ABC Systems	23
Bibliography	26

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: [Foreword — Supplementary information](#).

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

This corrected version of ISO/IEC TR 29195:2015 incorporates the following corrections.

Title: The title was corrected to *Traveller processes for biometric recognition in automated border control systems*.

5.4: The footnote “to be published” was removed from the reference to ISO/IEC TR 29196.

Traveller processes for biometric recognition in automated border control systems

1 Scope

This Technical Report provides recommended best practices and processes for automated border control systems using biometrics to verify an identity claim by a traveller that uses an ePassport or equivalent identity card as the basis for the claim. It indicates areas that organisations proposing to use biometric technologies will need to address during design, deployment, and operation. Much of the information is generic to all types of applications especially around signage; however, some information will be specific to the modality of biometric technology used and how that technology is physically implemented.

Biometric automated border control systems can have various biometric implementations, they can be manned or unmanned, and might or might not require the presentation of documentation. This Technical Report points out the different requirements relating to many of the different types of biometric application implementations.

The following are out of scope for this Technical Report.

- a. Watch lists, although biometric technology can be used to check watch lists as part of traveller processing in automated border control systems.
- b. Manual customs and immigration systems mandated by government for travellers.
- c. Trusted traveller systems (including token-less systems).
- d. ePassport PKI: Whilst PKI/PKD systems exist, they are not covered in this Technical Report. This subject is referenced in ICAO 9303.

The recommendations contained in this Technical Report are not mandatory.

2 Terms and definitions

For the purposes of this document, the following terms apply.

2.1

traveller

person subject to biometric verification by an automated border control system

2.2

automated border control system

employs biometric verification of travellers to meet the requirements and regulations of border stakeholders

Note 1 to entry: Often referred to as ABC systems.

2.3

border stakeholder

state or state-sanctioned entity that carries out border functions including, but not limited to, customs, immigration, transportation, and tourism

2.4

automated gate

subsystem of an automated border control system that incorporates physical entry/exit control, travel document reading (where applicable), and biometric verification.

2.5

kiosk

separate physical device that is part of the ABC system which can be used for assessing the eligibility of travellers for self-process.

3 Key drivers

Automated border control systems using biometrics have several key business drivers including increases in security, improving business processes and improving the traveller's experiences. Airlines are now starting to use larger aircraft, fitting more travellers on existing aircraft and deploying more flights. This creates problems when processing travellers due to the increase in traveller numbers and creates many key drivers for authorities (airport, border control etc.) to look at automated processing of travellers.

The key drivers for use of automated border control systems include to:

- Reduce the costs of the related processing of travellers.
- Decrease the traveller processing times.
- Make better use of finite floor space in border control processing areas.
- Contribute to making the traveller experience through border control points a positive one.
- Provide consistent and secure border control processing of travellers.
- Provide a lower cost scalable platform to meet growing traveller processing demands into the future.
- Give greater flexibility for workforce planning including staffing levels for the processing of increasing traveller numbers.

4 Overview of automated border control system

4.1 General

Automated border control systems may consist of one or more physical devices with which the traveller needs to interact.

Some systems use a separate physical device (for example: a kiosk) that travellers must use to determine their eligibility to 'self-process'. In other words, to have their identity claim processed automatically at a subsequent and separate physical device.

Other systems undertake the eligibility check and identify claim processing using a single device.

Typically, automated border control systems include other border control processing as required by a border control authority in addition to the eligibility and identity claim processing.

NOTE ABC systems are not intended to replace all manual/human border control policies and procedures. Current border control initiatives demonstrate a strong need to maintain human oversight and control over ABC systems.

4.2 The biometric process at the border

The automated border control system verifies the traveller's identity claim by capturing the biometric characteristic presented by the traveller (for example: face or fingerprint) and, using the biometric verification system component, comparing it with that encoded in the identity document.

The system will then, based on results, accept the claim and allow the traveller to pass, or not accept the claim and refer them for processing by a border control officer.

4.3 The processing steps

Automated border control systems using biometrics typically involve the following process steps. An example of the processing steps is depicted in [Figure 1](#). However this will depend on the individual business requirements. Not all the steps outlined below will apply and/or the order of these steps could be different. Each step may require an exception handling procedure that is not described in this document.

1. Detect traveller presence — sensors recognise that a traveller is proximate to the biometric sensor(s) and initiate the traveller processing by activating instructions for the traveller.
2. Detect Travel Document — the traveller places a travel document with an embedded chip on a reader, which reads biographic data and the biometric data from the chip.
3. Read Travel Document Data — The security features of the document are checked for possible tampering (where applicable) and the biometric and 'biographic data are read from the chip.
4. Present Questions — The traveller is asked to answer border control questions.
5. Assess Eligibility — The eligibility of the traveller to use automated process is assessed based on eligibility criteria.
6. Store Travel Document Data — Relevant data is read from the Travel Document and stored by the border control authority.
7. Issue token — The traveller is issued a token with unique identifier for use at the subsequent automated border control system component.
8. Initiate Biometric Verification Process — The biometric verification process is started based on the detection of the physical presence of the traveller, the token or other system designed trigger.
9. Retrieve Data — Biometric data and other biographic read from the Traveller Document and stored is retrieved from the relevant data source.
10. Acquire Traveller Biometric Sample — the traveller is prompted, if necessary, to present the biometric characteristic of interest and a sample of it is acquired. The suitability of the sample for biometric verification is assessed and the traveller is prompted to re-present the biometric characteristic of interest if a new sample is required.
11. Presentation attack detection test — The process performs liveness detection of a biometric sample and anti-spoofing tests to the specification as defined in ISO/IEC 30107 multi-part standard.
12. Biometric Verification — The system compares the acquired biometric sample against the stored biometric reference obtained from the travel document to verify that the traveller is the same person to whom the document was issued.
13. Clear Traveller — The biographic and biometric data obtained from the travel document is used to assess other border control entry/exit requirements, which may include checking for a valid visa and possibly watchlist processing. Watchlist processing may include comparison of the acquired biometric sample against biometric references contained in the watchlist.

This clearance processing may require retrieval of data from a central data repository or the transmission of data to a central repository. Note the exception handling for this stage can be complex.

14. Allow Traveller to Proceed — If all data is verified as valid and entry/exit is authorised, the traveller is allowed to proceed (for example: a gate is opened for the traveller to pass through). If entry/exit is not authorised, the traveller is referred for further assessment. The border control data and its outcome are logged.
15. End of process — System is set to ready status.

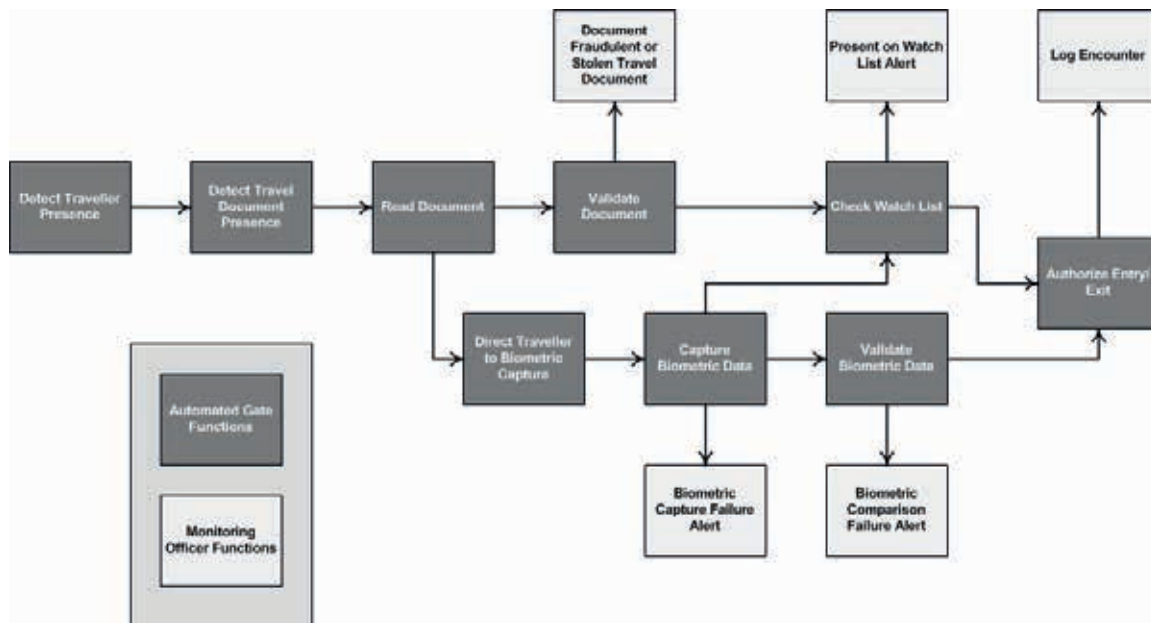


Figure 1 — Automated gate processing flow (an example)

5 Key Success Factors

5.1 Operational considerations

The following operational considerations will assist in designing a solution that meets the needs of the business and the traveller in automated border processing.

5.1.1 Traveller considerations

Most automated border control systems currently installed are for voluntary use by travellers. Assuming that the operational aim is to encourage more travellers to 'self-process', the following should be considered:

1. Potential new travellers may be influenced by the reported experience of previous users in choosing whether or not to use the systems.
2. Previous travellers may choose whether or not to use the system again, and whether to report positively or negatively to other potential travellers, based on their experience.
3. The use of ABC systems necessitates the traveller to hold an ePassport or equivalent document. This would require some travellers to replace their existing non ePassport at their own cost, to use the ABC system.
4. Groups/families travelling on mixed ePassport/ non ePassports are often unable to participate together in ABC systems
5. Families travelling with children that are under the eligible age for using the system tend not to self-process.
6. Ease of use and accessibility both have a strong influence on a traveller using a particular system more than once

5.1.2 Traveller processing

To facilitate the traveller and enable processing to be completed in a timely way consideration should be given to the following:

1. Travellers who, having interacted with the system, for whatever reason cannot be processed, should be offered priority referral for processing by a border control officer. (for example: those with eye conditions that are not able to be successfully processed by an iris biometric verification system)
2. Answering traveller questions about the technology, addressing any traveller concerns and handling people's objections.
3. Throughput rates (e.g. managing high-traffic flow areas such as airports with peak traffic).
4. Traveller interaction with the technology (e.g. a kiosk and a gate arrangement may be required, positioning of cameras or readers).
5. Displaying appropriate and universally recognisable signage to assist the traveller, in accordance with the draft multi-part standard ISO/IEC 24779, Information Technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, Icons and Symbols for use with Biometric Systems.
6. The guidance given in ISO/IEC TR 24714-1 helps build acceptance of the travellers and gives guidance on inclusive design (versus exception handling) and dealing with the objections of the travellers.

5.1.3 Operational environment

The characteristics of the operational environment can have an impact on the traveller's use of the system, and the ability of the system to perform as required. As a result, consideration should be given to:

1. Whether the operational environment needs to be monitored and controlled to assist travellers when using the system and minimise the risk of processing breaches.
2. Whether the operational environment can be left unmonitored and uncontrolled. This is unlikely in a border control context as there is generally at least CCTV coverage to monitor traveller flows and confirm biometric system responses.
3. The cleaning and maintenance of equipment for health and hygiene purposes and to minimise the chances of the coalescence of biometric samples collected from successive travellers. For example: ghost images lingering from previous users in fingerprint readers.
4. The impact of the environmental conditions on the performance of the biometric verification process. For example, the impact of ambient lighting, dirt and noise, and temperature and humidity.

5.1.4 Border stakeholder engagement

It is important for the key stakeholders to have a good understanding of the system and what it does, and a sense of a stake in its success. This means giving consideration to:

1. Allowing stakeholders to contribute to the design and implementation of the system in the operational environment.
2. Ensuring that the stakeholders are supportive of the physical installation aspects of the system and its use of available space. For example, Airports or Port Authorities have finite infrastructure available for the processing of travellers.
3. Keeping stakeholders informed about the ongoing performance of the system once it is implemented. This includes educating them about the meaning and the operational implications of the biometric performance metrics.

5.1.5 System management

The management of the system is an important consideration for its reliability and ongoing success. Consideration should be given to the following:

1. Administrator training requirements.
2. Ongoing relationship with supplier to ensure the system is monitored and upgraded with new algorithms in line with advances in the technology.
3. The border control authorities should understand and accept the risks associated with the biometric error rates. To do this the authorities will need to provide adequate resources to analyse the business requirement and determine the error rates of the biometric solution.
4. Monitoring the effects of change of biometric feature with time ('ageing'), e.g. in the case of automated facial recognition, the divergence of the image of an ageing face from the image stored as the reference in the travel document.
5. Provision of CCTV coverage to monitor traveller flows and traveller interaction with the ABC.
6. Disaster Recovery and Business Continuity.
7. System Monitoring for biometric performance.

5.1.6 Vulnerabilities

The following vulnerabilities of an ABC system using biometrics are similar to vulnerabilities in a manual border control process performed by an officer. These vulnerabilities (and possible mitigations) include:

1. A fraudulent biometric is used (e.g. a fingerprint appliqué).
 - a. Apply liveness detection techniques.
 - b. Verify claim against authoritative reference.
 - c. Have a security officer present when the biometric sample is provided.
2. A reference document (e.g. a passport) may be tampered with in a manner that substitutes an image of the fraudulent document holder for the person to whom it was initially issued (e.g. facial or iris image substitution).
 - a. Validate the security features of the document.
3. A person tailgates on the passage of another through the processing Gate.
 - a. Monitor the processing Gates using CCTV.
 - b. Position a security officer in the vicinity of the Gates to observe Gate usage.