TECHNICAL REPORT

ISO/IEC TR 29195

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

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

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

© ISO/IEC 2015

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

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

© ISO/IEC 2015 – All rights reserved

Contents

Page

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

 © ISO/IEC 2015 – All rights reserved

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

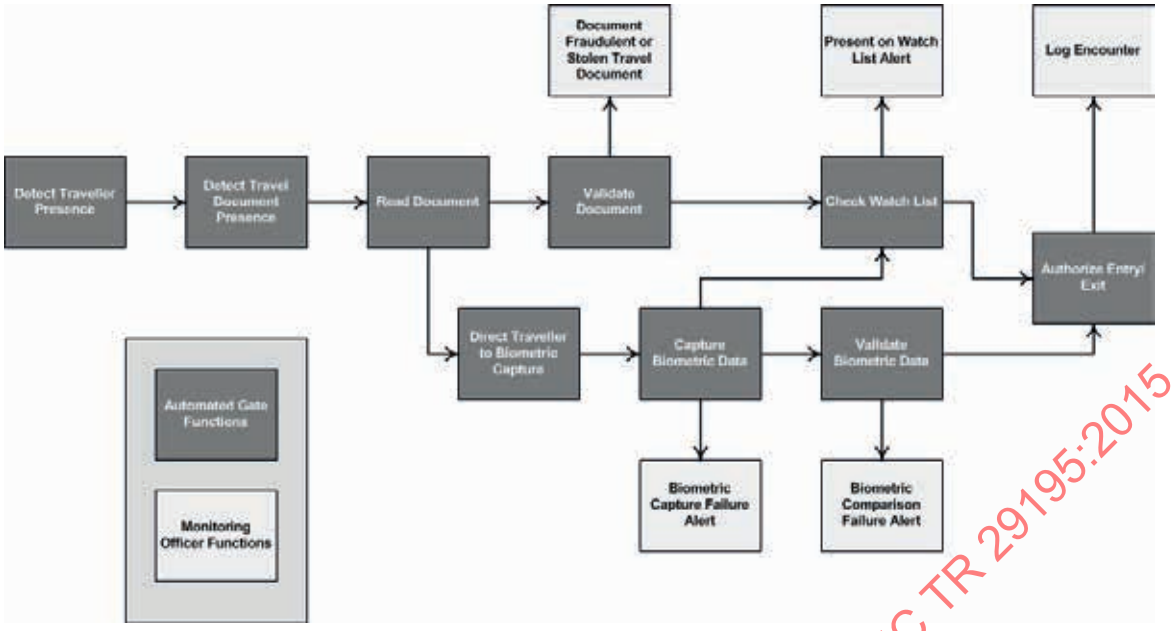

Figure 1 — Automated gate processing flow (an example)

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

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

© ISO/IEC 2015 – All rights reserved

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

 © ISO/IEC 2015 – All rights reserved

   c. Use mantrap type gates that have sensors that detect multiple traveller presence and can discriminate between travellers and baggage.

4. A malfunction in a processing Gate allows unverified persons to pass through.

   a. Where possible the Gate design should ensure the Gate closes when such a malfunction occurs or an alarm is triggered for security officer attendance in the event a Gate fails to close.

5. A person's biometric claim is incorrectly accepted (e.g. when they inadvertently use the passport of another person).

   a. Establish a biometric performance monitoring and review regime which includes periodic checks of selected transactions, gathering of operational biometric performance metrics and review of threshold settings.

The probability and method of potential fraudulent use will depend on the type of biometric modality and the security features of the document.

5.2 Technical considerations

The technology should support existing business solutions, be based on current standards to help with system interoperability and be flexible enough to accommodate future business changes. Business processes and supporting information systems need to be re-engineered together. New technologies, incorporating biometrics, should be implemented after work processes have been analysed, simplified, or otherwise redesigned as appropriate.

The design and implementation of automated border control systems using biometrics should be such that it is a fully integrated component of the existing suite of border control system components. This has a number of advantages including:

1. From a traveller perspective, it is apparent that a choice (of self-process or manual control) is available to them for border processing.

2. In the event that the 'self-processing' option is not available for any reason, the border control authority can readily accommodate processing for all travellers by border control officers.

3. The information collected through the 'self-processing' option can be utilised for further border control checks in the same way that information collected through border control officer processing is used for border control checks.

4. As traveller numbers increase, it is relatively easy to add additional 'self-processing' points as required.

To facilitate integration of the 'self-processing' option, into existing information and data holdings, software and technical infrastructure, the characteristics of the design should include:

1. Appropriate application of technology and biometric standards including those that enable data and system interoperability.

2. The collection, storage and use of biometric data in a format that facilitates biometric identification for watchlist purposes and subsequent disclosure to partner authorities subject to purpose limitations.

3. Use of biometric technology approaches that are security and privacy enhancing.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

5.2.1 Security/Privacy

Traveller confidence and trust in the system is important to encourage both first time and repeated use and to ensure authorities realise the benefits that traveller 'self-processing' brings. Confidence and trust can be enhanced through security and privacy measures which include:

1. Conformity with legislative requirements concerning privacy, including system access, use and data sharing constraints, and maintenance of data records.

2. Controls to safeguard the security of sensitive data whether stored or in motion over a network.

Confidence and trust also requires consideration of securing the system to prevent unauthorised access, especially with travellers having access to border networks via Kiosks and Gates.

5.3 Standards for interoperability

To promote interoperability between automated border control systems, border stakeholders should agree on biometric data interchange format standards for the exchange of biometric data.

5.4 Enrolment for automated border control systems

Since a successful biometric enrolment is key to the operation of automated border control systems, authorities responsible for the delivery of enrolment systems should design, deploy and operate these in a quality way. See guidelines provided in ISO/IEC TR 29196, Guidance for biometric enrolment. Authorities responsible for producing ePassports are considered to be providing enrolment services to travellers for use by border stakeholders.

It is important that authorities who issue the travel document engage with Border stakeholders to ensure that the biometric reference in their travel document is compatible with Border stakeholders' Systems. Quality control measures and testing regimes should be implemented to ensure that images conform to appropriate standards. For example, travel documents like ePassports should fully comply with the standards defined in ICAO Document 9303.

It is important that the biometric data provided in the travel document presented to the Border stakeholders should be of a suitable quality to allow biometric comparison.

Technical reports ISO/IEC TR 24714-1 and ISO/IEC TR 29196 provide further information and should be read in conjunction with each other.

Note that although the considerations and recommendations in ISO/IEC TR 24714-1 are directed to commercial applications, this report may contain material that can help in the design of enrolment processes.

5.5 Privacy background for ABC systems

Governments that have implemented, or plan to implement, ABC systems are responsible for protecting the privacy of the individuals that utilize the system. Privacy considerations include not only protecting the Personally Identifiable Information (PII) from unauthorized disclosure; it also includes ensuring that the PII is used only for its intended purpose and that the individual has the opportunity for redress.

The information provided by individuals for use in ABC systems includes both biographic and biometric information which are provided during the enrolment process and/or the verification process and should be kept to a minimum; only the information that is required to meet the business objectives should be requested and retained for the appropriate amount of time. As ABC systems are engineered differently to address various policies and use cases, the implementer should ensure that data is appropriately protected throughout the process, across the following subsystems — data capture, data storage, comparison, decision, signal processing, transmission and administration.

A full list of recommendations pertinent to privacy can be found in ISO/IEC TR 24714-1.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

 © ISO/IEC 2015 – All rights reserved

6 Guidance relating to specific modalities

Data interchange standards exist for multiple biometric modalities as documented in the ISO/IEC 19794 multipart standard. Although many of these modalities could be applied to ABC systems, to date only some these have been implemented.

This Technical Report does not endorse any particular modality. For examples of ABC implementations see Annex A.

Best practice regarding biometric enrolment for each modality can be found in ISO/IEC TR 29196.

6.1 Face

Automated face recognition systems use facial features to discriminate between individuals.

6.1.1 Presentation of subject to camera:

1. The traveller should be clearly directed to face towards the camera used for capturing the facial image. The traveller should not be confused by other cameras, such as those (generally placed overhead) used for security monitoring

2. The physical process for travellers to move through the automated gate should encourage the traveller to present themselves so that an optimal acquisition results. For example presenting the face to the camera in a forward facing, upright position and at a fixed distance from the camera. Due to the fact that self-positioning of the traveller is crucial for facial biometrics, some floor signage could be used — footprint, lines or other.

3. The camera should be positioned at eye level to the traveller's face and guidance should be positioned near the camera lens

4. Provide feedback on the biometric capture and successful verification process to the traveller. Other ways of providing feedback to the traveller should be considered, e.g. audible signals or clear visual instructions to indicate when to proceed through the gate.

6.1.2 Other factors

Other factors not addressed in this Technical Report may need to be considered:

1. Small children and subjects in wheelchairs or with other disabilities. In both cases carers may be present. They should not interfere with the process and their biometric samples should not be captured in error.

2. Travellers with certain disabilities may not be able to hold their head level and this should be handled in a sensitive way and preferably communicated to the traveller in advance of an attempt to use the system.

3. There are cross cultural factors that will affect travellers' use of an automated facial recognition ABC system, such as practices associated with religious or social customs.

6.2 Vascular (vein)

6.2.1 General

Vascular authentication uses the blood vessel patterns of the vein in the subcutaneous tissue of the human body to discriminate between individuals. In practical terms, blood vessel patterns of a hand, such as that of a palm, the back of a hand, or a finger, are used for authentication because such parts of the hand are easy to present to a sensor. Palm vein authentication systems generally use optical palm vein sensors for enrolment of the palm vein image or palm vein pattern. Finger vein authentication

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

systems generally use optical finger vein sensors for enrolment of finger vein images or finger vein patterns. Enrolment considerations are noted in ISO/IEC TR 29196.

6.2.2 Presentation of subject to vein sensors

1. The sensor device should be installed at a height between traveller's chest and waist, so as to improve its usability.
2. A vein authentication is used normally without the cradle. However, especially for those who are not familiar with the vein authentication, a cradle might be used.
3. If a cradle is used, the cradle should not obstruct the imaging of the hand/finger by the sensor.
4. Guidance from the GUI or audio prompts is the most effective way for users to place traveller's hands/fingers upon the sensor correctly.
5. The position of the sensor should be highlighted to assist the traveller in positioning their hand/finger.
6. It is important to provide feedback on the biometric capture and successful verification process to the traveller.
7. It is important to provide interactive feedback, which should be visually displayed and audible to the traveller and/or the instruction, for efficient the automatic gate process. Especially for finger vein, it should be noted that some users may place the finger tip on the image capturing sensor as they may misunderstand that the device is the fingerprint sensor.
8. If the traveller encounters a problem when using the device in a cold morning, one way of improving the performance is to warm the hands by rubbing them.

6.2.3 Other factors

Other factors not addressed in this Technical Report may need to be considered:

1. If there is the only one hand available, then only the palm vein image or pattern from this hand will be enrolled.
2. Quality check algorithms or verification test after enrolment should be used in the enrolment process.

6.3 Fingerprint

6.3.1 General

Fingerprint recognition uses the characteristics that can be found in the lines of a fingerprint images. When looking carefully at those lines, these characteristics can easily be distinguished. The three main characteristics are bifurcations (one line that splits into two lines, i.e. a "Y" shape), end-points (a line that ends in-between other lines), and a core. The latter can be regarded as the centre of a fingerprint around which the lines rotate. One or more core characteristics however may or may not be present.

Different technologies exist to capture fingerprint images. The most widely used technology in ABC applications is based on the "Frustrated Total Internal Reflection" principle. With this type of scanner visible light is used to capture an image of the fingerprint which is placed on a platen.

A second technology that is used for fingerprint capture is "Multi Spectral Imaging". In this technology, images using different wavelengths of light are combined in order to constitute a final image. Because this technology can measure ridge detail beneath the skin of the finger, it is less susceptible to deformations and contaminants on the surface of the finger.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

 © ISO/IEC 2015 – All rights reserved

A third technology consists of high-speed video image capture allowing a contactless acquisition of up to 4 fingers in less than one second. This technology provides ease of use for the traveller (natural single gesture of the hand), preventing also any risk of disease transmission (contactless nature).

A fourth technology is the solid-state fingerprint sensor. This technology is usually a grey scale, rugged, thin, low power, direct-contact fingerprint image capture device. It is able to capture a single flat fingerprint image in less than a second.

Finally, ultrasound can also be used to image a fingerprint. In this type of fingerprint scanners, an ultrasound signal is used to image the presented finger. A regular greyscale image results from the scanning operation. Also this type of scanner will be less susceptible to contaminants and bad fingerprint quality.

6.3.2 Enrolment

Biometric enrolment usually takes place when a person applies for an identity document. Today a significant number of travel documents already include biometric information. The facial image is de-facto integrated in every electronic ICAO compliant travel document. Other biometric modalities like fingerprints or iris images can be included as well. However, to gain access to those biometric modalities, special authentication mechanisms (EAC, SAC) must be used.

During the enrolment of the fingerprints, two aspects are important. First, the quality of the fingerprint itself, depending on the applicant (e.g. someone working in construction or in a chemical plant) it may be difficult to capture the fingerprints. In difficult situations, it is not unheard of to have a Failure to Enrol of 2 % of the applicants. Second, the technology used to capture the fingerprints plays a vital role in the ability of the enrolment system to capture high quality fingerprints that can later on be used to authenticate the person. As discussed in the introduction of this section, different technologies exist to capture fingerprints. Each of these technologies has their advantages and disadvantages.

Biometric characteristics captured during enrolment are typically stored in travel documents in an interoperable format, i.e., as images. Refer to ICAO Document 9303 for details on specific image encoding.

Biometric modalities are stored in electronic form in an ICC/RFID chip embedded in the travel document.

Automated border control solutions that are based on travel documents are typically not involved in the enrolment operation.

6.3.3 Verification

Fingerprint verification is the process of comparing live captured fingerprints against a (trusted) source of earlier captured fingerprints of that same person.

Within the scope of automated border control installation, the trusted source is most often an official travel document issued by a State. As indicated before, the biometric modalities that are more often used today in travel documents are the facial image. The facial image can be extracted from the travel document's RFID chip by reading the data page's Machine Readable Zone and calculating the access key (BAC). Fingerprint and Iris images however are more securely stored to extract as specialized authentication mechanisms are put in place to protect this sensitive information (EAC protocol).

At an automatic border control installation, fingerprints will be captured from the traveller and compared against the fingerprint information retrieved from the travel document.

Because the travel document contains fingerprint images, the same algorithm can be used to convert the images into fingerprint templates. The biometric algorithm will then compare both templates and provide a comparison score. Depending on the implementation rules, such a score will be regarded as an indication that both fingerprints come from the same person or not and what action should be taken accordingly.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

6.4 Iris

Iris recognition systems use random patterns that are visible within the iris of an eye to discriminate between individuals.

6.4.1 Presentation of subject to camera

1. The traveller should be clearly directed to look towards the camera used for capturing the irises -with other cameras, such as those (generally placed overhead) used for security monitoring carefully positioned to avoid confusion

2. The physical process for travellers to move through the automated gate should encourage the traveller to present themselves so that an optimal acquisition results. For example the traveller can stop not more than 2 seconds, presenting the face to the camera in a forward facing, upright position and at a fixed distance from the camera (e.g. at a distance of 1 m (±20 cm) assessed to be ideal in the ABC context). Due to the fact that self-positioning of the traveller is crucial for iris biometrics, some floor signage could-be used — footprint, lines or other.

3. The camera should be positioned at eye level to the traveller's face and guidance to users should be positioned near the camera lens (placing guidance at hand level will encourage users to look at hands)

4. Provide feedback on the biometric capture and successful verification process to the subject. Other ways of providing feedback to the traveller should be considered, e.g. audible signals or clear visual instructions to indicate when to proceed through the gate.

5. Attention should be paid when implementing the system that the camera and illumination technology is able to deal with persons wearing (optical/medical) eye glasses without the need for these persons to remove their glasses. Camera technology, illumination, and system setup should be chosen accordingly. Only in very few exceptional circumstances is it necessary for travellers to remove their glasses.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

Annex A
(informative)

Different types of ABC systems

There are a different number of different types of automated border control systems already in use around the world.

See the table below which describes some of the various types of solutions:

Real world system implementation		RAPID	Nexus	Privium	Smartgate
Biometric Modality		Face	Iris	Iris	Face
Location of biometric reference template	In a token held by the traveller.	Y			Y
	In a centralised system that is located by the traveller supplying their physical biometric		Y		
	In a centralised system that is located by the traveller supplying an identifier			Y	
	A combination of token and centralised system				
Appliance configuration	Kiosk where biometric reference is extracted and a printed reference is returned to the traveller.		Y		Y
	Kiosk where biometric reference is extracted and no printed reference is required.				
	Gate where biometric sample is taken from traveller.				
	Gate where printed reference is retrieved and biometric sample is taken from traveller.				Y
	Combined gate and kiosk process	Y		Y	
Printed reference required.	Ticket required	N	Y	N	Y

For each of these systems there will be different requirements and operational guidance. This Technical Report focuses in the main on face and iris systems which rely on the ICAO compliant machine-readable travel document as the biometric token and on iris systems with or without a token. The guidance will in most cases also be applicable to a wider range of situations.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

Annex B
(informative)

Examples of automated border control systems

Country	System Name	Modality
United Kingdom	Mifare IRIS ePassport Gates ACS	Iris, Face and Fingerprint Iris (identification only) Face Face and Fingerprint
Netherlands	Privium IET (Privium to US)	Iris Iris
Portugal	RAPID	Face
France	PEGASE/PARAFES	Fingerprint
Malaysia	MyKad	Fingerprint Standard-MS1901
Singapore	BioPass	Face and Fingerprint
Australia	SmartGate	Face
Germany	EasyPASS Frankfurt ABG	Face Iris
Finland	RAPID	Face
Japan	Automated Gate	Fingerprint
New Zealand	SmartGate	Face
USA	Global Entry	Fingerprint and Iris
USA	NEXUS (http://www.cbsa- asfc.gc.ca/prog/nexus/air-aerien-eng.html)	Fingerprint and Face (for enrolment and vetting only, no biometrics used for passage)
USA	SENTRI	Fingerprint and Face (for enrolment and vetting only, no biometrics used for passage)
Israel	Palestine Workers	Face and Hand Geometry
China	Hong Kong SAR	Fingerprint
Korea	KISS (Automated Gate)	Fingerprint

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

Annex C
(informative)

Malaysia Autogate System

C.1 Overview

The ePassport is now used extensively to enter and exit from the country. Currently, the major entry and exit points in the country have in place Autogate(s) which allow automatic clearance of Malaysian citizens holding ePassports.

C.2 System Description

Basically, the Autogate will recognise the Malaysian ePassport and then perform the necessary clearance processes according to the passport types.

When the system detects a passport, the biometrics matching and backend verification function needs to be invoked.

Data verifications ensure document presented is valid at the time of use.

Biometrics (fingerprint) matching enables accurate verification of the passport holder identity against the presented official document.

Backend verification ensures only allowed users can pass through.

C.3 System Workflow

The diagram below illustrates the high level process/operations flow performed by the Autogate System

Figure C.1 — Autogate system workflow

Basically, the workflow (referring to the above diagram) is as follows:

1. First the Autogate will detect for the presence of the travellers inside the barriers.
2. Then, the system will detect the placement of the passport on the Autogate system reader or sensor.
3. The system will then proceed to read and extract the required information from the passport.
4. The extracted data will be verified and validated against pre-set rules and conditions.
    a. Data is checked for document validity
    b. Data is checked for blacklist/whitelist

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

   c. Biometrics data is verified with live captures

5. If the verification process is successful, the traveller is cleared accordingly.

   a. Transaction log and audit trail are generated.

6. However, if the traveller fails the verification process, the traveller is required to revert to the manual counter for further action and investigation.

7. Transaction logs and audit trails are created for every transaction that took place.

C.4 System Design Considerations

1. Safety of users is ensured where users would not be injured by the mechanical and electronic components of the Autogate.

2. User friendliness and simple operating procedures are integrated to ensure users of different age, gender, height, size and educational background are able to use the Autogate with minimum assistance.

3. Accuracy is increased by the integrated intelligence and security control to minimize flaws in inspection and clearance process.

4. Performance of Autogate is optimized for efficient self-service clearance, capped at 15 seconds under normal usage and circumstances.

5. Contingencies are built-in to ensure minimum interruptions to the system operation and immigration clearance process.

6. Comprehensive design to enable human intervention to monitor and override automated process and manual processes handling.

7. Authentications to ensure genuine transactions via System Authentication, Terminal Authentication, Document Authentication and User Authentication.

C.5 Values Proposition of Autogate

1. Primary use of autogate is to automate the Immigration Inspection and clearance securely.

2. Reduces the manpower needed by the immigration for inspection and clearance.

3. Uses biometrics to identify the person to the electronic travel document presented.

4. Includes network connectivity to enable real-time blacklist, suspect list checking with Immigration hosts and upload of movement records.

5. Reduces usage of passport pages.

C.6 Lessons Learned

1. The recommended users or answers are those who are

   a. Able to enter the Autogate without any assistance

   b. Able to place passport or other acceptable document on the reader with minimum assistance remotely

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

 © ISO/IEC 2015 – All rights reserved

   c. 4 years old and above are able to perform Autogate clearance with minimum assistance remotely

2. Autogate to have sufficient built-in redundancy and flexibility to ensure

   a. User safety and 100% evacuation

   b. Maximum uptime

   c. Maximum accuracy

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

Annex D
(informative)

Nexus iris recognition system

NEXUS is a bi-national program implemented by both the CBSA and U.S. Customs and Border Protection that offers expedited border clearance in the air, land and marine modes of travel. Members can clear the border faster when travelling to both Canada and the United States.

CANPASS Air is a CBSA program. Members can clear the border faster when arriving in Canada from any country in the world. Canadian citizens, Canadian permanent residents, and US citizens may participate through an opt-in enrolment process. During enrolment, biographic information is collected along with iris biometrics and are stored in a secure government repository. Background checks are performed utilizing the information provided to ensure that all participants are low-risk.

CANPASS Air participants avoid the manual immigration process and perform the required immigration and customs processing at an automated kiosk. The CANPASS Air member is biometrically verified by comparing the iris images captured at the kiosk against those stored in a secure government repository. The CANPASS Air member does not need to present their membership card at the kiosk but must carry it with them.

NEXUS (http://www.cbsa- asfc.gc.ca/prog/nexus/air-aerien-eng.html)

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

Annex E
(informative)

United Kingdom

E.1 Use case 1: Facial Recognition Gate — Manchester

1. Trusted traveller scheme (EEA/Swiss nationals).
2. No registration required.
3. ePassport required as token.
4. Dual-stage process — double barrier construction.
5. Trial complete. System is now permanent.

E.1.1 Decision to use system

1. *Awareness of system existence:* Leaflet with new passports (UK), press launches/media coverage, announcement/film on flight, announcement on arrival at port, signage in participating ports.
2. *Traveller makes decision based on:*
   - Signage
   - Shorter queue
   - Faster
   - Past experience
   - Machines switched on and available to use
   - Assistance available/proactive encouragement to use
   - Others using
   - Instructions
   - *Eligibility:* Individual user only — no accompanying children/companion/helper. Age limit currently 18+ years old but looking at lowering to 12. Height over 1,4 m.

E.1.2 Stages of Transaction

1. *Access:* Gate opens when ePassport correctly positioned, scanned, chip opened, and background checks passed.
2. *Instructions:* Signage around gate, diagrammatic representation on screens. Screen running info-film at some ports.
3. *Assistance:* 'Hosts, being people employed to assist travellers to correctly use the automated border control system, pick eligible travellers from main queue and assist to use gates.
4. *Verification: This* takes place at the second stage of the process, after the first set of doors have opened.
5. *Process status:* Animated indication of process progress.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved

6. *Success:* Depends in part on understanding and expectation of process and experience of previous use — many automated processes are single-stage and user may expect the same if information is insufficient.

7. *Exit:* If user does not exit quickly, may become trapped in gates. Successful transaction but negative experience. Enhanced information/prompt required?

8. *Experience* to date suggests that an intercom would be useful so that the monitoring officer can communicate with the traveller.

E.1.3 Post-use stage

1. *At port*: signage; through Border Control, baggage reclaim, exit.

2. *Later:* report to others based on experience, choice to use system again.

E.2 Use case 2: Facial Recognition Gate — Stanstead Airport

1. Trusted traveller scheme (EEA/Swiss nationals).

2. No registration required.

3. ePassport required as token.

4. One stage process — single barrier construction.

5. Trial complete. System is now permanent.

E.2.1 Decision to use system

1. *Awareness of system existence:* Leaflet with new passports (UK), press launches/media coverage, announcement/film on flight, tannoy on arrival at port, signage in participating ports.

2. *User makes decision based on:* Signage, Shorter queue? Faster? Past experience? Machines on? Assistance available/proactive encouragement to use? Others using? Instructions?

3. *Eligibility:* Individual user only — no accompanying children/companion/helper. Age limit currently 18+ but looking at lowering to 12. Height over 1.4 M.

E.2.2 Process

1. *Access:* Gate opens when ePassport correctly positioned, scanned, chip opened, background checks passed, and facial recognition verification successful.

2. *Instructions:* Signage around gate, diagrammatic representation on screens.

3. *Assistance:* 'Hosts' direct eligible travellers towards gates and assist to use gates where necessary.

4. *Verification:* Once passport correctly positioned and chip opened.

5. *Process status:* Animated indication of process progress.

6. *Success:* Depends in part on understanding and expectation of process and experience of previous use. Sunlight in the terminal sometimes affects the process and can lead to failure to pass through the gates despite no user fault — frustrating/negative experience.

7. *Exit:* Simple and fast process can leave user unsure whether the Border Crossing process is complete.

8. *Experience* to date suggests that an intercom would be useful so that the monitoring officer can communicate with the traveller.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

 © ISO/IEC 2015 – All rights reserved

E.2.3 Post-stage use

1. At port: signage; through Border Control, baggage reclaim, exit.
2. Later: report to others based on experience, choice to use system again.

E.3 Use case 3: IRIS

1. Registered, trusted traveller system.
2. Voluntary participation.
3. Enrolment: unbooked, on departure at participating UK airports.
4. Verification: upon arrival at participating UK airports.

E.3.1 Pre-enrolment

1. User awareness of: system existence, location and availability of enrolment service.
2. Signage.
3. Eligibility: administrative e.g. immigration status,
4. Exception e.g. sight impaired, wheelchair user.

E.3.2 Enrolment

1. Assisted by officer.
2. Written, verbal and pictorial information provided; in English only.
3. Verification performed as part of enrolment stage but not using the actual gate.
4. Verbal instructions only with some visual prompt on correct positioning.

E.3.3 Verification stage — at the Border

1. First full system use separated in time from enrolment — next UK arrival.

E.3.4 Decision to use system

2. *User makes decision based on:* Signage, Shorter queue? Faster? Past experience? Machines on? Assistance available/proactive encouragement to use? Others using? Instructions?
3. *Eligibility:* Individual user only — no children/companion/helper.

E.3.5 Process

1. *Access:* Gate opens on proximity — assumption that only registered users will enter.
2. *Instructions:* Audio instructions in English; relies on memory of verification undertaken at enrolment.
3. *Information:* No indication of process progress — user uncertainty.

E.3.6 Post-stage use

1. *At port*: signage; through Border Control, baggage reclaim, exit.
2. *Later:* report to others based on experience, choice to use system again.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 29195:2015

© ISO/IEC 2015 – All rights reserved