PD CEN/TS 16634:2014

BSI Standards Publication

Personal identification — Recommendations for using biometrics in European Automated Border Control

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TS 16634:2014.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 83046 4

ICS 35.240.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2014.

Amendments issued since publication

Date	Text affected

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 16634

April 2014

ICS 35.240.15

English Version

Personal identification - Recommendations for using biometrics in European Automated Border Control

Identification personnelle - Recommandations pour l'usage de la biométrie lors des contrôles automatisés aux frontières de l'Europe

Persönliche Identifikation - Empfehlungen für den Einsatz von Biometrie bei der automatisierten Grenzübergangskontrolle in Europa

This Technical Specification (CEN/TS) was approved by CEN on 11 November 2013 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword

This document (CEN/TS 16634:2014) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by AFNOR.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

European countries are increasingly deploying technological solutions to support border guard officers in fulfilling their duties. Such solutions can consist of inspection systems that directly assist the officers in screening travellers or of electronic kiosk and gates offering various degrees of automation.

Electronic Machine Readable Travel Documents (eMRTD) as defined in ICAO Document 9303 [27] can contribute to a high degree of border automation. Under Council Regulation (EC) No 2252/2004 [21], EU Member States nowadays issue electronic passports containing biometric data (facial image, two fingerprint images). Ireland and UK are not bound by the Regulation and issue ePassports storing only the facial image of the holder. Currently a number of European countries have deployed ABC systems which automate border checks for EU citizens in possession of an electronic passport. The upcoming "Smart Borders Package" will foresee the introduction of an EU Registered Traveller Programme [23]. This would allow certain groups of frequent travellers (i.e. business travellers, family members, etc.) from third countries to enter the EU, subject to appropriate pre-screening, using simplified border checks at ABC systems. The European Commission proposes that this RTP makes maximum use of existing systems and tools, such as the Biometric Matching System which underpins the Visa Information System (VIS) and the fingerprint scanners which are used for this system.

There is a need to harmonize processes containing biometric elements, biometric technology tests and reporting frameworks (in accordance with Bibliographical Entries [11], [12], [13]) and to link biometric characteristics with supervision requirements.

This Technical Specification focuses on automated systems that can be supervised by an operator, but such supervision is not a requirement for the biometric comparison subsystem. The level of supervision is an operational decision that can be changed according to the needs of the operating authorities.

ABC systems can be classified into four profiles based on their document requirements:

- eMRTD based,
- MRTD based,
- Token other than MRTD - physical and logical, transferable,
- Tokenless.

Regarding the location of the eligibility check, ABC systems can be implemented as:

- One-Step Process,
- Integrated Two-Step Process,
- Segregated Two-Step Process.

This document has been drafted with the contribution of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex) and was adopted by CEN after public enquiry and formal vote according to the CEN Rules of Procedure.

1 Scope

This Technical Specification primarily focuses on biometric aspects of Automated Border Control (ABC) systems. Drawing on the first European and international ABC deployments, it aims to disseminate best practice experiences with a view to ensure consistent security levels in European ABC deployments. Furthermore, the best practice recommendations given here shall help make border control authorities' processes more efficient, speeding up border clearance, and delivering an improved experience to travellers.

ISO/IEC JTC1/SC 37 has published a series of standards dealing with biometric data coding, interfaces, performance tests as well as compliance tests. In order to promote global interoperability it is essential that all these standards are applied in European deployments. However, these standards do not consider national or regional characteristics; in particular, they do not consider European Union privacy and data protection regulation as well as European accessibility and usability requirements [22]. Thus, this Technical Specification amends the ISO standards with respect to special European conditions and constraints.

The Technical Specification systematically discusses issues to be considered when planning and deploying biometric systems for ABC and gives best practice recommendations for those types of systems that are or will be in use in Europe. The document deals with personal identification including ergonomic aspects that have an impact on the acquisition of biometric data.

Communication, infrastructure scalability and security aspects other than those related to biometrics are not considered. This document also does not consider hardware and security requirements of biometric equipment and does not recommend general border crossing procedures.

The enrolment process, e. g. for electronic passports, is out of scope of this document.

2 Terms and definitions

2.1
Automated Border Control (ABC) system
automated system which 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 of border crossing according to the pre-defines rules

2.2
biometric capture
collection of, or attempt to collect a signal(s) from a biometric characteristic(s), or a representation(s) of a biometric characteristic(s,) and conversion of the signal(s) to a captured biometric sample set [4]

2.3
biometric verification
process of confirming a biometric claim of the holder of an eMRTD through biometric comparison

2.4
border checks
checks carried out at border crossing points, to ensure that persons, including their means of transport and the objects in their possession, may be authorized to enter the territory of the Member States or authorized to leave it [24]

Note 1 to entry: See also “Border crossing point (BCP)”.

2.5
Border Crossing Point
BCP
crossing point authorized by the competent authorities for the crossing of external borders [24]

2.6
border guard
public official assigned, in accordance with national law, to a border crossing point or along the border or the immediate vicinity of that border who carries out, in accordance with the Schengen Borders Code and national law, border control tasks [24]

2.7
border management authority
public law enforcement institution which, in accordance with national law, is responsible for border control

2.8
database
application storing a structured set of data and allowing for the management and retrieval of such data

EXAMPLE The Schengen Information System (SIS) is a joint information system that enables the competent authorities in each Member State of the Schengen area, by means of an automated search procedure, to have access to alerts on persons and property for the purposes of border checks and other police and customs checks carried out within the country in accordance with national law and, for some specific categories of alerts (those defined in Article 96 of the Schengen Convention), for the purposes of issuing visas, residence permits and the administration of legislation on aliens in the context of the application of the provisions of the Schengen Convention relating to the movement of persons.

Note 1 to entry: See also “Schengen area” and “Watch List”.

2.9
database hit
instance of identifying an item of data which matches the requirements of a search

Note 1 to entry: See also “Database” and “Watch List”.

2.10
digital mirror
display showing the horizontally mirrored live image of the camera's capturing area

2.11
eGate
one of the components of an ABC system, consisting of a physical barrier operated by electronic means

2.12
eID
electronically enabled card that may be used as an identity document (typically compliant to ICAO Doc 9303 Part 3 [27])

2.13
ePassport
A machine readable passport (MRP) containing a contactless integrated circuit (IC) chip within which is stored data from the MRP data page, one or more biometric samples of the passport holder, and a security object to protect the data with Public Key Infrastructure (PKI) cryptographic technology, and which conforms to the specifications of ICAO Doc 9303, Part 1 [27]

2.14
EU citizen
person having the nationality of an EU Member State, within the meaning of Article 20(1) of the Treaty on the Functioning of the European Union

2.15
Frontex
European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union [29]

2.16
impostor
subversive biometric capture subject who attempts to be matched to someone else's biometric reference [4]

2.17
Machine Readable Zone
MRZ
area on a passport containing two lines of data (three lines on a TD-1 card) that are printed using a standard format and font as explained in ICAO Doc 9303

Note 1 to entry: See also "Visual Inspection Zone (VIZ)".

2.18
member state
country which is member of the European Union

Note 1 to entry: Within the context of the present Recommendations, the term also applies to those countries that, not being EU members, take part in the Schengen area. See also "Schengen area".

2.19
Machine Readable Travel Document
MRTD
official document (e.g. passport, visa), conforming with the specifications contained in ICAO Doc 9303, issued by a State or organization which is used by the holder for international travel (e.g. passport, visa, MRTD) and which contains mandatory visual (eye readable) data and a separate mandatory data summary in a format which is capable of being read by machine

2.20
operator
border guard officer who is responsible for the remote monitoring and control of the ABC system and whose tasks typically include:

a) monitor the user interface of the application;

b) react upon any notification given by the application;

c) manage exceptions and make decisions about them;

d) communicate with the assisting personnel for the handling of exceptions at the eGates;

e) monitor and profile travellers queuing in the ABC line and using the eGates looking for suspicious behaviour in travellers; and

f) communicate with the border guards responsible for second line checks whenever their service is needed

2.21
presentation attack
person can conduct a presentation attack by using artificial or non-living biometrics [4]

2.22
Registered Traveller Programme
RTP
scheme aiming to facilitate border crossing for frequent, pre-vetted and pre-screened travellers, often making use of ABC systems

2.23
Schengen Area
area without internal border control which encompasses 26 European countries, including all EU Member States except Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom, as well as four non EU countries, namely Iceland, Lichtenstein, Norway and Switzerland, and which takes its name from the Schengen Agreement signed in Schengen, Luxembourg, in 1985 and later incorporated into the EU legal framework by the 1997 Treaty of Amsterdam

2.24
spoof attack
attack on a biometric system wherein an artefact is presented to a sensor for the purpose of being enrolled or recognized, or for the purpose of circumventing an enrolment or recognition process

2.25
third country national
person who is not an EU citizen within the meaning of Article 20(1) of the Treaty on the Functioning of the European Union and who is not a person enjoying the Union right to freedom of movement, as defined in Article 2(5) of the Schengen Borders Code

2.26
Visual Inspection Zone
VIZ
portions of the MRTD (data page in the case of an ePassport) designed for visual inspection, i.e. front and back (where applicable), not defined as the MRZ

Note 1 to entry: See also “Machine Readable Zone (MRZ)”.

2.27
watch list
list of individuals, groups, or items that require close surveillance

3 Abbreviated terms

ABC	Automated Border Control
BCP	Border Crossing Point
CEN	European Committee for Standardization
DG2	Data Group 2 (eMRTD face image)
DG3	Data Group 3 (eMRTD fingerprint image)
DET	Detection Error Trade-off
EEA	European Economic Area
eMRTD	Electronic MRTD
EU	European Union
EU/EEA/CH	European Union/European Economic Area/ Switzerland
FAR	False accept rate
FRR	False reject rate
ICAO	International Civil Aviation Organization
IR	Infrared
ISO	International Organization for Standardization
JPEG	Joint Photographic Experts Group

JPG	JPEG compression format for images
JPG2000	JPEG 2000 compression format for images
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
MS	Member State of the Schengen Agreement
PC	Personal Computer
RFID	Radio Frequency Identification
RTP	Registered Traveller Programme
SC	Subcommittee
SDK	Software Development Kit
TC	Technical Committee
TCN	Third Country Nationals
TS	Technical Specification
UV	Ultraviolet
VIS	Visa Information System
VIZ	Visual Inspection Zone
WG	Working Group

4 ABC systems - an overview

4.1 Concept

An ABC system “authenticates the eMRTD, establishes that the traveller is the rightful holder of the document, queries border control records, then automatically determines eligibility for border crossing according to pre-defined rules” [28].

An ABC solution checks the authenticity of the travel document presented by a traveller and the traveller's ownership of that document using his/her biometric data. An eMRTD based ABC system may make use of all the biometric modalities recommended by ICAO, i.e. face, finger and iris. While other biometric modalities could be used for ABC, this TS concentrates on the ones approved by ICAO.

As ABC systems might also be based on another token than an eMRTD or might be tokenless, the authenticity check of the travel document might have been done at the time of enrolment for the system.

An important issue concerns the need for clearly defined protocols when failures appear in a fully automatic system (without human supervision). Failures can lead to genuine user rejection or problems with outliers (i.e. people that have difficulty in fully showing their face due to cultural reasons). In such situations, and in order to avoid raising acceptance issues, an alternative procedure can be needed. Such an alternative procedure can consist of performing border checks in a dedicated, assisted border control booth. The definition of these protocols is out of scope of this Technical Specification.

4.2 Biometric references

The use of biometric data is the key for ensuring a close binding between the person and the document.

As described in [26] two general types of ABC systems can be identified in relation to their use of biometric references, token-based or tokenless:

- Token based systems require the traveller to present a token (eMRTD, MRTD or any other issued or approved token) to the system, in order to provide additional authentication information or biometric references.

- If local legislation does not require the presentation of a travel document for border crossing, it is possible to rely only on live biometrics capture of pre-enrolled qualified (vetted) travellers at the time of the border crossing. In this case immediate (1:N) comparison against an up-to-date list of authorized travellers would take place without any document inspection during the ABC process. Legislation might require that travellers carry a valid travel document even if this document does not have to be presented for inspection.

This document focuses on the biometric aspects of both types of ABC solutions.

4.3 Types of travel documents

4.3.1 General

Usually, travellers wishing to enter the European Union are required to carry a passport as a travel document compliant with the ICAO Doc 9303 attesting the holders' nationality and their demographic data. Personal identification information is available both in printed form on the data page of the document, as well as stored in the RFID chip (ISO/IEC 14443 [6]) complying with the ICAO Doc 9303 for national identity documents. It therefore carries the capabilities for biometric identification using a facial comparison system external to the document itself. The following travel ID documents are currently in use or could be used in the future for ABC in the Member States:

- ePassports issued to EU/EEA/CH citizens;

- National ID cards (in Germany and Spain for their own citizens).

In the future, if legislation and technical means allow it, other documents e.g. ePassports of third country nationals (visa waiver), registered traveller cards and Schengen visa could also be used.

4.3.2 National identity cards

Electronic national identity cards are used in a number of countries including the EU/EEA/CH. Such cards identify physically and/or electronically a person as a national of the issuing country, and accredit the biographic data of that person. They store personal identification information both in the VIZ of the document as well as in the MRZ according to ICAO Doc 9303 Part 3. National ID cards issued by the Member States are accepted as travel documents entitling the holder to cross the external borders in the EU/Schengen context.

Some national ID cards provide eID capabilities using biometric functionality for "comparison-on-card" as well as for "comparison-off-card" in accordance with the standards for 2nd generation electronic passports. CEN/TS 15480 (all parts) standardizes these documents [2].

Currently, national eID cards can be used only in a limited number of ABC systems and by own citizens of the deploying country although greater interoperability may be achieved in the future.

4.3.3 Biometric passports

Such passports are travel documents compliant with ICAO Doc 9303 Part 1. They attest the nationality and the biographic data of a certain person. Personal identification information is stored in the VIZ and in the MRZ of the document, as well as in the RFID chip complying with ICAO Doc 9303. Biometric passports carry reference data for two types of biometric identification:

- a facial image is stored in all biometric passports.

- depending on the country of issuance the passport may store, in addition, the images of the two (in the most cases) index fingerprints, the two iris images, or both; using fingerprints is mandatory for all countries bound by Regulation EC 2252/2004 [21].

Biometric passports have no biometric verification capabilities (facial, and/or fingerprint or iris), thus external verification units are required for the automated biometric verification of the passport holder.

4.3.4 Schengen visa

Nationals of certain countries require a visa in order to cross the borders of the Schengen area. Personal identification information is printed in the VIZ as well as in the MRZ of the document.

Additionally, the Schengen biometric visa, issued by EU/EEA/CH countries covered by Schengen agreements, contains reference to fingerprint data stored in the European Visa Information System (VIS). If future legislation allows it, such visas could be used in ABC systems.

4.4 Topologies of ABC systems

In general there are three topologies of ABC systems in use:

- one-step process which combines the verification of the traveller and their passage through the border; this design allows the traveller to complete the whole transaction in one single process without the need to move to another stage;

- integrated two-step process, which is a variation on the one-step design described above: the difference between the two topologies is that in an ABC system designed as an integrated two-step process the traveller will initiate the verification of the document and the traveller’s eligibility to use the system at the first stage, and then if successful move to a second stage where a biometric comparison and other applicable checks are carried out;

- segregated two-step process where the process of traveller verification and their passage through the border control are completely separated; the traveller verifies at the first stage, a tactical biometric is captured or a token is issued, and then the traveller proceeds to the eGate where the tactical biometric or the token is checked to allow border crossing.

5 Biometric systems in ABC

5.1 General recommendations

5.1.1 Usability and accessibility

In automated systems, the usability of the system for the traveller is a key factor for system performance as well as for traveller acceptance.

Usability consists of:

- ergonomic aspects of the user interfaces (e.g. sensors, input devices, displays);

- aspects of user guidance (e.g. signage, feedback, user information).

To enhance the usability of systems, the following factors with regard to the system environment should be considered:

- climate;

- contamination;

- external or public areas;
- throughput and data subject population;
- access to the devices (position and location of the devices);
- illumination.

NOTE 1 Further guidance on these aspects is given in ISO/IEC/TR 24714-1 [14].

The use of the system should be intuitive and the sequence of actions should be logical.

The EN 1332 series [1] specifies requirements for the user interface of identification card systems and should be applied when designing a biometric ABC system. With regard to the ergonomic aspects of user guidance displays, the relevant standards of the ISO/IEC 9241 series [5] should also be taken into account. Specific attention should be paid to legibility (e.g. font size and contrast) and colour coding. Colour and shape based information should always be used simultaneously. Multiple colours or harsh contrasts within graphics should be avoided to enable travellers with visual impairment to use the system easily.

In order to maximize accessibility, ABC systems should be designed to cater for travellers who have permanent or temporary physical or psychological disabilities. They should be easy to use and flexible enough to deal with handling errors. For travellers that cannot use the biometric system alternative systems are necessary and should be provided.

Disabled travellers might need extra assistance on the use of biometric systems. Furthermore, the specific needs of disabled people should be considered during the specification phase of a system and tests should be performed as early as possible.

Consideration should be given to traveller ergonomics as these will impact on usage and transaction times. Recommendations are listed below [30]:

- ePassport readers should be at a height which makes them easy to reach by the majority of travellers (average elbow-height), and placed on the right hand side of the eGate.
- The usage of ABC systems should require the minimum essential number of physical interactions. This will reduce the number of times that a traveller shall swap hands with baggage. The system should take into account the prevalence of large trolley bags with travellers.
- ABC systems should be usable with low physical effort.
- ABC systems should be designed to be inclusive with respect to height of travellers. Minimum and maximum acquisition heights should be as wide as possible to enable more travellers to use the system.

User guidance should be given by:

- early information of eligibility to use the ABC System;
- information about the status of the system, the current step to be performed by the traveller, and the remaining steps including time estimates;
- clear, intuitive, and self-explanatory instructions: the instructions should consider languages that are likely to be understood by the traveller, using simple wording;
- pictograms demonstrating the correct facial pose, digital mirrors reflecting the facial image of the traveller and visual indications which attract the traveller’s attention to notify the user how to properly stand in front of the camera(s) for the facial image acquisition: a diagram of the hand, with the finger required for the verification properly marked can avoid wrong finger placement errors;

- enhancements such as blinking lights or other effects to attract the attention of travellers at critical stages should also be considered;
- feedback that indicates success or failure as well as responses expected from the traveller;
- an indication that biometric capture is taking place (especially when the traveller is not required to take actions);
- the availability of a help or support facility;
- adequate signage and user information that is clear and carefully positioned for maximum visibility.

For the purpose of consistency and understanding, standardized symbols, icons and pictograms should be used. An example is given in Bibliographical Entry [20].

Standards providing further guidance on the use of symbols, icons and pictograms in biometric systems are currently drafted in the standardization committee ISO/IEC JTC1/SC 37 in the project ISO/IEC 24779 series [16]. It is recommended that all deployed ABC systems make use of the same set of pictograms to reach a unique traveller perception and to facilitate and to cause training effects in order to lower error rates. As there is no such set of pictograms available, a close cooperation between all agencies operating ABC systems is recommended.

When implementing ABC systems in parallel one should avoid or at least minimize any interference between systems.

The influence of daylight coming through windows should be considered.

NOTE 2 Airports, railway stations and sea ports usually have indoor facilities for border clearance. In such facilities the environmental conditions are more stable than in outdoor systems.

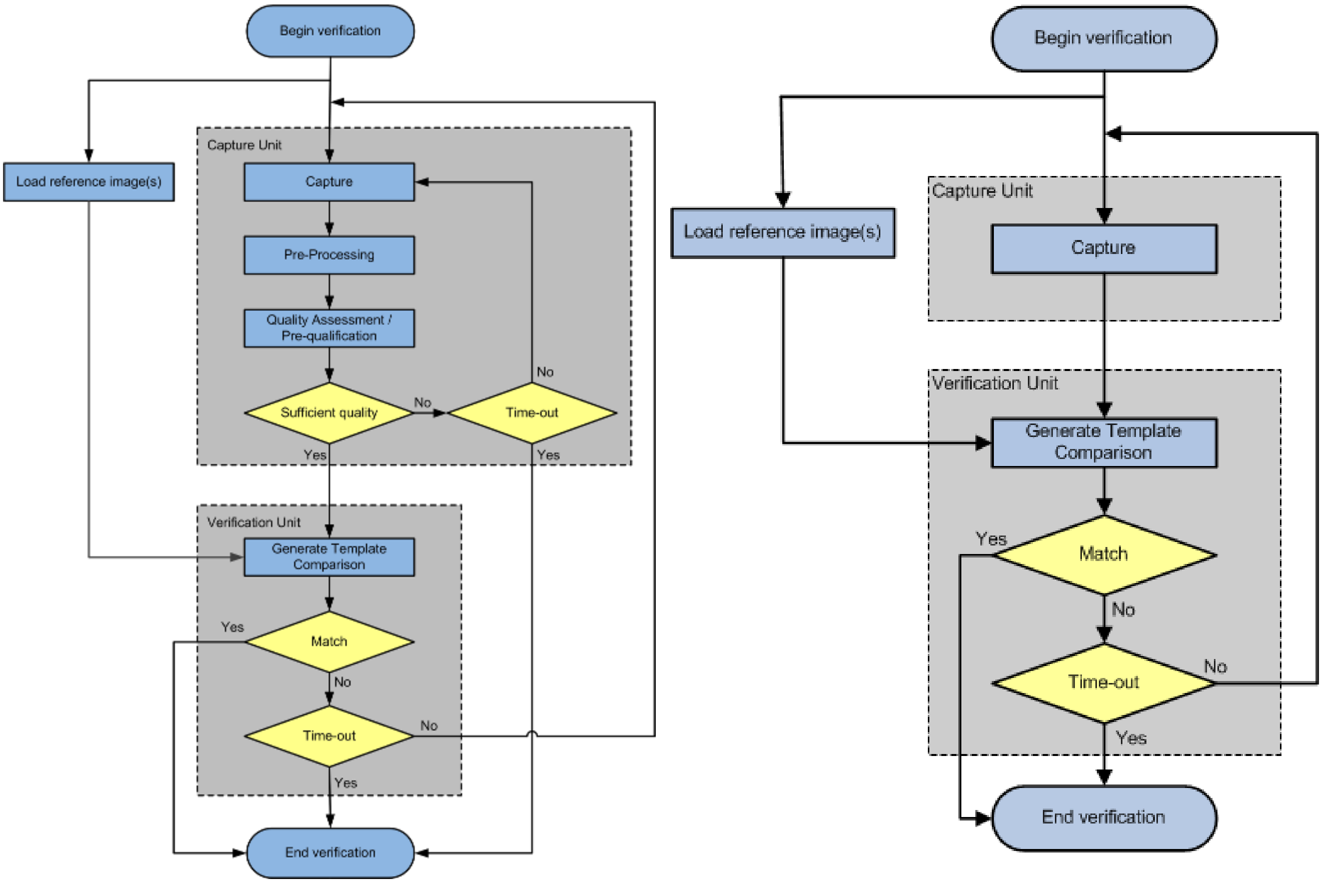
5.1.2 Architecture

Member States can define specific process flows in order to ensure compliance with EU and national border control regulations. To optimize the time required for the verification of each traveller, all technical processes should be carried out in parallel to the extent possible if it speeds up the overall process.

The biometric verification process is composed of two separate steps:

- biometric capture sub-process, carried out by the face, fingerprint or iris capture unit;
- biometric verification sub-process, carried out by the face, fingerprint or iris verification unit.

In general there are two recommended options for the implementation of a biometric verification process within an ABC system. Within the modular approach separate units for capture and verification are used, which provides a high degree of flexibility to the deployed solution, e.g. an easier migration of the comparison algorithm. In this scenario the capture system needs to be able to do pre-qualification and pre-processing to ensure that only images of sufficient quality are provided to the verification process (see Figure 1).



a)

b)

Figure 1 — Verification with quality driven approach a) and score driven approach b)

In the “score driven” method, biometric characteristics from multiple capture attempts are compared with a biometric reference until the comparison score reaches a threshold or a timeout is exceeded. In each capture attempt biometric characteristics are searched for and, if found, encoded and compared against the reference from the passport. If the comparison score is above a threshold, entry is granted, data may be recorded and/or printed and the process is stopped. If the score is not above the threshold then entry is not granted and the traveller is directed to an alternative process.

In the “quality driven” method, biometric characteristics from multiple capture attempts are assessed for quality until a quality level above a threshold is achieved or a timeout is exceeded. In each capture attempt biometric characteristics are searched for and, if found, assessed for their quality. If the quality is above a threshold, the biometric characteristics are encoded, and compared against the biometric reference. If the comparison score is above a threshold, entry is granted, data may be recorded and/or printed and the process is stopped. If the score is not above the threshold then entry is not granted and the traveller is directed to an alternative process.

Those two basic methods can be enhanced or mixed.

When a “score driven” method is used, there is a difference between the FAR computed (as the reference biometric characteristic is used all along the process to determine if the acquisition should end or not) and the operational FAR as the template generated during a genuine acquisition would not necessarily be the same as the one generated if the acquisition had been of an imposter.

By choosing a “quality driven” method, the template generation depends only on the quality of the acquisition and is not linked in any way to quality measured on the reference image.

For the “quality driven” method a DET curve corresponding to the operational performance can be computed offline, as the used and logged image does not depend on the passport image or the acceptance threshold. That way, the impact of a threshold modification on FRR and FAR can be estimated. This allows an analysis of the influence of external factors, such as passport origin, airport environment, frequent users or passport aging on the performance of the biometric subsystem, including their evolution across time.

For the “score driven” method, the FAR cannot be computed offline as the acquisition process relies on the reference image read from the passport. According to ISO/IEC 19795-1:2006, B.1.2, several thousands of independent tests are necessary to claim a FAR of 0,5 %. It does not seem feasible to have so many people using the system with someone else's passport. Moreover, it is not possible to analyse the influence of other factors on the performance of the biometric subsystem.

Another option to measure the operational FAR for a “score driven” method would be to compute FAR based on logged data and to estimate the maximum bias with operational performances.

It is recommended to use interfaces according to BioAPI [7] for the capturing of the biometric data. However, the ABC operator may also allow proprietary vendor-specific SDK interfaces for the integration of the capture unit, if this leads to reasonable advantages.

5.1.3 Biometric security functions

5.1.3.1 General

The reduction of human interaction in automated systems causes new security threats which shall be addressed and treated differently than threats on systems with human interaction. For that reason, it is essential to perform a complete security assessment for any ABC solution in its application context.

5.1.3.2 Tailgating prevention and detection

For the time being, it should be checked that only one person is using the ABC system at a time to prevent improper use of the system. Therefore, the system can provide technical features to check for uniqueness.

This includes:

- acceptance of each individual;
- refusal of two or more individuals within the biometric data acquisition area; this also includes babies carried by adults using the system;
- capability to detect items behind or in front of individuals (i.e. bags or suitcase).

The restrictions for luggage, hats, glasses, etc. only hold for the face recognition/verification system. Fingerprint verification procedures are not affected by these circumstances but user should be instructed to remove gloves if wearing any.

NOTE In the future, it might be possible to check more than one person at once. This could allow the processing of families and people with special needs.

5.1.3.3 Acquisition of biometric reference data

The traveller puts his/her passport open by the data page (or trusted token) on the document reader. The ABC system reads the biometric data contained in the passport's chip, or calls the stored reference data from a reference database (if a token without data storage capacity is used). For tokenless systems, this acquisition step is skipped.

NOTE The second generation of the data format standards ISO/IEC 19794-4 [8] and ISO/IEC 19794-5 [9] has been published in 2011. Currently, passports implement data groups following the 2005 versions of these standards. At some time ICAO might decide to start a transition to the 2011 version.

Integrity and authenticity of the reference data should be checked. For eMRTDs the security protocols according to [27] and [21] should be used. In case of using a reference database appropriate security mechanisms should be implemented.

The solution should be compatible with all eMRTD according to ICAO Document 9303 and all other eligible travel documents specified by EU or Member State legislation (see 4.3).

5.1.3.4 Biometric comparison

The biometric verification component should compare the traveller's biometric data captured live with those acquired as his/her reference data.

The maximum time necessary for the biometric verification (and, additionally, the maximum number of attempts) should be set for all ABC systems in a way to avoid acceptance issues. The system should give feedback about the current status shortly after the process has started. The maximum time and number of attempts set depend on the application case and should be established taking into consideration accuracy and throughput constraints.

In the case of identification, the traveller's biometric reference data should be present in the database of authorized travellers.

NOTE In specific cases, additional biometric functions as the automatic comparison with search lists could be applied during border crossing. Even if identification is not the main functionality of biometrics in a border control context where the idea is to ensure that the person crossing the border is the person he/she claims to be, automatic recognition of searched people is a valuable functionality. In order to perform this task, and if the technology allows fast comparison operations, identification against watch lists can be run using the biometric data included in the passport, acquired directly from the traveller, or both.

ABC vendors should state the expected FAR and FRR, and this statement should be verified by analysing operational data, e.g. by doing offline verification replay.

It is recommended that the achievable performance of the biometric verification algorithm is measured by an independent test laboratory at regular intervals.

5.1.3.5 Multimodal verification

Multibiometric fusion has been considered in ISO/IEC/TR 24722 [15] and can be applied at different levels:

- Sample level: Each biometric process has a collection of samples. That collection of samples is then merged into a single sample. This model can be applied in almost all cases of ABC systems. For instance, it is applied in the fusion of facial recognition algorithms provided by the same supplier who controls the video captures of a traveller in order to provide the better facial image to process.

- Feature level: The extracted features from different samples are merged in a single target feature set. This might happen in ABC systems as part of a multi-input capable algorithm.

- Score level: Each individual biometric process typically generates a score for comparison only, but it could also generate multiple outcomes. These possible outcomes are then merged into one single score or decision, compared with the acceptance threshold system. This model can be applied in almost all cases of ABC systems. For instance, it is applied in the fusion of facial recognition and fingerprint recognition algorithms. It requires an analysis of the score distribution of the single algorithms to derive a fusion mapping.

- Decision level: Each individual biometric process usually provides its own boolean result. The fusion process is solved by a combination algorithm, which could be as simple as AND or OR, or possibly having additional parameters such as levels of quality of the input sample, environmental conditions, etc.

Multibiometric verification can be used to increase the desired security level, to lower error rates or to address more travellers.

As an example, multimodal biometric systems take the input of one or more sensors to capture two or more different types of biometric characteristics. A multimodal biometric fusion with an AND approach can increase the security level by forcing a match for all the modalities. In that case, multimodal technology can increase robustness against spoofing by requiring an impostor to spoof all different modalities. The OR approach can be used to lower FRR or to cater also for those travellers who cannot use a specific biometric modality (for instance if their fingerprints cannot be acquired or compared). More complex fusion functions might result in better performance values than AND and OR.

NOTE When designing the ABC system note that capturing multiple biometric modalities can add more time to the verification process and could raise acceptance issues.

5.1.3.6 Error rates reduction

Due to the nature of ABC systems, error rates can be classified into three different categories:

- technical errors,
- operational errors due to traveller behaviour,
- operational errors derived from system characteristics.

The proper nature of every error should be identified and valuable and anonymous operational information should be stored in the system (complying with the limitations imposed by national and European Data Protection regulations), not only for testing and corrective maintenance purposes, but also for quality control and statistical analysis.

Some examples of technical errors are:

- false acceptance and false rejection rates inherent to the biometric algorithms,
- electrical or mechanical failure,
- bad quality samples due to dirt or environmental issues,
- interoperability issues caused by the acquired data (i.e. wrong image format, record header standard compliance, physical or logical data mismatch for the same kind of travel document, etc).

Error rates due to technical errors can be easily identified by means of a proper system logging. It is recommended that such information is logged at local level, as it is unlikely to be useful for operational analysis.

Operational errors attributable to traveller behaviour are difficult to isolate within the operationally logged data, as the consequent errors are not easily distinguishable from those related to technical reasons (i.e. placing a wrong finger in the sensor and a bad quality acquisition will result in a false rejection error). Generally, the recommendations in 5.1.1 on usability and accessibility should be considered to avoid operational errors. Some operational errors that fall into this category are:

- placing a wrong finger during fingerprint acquisition;
- standing in front of the camera in a non-frontal pose of the face;

- wearing non allowed objects, like sunglasses or hats;
- removing the ePassport before the reference data acquisition process is complete;
- moving finger or face during capturing process, so that no image could be captured with sufficient image quality.

Traveller’s operational errors can be minimized by optimization of the biometric acquisition process. Instead of using a single image for the facial verification process, a series of images can be used. Therefore, the comparison score calculated over the sequence will improve the facial verification result, as more than one single image is likely to match the reference data. The system can give guidance if it is able to recognize traveller behaviour leading to operational errors.

The operational errors inherent to the system characteristics are normally related to ergonomics and can be minimized by usable and ergonomic system design as recommended in 5.1.1. Reasons for such errors can be, e.g.:

- inappropriate placement of the fingerprint scanners;
- inappropriate placement of the user interface screen;
- lack of digital mirror or other guidance.

5.1.3.7 Spoof prevention

Spoofing is a risk for any biometric system including ABC systems.

ABC systems should integrate countermeasures such as artefact detection and liveness detection to prevent spoofing according to a risk analysis.

The use of multimodal biometrics can lower the risk, due to the fact that a spoofing attack highly depends on the type of biometric. Multimodal biometrics requires an appropriate fusion function (see 5.1.3.5), the benefit of using multimodal biometrics shall be evaluated for the specific use case.

The performance of the spoof detection mechanism should be analysed with a repeatable test set to establish an appropriate operating point of the system. Any method used for automated spoof detection needs to be reliable to avoid higher false rejection rates of the overall biometric system.

Spoof prevention measures should be taken based on the results of a risk analysis process. For any deployed system, there will be different threats that are relevant or not relevant to that particular system.

Spoof prevention can be based on, e.g.:

- operator supervision;
- dedicated sensors;
- software-based mechanisms.

The project ISO/IEC WD 30107 [17] gives a useful overview of methods and techniques available.

5.1.3.8 Face

A common technique to spoof face recognition systems is to display printed photographs of a spoofed identity to the face capture device. In connection with travel documents one of the easiest attacks could be to present the data page of the eMRTD with the printed face image to the capture device. Two of the possible options to address this threat are the following:

- The capture system can exclude images captured from small objects like printed facial images in MRTD from the further processing. So an attacker is forced to use a face size printed image on a separate sheet. This can be detected much easier by the monitoring officer.

- The robustness of facial recognition can be improved by technologies using additional information, e.g. 3D acquisition/recognition data, illumination data from different spectral ranges, video sequence analysis data, etc. These technologies can detect any changes or inconsistencies in the presented face distinguishing it from printed facial images, or in the position of the head.

Other technologies could use additional information, for example: blinking detection (in video sequences) or pupil detection (in IR images).

5.1.3.9 Fingerprint

A common technique to spoof fingerprint recognition systems is to apply artefacts or non-living biometrics, e.g. paper prints, gelatine or wood glue covered fingers or fake digits on the fingerprint capturing device. These artefacts are hard to discover by operational means.

Fingerprint fake and spoof detection can be based on various features extracted with hard- and/or software during the capturing process and/or in the image analysis phase after the signal capturing.

Countermeasures can be based on passive and active characteristics of fingerprints.

- One possible option to address the use of finger spoofs is the deployment of four finger scanners. To lower the risk of a successful spoofing attack, as much biometric information as possible should be presented, to mitigate the natural variance of fingerprints.

- Four finger scanners could be able to detect a spoof by comparing the skin condition and the general ridge pattern properties of all four or of several captured fingerprint images. Attempting a four finger spoof requires more information.

- Blood flow analysis could be used to determine the changing presence of oxygenized and de-oxygenized blood in the presented finger. Alternatively, periodic micro-pulsations of the finger could be measured.

- The skin conditions of the captured fingers could be analysed. The fingers should be equally wet, have an appropriate size, and the fingertips should be located appropriately. In case DG3 doesn’t contain index finger prints, it could be examined if the quality of the index finger prints is really suboptimal.

- Ridge pattern properties of the fingers could also be analysed. Ridge distance, ridge thickness, pore distance (if visible) could be examined and should be similar for all fingers of the same person.

NOTE This technique can be performed with multiple fingerprint scanners. Single fingerprint scanners can also work, at the cost of additional capture time.

Any type of sensor should have liveness and spoof detection capabilities.

There are vendor comparisons (like LivDET [Marcialis et al. “First International Fingerprint Liveness Detection Competition—LivDet 2009”] and LivDET II [Yambai et al. “LivDet 2011 — Fingerprint liveness detection competition 2011”]) and a Common Criteria certification for fingerprint liveliness detection is under development [18].

If a spoof is detected, an alarm is sent to the operator of the ABC system. No information is provided to the user.

5.1.3.10 Iris

A typical spoof for iris recognition systems is the use of contact lenses with iris images of another person.

Countermeasures can be based on passive and active characteristics of irises, e.g.:

- eye blinking or 3D information to prevent photo presentation;
- high resolution images and frequency analysis, e.g. by Fourier transforms to detect evidence of printer traces.

5.1.4 Logging, data protection and privacy

Any set of operational data to be stored on a permanent basis in an ABC system should comply with the limitations imposed by national and European Data Protection regulations. Therefore personal data should not be stored for the purposes of quality control and statistics extraction unless properly anonymized.

Any information should be stored within a structured data schema (e.g. a relational database, XML entries).

It is recommended that anonymous operational data are stored in a centralised way at least at the ABC installation level (i.e. at the group of gates and monitoring stations at a given airport/port hall). Detailed maintenance and software debug traces may be stored at the local level, since such data are unlikely to be of use when analysing operational performance. It is recommended that a clear interface for data extraction is defined.

An entry in the operational register should be created for any transaction taking place in an ABC system, regardless of its degree of success. Thus, apart from data from successful border crossings, anonymous data for at least the following types of transactions should be logged:

- access attempts with documents not accepted by the system (e.g. non electronic passports, not a passport, passport not opened, wrong page presented).
- access attempts with non-eligible documents (e.g. underage Schengen citizens holding an ePassport, third country nationals holding an ePassport).
- access attempts by an eligible traveller, with a valid ePassport but whose verification was not successful (for example due to a biometric verification error).

It is recommended that each entry within the operational register is as complete as possible, depending on how far the verification process could be completed. If a field of the transaction entry cannot be filled at the moment (e.g. the nationality is unknown or a check is not applicable for a certain document), a distinctive value should be used as placeholder, so that these gaps can be easily identified when processing the data.

5.2 Recommendations for face biometrics

5.2.1 Condition for good quality sample acquisition

The process design should guide the traveller to look straight into the camera. If the camera and the flow of the traveller form an angle greater than 45°, it is likely to slow down flow. While the live face images are captured other actions by the traveller should not be necessary and no eye-catchers apart from the camera or feedback modules should draw off the traveller’s attention. The feedback modules (display, LEDs, etc.) should be installed as close as possible to the camera, so the traveller looks to the display and can see guidance simultaneously to improve face position.

The depth of the view field depends on the setup (mantrap, single gate or kiosk); it is recommended that it is adjusted to the area where the travellers face is typically located. A frame rate of at least 10 frames per second is recommended. The parameters of the camera should ensure the provision of face images within a broad range of contrasts. The face images provided by the capture unit should have at least 90 pixels between the centres of the eyes (see [9]).

The face capture unit should be able to capture frontal images of persons of a height between 140 and 200 cm. Depending on the usage scenario (e.g. an eGate for use with a wheelchair) other ranges can be appropriate. Possible technical solutions include:

- a moving camera,
- a pan-tilt camera,
- a movable mirror (1- and 2-axes),
- a single wide angle camera,
- several cameras at different heights.

The unit may automatically adjust in order to capture proper images for the biometric comparison. The time period required for this adjustment (e.g. height adjustment by movement of the camera) should be minimized in order to avoid delays within the face capture process.

The face capture unit should give feedback on the expected action to the traveller, e.g. by an integrated display. It is recommended to show the live stream that is currently captured (digital mirror) and to give an indication if the image is good enough to be used by the face verification unit. If the feedback is realized as a digital mirror, it is recommendable to move it with the camera (if a movable camera unit is used). The feedback should not interfere with the face capture process.

The traveller should be able to provide his data without additional effort. In particular, capturing systems should be able to address travellers wearing transparent eyeglasses without requiring them to remove the glasses.

It is recommended to perform a quality assessment on the captured images for providing good quality images to the verification process if the quality driven approach architecture is applied. The quality assessment should cover at least face and eye finding. ISO/IEC 19794-5 [9] gives guidelines for image quality analysis. Additionally, quality assessment might be useful for test and evaluation purposes as suggested in ISO 12233 [3].

It is recommended to provide uncompressed or lossless compressed live images.

In any other case it should be ensured that the loss of information has no significant impact on the recognition performance of the face verification unit.

Additionally the following should be considered:

- The designated acquisition area should be appropriately illuminated.
- The face tracking (from entrance of the ABC system) for the fast capturing can be applied.
- The capturing devices with higher resolution for facial image capture that reduces the need for zoom lenses should be considered.

5.2.2 Biometric verification and process design

For live operation of the system, it is recommended to determine a proper algorithm configuration based on image data and verification results (cross-comparisons between different travellers) from the actual operational environment and a representative catalogue of test users and not to rely only on the standard configuration of the algorithm provider. It is recommended to monitor the error rates (especially the FAR) continuously or at least periodically (e.g. once a year) and to adjust the configuration if needed.

Biometric performance should be measured with following criteria: false acceptance rate (FAR), false rejection rate (FRR), and time until first hit (Th). It is recommended to keep the FAR under 0,001 (0,1 %). At a configuration of FAR = 0,1 %, the FRR should be lower than 0,05 (5 %) [30] and Th under 30 s.

NOTE The FRR is linked to the FAR and also depends n external conditions and the quality of biometric reference data.

The verification process may run locally within each ABC system or as a centralized service.

The verification unit should process DG2 reference images which may be stored in data formats JPG and JPG2000. It should process live images and crop images in uncompressed or lossless compressed data formats.

To analyse the performance of biometric subsystem in ABC, it is useful to check the reference data obtained from electronic documents or from the database. The quality check of those data helps identify the weak points of the biometric subsystem.

If the face image acquisition and/or the biometric verification are not successful the process should stop after a time-out. This time-out should be configurable. The system should acquire facial images as soon as the person enters the acquisition area and start the comparison process in parallel, as soon as the document authentication is successful and the reference image is available.

Generally, the passage through a facial recognition based ABC system should not take more than 30 s from the moment the passport is placed on the reader until the traveller exits ABC system.

It is recommended to include a subsystem for the logging of statistical and technical data regarding the biometric verification process, for the purpose of having a continuous quality control, extraction of business statistics and improvements of the ABC. It is recommended that the following details of the facial verification process are part of a data entry:

- overall result of the face capture and verification process;
- error messages from the face capture unit and the verification unit;
- time effort for the biometric verification process from the beginning of image capturing until the provision of the final verification result;
- delays resulting from the traveller's behaviour, i.e. the time effort from starting the capture process until the first successfully captured image are provided to the verification unit;
- amount of single verification events within the verification process;
- at least the best comparison score of all single verification events within the face capture and verification process;
- the best quality score of all successfully captured facial templates;
- the threshold the verification scores were compared with.

5.2.3 Security

As required in ICAO Doc 9303 [27] the facial image printed on the data page should be the same as stored in DG2. This information can also be taken into account when the image taken from the printed data page and DG2 are compared.

The comparison scores achieved by comparing the data page image with DG2 and the live image will depend on the used comparison algorithm, the issuer and the series of the document. However, it is recommended to display the live image, the DG2 image as well as the data page image to the supervising officer. Whenever the automated process fails and a manual control takes place, the cropped image and the DG2 image should be handed over and displayed close together to the officer performing the manual checks.

Images scanned from passport data page (visual inspection zone) typically will have a low resolution and are influenced by layout and security features (e.g. holograms). These images might be less suited for comparison with live captured images. It is recommended to use the stored facial image from the passport chip (DG2) for any biometric comparison purposes.

5.2.4 Usability and environment

The face capturing unit should contain illumination modules to ensure a proper illumination of the face region. The lighting should not cause reflections on glasses or the skin of the face. The lighting should be switched on during the complete capture process and brightness may be varied to get best contrast and illumination. The light source may be used permanently or be switched off in times where no face images are captured. Sunlight will vary both on a daily and on a seasonal basis. It is recommended to test that the system will perform adequately under different sunlight conditions. It is recommended that direct sunlight is avoided, and environmental illumination should be controlled for best capture results.

In cases where it is not possible to avoid a strong backlight e.g. if there are large windows with direct sunlight located behind the ABC in the camera’s field of view, it is optional for the cameras with standard sensitivity (approximately 60dB) to turn off the automatic image balancing on the global scene and switch to alternative camera control. Such camera control can include two modes:

- Mode 1, no facial image detected: Continuously varying (oscillating) camera settings (exposure/gain), in effect continuously offsetting the global image balance levels in order to potentially achieve proper balance levels in the region of the image with a human face.

- Mode 2, facial image detected: the camera performs image balancing based on the facial region only and performs continuous face tracking. If the facial region cannot be detected after a certain period, the camera control switches back to Mode 1.

The recommended setting should be tested under different lighting conditions during the system design phase.

5.3 Recommendations for fingerprint biometrics

5.3.1 Condition for good quality sample acquisition

Only sensors certified to be compliant to ISO/IEC 19794-4:2011, B.1 or B.3 [8] should be deployed. Additionally, sensors certified according to EBTS/F [25] and BSI TR-03121 [19] might also be used.

It is recommended that the sensor device provides methods for re-calibration in the field or at least calibration tests to be performed by qualified service staff unless the device technology does not need such maintenance function.

For a better image quality sensors should provide a raw resolution of 500 DPI. The scan area should be large enough to capture full plain fingerprint images.

It is recommended that the compliance of a sensor device to the applicable quality standard can be verified at any time in the operational environment.

NOTE The need for calibration or re-calibration depends on the sensor technology and calibration might not be necessary for all devices.

It could be problematic to acquire a good quality image from certain fingers, due to their skin conditions. A wet finger can produce a too dark fingerprint scan where the valleys and ridges are not sufficiently distinguishable, whereas the image from a too dry finger can be too light and lack enough contrast. It is recommended that the sensors provide image enhancement mechanisms in order to minimize adverse effects of skin condition during the acquisition process.

It is recommended to clean the sensors periodically. It is necessary to carefully follow the manufacturer’s instructions in order to avoid damaging the sensor, which will negatively affect the system performance.

5.3.2 Biometric verification and process design

The fingerprint verification consists of comparing a pre-enrolled fingerprint template or image with a live scanned image of a traveller. Therefore the fingerprint information from DG3 should be read and transmitted to the verification process.

An extraction of fingerprint features (templates) could be necessary because passports store images to avoid conflicts with vendor specific feature extraction algorithms.

The verification process itself compares two templates and calculates a score (so called comparison score). A threshold should be configurable to decide which score is accepted and which is declined for further border processing.

The system performance depends on several processing steps:

- manual interaction with the system (entrance into the ABC suite/kiosk/gate, reading display information/guidance on the screen);

- manual interaction with the document reading system (placing the document on reader, wait for reading/analysis of data);

- interaction with the biometric scanners (placing hand/finger on scanner, wait for capturing);

- wait for biometric process (wait for fingerprint analysis, quality analysis, encoding and template verification with former read out template/image from document);

- react on result (if verification true, go through gate/finish procedure, if verification false – repeat steps or wait for staff members).

Biometric performance should be measured with following criteria: false acceptance rate (FAR) and false rejection rate (FRR). It is recommended to keep the FAR under 0,001 (0,1 %). At a configuration of FAR = 0,1 %, the FRR should be lower than 0,03 (3 %) [30].

NOTE The FRR is linked to the FAR and also depends on external conditions and the quality of biometric reference data.

5.3.3 Usability and environment

The fingerprint scanner should be ergonomically positioned so that the traveller can easily place any finger of each hand on the scanner. Therefore angle and height of the sensor position should be considered. A mobile fingerprint scanner for persons with disabilities may be useful.

System usability highly depends on cooperation with the traveller – so acceptance and confidence in the system will highly increase the reliability of the process. Especially the FRR will highly influence the usability of the whole system. Travellers would not accept a system with many false alarms.

For correct fingerprint scanning the illumination should not be directed to the glass. Exposure of the housing of the optics to direct sunlight should be avoided.

Normally, one fingerprint from each hand will be available as the reference image or template inside the travel document chip. The system should read first the available reference fingerprints from the chip and display the requested finger for live capture. The system can prioritize the first requested fingerprint following either ergonomics or technical considerations:

- For the most travellers right hand fingers can be placed on the sensor more easily than left hand fingers.
- Index fingers can be placed on the sensor more easily than thumbs.
- Comparison-on-card systems can limit the number of comparison attempts, so it is recommended that the system selects first the fingerprint with more attempts available in order to avoid locking the chip.
- It is recommended that the system assesses the quality of the available reference images and select the higher quality sample first in order to minimize the FRR.

The decision on ergonomic aspects should be balanced with the requested security targets of the system.

When there is a significant difference between the finger and the sensor surface temperatures (i.e. in a cold environment), undesired artefacts could arise during the acquisition process, in the form of a halo around the finger. Skin dryness can also be an issue (see 5.3.1 on Condition for good quality sample acquisition), especially after intercontinental flights. It is recommended that the sensor includes mechanisms to avoid these situations, like platen heater or software halo removal.

5.4 Recommendations for iris biometrics

5.4.1 Condition for good quality sample acquisition

The image quality delivered by any deployed sensor should comply with the quality specifications from ISO/IEC 19794-6 [10].

It is recommended to use anti-spoofing techniques such as artefact detection and liveness detection to prevent spoofing according to a risk analysis.

The process design should guide the traveller to look straight into the camera. If the camera and the flow of the traveller form an angle greater than 45°, it is likely to slow down the flow.

While the iris images are captured other actions by the traveller should not be necessary and no eye-catchers apart from the camera or feedback modules should exist that might catch the traveller’s attention. The feedback modules (display, LEDs etc.) should be installed as close as possible to the camera.

The iris images provided should have at least a definition of 10 pixels per millimetre with horizontal margin of at least 60 % of iris radius and vertical margin of at least 20 % of iris radius (see [10]).

The iris capturing unit should be able to capture iris images of persons of a height between 140 and 200 cm. Depending on the usage scenario (e.g. an eGate for use with a wheelchair) other ranges can be appropriate.

Possible technical solutions include:

- a moving camera,
- a pan-tilt camera,
- a movable mirror (1- and 2-axes),
- a single wide angle camera,
- several cameras at different heights.

The acquisition process should allow a positioning margin of at least 40 cm in depth and width as a minimum range for good usability to avoid a wrong positioning of the user.

The distance of acquisition should be centred around 1 m (between 80 cm and 1,2 m according the previous point) in order to support integration into eGates.

The unit may automatically adjust the capture range and position in order to capture proper images for the biometric comparison. The time period required for this adjustment (e.g. height adjustment by movement of the camera) should be minimized in order to avoid needless delays within the iris capture process.

The traveller should remove patterned/opaque contact lenses at all times. It should not be necessary to remove transparent eyeglasses.

It is recommended to perform a quality assessment on the captured images to provide good quality images to the verification process if the quality driven approach architecture is applied.

The quality assessment should at least give a global quality score (an example is given in IREX II [31]).

Others useful metrics relevant for the traveller to improve acquisition could possibly include (see [31]):

- occlusion score,
- off-axis score,
- blur score,
- patterned/opaque contact lenses detection score.

It is recommended to show the live stream that is currently captured (digital mirror) and to give an indication if the image is good enough to be used by the iris verification unit. If the feedback is realized as a digital mirror, it is recommended to move it with the camera (if a movable camera unit is used).

5.4.2 Biometric verification and process design

For live operation of the system, it is recommended to determine a proper algorithm configuration based on image data and verification results (cross-comparisons between different travellers) from the actual operational environment and a representative catalogue of test users and not to rely only on the standard configuration of the algorithm provider.

A given matching threshold should always result in the same FAR, regardless of the evolution of the size of the database for one-to-many comparison (see IREX III [32]).

It is recommended to monitor the error rates (especially the FAR) continuously or at least periodically (e.g. once a year) and to adjust the configuration if needed.

It is recommended to include a subsystem for the logging of statistical and technical data regarding the biometric verification process, for the purpose of having a continuous quality control, extraction of business statistics and improvements of the ABC.

It is recommended that the following details of the iris verification process are part of such a data entry:

- overall result of the iris capture and verification process;
- error messages from the iris capture unit and the verification unit;
- time effort for the biometric verification process from the beginning of image capturing until the provision of the final verification result;

- delays resulting from the traveller's behaviour, i.e. the time effort from starting the capture process until the first successfully captured image are provided to the verification unit;

- amount of single verification events within the verification process;

- at least the best comparison score of all single verification events within the iris capture and verification process;

- best quality score of all successfully captured iris templates;

- occlusion score in order to detect possible illumination problem, and others metrics such as blur or off-axis;

- the threshold the verification scores were compared with.

Biometric performance should be measured with following criteria: false acceptance rate (FAR), false rejection rate (FRR). It is recommended to keep the FAR under 0,0001 (0,01 %). At a configuration of FAR = 0,01 %, the FRR should be lower than 0,01 (1 %).

NOTE The FRR is linked to the FAR and also depends on external conditions and the quality of biometric reference data.

The verification unit should process reference images which may be stored in data formats PNG or JPG2000, preferably uncompressed or lossless compressed.

If storage size below 100 kb is needed, cropped or cropped_and_masked format with lossless compression should be used (see [10]).

To analyse the performance of biometric subsystem within an ABC, it is useful to check the reference data obtained from electronic documents or from the database. The quality check of this data will help to identify the weak points of the biometric subsystem.

5.4.3 Security

The capture unit should capture 2 irises at the same time, and for optimum throughput, one attempt of acquisition should take less than 3 s.

As the False Reject Rate might be increased by a factor of at least 2 or 3 if only one eye is available (see [32]), two eyes acquisition should be attained as often as possible. If an acquisition returns only one eye with sufficient quality, a new acquisition should be tried while the comparison of the first acquisition process is started in parallel. Both eyes can be captured at the same time, to improve timing and traveller usability.

5.4.4 Usability and environment

The iris camera should be the dominant source of illumination. No other illumination should be directed to the traveller, either sun or artificial illumination.

The illumination should be adequately strong enough to avoid big pupil/iris ratios which could impact the FRR. Dim ambient light will cause the pupil to dilate while excessive lighting will cause the pupil to constrict.

The traveller should face a featureless scene:

- iris capture should not take place in front of windows,

- camera should not be directed to sunlight,

- the traveller should not be facing a mirror.

Sunlight will vary both on a daily and on a seasonal basis. It is recommended to test that the system will perform adequately under different sunlight conditions.

The iris capture unit should give feedback of the expected action to the traveller by an integrated display. The feedback should not interfere with the iris capture process.

Such feedback messages could be:

- move closer or back,
- open eyes wider,
- remove glasses,
- remove patterned/opaque contact lenses,
- look straight (in order to avoid off-axis acquisition).

Annex A
(informative)

Testing examples — Facial Images

For systems based on facial images it is recommended to perform the FAR calculation of the ABC system as an independent but parallel process as follows:

- The reference face templates (DG2 templates) of the last 10 passport verifications are temporarily and anonymously stored in a dynamic list.
- The live face template from the actual face verification process is compared against all other faces in the dynamic list and the comparison scores are saved (impostor comparisons). It shall be ensured that during the process a comparison of face templates of the same person is avoided, which might happen due to multiple verification attempts of the same person.
- The actual live face template is compared against the corresponding reference face template and the comparison score is saved (genuine comparison).
- The reference face template is added to the dynamic list.
- The oldest face template in the dynamic list and the actual live face template are discarded and deleted safely. Storage and deletion of the face template data shall be implemented in accordance to the applicable data protection regulations.
- Calculate the FAR based on the impostor comparison scores. Genuine comparison scores may be used to calculate the corresponding FRR. Care shall be taken about the statistical base for the FAR calculation. In order to measure the performance of the face verification algorithm up to a security level (FAR) of 0.001 (0.1 %), it is recommended to perform the FAR calculation on the basis of at least 30.000 impostor comparisons.

Annex B
(informative)

Example process for multi-camera systems for 3D face recognition

With a multi-cameras system, a variety of information is available to estimate the face shape and texture in 3D.

For illustration purposes, an example of the acquisition process with a multi-camera system is presented in Figure 2. To accelerate the whole process of authentication, no specific interaction of the user is mandatory. During its move through the gate, the face of the user and its landmarks are detected and tracked. The parameters of the 3D model (e.g. pose, shape parameters, texture) are estimated and consolidated during the whole acquisition.

At each timestamp, new observations are available and feed the estimation; new views can then be generated, in particular a frontal view even in a non-cooperative scenario. Views acquired by the systems or frontal views generated from the 3D estimations are coded and compared with a given database (identification scenario) or with photographs stored in the travel documents (authentication scenario).

This process is illustrated in Figure 2.

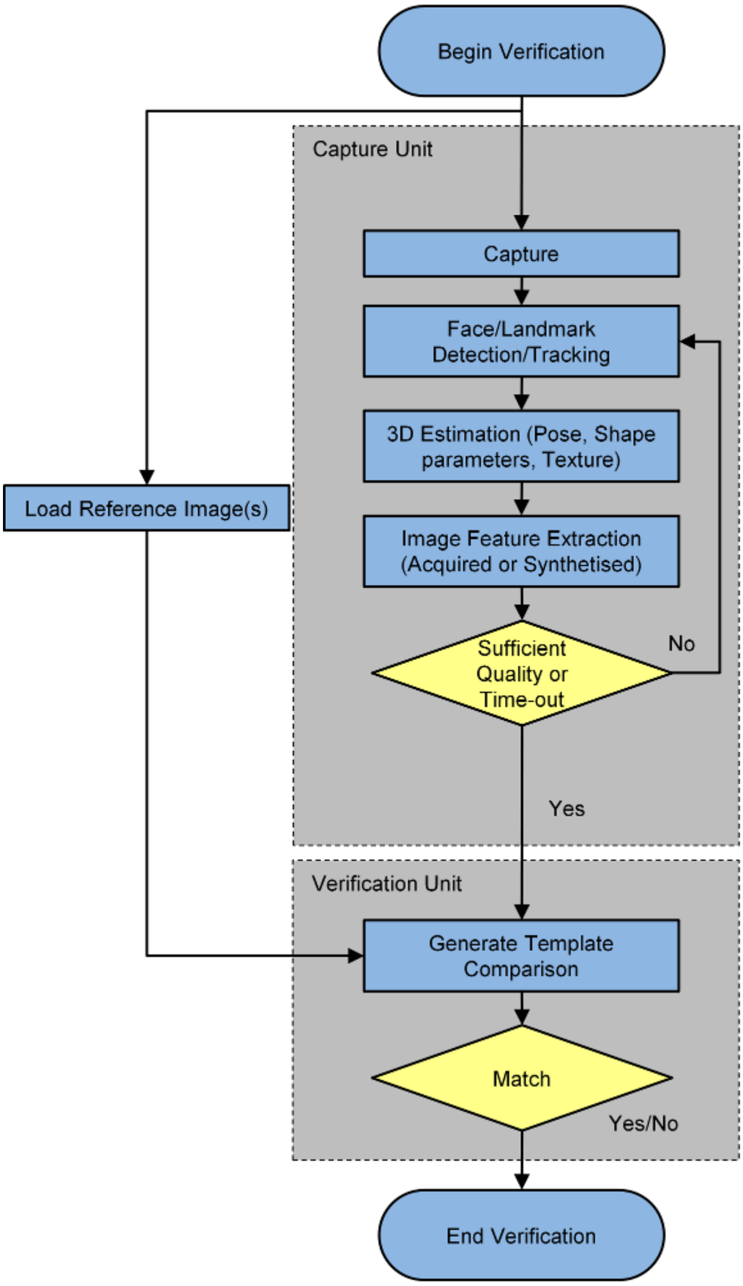

Begin Verification
Capture Unit
Capture
Face/Landmark Detection/Tracking
3D Estimation (Pose, Shape parameters, Texture)
Image Feature Extraction (Acquired or Synthetised)
Sufficient Quality or Time-out
No
Yes
Load Reference Image(s)
Verification Unit
Generate Template Comparison
Match
Yes/No
End Verification

Figure 2 — Framework 3D facial acquisition system

Bibliography

[1] EN 1332 (all parts), *Identification card systems — Man-machine interface*

[2] CEN/TS 15480 (all parts), *Identification card systems — European Citizen Card*

[3] ISO 12233, *Photography — Electronic still picture imaging — Resolution and spatial frequency responses*

[4] ISO/IEC 2382-37:2012, *Information technology — Vocabulary — Part 37: Biometrics*

[5] ISO/IEC 9241 (all parts), *Ergonomics of human-system interaction*

[6] ISO/IEC 14443, *Identification cards — Contactless integrated circuit cards — Proximity cards*

[7] ISO/IEC 19784-1:2006, *Information technology — Biometric application programming interface — Part 1: BioAPI specification*

[8] ISO/IEC 19794-4:2011, *Information technology — Biometric data interchange formats — Part 4: Finger image data*

[9] ISO/IEC 19794-5:2011, *Information technology — Biometric data interchange formats — Part 5: Face image data*

[10] ISO/IEC 19794-6, *Information technology — Biometric data interchange formats — Part 6: Iris image data*

[11] ISO/IEC 19795-1:2006, *Information technology — Biometric performance testing and reporting — Part 1: Principles and framework*

[12] ISO/IEC 19795-2, *Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation*

[13] ISO/IEC 19795-6, *Information technology — Biometric performance testing and reporting — Part 6: Testing methodologies*

[14] ISO/IEC TR 24714-1, *Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance*

[15] ISO/IEC/TR 24722, *Information technology — Biometrics — Multimodal and other multibiometric fusion*

[16] ISO/IEC 24779 (all parts) (under development), *Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems*

[17] ISO/IEC WD 30107 (under development), *Information Technology — Biometrics — Presentation attack detection*

[18] ISO/IEC 30127 *(currently at drafting stage), Information technology — Security techniques — Detailing software penetration testing under ISO/IEC 15408 and ISO/IEC 18045 vulnerability analysis*

[19] BSI TR-03121, *Technical Guideline Biometrics for Public Sector Applications*

[20] Face Symbol - Report on the design, development and testing of 11 instructional symbols for use with biometric, facial recognition, identity systems, BSI UK

[21] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States

[22] Council of Europe, Commissioner for Human Rights. Protecting the right to privacy in the fight against terrorism

[23] Communication From The Commission to the European Parliament and the Council, "Smart borders - options and the way ahead", COM(2011) 680 final, 25.10.2011

[24] European Union: Regulation (EC) No. 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 105, 13 April 2006, pp. 1–32 (consolidated version of April 2010)

[25] EBTS V 8.002 Appendix F http://www.fbibiospecs.org/fbibiometric/docs/EBTS%20V8.002%2004-01-08-final.pdf

[26] Grant Agreement BC/CEN/ENTR/000/2007-23 – Final Version of the conformance/interoperability report – 2009-06-11

[27] ICAO. 9303 Machine Readable Travel Documents, multiple documents, International Civil Aviation Organization, http://www.icao.int/Security/mrtd/Pages/Document9303.aspx

[28] ICAO TAG/MRTD. Guidelines on electronic - Machine Readable Travel Documents & Passenger Facilitation. Version 1.0. April 17, 2008. http://www.icao.int/Security/mrtd/Downloads/GuidanceMaterial/MachineReadableTravelDocuments-PassengerFacilitation.pdf

[29] FRONTEX. http://www.frontex.europa.eu

[30] FRONTEX. Best Practice Operational Guidelines for Automated Border Control (ABC) Systems & Best Practice Technical Guidelines for Automated Border Control (ABC) Systems. Version 2.0. Warsaw, August 2012

[31] IREX II Iris Quality Calibration and Evaluation - NIST report 2011 http://www.nist.gov/itl/iad/ig/irexii.cfm

[32] IREX III Iris - NIST report 2012 http://www.nist.gov/itl/iad/ig/irexiii.cfm

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™