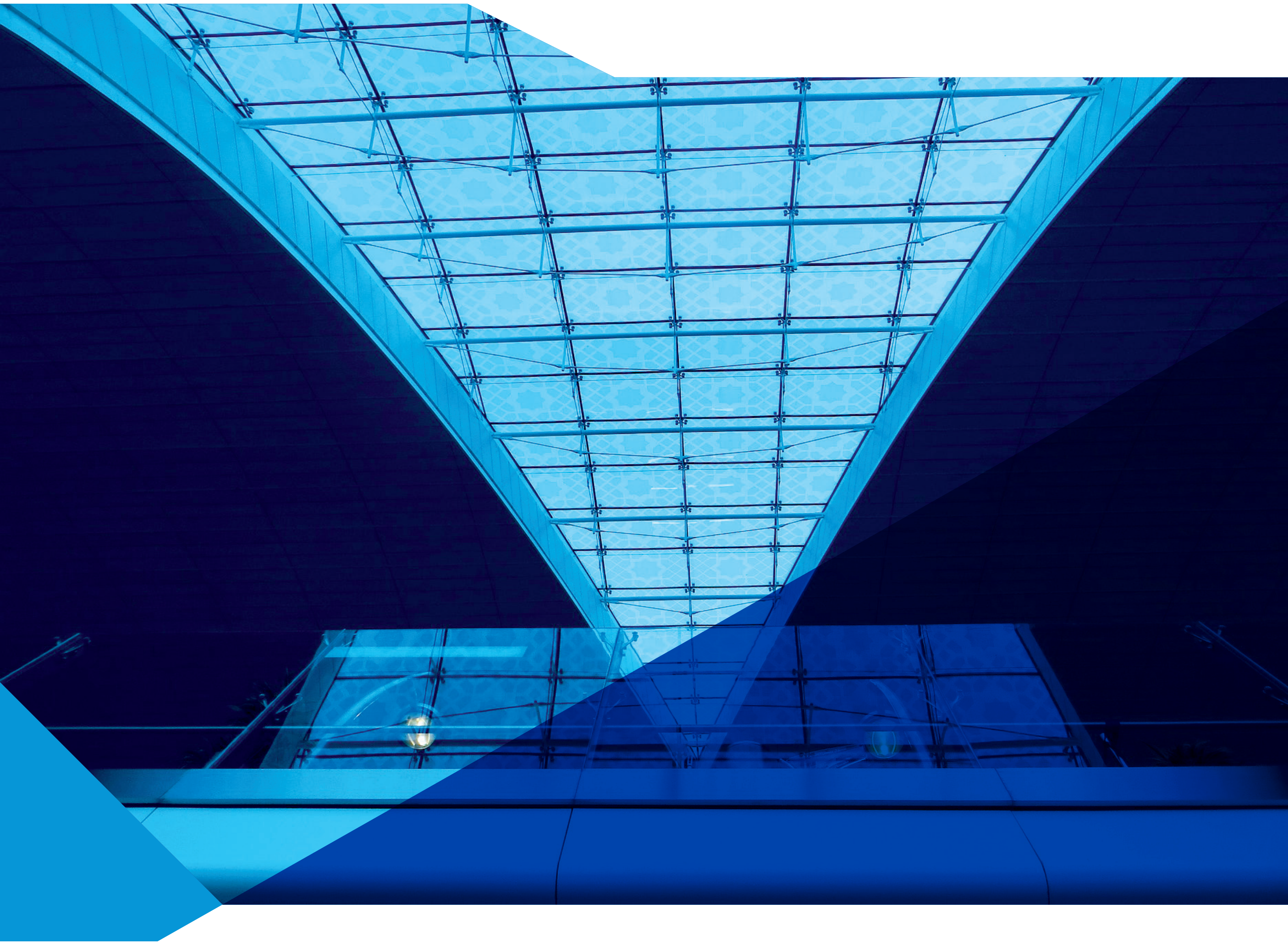
FRONTEX



Best Practice Technical Guidelines for Automated Border Control (ABC) Systems

FRONTEX

Best Practice Technical Guidelines for Automated Border Control (ABC) Systems

Research and Development Unit

FRONTEX

European Agency for the Management
of Operational Cooperation at the External Borders
of the Member States of the European Union

Research and Development Unit
Capacity Building Division

Plac Europejski 6
00-844 Warsaw, Poland

T +48 22 205 95 00
F +48 22 205 95 01

frontex@frontex.europa.eu
www.frontex.europa.eu

Print version:
TT-02-16-152-EN-C
ISBN 978-92-95205-51-2
DOI 10.2819/86138

Online version:
TT-02-16-152-EN-N
ISBN 978-92-95205-50-5
DOI 10.2819/39041

Date: September 2015

Contents

Release Note and Table of Changes

This report supersedes the previous version of the Best Practice Technical Guidelines for Automated Border Control (ABC) systems. The main changes are summarised in the table below.

Table of changes

Section altered	Change
Acknowledgements	Names of experts, stakeholders and Frontex staff who contributed to the revision updated accordingly
About Frontex	Changes made in the title of this section as well as in the sentence about the core objective of the Capacity Building Division
Preamble	Removed
Glossary	Introduction of terms and definitions
Executive Summary	Updated according to the text
Section 1.1.	Introduction of clarification regarding the purpose of the guidelines
Section 1.2.	Introduction of a reference to the Smart Border Package, introduction updates regarding the biometrics used and types of border crossing points, as well as introduction of updates regarding the methodology
Section 1.3.	Introduction of clarifications and updates regarding the definition of best practices
Section 4.3.	Changes to Figure 1; introduction of PACE and of the sequence for reading data groups
Section 4.4.4.	Introduction of clarification regarding the DS certificate revocation status
Section 4.4.5.	Introduction of clarifications regarding EF.SOD and EF.COM
Section 4.4.7.	Introduction of a remark regarding non-ICAO-compliant use of optional MRZ data
Sections 4.6.1.1. and 4.6.1.2.	Introduction of updates and clarifications regarding national ID cards; additional section 4.6.1.3 added highlighting the main differences between e-Passport, German ID and Spanish ID card
Chapter 6	Changes made in the title of the section and introduction of clarifications regarding quality control and quality assurance
Section 6.5.	Some text removed as regards collection of biometric verification data
Annexes 1 and 2	Update of the references
Annex 3	Introduction of updates regarding the operational and planned ABC systems in the EU

Legal notice

All rights reserved

Before citing the Frontex Best Practice Technical Guidelines for Automated Border Control (ABC) Systems, the following procedure should be observed.

1. Please contact the Frontex Research and Development Unit in order to get the latest version of the guidelines and support for using them in your document.

In the introductory part of the document.

2. Include a brief text declaring that Frontex ABC guidelines have been used in the document. Mention explicitly which sections in the document are (totally or partially) based on these.
3. Explain briefly why Frontex ABC guidelines have been used in the document, and in case of total or partial use of particular sections, explicitly state why these sections are copied in full and what the added value is. Provide some background about how using Frontex guidelines best serves the purposes of the document.
4. Briefly mention that Frontex guidelines are the result of a collaborative effort among EU Member States (coordinated by Frontex) who at the time of writing have an operational or piloting ABC system in place.

In the body of the document.

5. In those parts of the document based on Frontex guidelines, make a reference to the Frontex document (see references below).

In the references section.

6. Include a proper reference to the Frontex ABC guidelines document (title, version and issuing date, ISBN reference, plus a download link to the Frontex web page hosting the latest version).
7 Include Frontex Research and Development Unit contact data at the end of the document.

Frontex RDU contact data:

Research and Development Unit
Capacity Building Division
Frontex
Plac Europejski 6, 00-844 Warsaw, Poland
E-mail: rd@frontex.europa.eu
Tel. +48 22 205 96 25
Fax +48 22 205 95 01

Acknowledgements[1]

This report was prepared by the Research and Development Unit (RDU) of Frontex in close collaboration with experts from a number of EU Member States which, at the time of writing, were operating or testing an ABC system at selected border crossing points of the European Union. Frontex would like to particularly acknowledge the work of Markus Nuppeney, Head of Section and Florian Rienhardt, Technical Officer at the Federal Office of Information Security (BSI) who took the lead in revising these guidelines. Frontex would also like to thank the following persons who participated in the Working Group on Automated Border Controls and contributed to this report.

- Bulgaria: Lyubomir Dilov and Aleksandr Kamburov (Border Police).
- Czech Republic: Mylan Frydrych and Petr Malovec (Border Police).
- France: Dominique Gatinet (French Secure Documents Agency), Eric Clement Pierre Alexander Gelas and Laurent Mucchielli (Border Police).
- Finland: Max Janzon, Janne Kurvinen, Pasi Nokelainen, Alapelto Pentti and MIkko Väisänen (Finnish Border Guard).
- Germany: Markus Nuppeney, Florian Rienhardt (Federal Office for Information Security) and Maik Rudolf (Federal Police).
- Ireland: Kevin Ryan (Irish Naturalisation and Immigration Service).
- Netherlands: Yvonne Bakker, Kier-co Gerritsen, Joost van Aalst (Ministry of Justice), Rijck van de Kuil and Hans De Moel (Royal Netherlands Marechaussee).
- Portugal: Paula Maria Azevedo Cristina and Maria Conceição Bértolo (Immigration and Border Service).
- Spain: Javier Núñez Alonso, Ángel L. Puebla and Alberto Raez Liria (Spanish National Police).
- United Kingdom: Andrew Clayton, Daniel Soutar and Glen Wimbury (UK Border Agency).

In addition Frontex is grateful to Ciaran Carolan (eu-LISA, the EU Agency for the operational management of large-scale IT systems), Ted Dunstone (Biometrics Institute and Biometix), and Kerry Kwan (Immigration Department of the Hong Kong Administrative Region) who have extensively contributed to the revision of this document.

Moreover, the following staff from the Frontex RDU participated in the drafting and editing process: Aurelie Gaudron, Karolina Lopacka, Rasa Karbauskaite, María Duro Mansilla, Gustav Soederlind and Ignacio Zozaya. Frontex is also grateful to all those other stakeholders (not mentioned here) who contributed to the review process.

[1] Member States' experts and Frontex staff have been acknowledged in alphabetical order according to the first letter of their surnames.

About Frontex

The mission of Frontex is to facilitate and render more effective the application of existing and future European Union measures relating to the management of external borders, in particular the Schengen Borders Code. As such, the Agency is to play a key role in analysing and defining the capability needs in border control and in supporting the Member States in development of these capabilities. Frontex also provides qualified expertise to support the EU policy development process in the area of border control.

One of the core objectives of the Capacity Building Division is to drive the process of harmonisation and standardisation for border control and promote greater interoperability. As part of the Capacity Building Division at Frontex, RDU is tasked to develop best practices and procedures, both technical and operational, for border control. RDU proactively monitors and participates in the development of research relevant to the control and surveillance of external borders and keeps Member States and the European Commission informed concerning technological innovations in the field of border control. In particular, one of RDU's main areas of work is the exploration of the potential offered by new border management technologies to meet the dual objective of enhancing security while facilitating travel.

Acronyms and abbreviations

AA	Active Authentication
ABC	Automated Border Control
B900	IR sensitive ink
BAC	Basic Access Control
BCP	Border Crossing Point
BioAPI	Biometric Application Programming Interface
BMP	Image format Windows Bitmap v3
BPGs	Best Practice Guidelines
BPOGs	Best Practice Operational Guidelines
BPTGs	Best Practice Technical Guidelines
CA	Chip Authentication
CAN	Card Access Number
CCTV	Closed Circuit Television
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
CV	Card Verifiable
CVCA	Country Verifying Certification Authority
DG	Data Group, elementary file on e-Passport chip
DG1	Data Group 1 of the e-Passport chip (machine readable zone data)
DG2	Data Group 2 of the e-Passport chip (encoded face data)
DG3	Data Group 3 of the e-Passport chip (encoded finger(s) data)
DG14	Data Group 14 of the e-Passport chip (chip authentication public key data)
DG15	Data Group 15 of the e-Passport chip (active authentication public key data)
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
EBF	External Borders Fund
EF.COM	Common Data Object of the e-Passport chip (version information and tag list)
EF.SOD	Document Security Object of the e-Passport chip (data integrity and authenticity information)
e-ID	Electronic ID
EMC	Electromagnetic compatibility
e-MRTD	Electronic MRTD
EMV	Europay, Mastercard and Visa
EU	European Union
EU/EEA/CH	European Union, European Economic Area, Switzerland
FAR	False accept rate
FRR	False reject rate
FTA	Failure to acquire
ICAO	International Civil Aviation Organisation
ID	Identity Document
IR	Infrared light
IS	Inspection System
ISO	International Organisation for Standardisation
JPEG	Joint Photographic Experts Group
JPG	JPEG compression format for images
JPG2000	JPEG 2000 compression format for images
LDAP	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
MS	EU Member State
OCR	Optical Character Recognition
PA	Passive Authentication
PACE	Password Authenticated Connection Establishment
PC	Personal Computer
PC/SC	Personal Computer/Smart Card (specification for smart-card integration into computing environments)
PCD	Proximity Coupling Device
PKI	Public Key Infrastructure
PPI	Pixels per Inch
QES	Qualified Electronic Signatures
RF	Radio Frequency
SDK	Software Development Kit
SW	Software
TA	Terminal Authentication
TCC	Terminal Control Centre
USB	Universal Serial Bus
UV-A	Ultraviolet light A (400 nm–315 nm wavelength)
VIZ	Visual Inspection Zone
WSQ	Wavelet Scalar Quantisation
XML	Extensible Markup Language

Glossary[2]

Active Authentication (AA): Explicit authentication of the chip. Active authentication requires processing capabilities of the e-MRTD's chip. The active authentication mechanism ensures that the chip has not been substituted, by means of a challenge-response protocol between the inspection system and the e-MRTD's chip. See also '*Passive Authentication*'.

Assisting Personnel: Border guard officer(s) who are responsible for handling the exceptions that occur at an ABC system, redirecting travellers as required (for example, to second line checks), and assisting them in specific situations. Assisting personnel work in close co-operation with the operator of the e-Gates.

Automated Border Control (ABC) system: An 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-defined rules.

Basic Access Control (BAC): Challenge-response protocol where a machine (RF) reader must create a symmetric key in order to read the contactless chip by hashing the data scanned from the MRZ. See also '*Extended Access Control (EAC)*'.

Biometric Capture: The process of taking a biometric sample from the user.

Biometric Spoofing: A deception technique taking advantage of a biometric vulnerability of an ABC system caused by the manufacture of a disguise, prosthetic or other obscuration, aimed to either avoid detection or to be incorrectly identified as another person.

Biometric Verification: The process of confirming the identity of the holder of an e-MRTD by the measurement and validation of one or more distinctive properties of the holder's person.

Border Checks: The checks carried out at border crossing points, to ensure that persons, including their means of transport and the objects in their possession, may be authorised to enter the territory of the Member States or authorised to leave it. See also '*Border Crossing Point (BCP)*'.

Border Crossing Point (BCP): Any crossing-point authorised by the competent authorities for the crossing of external borders.

Border Guard: Any public official assigned, in accordance with national law, to a border crossing point or along the border or in the

[2] The definitions included in this section are based on a number of relevant glossaries and dictionaries, namely the European Migration Network Glossary, the Eurostat Glossary; the ICAO MRTD Glossary, the OECD Glossary of statistical terms, and the Oxford Language Dictionary. Other sources of definitions are the European Commission 'Communication on Smart Borders'; the European Union 'Schengen Borders Code'; the Federal Office for Information Security of Germany 'Defect List: Technical Guideline TR-03129'; and ICAO 'Doc 9303 Machine Readable Travel Documents', 'Guidelines on electronic – Machine Readable Travel Documents & Passenger Facilitation' and its 'Primer on the ICAO PKD Directory' (for further details see the reference list in Annex I). Finally, a number of definitions have been devised and agreed by the Frontex Working Group on Automated Border Controls.

immediate vicinity of that border who carries out border control tasks in accordance with the Schengen Borders Code and national law.

Border Management Authority: Any public law enforcement institution which, in accordance with national law, is responsible for border control.

Certificate: An electronic document establishing a digital identity by combining the identity name or identifier with the public key of the identity, a validity period and an electronic signature by a third party.

Certificate Revocation List (CRL): A list enumerating certificates whose validity is compromised along with the reasons for revocation.

Change Management: Within the context of these Best Practice Guidelines, the term refers to the strategies adopted by the border management authority to deal in a constructive way with the uncertainty associated with the introduction of new border control technologies. The aim is to promote the development among the staff of new attitudes and behaviour that are instrumental to the introduction of the new processes required for the operation of those technologies (i.e. the ABC system).

Chip Authentication (CA): Implicit authentication of the chip. Chip authentication requires a key pair specific to a particular chip, where the private key is stored in a non-accessible area of the chip. The chip authentication mechanism serves for initiation of a secure channel between the chip and the inspection system terminal. It ensures implicitly that the chip has not been substituted. See also '*Active Authentication*'

Cost Benefit Analysis: Technique for deciding whether to make a change. As its name suggests, it compares the values of all benefits from the action under consideration and the costs associated with it.

Customer Service Personnel: Within the context of these Best Practice Guidelines, the term refers to the staff of the port operator who are tasked with providing guidance, advice and assistance to travellers in using the ABC system. Some Member States use the term 'hosts' to refer to such personnel.

Database: An application storing a structured set of data and allowing for the management and retrieval of such data. For 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. See also 'Schengen area' and '*Watch List'*.

Database Hit: An instance of identifying an item of data that matches the requirements of a search. See also 'Database' and 'Watch *List*'.

Defect: A production error affecting a large number of documents. The withdrawal of already issued documents is impractical or even impossible if the detected defect is contained in foreign documents.

Defect List: A signed list to handle defects. Defects are identified by the Document Signer Certificate(s) used to produce defect documents. Defect Lists are thus errata that not only inform about defects but also provide corrigenda to fix the error where possible. See also '*Defect*'.

e-Gate: One of the components of an ABC system, consisting of a physical barrier operated by electronic means. This covers different types of e-Gates: A single-door e-Gate is a system with one barrier to pass. A double-door e-Gate is a system with an entry and an exit barrier (mantrap).

e-ID: An electronically enabled card used as an identity document.

e-MRTD: A machine readable travel document (MRTD) equipped with an electronic contactless chip according to Doc 9303. See also '*MRTD*'.

e-Passport: A machine readable passport (MRP) containing a Contactless Integrated Circuit (IC) chip containing data from the MRP data page, a biometric measure of the passport holder, and a security object to protect the data with PKI cryptographic technology, and which conforms to the specifications of the ICAO Doc 9303, Part 1.

EU citizen: Any 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. See also 'Persons enjoying the Community right to free movement' and 'Freedom of Movement (Right to)'.

Extended Access Control (EAC): Protection mechanism for additional biometrics included in the e-MRTD. The mechanism will include State's internal specifications or the bilateral agreed specifications between States sharing this information. See also 'Basic Access Control (BAC)'.

Failure to Acquire (FTA): The failure of a biometric system to obtain the necessary biometric feature to verify a person.

False Accept Rate (FAR): The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The false acceptance rate may be estimated as FAR = NFA/NIIA or FAR = NFA/NIVA where FAR is the false acceptance rate, NFA is the number of false acceptances, NIIA is the number of impostor identification attempts, and NIVA is the number of impostor verification attempts.

False Reject Rate (FRR): The probability that a biometric system will fail to identify an enrolee or verify the legitimate claimed identity of an enrolee. The false rejection rate may be estimated as follows: FRR = NFR/NEIA or FRR = NFR/NEVA where FRR is the false rejection rate, NFR is the number of false rejections, NEIA is the number of enrolee identification attempts, and NEVA is the number of enrolee verification attempts. This estimate assumes that the enrolee identification/verification attempts are representative of those for the whole population of enrolees. The false rejection rate normally excludes 'failure to acquire' error.

First-Line Check: Default check carried out at border crossing points to ensure that travellers are authorised to enter the territory of the EU/EEA/CH. See '*Second-Line Check*'.

Freedom of Movement (Right to): A fundamental right of every citizen of an EU Member State or another European Economic Area (EEA) state or Switzerland to freely move, reside and work within the territory of these states. See also 'EU citizen' and 'Persons enjoying the Community right to free movement'.

Impostor: A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his physical appearance to represent himself as another person for the purpose of using that person's document.

Integrated Two-Step Process: One of the possible topologies of ABC systems. In an ABC system designed as an integrated two-step process, the traveller initiates the verification of the document and of the traveller's eligibility to use the system at the first stage, and then if successful moves to a second stage where biometric verification and other applicable checks are carried out. This topology is invariably implemented by using a mantrap e-Gate. See also '*One-Step Process*' and '*Segregated Two-Step Process*'.

Interoperability: The ability of several independent systems or subsystem components to work together.

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

Machine Readable Zone (MRZ): The area on a passport containing two lines of data (three lines on a visa) printed using a standard format and font. See also '*Visual Inspection Zone* (VIZ)'.

Member State: A country that is a member of the European Union. Within the context of these Best Practice Guidelines, the term also applies to those countries that, not being EU members, take part in the Schengen area. See also 'Schengen area'.

Monte Carlo Method: The Monte Carlo method for auto-correction is an automatic correction method in which the corrected data value is randomly chosen on the basis of a previously supplied probability distribution for this data item. The method employs computer algorithms for generating pseudo-random variables with the given probability distribution.

Multi-biometrics: Refers to the combination of information from two or more biometric measurements. It is also known as 'Fusion' and 'Multimodal biometrics'.

One-Step Process: One of the possible topologies of ABC systems. An ABC system designed as a one-step process combines the verification of the traveller and the traveller's secure passage through the border. This design allows the traveller to complete the whole transaction in a single process without the need to move to another stage. It usually takes the form of a mantrap e-Gate. See also '*Integrated Two-Step Process*' and '*Segregated Two-Step Process*'.

Operator: The border guard officer responsible for the remote monitoring and control of the ABC system. The tasks performed by the operator typically include: (a) monitoring the user interface of the application; (b) reacting to any notification given by the application; (c) managing exceptions and making decisions about them; (d) communicating with the assisting personnel for the handling of exceptions at the e-Gates; (e) monitoring and profiling travellers queuing in the ABC line and using the e-Gates, looking for suspicious behaviour in travellers; and (f) communicating with the border guards responsible for second-line checks whenever their services are needed. See also 'Assisting Personnel'.

Passive Authentication (PA): Verification mechanism used to check if the data on the RF chip of an e-MRTD is authentic and not forged by tracing it back to the Country Signing Certificate Authority (CSCA) certificate of the issuing country. See also '*Active Authentication*'.

Password Authenticated Connection Establishment (PACE): Password authenticated Diffie-Hellman key agreement protocol that provides secure communication and explicit password-based authentication between an e-MRTD chip and an inspection system. See also '*Extended Access Control (EAC)*'.

Persons enjoying the Community right of free movement: According to Article 2(5) of the Schengen Borders Code these are: a) Union citizens within the meaning of Article 20(1) of the Treaty on the Functioning of the European Union and third country nationals who are members of the family of a Union citizen exercising his or her right to free movement to whom Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States; and b) third country nationals and their family members, whatever their nationality, who, under agreements between the Community and its Member States, on the one hand and those third countries, on the other hand, enjoy rights of free movement equivalent to those of Union citizens. See also '*Freedom of movement (Right to)*' and '*Persons enjoying the Community right to free movement*'.

Port Operator: Also known as 'Port Authority'. The public institution and/or private company that operates the port facility, at either air or sea borders.

Public Key Directory (PKD): A broker service that publishes certificates and revocation lists for download.

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

Registered Traveller: See also 'Registered Traveller Programme'.

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

Second-Line Check: A further check that may be carried out in a special location away from the location at which all travellers are checked (first line).

Segregated Two-Step Process: One of the possible topologies of ABC systems. In an ABC system designed as a Segregated Two-Step Process the process of traveller verification and of passage through the border control are completely separated. The traveller is verified at the first stage, a tactical biometric is captured or a token is issued, and then the traveller proceeds to the second stage where the tactical biometric or token is checked to allow exit. It typically takes the form of a kiosk for verification of the document and the holder, while border passage occurs at an e-Gate. See also '*One-Step Process*' and 'Integrated *Two-Step Process*'.

Service Level Agreement (SLA): Part of a service contract where the level of service is formally defined. SLAs record a common understanding about services, priorities, responsibilities, guarantees and warranties of the services provided.

Terminal Authentication (TA): Mechanism ensuring that only authorised inspection system terminals get access to sensitive chip data. Part of the EAC protocol. See '*Extended Access Control*'.

Third Country National: Any 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. See also 'EU citizen' and 'Persons enjoying the Community right of free movement'.

Topology: The way in which the constituent parts of a system are interrelated or arranged.

Vulnerability: A weakness in an ABC system that might be exploited to bypass some aspect of the system integrity.

Visual Inspection Zone (VIZ): Those portions of the MRTD (data page in the case of an e-Passport) designed for visual inspection, i.e. front and back (where applicable), not defined as the MRZ. See also *'Machine readable zone (MRZ)'*.

Watch List: A list of individuals, groups, or items that require close surveillance. See also 'Database' and '*Database Hit*'.

Executive summary

This document constitutes a compendium of best practice guidelines on the design, deployment and operation of automated border control systems with a focus on their technical dimension.

These BPGs have been drafted by the Frontex Working Group (WG) on ABC in an effort to promote harmonisation of practice, similar traveller experience and consistent security levels at the different BCPs where ABC systems have been deployed. The **intended audience** is technical experts involved in the design and implementation of ABC systems in the EU Member States, including project managers and system architects from border management authorities. While these ABC Best Practice Technical Guidelines have been conceived as a stand-alone resource, ideally they should be read in combination with the Frontex 'Best Practice Operational Guidelines for ABC Systems'. Additional documents such as Guidelines for Processing Third Country Nationals through ABC and ABC Challenge Catalogue (forthcoming in 2015) should serve as the complementary documents to these BPGs.

The document focuses on ABC systems based on the use of an electronic travel document (generally an ICAO compliant e-Passport) which can be used by EU citizens without the need for pre-enrolment. Registered Traveller Programmes (RTPs) are outside its scope. The **biometric markers** covered include both facial recognition and fingerprints.

The BPGs are structured in **four main sections**, which focus respectively on: (1) the physical architecture of an ABC system; (2) the document authentication process; (3) the biometric verification process; and (4) quality control.

Architecture of an ABC system

The **key components** of an ABC system include: one or two physical barriers (e-Gates); a document reader; one or several biometric capture devices (camera and/or fingerprint reader); user interfaces (monitors, LED signals, audio devices); processing units and network devices; and monitoring and control stations for the operators.

There are three main topologies of ABC in use. '**One-step process'** topologies enable the traveller to complete the whole transaction, including the document and the biometric verification, in one single process without the need to move to another stage. A variation from this is the '**integrated two-step process'** topology, in which 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. Finally, in the '**segregated two-step process topology'** the verification processes and the crossing of the actual border take place at separate locations.

Irrespective of the particular configuration chosen, an ABC system must meet basic requirements regarding the **physical installation** and **security and safety** considerations. This includes protecting the modules which are installed in public areas against tampering and vandalism, for instance by using materials that are scratch proof and impact-resistant. The system must also be constructed in such a way as to ensure that only the traveller who has been cleared is allowed to cross the border, while those who have been refused are appropriately redirected to a border guard officer. This is typically achieved by the use of single-door or double-door e-Gates and tailgating detection/prevention mechanisms, or by operating the system in a secure area. Long-term reliability and future-proofness are other important features of a qualitative ABC system.

The document authentication process

Document authentication is the process by which the e-MRTD presented by the traveller is checked in order to determine whether it is a genuine one and enabling the traveller to cross the border. A **document reader** is required as a hardware subcomponent of the ABC system in order to check the authenticity of an e-Passport. The associated document authentication process is considered to be composed of three separate steps: (1) carrying out optical document checks; (2) accessing and reading e-Passport data; (3) verifying e-Passport data.

The document reader subcomponent of an ABC system should have a number of capabilities, including an integrated Radio Frequency (RF) module which meets ISO standards, a dedicated wired connection as physical interface to a host system (e.g. a PC), a state-of-the-art operating speed and a user-friendly design. It should also be future-proof in order to accommodate future enhancements provided by the market.

Mandatory optical checks on the e-Passport relate to the MRZ consistency, the visibility of the MRZ in the infrared light (IR) image of the biographical data page and UV-A brightness. In addition, the e-Passport may be checked in order to compare the information taken from the MRZ (e.g. name, nationality or gender) with the data that was extracted from the visual inspection zone (VIZ) and to verify security patterns (UV, IR, visible) using a database for pattern checks. Such databases should be kept up to date in order to avoid significant increases in the False Reject Rate (FRR).

In **accessing and reading the e-Passport data**, ABC systems must at least support the reading and decoding of the following files/data groups from e-Passports: EF.SOD, EF.COM, DG1, DG2, DG14 and DG15. When fingerprints are used in the biometric verification process, the ABC system must also support the reading and decoding of DG3. **Supported security protocols** must include Passive Authentication (PA), Basic Access Control (BAC), Password Authenticated Connection Establishment (PACE), Active Authentication (AA), Chip Authentication (CA) and, when fingerprints are part of the biometric verification process, Terminal Authentication (TA) as well.

In addition to reading it, ABC systems have to verify the data stored in the e-Passport. **Document verification** is mainly covered by the Passive Authentication (PA) security method, the reliability of which is guaranteed by the use of trustworthy Document Signer (DS) and Country Signing Certification Authority (CSCA) certificates only. Thus, a trusted certificate store must be available. The PA procedure consists of the following sub-steps: (1) EF.SOD verification; (2) DS certificate signature verification; (3) Certificate validity period check; (4) DS certificate revocation status; (5) comparison between EF.SOD and EF.COM if EF.COM is present; and (6) Datagroup integrity check. Additional checks to complete the e-Passport data verification process are the comparison of optical and electronic biographical data (DG1 vs MRZ) and the issuing country comparison (country as referenced in DG1 vs country named in the DS certificate). The overall result of the e-Passport data verification process is not to be considered as 'Passed' or 'Successful' if one or more of the particular sub-steps listed above end up with the result 'Failed'. It is also recommended to use information on defects during the process of e-Passport data verification.

It is up to MSs to decide whether and what kind of **alternative e-MRTDs** are supported by their ABC systems. Currently, both Germany and Spain have ABC implementations that support their national e-ID cards.

Biometric verification

Biometric verification is the process whereby, using biometric technology, it is ascertained that the person holding the e-MRTD is actually the owner of the e-MRTD. ICAO recommends face recognition as the main global interoperable biometric for identity verification of travellers, although ABC systems may also support fingerprints or other biometric markers (e.g. iris).

The biometric verification process is composed of two separate steps: (1) the biometric capture sub-process, carried out by the face or fingerprint capture unit; (2) the biometric verification sub-process, carried out by the face or fingerprint verification unit.

As regards **face capture and verification**, a number of key recommendations on the biometric capture process refer, among others, to the positioning of the face capture unit (in the traveller flow, in order to avoid delays), the resolution of the cameras and their lighting modules, the feedback provided to the traveller during the face capture process, and the pre-processing and quality assessment on the images provided by the capture to the verification unit. As for the verification process, the configuration of the face verification algorithm has to ensure a security level in terms of the False Accept Rate (FAR) of 0.001 (0.1 per cent) or less. At this configuration the False Reject Rate (FRR) should not be higher than 0.05 (5 per cent). Such performance levels should be ascertained by an independent test laboratory or an official agency, and not only by the supplier.

Concerning **fingerprints,** recommendations are provided in relation to the architecture and setup of the fingerprint reader, including the minimum capture area (16 mm width and 20 mm height for single fingerprint sensors), the possibility of recalibration by qualified service staff, the optimal temperature of the room for good quality capture, and the feedback provided to the traveller during the transaction. As in the case of facial recognition, the images provided by the capture to the verification unit should be subject to pre-processing and pre-qualification to ensure that the requisite quality standards are met. The configuration of the fingerprint verification algorithm shall ensure a security level in terms of FAR of 0.001 (0.1 per cent). At this configuration the FRR should not exceed 0.03 (3 per cent).

The monitoring and control station should receive the results of the biometric verification process, both regarding face and/or fingerprints. At least the overall verification result must be displayed in the summary view on the monitoring screen, although it is advisable that further details regarding the verification process are shown on request by the operator.

On the other hand, the use of two or more biometric modalities may be incorporated in national ABC implementations. **Multi-biometrics** allow for better results than a process based on a single biometric, reducing the risk of false positives and negatives. Several types of multi-biometrics can be applied directly to ABC systems in order to improve performance and accuracy: (1) sample level fusion; (2) score level fusion; and (3) decision level fusion. A detailed description of these modalities is available in ISO 24722.

Quality control and quality assurance

Quality control (QC) is the process whereby the quality of all factors involved in the operation and exploitation of the ABC system are measured. While not part of the core functions of an ABC system, quality control is nevertheless essential to assess the performance of the system, identify potential problems and, in sum, serve as the basis for **quality assurance (QA)** to ensure that the system meets the expectations of travellers and border management authorities.

The BPGs focus on the **minimum recommended anonymous operational data** to be collected for QC/QA and the extraction of business statistics in ABC systems. The data stored should include information on at least the following types of transactions: access attempts with documents not accepted by the system (e.g. non-electronic passports); access attempts with non-eligible documents (e.g. third country nationals (TCNs) holding an e-Passport); and access attempts by an eligible traveller with a valid e-Passport but whose verification was not successful (e.g. due to a biometric verification error). Importantly, the collection and storage of data should comply with the limitations imposed by EU and national data protection regulations in the Member States. Thus, personal data should not be stored unless properly anonymised.

In order to allow for detailed performance and trend analysis, all data entries must be time-stamped. They must also provide a summary of the final outcome of the verification process, that is, whether the traveller was granted permission to cross the border without the requirement for further, manual, action by the officers monitoring the BCP. Data entries should include information on the nationality of the document issuer, and the traveller's age and gender. The total verification time and the access time (the total time spent by an eligible traveller in the process since the first interaction with the system) should also be recorded.

Specific subsystems should be available for the logging of statistical and technical data regarding the document authentication process and the biometric verification process, for the purpose of maintaining continuous quality control, the extraction of business statistics and the introduction of improvements to the ABC system. When an ABC system runs other background checks in parallel to the document authentication and biometric verification processes, some data should also be stored on those background checks.

Finally, for the purposes of QC/QA, each ABC installation, as well as each of its components, should be uniquely identified.

Terminology

Although the recommendations and guidelines presented in this document are non-binding for MSs, the terminology below[3] has been adopted in order to provide an unambiguous description of what should be observed in order to achieve a coherent approach with a common security baseline across Schengen borders.

SHALL This word, or the terms 'REQUIRED' or 'MUST', means that the definition is an absolute requirement.

SHALL NOT This phrase, or the phrase 'MUST NOT', means that the definition is an absolute prohibition.

SHOULD This word, or the adjective 'RECOMMENDED', means that there may exist valid reasons in particular circumstances to ignore a particular aspect, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT This phrase, or the phrase 'NOT RECOMMENDED', means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

MAY This word, or the adjective 'OPTIONAL', means that an item or feature is truly optional. A vendor may choose to include the option because a particular marketplace requires it or because the vendor feels that it enhances the product, while another vendor may omit the same item or feature. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same sense an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option.

[3] See Bradner, Scott. Key words for use in RFCs to indicate requirement levels, RFC 2119, 1997.

1. Introduction

1.1. Purpose and audience

This document aims to provide a compendium of best practice guidelines on the technical design of automated border control (ABC) systems. These have been prepared in an effort to achieve harmonisation and convergence in the basic technical features concerning the document authentication, biometric verification and quality control processes, as well as consistent security levels at the different border crossing points of the European Union/Schengen Area where ABC solutions are deployed.

The intended audience consists of technical experts involved in the design and implementation of ABC systems in the EU Member States. The project managers and system architects from border management authorities will find detailed information in order to define its requirements and procure and implement a system that performs up to standards, while avoiding previously known risks and dead-end streets. Finally, current and prospective practitioners and decision-makers at national and EU levels may also benefit from a better understanding of the technical features of ABC systems.

It should be borne in mind that this report and the best practices identified do not create or alter any of the Member States' obligations as set out in the relevant legislation, in particular, the Schengen Borders Code, nor do they constitute an amendment to the Schengen Catalogue and Handbook. Their purpose is mainly descriptive and analytical: they aim to provide additional reference material to technical experts and practitioners working in the area of ABC.

1.2. Scope and methodology

The scope of this document is aligned with the European Commission and International Civil Aviation Organisation recommendations, as available at the time of writing, on the use of e-Passports for automated border control without enrolment[4].

Travel documents considered

ABC systems can be divided into two types: (a) systems without enrolment based on the use of an electronic travel document; and (b) systems based on pre-enrolment which generally take the form of registered traveller programmes. The EC encourages MSs to deploy ABC systems without pre-enrolment for EU citizens carrying ICAO compliant e-Passports.

This document focuses on ABC systems based on first and second generation e-Passports and also national e-ID cards[5]. There are no

[4] See in particular EC, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Preparing the next steps in border management in the European Union', COM(2008) 69 final, 13. 2.2008; ICAO, 'Guidelines for electronic – Machine Readable Travel Documents & Passenger Facilitation', Version – 1.0, 17.4.2008.

[5] ICAO 'Doc 9303 Machine Readable Travel Documents', Third Edition 2008 defines the e-Passport as 'a machine readable passport (MRP) containing a Contactless Integrated Circuit (IC) chip within which is stored data from the MRP data page, a biometric measure of the passport holder, and a security object to protect the data with PKI (Public Key Infrastructure) cryptographic technology, and which conforms to the specifications of Doc 9303, Part 1.' First generation e-Passports contain the facial image of the holder; second generation (obligatory in the EU since June 2009) also contain two fingerprints in addition to the facial image.

specific provisions in this document for combined or stand-alone use of ABC systems serving RTPs. However, given the future implementation of the Smart Borders Package[6], this document will be revised later to address technical issues related to the use of ABC systems serving RTPs.

Biometric markers used

Most ABC systems currently in use support facial recognition as the main biometric authentication method. However, there is a large base of second generation e-Passports carrying both facial and fingerprint data and there are some MSs which have gained relevant experience in the use of fingerprints for identity verification in ABC systems. Thus, fingerprint recognition is explicitly covered in the present version of this document.

The iris has been considered by a few MSs as an alternative for identity verification, but it has not been used as such until now. It is therefore not addressed in this document, but it might be in the future.

Types of Border Control Points

This document mainly focuses on the use of ABC at air BCPs as these systems have so far been mostly implemented at airports except for a few cases in MSs where ABC is implemented at land and sea BCPs.

Methodology

This report has been drafted by Frontex in cooperation with a Working Group (WG) on ABC composed of the following Member States: Germany, Spain, France, the Netherlands, Portugal, Finland, and the UK (as of 2010) and Bulgaria, Czech Republic, and Ireland (as of 2013). In addition, Hong Kong joined the WG in 2013. The WG was created to provide a platform for discussions on ABC related topics among the MSs and other stakeholders so as to fill the knowledge gap and to derive best practices and guidelines in this area.

This document is based on the first release of *Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Control Systems*, published in March 2011, and the follow up release of *Best Practice Technical Guidelines* for *Automated Border Control Systems*, published in August 2012. The document is an attempt to gather and disseminate knowledge on state-of-the-art technologies and best current practices regarding ABC systems.

The methodology used by the WG to develop the initial BPGs was based on the tasks listed below.

- State the problem and goals.
- Elaborate the list of relevant topics to be covered.
- Carry out research on current practice based on questionnaires, interviews and technical meetings.
- Analyse results and extract individual best practices.
- Debate and agree on proposed best practices.
- Build the document.
- Conduct an internal and external review of the document.
- Approve these guidelines.

The WG decided to revise the 2012 release of the BPTGs to reflect new developments and changes in MSs' practice. The main changes are summarised in the Table of changes included at the beginning of this document. During the revision process, information has been collected through regular expert discussions at the WG meetings, field visits to MSs with ABC systems in operation, as well as by

[6] European Commission. Memo: 'Smart Borders' for an open and secure Europe. 28.2.2013. http://europa.eu/rapid/press-release_MEMO-13-141_en.htm

gathering feedback from external stakeholders. The document has undergone extensive internal and external revision and the main modifications introduced have been debated and agreed during the expert WG meetings.

While there are limitations to the reliability of expert judgement in classifying certain practices as 'best'[7], it is understood that the BPGs outlined in this document are only recommendations that are **useful** and **effective.** They have proved their relevance to meet the needs and achieve the goals of the border management authority; they are potentially **transferrable** and **adaptable.**

This document is intended to be a living one, subject to regular updates in an attempt to gather and disseminate knowledge on state-of-the-art technologies and best current practices regarding ABC systems. The aim is to validate it through consultations with the relevant stakeholders in the field of ABC and with technical experts.

1.3. About best practices and guidelines

The identification of best practices for automated border controls should be put into the context of conceptual and methodological issues pertaining to best practice research. While there is not a generally agreed understanding of what 'best practices' are, the Schengen Catalogue, which is used as a reference tool for Schengen evaluations, defines the term as 'a non-exhaustive set of working methods or model measures which must be considered as the optimal application of the Schengen *acquis*, on the understanding that more than one best practice is possible for each specific part of Schengen cooperation'[8]. For the sake of consistency, this is the definition followed in this document.

The mechanisms and limitations of best practice research (i.e. of the various methods and approaches in use to identify best practices) have been examined rather extensively in the public policy and management literature[9]. Yet, despite existing methodological shortcomings, the identification and sharing of best practices present important added value from a practical and policy-oriented point of view. Crucially, best practice research enables organisations to learn from others in the same domain and re-use their experiences. Even the investigation of a simple exemplar case may be useful to practitioners if it allows them to get ideas and to solve similar problems they face[10]. In sum, best practice research is a way to generate useful knowledge and to promote the accumulation of experience in a given field.

A **guideline**, on the other hand, is any document that aims to streamline particular processes according to a set routine. By definition, following a guideline is never mandatory (protocol would be a better term for

[7] As described in Bretschneider, S. et al., 'Best Practices Research: A Methodological Guide for the Perplexed', *Journal of Public Administration Research and Theory*, Vol. 15, No 2, 2005, pp. 307–323.

[8] Council of the EU, EU Schengen Catalogue: External borders control, Return and readmission - Recommendations and best practices, Council document No 7864/09, 19.3.2009, p. 6.

[9] For an overview, see Veselý, A., 'Theory and Methodology of Best Practice Research: A Critical Review of the Current State', *Central European Journal of Public Policy*, Vol. 5, No 2, December 2011, pp. 98–117.

[10] Ongaro, E., 'A protocol for the extrapolation of "Best" Practices: How to draw lessons from one experience to improve public management in another situation', 2009, available at: http://epsa2009.eu/files/Symposium/An%20approach%20to%20the%20extrapolation%20of%20practices_EOngaro.pdf last accessed on 2.6.2015.

a mandatory procedure). Guidelines may be issued and used by any organisation (governmental or private) to make the actions of its employees or divisions more predictable, and presumably of higher quality.

Too often it is not easy to draw the line between best practices and guidelines, and often they are used together. Thus the term Best Practice Guidelines has been widely adopted in public and private organisations to reflect that knowledge, typically based on experience, which can be shared in order to achieve improved results towards specific objectives. Throughout this document, the term Best Practice Guidelines will be used.

1.4. How to read this document

While the ABC Best Practice Technical Guidelines have been conceived as a stand-alone resource, ideally they should be read in combination with the Frontex 'Best Practice Operational Guidelines for Automated Border Control (ABC) Systems' (also referred to as BPOGs) and 'Guidelines for Processing Third Country Nationals through Automated Border Control'.

This document provides detailed insight on the functioning and requirements concerning:

- the physical architecture of an ABC system;
- the document authentication process;
- the biometric verification process; and
- quality control and assurance aspects of ABC systems.

A clarification of the terminology used, a glossary and a list of acronyms and abbreviations can be found at the beginning of the document. These guidelines are also complemented with a series of annexes outlining a list of the reference material used and of additional reading, as well as providing an overview of the ABC systems which, at the time of the writing, are operational and planned in the EU MSs.

2. General overview of ABC systems

The traditional solution of border guard officers manually processing travel documents and travellers has been working effectively for as long as international travel has existed, but this approach is not free from problems. In a matter of few seconds, border guards have the responsibility to verify that: (a) the traveller standing in front of the officer is carrying a valid travel document; (b) the traveller is the person as claimed in the travel document (c) the traveller is eligible to enter the country; and lastly (d) the traveller does not pose a threat to the country's citizens or institutions. With the improvement of technology applied to forging documents, the use of aliases and look-alikes, and the time pressure associated with border control, among others, it is not surprising that the traditional manual approach is now under revision.

After some trials in different countries, ABC systems have proved to be a promising way to meet the need to increase throughput at BCPs while maintaining the requisite levels of security. Virtually all these systems rely on some form of biometrics in order to verify the identity of the travellers. Biometric technology uses a person's unique physiological characteristics – for example, the face and the fingerprints – to verify their identity: in short, to confirm that someone is precisely who he or she claims to be. Computer technology is used to authenticate identity by matching the characteristics of individuals in real time against previously stored records. ICAO recommends facial recognition as the 'globally interoperable biometric technology for machine-assisted identity confirmation', while acknowledging that some authorities may supplement this with fingerprint and iris recognition[11]. e-Passports contain traveller data (including the biometric markers) inside an embedded chip. This chip has been designed with different data protection mechanisms in place to ensure that only authorised parties can access the information contained within. First generation e-Passports contain the facial image of the holder; second generation (obligatory in the EU since June 2009) contain also two fingerprints in addition to the facial image[12].

A number of ABC systems have been developed by the industry, according to requirements established by national border management authorities, which are intended to allow for more efficient and reliable border crossing by means of automation of routine tasks. Although no two ABC systems are equal by design, they can be defined as the use of automated or semi-automated systems that can verify both the authenticity of the travel document used by travellers, the identity of travellers and their authorisation to cross the border at a BCP without the need for human intervention.

[11] ICAO, 'Doc 9303 Machine Readable Travel Documents', Third Edition 2008.

[12] Under Regulation (EC) No 2252/2004 of 13.12.2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

3. Architecture of an ABC system

In general, an ABC system consists of several components. This includes, but is not limited to:

- physical barriers (single-door or double-door e-Gates);
- a monitoring and control station and equipment for the operator;
- a document reader (optical devices including a radio frequency reader module);
- a biometric capture device (camera, fingerprint reader);
- user interfaces (monitors, LED signals, audio devices, panic button);
- processing units and network devices (PC, controller, hubs);
- cameras/sensors for surveillance (CCTV, tailgate detection, left luggage detection).

There are different options for the deployment of ABC systems (see sub-section 3.6.1. of the Frontex ABC BPOGs on 'Topologies of ABC system'):

One-step ABC system

- The traveller is able to complete all transactions (i.e. document, biometric verification and border passage) in one single process without moving to another stage.
- It usually takes the form of a mantrap e-Gate.

Integrated two-step ABC system

- The traveller verifies the document at the first stage and then, if the document verification is successful, moves to a second stage within the same physical structure where the biometric verification is carried out.
- It is invariably implemented by using a mantrap e-Gate.

Segregated two-step ABC system

- The processes of document authentication and traveller verification are completely separated from the passage through border control.
- It typically takes the form of a kiosk for verification of the document and the holder, while border passage occurs at an e-Gate through the use of a temporary token.

In any of these options, the ABC system MUST meet basic requirements regarding the physical installation and security and safety considerations. These requirements are described in the following sub-section. Irrespective of the physical design of the ABC system, the requirements on the document authentication modules and the biometric components are given in section 4 on 'the document authentication process' and section 5 on 'the biometric verification process' of this document.

3.1. Requirements of the physical installation

For the modules of the ABC system that are installed in public areas, appropriate mechanisms against tampering and vandalism SHOULD be implemented. This includes the use of secure locked panels for accessing the interior of the system. Furniture, fixings, door mountings, cylinders and locks SHOULD follow the respective standards. Materials and parts SHOULD be scratch proof and impact-resistant to a reasonable extent.

The physical parts of the ABC system MUST comply with the applicable fire protection requirements.

ABC systems SHOULD make the best use of available space in a way that caters to all users. A smooth passage through the ABC system for everyone, including for travellers with trolleys or other luggage, MUST be ensured.

The installation SHOULD be as non-invasive as possible for the existing infrastructure. This covers, among others, the need for drilling, mounting of additional barriers, and wiring requirements (power and data).

3.2. Security and safety

Physical barriers SHOULD be used to ensure that only the traveller who has been cleared is allowed to cross the border (i.e. no tailgating), and that travellers who have been rejected are properly handled (e.g. refused in order to be redirected to the manual control). ABC systems MUST be constructed in such a way as to form a robust barrier so that a person may not gain access over, under, by the side of or through the ABC system.

This is typically achieved by the use of single-door or double-door e-Gates and tailgating detection/prevention mechanisms, or by operating the system in a secure area. In case of errors, the traveller MAY be directed to manual clearance or MAY be contained until handled by a border guard officer.

All equipment and fittings MUST comply with EU safety requirements and applicable standards. When the physical barriers within the ABC system are closing, they MUST NOT close with such physical force as to cause injury to the traveller. Other moving parts (e.g. the camera unit) SHOULD NOT be accessible by the traveller. If this cannot be ensured by design, any risk of injury MUST be avoided by other reliable means.

3.3. Long-term reliability

All mechanical and hardware components MUST be reliable, robust and designed to meet anticipated load and throughput for the lifetime of the hardware (minimum of 5 years).

To be future-proof, an ABC system MAY be designed and configured so that it does not preclude any future enhancements for document authentication modules or biometric systems for the lifetime of the hardware.

4. The document authentication process

Document authentication is the process by which the electronic machine readable travel document (e-MRTD) – generally an e-Passport[13] – presented by the traveller is checked in order to determine whether it is a genuine document, enabling the traveller to cross the border.

A document reader is required as a hardware subcomponent of the ABC system in order to check the authenticity of an e-Passport. The associated document authentication process (typically performed by software) is considered to be composed of three separate steps:

- Carrying out optical document checks.
- Accessing and reading e-Passport data.
- Verifying e-Passport data.

Requirements and best practices regarding the document reader and the document authentication process are detailed in this section.

4.1. Document reader requirements

ABC systems SHALL use a full-page document reader that provides at least the key technical specifications and capabilities detailed below.

It is generally recommended that the design of the system SHOULD NOT exclude future enhancements regarding document readers that the market may provide for.

4.1.1. Technical requirements

The document reader subcomponent SHOULD be designed so that it can be used effectively in self-service environments. This includes easy usage for both right- and left-handed people and easy handling of e-Passports with flexible biographical data pages. Note however that flexible biographical data pages might cause difficulties as they may get folded when placed on the document reader, which must be avoided in order to ensure that the e-Passport is properly read.

e-Passports SHOULD be placed on the document reader lengthwise, i.e. with the biographical data page facing down and the MRZ side first, on the document reader.

The document reader SHALL have an integrated RF module according to ISO 14443 Type A and Type B that is accessible via a PC/SC interface. The transfer rate of the RF module SHOULD be as high as possible (at least 424 Kbit/s).

The document reader SHALL have a dedicated wired connection as physical interface to a host system (e.g. a PC) with a state-of-the-art transfer rate (e.g. USB 2.0, 480 Mbit/s). It is RECOMMENDED to operate the document reader with a power supply that is independent from the physical interface to the host system.

The document reader SHALL be able to capture images at IR, UV-A and visible light. The optical resolution SHALL be at least 385 PPI.

[13] Concerning the use of alternative e-MRTDs, see section 4.6.

The document reader SHOULD have proper shielding against the interference of external light.

The document reader MUST comply with the existing regulations regarding EMC and UV-A light emission.

4.1.2. Capability requirements

ABC systems SHOULD be equipped with a document reader that is future-proof. Therefore, the document reader SHOULD support all ICAO compliant e-MRTDs, including form factors of ID1, ID2 and ID3.

The document reader MUST have a state-of-the-art operating speed. On average, optical images of the biographical data page SHOULD be captured within 2 seconds, and reading of the electronic data (at least EF.SOD, EF.COM, DG1 and DG2) from a typical first generation e-Passport SHOULD NOT take more than 8 seconds.

4.2. Performing optical checks on the e-Passport

ABC systems SHALL perform a verification of the optical security features of the e-Passport as explained below.

4.2.1. Mandatory optical checks

The following are the mandatory optical checks to be carried out on the e-Passport.

MRZ consistency
ABC systems SHALL verify that the optically extracted MRZ is consistent, using the MRZ checksum digits.

B900 ink
ABC systems SHALL verify that the MRZ is completely visible in the IR image of the biographical data page.

UV-A brightness
ABC systems SHALL verify that no bright paper or remains of glue are visible in the UV-A image of the biographical data page.

4.2.2. Optional optical checks

The following are optional optical checks which may be carried out on the e-Passport.

MRZ vs VIZ
ABC systems MAY compare information taken from the MRZ (e.g. name, nationality or gender) with data that was extracted from the visual inspection zone.

Pattern checks
It is RECOMMENDED that ABC systems verify optical security patterns (UV, IR, visible) using a database for pattern checks. This verification MAY also be used to identify the type of document. In this regard, it is RECOMMENDED to use a dedicated database for the ABC scenario consisting of reliable patterns for the targeted user group only. The patterns database MUST be updated on a regular basis; otherwise the False Reject Rate (FRR) due to the pattern checks will increase significantly.

It is further RECOMMENDED to use a pattern database that allows for maintenance and support by the operating agency or by a trusted third-party provider under a contract with the supervision of the operating agency. The use of a pattern database that does not allow for content modifications by the operating agency (a black-box database) is NOT RECOMMENDED.

4.3. Accessing and reading e-Passport data

ABC systems MUST at least support reading and decoding of the following files/data groups from e-Passports: EF.SOD, EF.COM, DG1, DG2, DG14 and DG15. When fingerprints are used in the biometric verification process (see section 5), the ABC system MUST support the reading and decoding of DG3 as well.

ABC systems MUST at least support following security protocols: Passive Authentication (PA)[14], Basic Access Control (BAC), Password Authenticated Connection Establishment (PACE), Active Authentication (AA) and Chip Authentication (CA). If access to the chip data of a specific e-Passport is protected by PACE or BAC, the appropriate protocol (PACE or BAC) MUST be performed prior to reading data groups. For e-Passports that support both PACE and BAC, either PACE or BAC MUST be performed. Further details on PACE and BAC are given in ICAO SAC and ICAO 9303. During the reading process, AA or CA MUST be performed if supported by the specific e-Passport. For e-Passports that support both CA and AA, only CA is REQUIRED. In such a case AA MAY be performed additionally, after CA. When fingerprints are used in the biometric verification process, the ABC system MUST support the security protocol Terminal Authentication (TA) as well.

TA requires the terminal to prove to the e-Passport that it is entitled to access sensitive – protected with Extended Access Control(EAC) – data on the chip. Such a terminal MUST at least be equipped with an according set of card verifiable (CV) certificates – Document Verifier (DV) certificate and Inspection System (IS)certificate – and the private key corresponding to the public key encoded in the IS certificate. After the terminal has verified this private key, the e-Passport chip will grant access to sensitive data as indicated in the CV certificate chain.

The EAC-Public Key Infrastructure (PKI) required for issuing and validating IS certificates consists of the following entities.

- Country Verifying CA (CVCA) – root CA (national trust point) that issues DV Certificates.
- A Document Verifier (DV) – an organisational unit within the EAC-PKI that manages a group of inspection systems (e.g. terminals operated by a State's border police) by issuing IS certificates.
- An Inspection System (IS).

Further details on EAC are given in BSI03110.

ABC systems SHOULD implement the general high-level sequence for the RF chip reading process as shown in **Figure 1**.

4.4. Verification of e-Passport data

Once the e-Passport chip has been read, ABC systems MUST verify the data. Such an e-Passport data verification process is mainly covered by the Passive Authentication (PA) security method defined in ICAO9303.

The reliability of the PA security method is only assured if trustworthy certificates (Document Signer (DS)certificates and CSCA certificates) are applied to the verification process[15]. If it cannot be verified that the DS certificate originates from a trusted source or has been issued by an official and trusted CSCA, the result of the entire e-Passport data verification process cannot be depended upon and is thus rendered useless. Therefore, the ABC system MUST be provided with certificates from a trusted certificate store.

[14] See section 4.4 for a detailed description of the process for verification of e-Passport data by Passive Authentication (PA).

[15] The ICAO PKD system as well as Master Lists published by the responsible authorities on their websites MAY for example serve as an external source for DS or CSCA certificates.

It is RECOMMENDED to implement this trusted certificate store as a centralised system. In this case, the integrity and authenticity of the certificate store (which is absolutely crucial for the reliability of the entire e-Passport data verification process) MUST be ensured 'only once' on the central side so that efforts aimed at assuring the integrity and authenticity locally on each client ABC system can be saved. As an add-on when implementing a centralised trusted certificate store, sub-steps 2, 3 and 4 of the PA procedure (see below) MAY be implemented as a centralised service as well. Note that details about the technical implementation of the trusted certificate store (e.g. central Lightweight Directory Access Protocol (LDAP) directory, local signed file, etc.) as well as the mechanisms used to safeguard the trust relationship between the certificate store and the ABC system (e.g. through a secure communication channel) are outside the scope of this document.

The PA procedure consists of the following sub-steps, which MUST be supported by the ABC system.

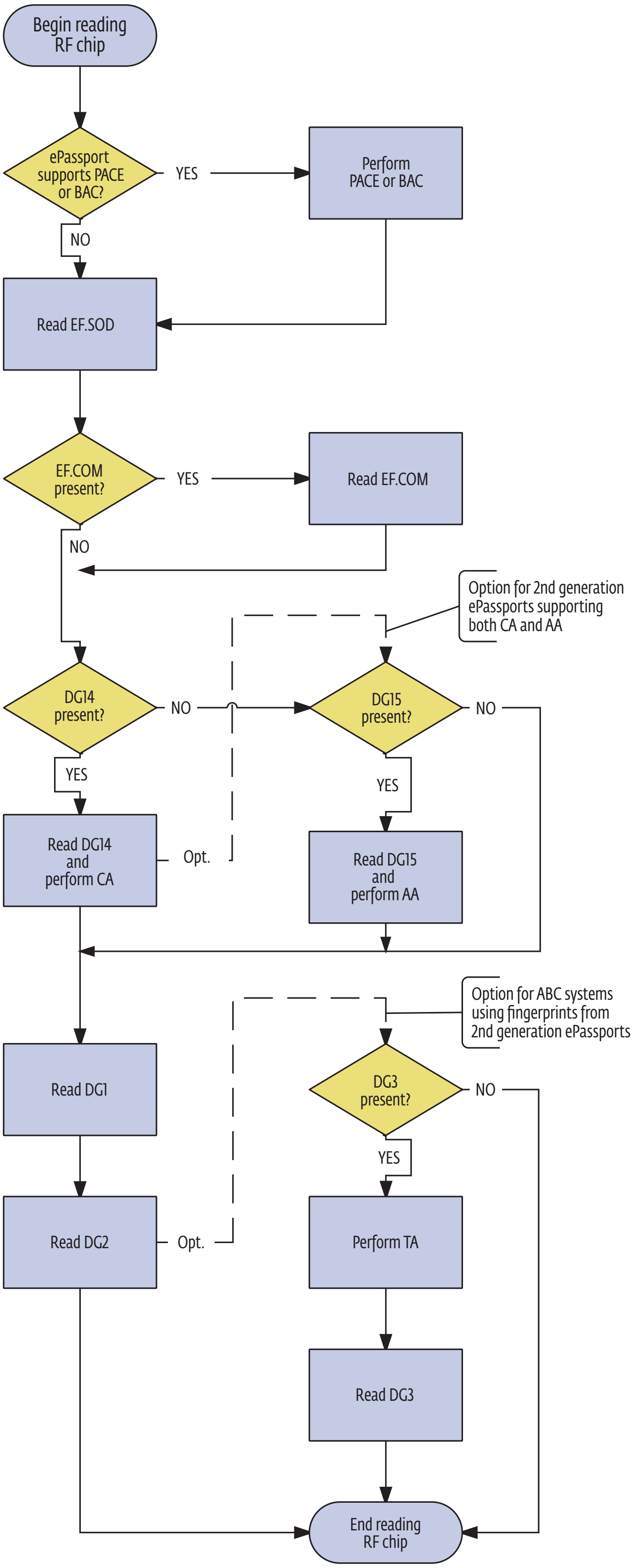
1. EF.SOD verification.
2. DS certificate signature verification.
3. Certificate validity period check.
4. DS certificate revocation status.
5. Comparison between EF.SOD and EF.COM if EF.COM is present.
6. Data group integrity check.

In addition to the PA procedure, the following sub-steps MUST be performed by the ABC system in order to complete the e-Passport data verification process.

7. Comparison of optical and electronic biographical data (DG1 vs MRZ).
8. Issuing country comparison (DG1 vs DS certificate).

The overall result of the e-Passport data verification process MUST NOT be considered as 'Passed' or 'Successful' by the ABC system

Figure 1: **High-level sequence for RF chip reading**



if one or more of the particular sub-steps 4.4.1–4.4.8 (see details below) are concluded with the result 'Failed'.

During the PA procedure, additional information about DS certificates or data groups (in particular regarding personalisation errors and defects) MAY be used to verify the e-Passport data (see section 4.4.9.).

4.4.1. EF.SOD verification

The structure of EF.SOD is defined by ICAO 9303 as a Signed Data structure conforming to RFC3369 and ABC systems MUST verify its signature. To perform this signature verification procedure, a DS certificate corresponding to the particular EF.SOD is required. ICAO 9303 provides that the DS certificate MAY be included in EF.SOD. In practice, most countries are issuing e-Passports that contain the corresponding DS certificate. Thus, ABC systems MUST be able to process EF.SOD files with zero or more DS certificates. Additionally, ABC systems SHOULD be able to obtain a DS certificate from an **external source** (e.g. PKD) if the particular EF.SOD does not contain the proper DS certificate.

If the verification of the EF.SOD signature is successful, the result of this sub-step MUST be considered as 'Passed' by the ABC system. If the verification of the EF.SOD signature is not successful or could not be completely performed (e.g. due to a missing DS certificate), the result of this sub-step MUST be considered as 'Failed'.

4.4.2. DS certificate signature verification

Verification of the certificate chain up to a known trusted certificate is an essential step in the overall process. Claims by researchers regarding the faking of an official e-Passport often involve the creation of a new EF.SOD and its signature with a new key after a data group was modified or exchanged. If it is not verified that the DS certificate originates from a trusted source or has been issued by an official and trusted CSCA, the results of all other security checks become worthless.

Therefore, the following requirements SHALL apply to ABC systems.

- If the signature of the EF.SOD has been verified with a DS certificate that has been taken from the EF.SOD or from a non-trusted external source (like an unauthenticated database), ABC systems MUST verify the signature of the DS certificate as well. This requires an appropriate CSCA certificate that originates from a trusted source.
- If the DS certificate originates from a trusted source (explicitly not from the EF.SOD), ABC systems MAY skip the verification of the DS certificate signature.
- Except for very few exceptions, it is common that the DS certificate used to verify the signature of EF.SOD is contained in EF.SOD itself and that its authenticity is verified with the corresponding CSCA certificate. In order to do so, ABC systems have to search the proper CSCA certificate out of a larger set of certificates provided by the trusted certificate store. It is RECOMMENDED that ABC systems extract the Authority Key Identifier extension from the DS certificate and search for a CSCA certificate with the corresponding value in its Subject Key Identifier extension. Although the usage of these extensions is specified as mandatory by ICAO 9303, there are some countries that have issued e-Passports without them. Thus, it is RECOMMENDED that in the event that no matching CSCA certificate can be found by comparing key identifiers, ABC systems SHOULD perform only a subject-based search for CSCA certificates using the issuer information from the DS certificate.

- When one or more suitable CSCA certificates have been found using the search criteria described above, the DS certificate signature verification result MUST be considered as 'Successful' if the signature of the DS certificate can be verified with one of these CSCA certificates and the particular CSCA certificate subject is equal to the DS certificate issuer. If none of the found CSCA certificates meets these two requirements, the DS certificate signature verification sub-step MUST be considered as 'Failed'.
- As some countries issue CSCA certificates that are not self-signed, it is RECOMMENDED that the signature of the CSCA certificate is not verified, or it might be unavoidable to use CSCA link certificates for the DS certificate signature verification. Since all CSCA certificates that are used by the ABC system MUST originate from a trusted source this is not seen as a security flaw.

4.4.3. Certificate validity period check

ABC systems SHALL verify that the current time is within the validity period of the DS certificate. Additionally, ABC systems SHOULD also check if the current time is between the start and the end of the validity period of the CSCA certificate. It is RECOMMENDED to set up appropriate mechanisms to ensure that the current time is valid.

If the validity period checks performed are successful, the result of this sub-step MUST be considered as 'Passed' by the ABC system. If the performed validity period checks fail, the result of this sub-step MUST be considered as 'Failed'.

4.4.4. DS certificate revocation status

Generally, checking the DS certificate revocation status is a mandatory sub-step of the PA procedure. Given the present practice regarding the official distribution of certificate revocation information, it is very difficult to check the DS certificate revocation status for a broad range of e-Passport issuing countries. Therefore, ABC systems SHOULD check the DS certificate revocation status if the corresponding revocation information – for example a Certificate Revocation List (CRL) – is available.

If the DS certificate revocation status could be checked as 'Not revoked' on the basis of trusted according-to-certificate revocation information, the result of this sub-step MUST be considered as 'Passed' by the ABC system. If the DS certificate revocation check results in 'Revoked' based on trusted according-to-certificate revocation information, the result of this sub-step MUST be considered as 'Failed'. If the DS certificate revocation status could not be checked, the result of this sub-step SHOULD NOT be considered as 'Failed'.

4.4.5. Comparison between EF.SOD and EF.COM

Because EF.SOD does not contain a digest (hash-value) of EF.COM, a modification of EF.COM cannot be detected by just verifying the signature of the EF.SOD. Thus, ABC systems MUST use EF.SOD to receive a trustworthy list of data groups contained in a given e-Passport chip. If EF.COM is present in the e-Passport chip (in addition to EF.SOD), ABC systems SHALL compare the content of EF.COM with EF.SOD to ensure that each DG listed in EF.SOD is also contained in EF.COM and vice versa. If a mismatch between EF.COM and EF.SOD is detected, the result of this sub-step MUST be considered as 'Failed' by the ABC system. If EF.COM and EF.SOD correspond to each other, the result of this sub-step MUST be considered as 'Successful'.

4.4.6. Data group integrity check

For each data group that was read from the e-Passport chip, ABC systems MUST calculate the data group's digest (hash-value) and compare it with the corresponding digest contained in EF.SOD. ABC systems SHALL rely on the content of a data group for further processing (e.g. biometric verification) only if the digests are equal. In case the e-Passport chip supports AA and/or CA, the ABC system MUST also verify the digest of the corresponding data group (DG14 in case of CA and DG15 in case of AA).

If all of the performed data group integrity checks are successful, the result of this sub-step MUST be considered as 'Passed' by the ABC system. If one or more integrity checks fail, the result of this sub-step MUST be considered as 'Failed'.

4.4.7. Comparison of optical and electronic biographical data (DG1 vs MRZ)

If the overall border control process includes background checks, the information to perform these queries is typically taken from the optically scanned MRZ, which is usually the first information available.

If an e-Passport enforces the performance of the BAC protocol, some parts of the MRZ are implicitly verified against OCR errors if the protocol execution was successful. Nevertheless, it is possible for an attacker to falsify other parts of the MRZ that are not used for BAC (e.g. surname and/or given names). To prevent this attack, ABC systems MUST verify the whole content of the optical MRZ against DG1.

If the verification of the optical MRZ against DG1 is successful, the result of this sub-step MUST be considered as 'Passed' by the ABC system. If the verification of the optical MRZ against DG1 fails, the result of this sub-step MUST be considered as 'Failed'.

REMARK: Because of non-ICAO-compliant use of optional MRZ data in some e-Passports these special entries may not be coded identically in the DG1. Thus, it is the responsibility of the border management authority of the Member State to define how to deal with this special issue of the document verification sub-step.

4.4.8. Issuing country comparison (DG1 vs DS certificate)

An attacker may also falsify an e-Passport by managing to sign their manipulated data using a DS of a country other than the purported e-Passport issuing country. By doing so they could, for example, try to bypass visa regulations by appearing under a false nationality.

Thus, ABC systems SHOULD extract the country attribute from the issuer name in the DS certificate and compare it to the issuing country information stored in DG1. This check can only be performed if the following preconditions are fulfilled.

- A mapping table with a distinct mapping between ICAO 3-letter country codes and ISO 2-letter country codes MUST be defined. This is not necessarily a distinct mapping for each particular country (e.g. an ISO 2-letter country code may map to multiple ICAO 3-letter country codes).
- The issuer name of the particular DS certificate contains a country attribute with a properly encoded ISO 2-letter country code.

It is RECOMMENDED to implement this sub-step as follows.

- Extract the ICAO 3-letter country code from DG1 (called CountryICAO).
- Extract the ISO 2-letter country code from the DS certificate (called CountryISO).

- Compare CountryICAO against CountryISO based on the defined mapping table.

If CountryICAO and CountryISO correspond to each other according to the mapping table, the result of this sub-step MUST be considered as 'Successful' by the ABC system. If CountryICAO and CountryISO do not correspond to each other according to the mapping table, the result of this sub-step MUST be considered as 'Failed'.

4.4.9. Defect handling

A 'Defect' is defined as a personalisation error affecting a large number of e-Passports (e.g. the set of e-Passports based on one particular DS certificate). The withdrawal of already issued e-Passports affected by a Defect is generally impractical or even impossible if the Defect relates to foreign e-Passports.

A Defect List according to BSI03129 is a signed data structure to handle such Defects. Particular Defects within a Defect List are identified by the corresponding DS certificates. Defect Lists are thus errata that not only inform about erroneous e-Passports but also provide corrigenda to fix the errors where possible. Regular DS certificate revocation information (e.g. from CRLs) can also be included into such Defect Lists.

It is RECOMMENDED to use such Defect information about erroneous e-Passports during the process of e-Passport data verification.

4.5. Design of the document authentication process

There are several interdependencies among the separate steps of the document authentication process (optical checks, reading RF data and e-Passport data verification). Generally, each step or sub-step SHOULD be started as soon as the required input data (e.g. optical MRZ, particular data group, etc.) is available. Performing these steps concurrently (that is, running several tasks in parallel) as much as possible allows for the minimisation of time required for the entire document authentication process.

A high-level illustration of the RECOMMENDED document authentication process for ABC systems is shown in **Figure 2** (see overleaf).

4.6. Alternative e-MRTDs

Usually, travellers wishing to enter the EU must carry a passport as a travel document. However, there are additional e-MRTDs that MAY be used in ABC systems.

It is at the discretion of MSs to decide what kinds of alternative e-MRTDs, if any, are supported by their ABC systems.

4.6.1. MSs national identity cards

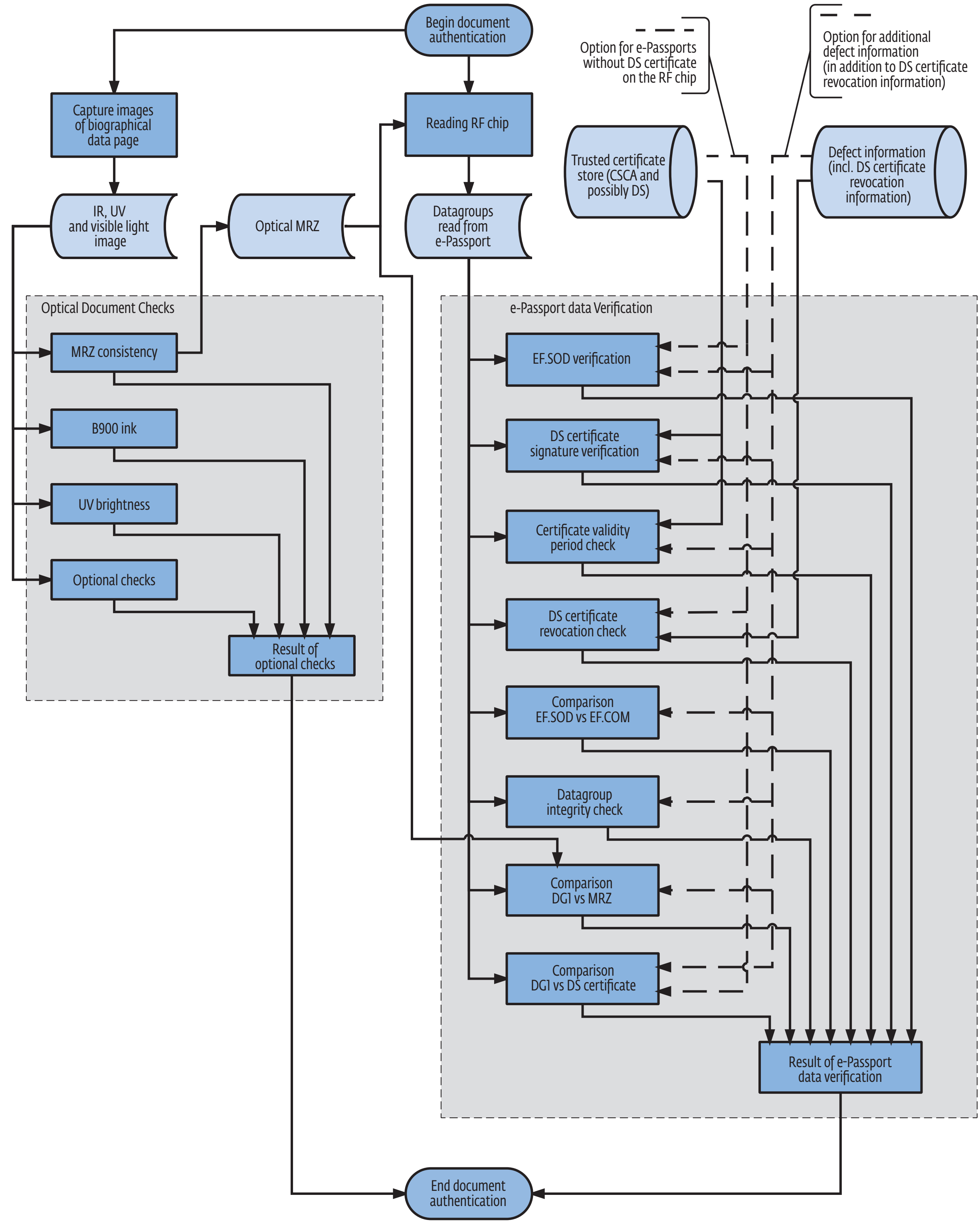
For verification of alternative e-MRTDs, the ABC system MAY need a connection to the specific national systems allowing for validation of the document and for access to its protected data areas.

Currently, there are a number of approaches to national ID cards with biometric capabilities. At the time of writing, Germany and Spain had ABC implementations supporting e-ID cards. Details on both systems are presented in the case studies below, for illustration purposes.

4.6.1.1. German electronic ID card

The German e-ID was introduced in November 2010. The card is in ID1 format and a contactless chip (similar to e-Passports) is embedded in it.

Figure 2: **Document authentication process**


Begin document authentication
Capture images of biographical data page
Reading RF chip
IR, UV and visible light image
Optical MRZ
Datagroups read from e-Passport
Option for e-Passports without DS certificate on the RF chip
Option for additional defect information (in addition to DS certificate revocation information)
Trusted certificate store (CSCA and possibly DS)
Defect information (incl. DS certificate revocation information)
Optical Document Checks
MRZ consistency
B900 ink
UV brightness
Optional checks
Result of optional checks
e-Passport data Verification
EF.SOD verification
DS certificate signature verification
Certificate validity period check
DS certificate revocation check
Comparison EF.SOD vs EF.COM
Datagroup integrity check
Comparison DG1 vs MRZ
Comparison DG1 vs DS certificate
Result of e-Passport data verification
End document authentication

The chip of the ID card contains three different applications:

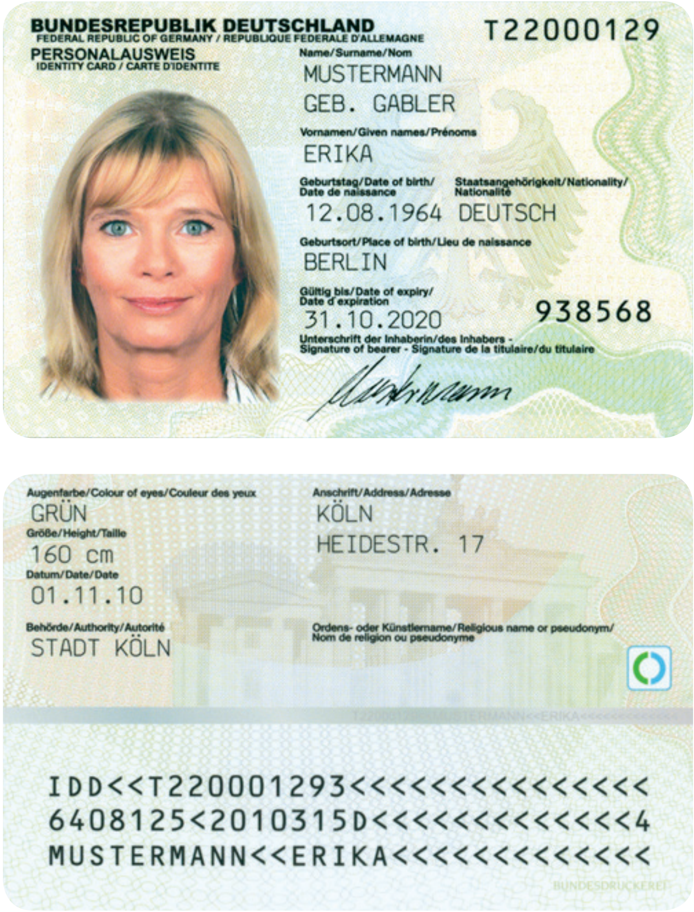
- biometric application to serve as an e-MRTD;
- e-ID application supporting secure e-Business and e-Government systems;
- QES application for doing qualified electronic signatures.

For use within the border control context only the biometric application of the ID card is relevant. The data stored in the biometric application is exactly the same as in the e-Passport with one exception: fingerprints in DG3 are optional for the ID card, whereas they are mandatory for the e-Passport. Further details on biometric standards and use cases of the ID card are specified in BSI 03121.

The main difference between the e-ID card and the e-Passport as regards reading of data groups is the protection of the stored data from unauthorised access. While for EU e-Passports DG1 and DG2 are protected by BAC only, all data stored on the ID card is protected by EAC, including DG1 and DG2.

EAC [BSI03110] provides security mechanisms to ensure that only authorised instances and readers get access to specific data on the ID card. Therefore, a secure communication (Password Authentication Connection Establishment, PACE) has to be established and access to sensitive data is granted to an IS if a certificate chain with sufficient entitlements is available for the mechanism of EAC Terminal Authentication. A corresponding Public Key Infrastructure (EAC-PKI) is required to provide a valid certificate chain for the IS.

While the establishment of the secure communication for BAC-protected EU e-Passports is based on the information derived from the two-line MRZ, the PACE protocol is established by using the Card Access Number (CAN) from the front side of the ID card or, alternatively, from the three-line MRZ on the back side.



BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE

T22000129

Name/Surname/Nom
MUSTERMANN
GEB. GABLER

Vornamen/Given names/Prénoms
ERIKA

Geburtstag/Date of birth/ Date de naissance
12.08.1964

Staatsangehörigkeit/Nationality/ Nationalité
DEUTSCH

Geburtsort/Place of birth/Lieu de naissance
BERLIN

Gültig bis/Date of expiry/ Date d'expiration
31.10.2020

938568

Unterschrift der Inhaberin/des Inhabers - Signature of bearer - Signature de la titulaire/du titulaire
Mustermann

Augenfarbe/Colour of eyes/Couleur des yeux
GRÜN

Größe/Height/Taille
160 cm

Datum/Date/Date
01.11.10

Behörde/Authority/Autorité
STADT KÖLN

Anschrift/Address/Adresse
KÖLN
HEIDESTR. 17

Ordens- oder Künstlername/Religious name or pseudonym/ Nom de religion ou pseudonyme

```
IDD<<T220001293<<<<<<<<<<<<<<<
6408125<2010315D<<<<<<<<<<<<<4
MUSTERMANN<<ERIKA<<<<<<<<<<<<<
```

BUNDESDRUCKEREI

Figure 3: **German electronic ID card (front and back)**

The IS used by the German Federal Police to verify ID cards and e-Passports follows a distributed approach. A Terminal Control Centre [BSI03129] (TCC) offers a central service that connects the distributed readers (for example, those that are part of an ABC system). The TCC supports different application scenarios for BAC and EAC protected documents. Secure centralised key and certificate storage are part of the solution allowing the TCC to take over the authentication procedure for permitted readers. Besides the EAC

Terminal Authentication protocol the TCC additionally supports DS certificate verification (part of the ICAO Passive Authentication security method).

The main differences between e-Passport and ID card are shown in the following table:

Since August 2011 the EasyPASS ABC system in Germany has been ready to read and verify the electronic ID card in addition to ICAO compliant e-Passports.

4.6.1.2. Spanish ID card

The Spanish national e-ID card was introduced in May 2006. The card is in ID1 format and a contact chip (similar to EMV cards) is embedded in it.

The chip of the ID card contains two different applications:

- match-on-card biometric application (ISO 7816–11 compliant) using fingerprint patterns (ISO 19794–2 compliant);
- application for recognised electronic signatures.

The data is stored in the biometric application in ISO 19794-2 short format and the match-on-card software can be executed in secured environments only. Currently, it is not possible to execute this component in systems other than the Spanish ABC.

The interface of the match-on-card software is compliant with ISO 7816-11 standards.

In addition, the Spanish ID card stores a photograph of the citizen within the chip. The access is secured and unavailable by general applications due to Spanish policy on data protection.

Since May 2010 the ABC system in Spain has been ready to read and verify the Spanish electronic ID card in addition to ICAO compliant e-Passports.

4.6.1.3. Comparison of Spanish and German e-ID cards and EU e-Passport

The main differences between e-Passport, Spanish ID card and German ID card are shown in the following table:

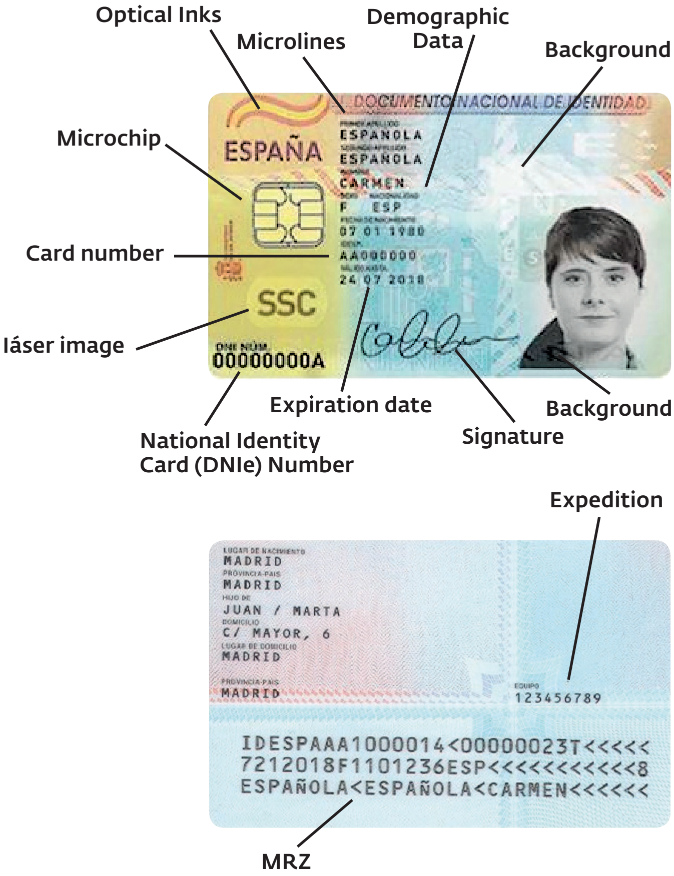


Figure 4: **Spanish electronic ID card (front)**

Table 1: **Comparison of e-Passport, Spanish e-ID card and German e-ID card.**

	EU e-Passport (ID3 size)	**German e-ID card (ID1 size)**	**Spanish e-ID card (ID1 size)**
Optical data			
MRZ	2 lines printed on front side of data page	3 lines printed on back side of ID card	3 lines printed on back side of ID card (ICAO compliant)
CAN	Not available	printed on front side of ID card	Not available
Electronic data			
(MRZ data)	Mandatory (DG1 format)	Mandatory	Mandatory (ASN.1 format)
(face image)	Mandatory (DG2 format)	Mandatory	Mandatory (ISO 19794-5)
(fingerprint images)	Mandatory (DG3 format)	Optional	Mandatory (ISO 19794-2)
Access control	BAC (DG1, DG2) PACE (DG1, DG2; from 2014 on) EAC1 (DG3)	PACE with EAC2 (all DGs)	Secured by CWA 14890 protection profile CWA 14169

5. The biometric verification process

Biometric verification is the process whereby the identity of the e-MRTD owner is verified with the use of biometric technology.

Self-service ABC systems based on ICAO compliant e-MRTDs SHALL follow the recommendations of ICAO9303 and SHALL use face recognition technology as the main biometric marker for identity verification of travellers. They MAY support fingerprints or other biometric markers in compliance with ICAO 9303 at present or in the future.

The biometric verification process is considered to be composed of two separate steps.

1. Biometric capture sub-process, carried out by the face or fingerprint capture unit.
2. Biometric verification sub-process, carried out by the face or fingerprint verification unit.

Requirements and best practices regarding the units and sub-processes are detailed in this section.

It is generally recommended that the design of the system SHOULD NOT exclude future enhancements regarding biometric capture and verification that the market may provide.

5.1. Face verification

5.1.1. Face capture unit

5.1.1.1. Architecture and setup

The face capture unit SHOULD be in the traveller flow (a straight-line for the traveller to walk and look in the camera). If the camera and the flow form an angle greater than 45°, this is likely to slow down the flow.

The cameras within the face capture unit (one or more cameras per capture unit) SHALL have a resolution of at least 2 Megapixel. It is RECOMMENDED to use high-quality cameras that are able to provide at least images according to the photographic and digital requirements of ISO 19794-5. The depth of the field depends on the setup (mantrap, single e-Gate or kiosk); it MUST be adjusted to the area where the traveller's face is located in the regular use case. A frame rate of at least 10 frames per second is RECOMMENDED.

The unit SHOULD contain lighting modules to ensure a proper illumination of the face region. The lighting SHALL NOT cause reflections on glasses or the skin of the face. The lighting be active during the complete capture process and brightness MAY be varied to get best contrast and illumination. It MAY be a permanent light source or it MAY be switched off during times when no face images are captured. Sunlight will vary both on a daily and 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 is controlled for best capture results. The unit SHALL also fit with other environmental conditions (e.g. temperature and humidity) at the place where the ABC system is installed.

The unit SHALL be able to capture frontal images of persons at the height of at least between 140 and 200 cm. For instance, most of the deployed solutions make use of a moving camera, a single wide angle camera, or several cameras at different heights.

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

The face capture unit SHOULD give feedback to the traveller through 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 of sufficient quality for it to be used by the face verification unit. If the feedback is realised as a digital mirror on a display, the display MUST move with the camera (if a movable camera unit is used). The feedback SHOULD NOT interfere with the face capture process.

The capture unit MAY be connected directly to the PC that controls the complete ABC process or indirectly via a pre-processing unit. To connect the capture unit to the control PC, state-of-the-art interfaces (e.g. USB2.0, Ethernet, FireWire) SHALL be used.

It is RECOMMENDED to use standard interfaces according to BioAPI in ISO 19784-1 for capturing the biometric data. The agency operating the e-Gates MAY decide to allow proprietary vendor-specific SDK interfaces for the integration of the capture unit.

5.1.1.2. Functionality

The face capture unit MUST provide facial images to the face verification unit.

The term 'pre-processing' used here means the provision of a face image from a frame, whereas 'quality assessment' means the provision of an appropriate face image from a set of face images.

It is RECOMMENDED to provide pre-processed and quality-assessed images to the verification unit. Pre-processing SHOULD cover at least the following.

- Detecting the face in a frame.
- Cropping the face from the frame.
- De-rotating the face to ensure that the centres of the eyes are nearly on a horizontal line.

It is RECOMMENDED to perform a quality assessment on the images. The quality assessment SHOULD cover at least face- and eye-finding; it MAY contain a quality estimation based on criteria specified in ISO 19794-5. If a quality assessment is performed within the capture unit, the best image according to the applied criteria SHOULD be provided to the verification unit. This speeds up the whole process because template generation and verification on clearly inadequate images is avoided.

The parameters of the camera, the pre-processing and the quality estimation steps MUST 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 ISO 19794-5). Depending on the verification unit, additional characteristics MAY be required.

It is RECOMMENDED to provide uncompressed (e.g. BMP) or lossless compressed live images. Alternatively, non-lossless compression MAY be used, e.g. JPG. In this case it MUST be ensured that the loss of information has no significant impact on the recognition performance of the face verification unit.

The complete process of capturing (including pre-processing, quality assessment and provision of the resulting face image to the face verification unit) SHOULD NOT take more than 1 second per frame.

5.1.2. Face verification unit

5.1.2.3. Architecture and setup

The face verification unit SHOULD run on standard, industrial grade PC hardware. The agency operating the ABC system MAY decide to allow for more complex requirements.

The verification process MAY run locally within each ABC system or as a centralised service.

It is RECOMMENDED to use standard interfaces according to BioAPI [ISO19784-1] for the biometric verification process. The agency operating the ABC system MAY decide to allow proprietary vendor-specific SDK interfaces for the integration of the face verification unit.

5.1.2.4. Functionality

The face verification unit MUST compare the DG2 reference image and the captured live image.

Additionally it is RECOMMENDED to compare the DG2 reference image and the cropped image scanned from the biographical data page. The benefit of this optional check concerns the detection of forged data pages (substitution of printed face image). Note, however, that because of the optical security features within the data page, the comparison of DG2 and cropped image may result in a FRR of about 10 per cent. Thus, this additional check may alert the official to have a more detailed look at the cropped image.

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

One face verification attempt (consisting of template generation and comparison) SHOULD NOT take more than 1 second.

The configuration of the face verification algorithm SHALL ensure a security level in terms of the false accept rate of 0.001 (0.1 per cent) or less. At this configuration (comparison threshold) the FRR SHOULD NOT exceed 0.05 (5 per cent). It is RECOMMENDED that the achievable performance of the face verification algorithm is measured by an independent test laboratory or an official agency. The operating agency SHOULD NOT rely on performance figures given by the algorithm provider only.

The operating agency SHOULD NOT rely solely on the standard configuration of the algorithm provider. 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. 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.

NB: For systems based on the facial image biometric, it is RECOMMENDED to perform the FAR calculation of the ABC system as an independent but parallel process as shown below:

- The reference face images (DG2 images) of the last 10 e-Passport verifications are temporarily and anonymously stored in a dynamic list.
- The live face image from the current face verification process is compared against all other faces in the dynamic list and the comparison scores are saved (impostor comparisons). It has to be ensured that a comparison of face images of the same person, which may happen due to multiple

verification attempts on a particular traveller, is avoided during the process.

- The actual live face image is compared against the corresponding reference face image and the comparison score is saved (genuine comparison).
- The reference face image is added to the dynamic list.
- The oldest face image in the dynamic list and the actual live face image are discarded and deleted safely. Storage and deletion of the face image data has to be implemented in accordance with 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. Attention has to be paid to the statistical base for the FAR calculation. In order to measure the performance of the face verification algorithm up to a FAR security level of 0.001 (0.1 per cent), it is RECOMMENDED to perform the FAR calculation on the basis of at least 30 000 impostor comparisons.

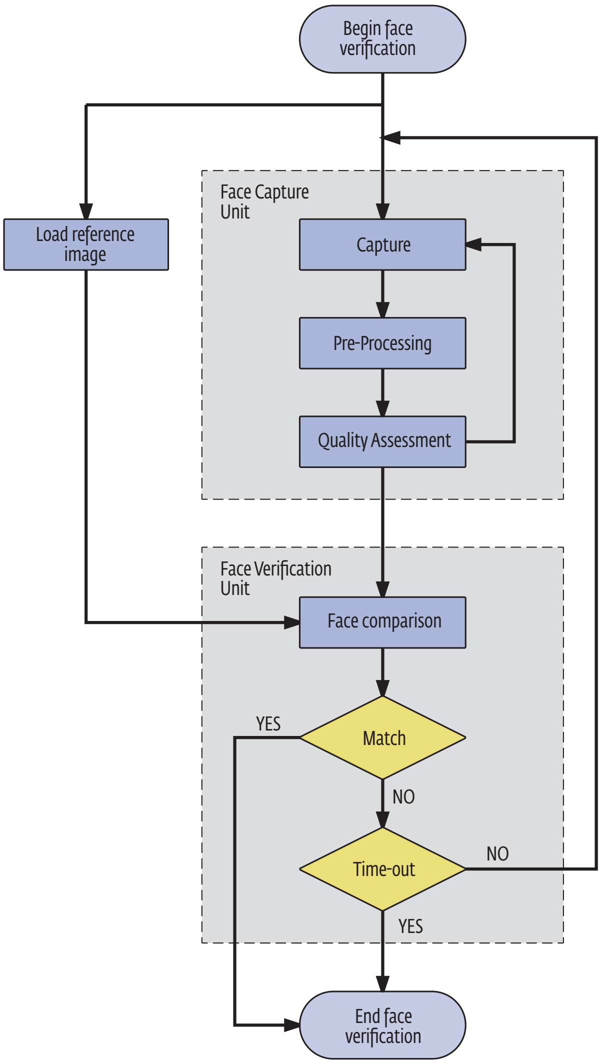
5.1.3. Design of the face capture and verification process

If the face image acquisition and/or the biometric verification are not successful, the process SHALL stop after a time-out. This time-out SHOULD be configurable.

The process design SHALL guide the traveller to look straight into the camera. 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 distract the traveller's attention. The feedback modules (display, LEDs etc.) SHOULD be installed very close to the camera.

The result of the biometric verification process SHALL be provided to a monitoring and control station. At least the overall verification result SHALL be displayed in the summary view appearing on the monitoring screen. Additionally, the image data (DG2 image and live image used for the verification) SHOULD be shown in the summary view on the monitoring screen. It is RECOMMENDED that further details regarding the detailed checks of the biometric verification process are displayed upon request by the operator of the ABC system.

Figure 6: **Face capture and verification process**



The process SHOULD include a fake detection (or liveness detection) mechanism to detect fake attacks or improper use. Therefore, the biometric components MAY provide technical features for fake detection such as dedicated sensors or software-based mechanisms. For this purpose, video streams MAY also be provided to the operator through video surveillance.

A high-level illustration of the RECOMMENDED face capture and verification process is shown in **Figure 6**.

5.2. Fingerprint verification

5.2.1. Fingerprint capture unit

In addition to the guidelines provided in the following sub-sections, it is RECOMMENDED to take account of ISO 19794-4, Annex D 'Conditions for capturing finger image data'.

5.2.1.1. Architecture and setup

Any deployed fingerprint sensor SHOULD comply with the quality specifications from ISO 19794-4, sections B.1 or B.3. The sensor SHALL be able to capture flat fingerprints; additionally it MAY have the capability to capture rolled fingerprints. The minimum capture area SHOULD be 16 mm width and 20 mm height (for single fingerprint sensors).

Optionally, the sensor device MAY provide methods for recalibration in the field or, at least, necessary recalibration MAY be possible for qualified service staff. It is RECOMMENDED that the compliance of the sensor device with the applicable quality standard can be verified at any time in the operational environment.

Any strong light sources SHALL NOT directly illuminate the sensor prism. This applies to all direct light. It is RECOMMENDED to ascertain through testing that the system will perform adequately under different sunlight conditions.

In order to prevent halo effects due to condensation in the captured images, the room temperature SHOULD be set such that large temperature differences between sensor surface and finger(s) are avoided (between 18 °C and 25 °C). Some sensors are able to work under far larger temperature constraints, e.g. because they have heated prisms. Furthermore, for other than indoor use, the chosen sensors should be able to operate under other (usually rougher) environmental constraints.

The unit SHALL be mounted in such a way that users are easily able to position themselves in order to place their hands and thumbs on it. The ideal height for acquisition is elbow height.

The fingerprint capture unit SHOULD give feedback to the traveller. Feedback MAY be given, for example, by:

- a screen attached close to the sensor;
- illuminated pictograms;
- LEDs assigned to pictograms directly on the sensor.

The information listed below SHOULD be given to the user.

- Assistance for finger positioning with images and/or video on the screen and/or audio instructions (e.g. to instruct the user to move fingers to the left/right/top/bottom).
- Visual and/or audio notification when a successful acquisition has been completed.
- A quality indicator for each acquisition. This indicator should be simple, for example a two-state logic (good/bad) or similar.
- If possible, the reason for a bad quality acquisition (e.g. wrong positioning of the hand).

The fingerprint sensor MAY be connected directly to the PC that controls the complete ABC process or indirectly via a pre-processing unit. To connect the capture unit to the control PC, state-of-the-art interfaces (e.g. USB2.0) SHALL be used.

It is RECOMMENDED to use standard interfaces according to BioAPI in ISO 19784-1 for the capturing of the biometric data. The agency operating the ABC system MAY decide to allow proprietary vendor-specific SDK interfaces for the integration of the capture unit.

5.2.1.2. Functionality

The fingerprint capture unit MUST provide fingerprint images for the fingerprint verification unit.

The term 'pre-processing', used henceforth, means the provision of a fingerprint image from a frame, whereas 'pre-qualification' means the provision of an appropriate fingerprint image from a set of fingerprint images.

The activation of the acquisition MUST occur automatically. For the acquisition process, a pre-qualification of the fingerprints to prefer high-quality images is RECOMMENDED. The process of capturing SHOULD prefer the highest quality image of a sequence, or at least the last-captured image (after timeout) of a sequence.

If the sensor was not able to capture an image (e.g. because no finger was placed on it), it is not required to return an image after the time-out. In this case, an adequate error code SHALL be returned.

It is RECOMMENDED to provide pre-processed images to the verification unit. The pre-processing MUST cover at least segmentation (segmentation for single-finger sensors is OPTIONAL).

For this segmentation process, the requirements listed below SHALL be fulfilled.

- The fingerprint capture unit should have the ability to accept rotated fingerprints having the same direction at an angle of up to 45°.
- Rotated fingerprints having the same direction should be corrected to be vertical.
- The first phalanx of the finger should be segmented. Segmentation SHALL occur on uncompressed data.

The fingerprint images provided by the capture unit SHOULD comply with the quality requirements of ISO 19794-4. Depending on the verification unit, additional characteristics MAY be required.

It is RECOMMENDED to provide uncompressed (e.g. BMP) or lossless compressed live images. Alternatively non-lossless compression MAY be used. In this case, fingerprint images should be compressed according to the recommendations of ISO 19794-4, section 8.3.17 'Image compression algorithm'. The compression ratio SHOULD not be too high; a maximum compression ratio of 15 is recommended. The implementation of the WSQ algorithm used SHOULD be certified by the Federal Bureau of Investigation (FBI) and SHOULD be referenced by the respective certificate number (coded in the WSQ header).

Multiple lossy compressions SHOULD be avoided as they harm image quality.

The complete process of capturing (including pre-processing, pre-qualification and provision of the resulting fingerprint image to the fingerprint verification unit) SHOULD NOT take more than 1 second per frame.

REMARK: Because of disabilities or very weak fingerprints, it might not be possible to capture fingerprint images of sufficient quality for a certain number of travellers. This Failure-to-Acquire (FTA) Rate is expected to be lower than 0.03 (3 per cent).

5.2.2. Fingerprint verification unit

5.2.2.3. Architecture and setup

The fingerprint verification unit SHOULD run on standard, industrial grade PC hardware. The agency operating the ABC system MAY decide to allow more complex requirements.

The verification process MAY run locally within each ABC system or as a centralised service.

It is RECOMMENDED to use standard interfaces according to BioAPI ISO 19784-1 for the fingerprint verification process. The agency operating the ABC system MAY decide to allow proprietary vendor-specific SDK interfaces for the integration of the verification unit.

5.2.2.4. Functionality

The fingerprint verification unit MUST compare the DG3 reference image(s) and the captured live image. The verification unit MUST process DG3 reference images stored in WSQ data format. It SHOULD process live images in uncompressed or lossless compressed or WSQ data formats.

One fingerprint verification attempt (consisting of template generation and comparison) SHOULD NOT take more than 1 second.

The configuration of the fingerprint verification algorithm SHALL ensure a security level in terms of FAR of 0.001 (0.1 per cent). At this configuration (comparison threshold) the FRR SHOULD NOT exceed 0.03 (3 per cent).

REMARK: The Operational Reject Rate consists of the algorithm-specific FRR and the additional FTA (see section 5.2.1.2. above).

It is RECOMMENDED that the achievable performance of the fingerprint verification algorithm is measured by an independent test laboratory or an official agency. The operating agency SHOULD NOT rely on performance figures given by the algorithm provider only. 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. 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.

NB: It is RECOMMENDED to perform the FAR calculation for the ABC system as an independent but parallel process as shown below.

- The reference fingerprint images (DG3 images) of the last 10 e-Passport verifications are temporarily and anonymously stored in a dynamic list.
- The live fingerprint image from the actual fingerprint verification process is compared against all other fingerprints in the dynamic list and the comparison scores are saved (impostor comparisons). A comparison of fingerprint images of the same person, which may happen due to multiple verification attempts of the same traveller, should be avoided.
- The actual live fingerprint image is compared against the corresponding reference fingerprint image and the comparison score is saved (genuine comparison).
- The reference fingerprint images are added to the dynamic list.
- The oldest fingerprint images in the dynamic list and the current live fingerprint image are discarded and deleted safely. Storage and deletion of the fingerprint image data has to be implemented in accordance with the applicable data protection regulations.
- The FAR is calculated on the basis of impostor comparison scores. Genuine com-

parison scores MAY be used to calculate the corresponding FRR. Due attention should be paid to the statistical base for the FAR calculation. In order to measure the performance of the fingerprint verification algorithm up to a security level (FAR) of 0.001 (0.1 per cent), it is to perform the FAR calculation on the basis of at least 30 000 impostor comparisons.

5.2.3. Design of the fingerprint capture and verification process

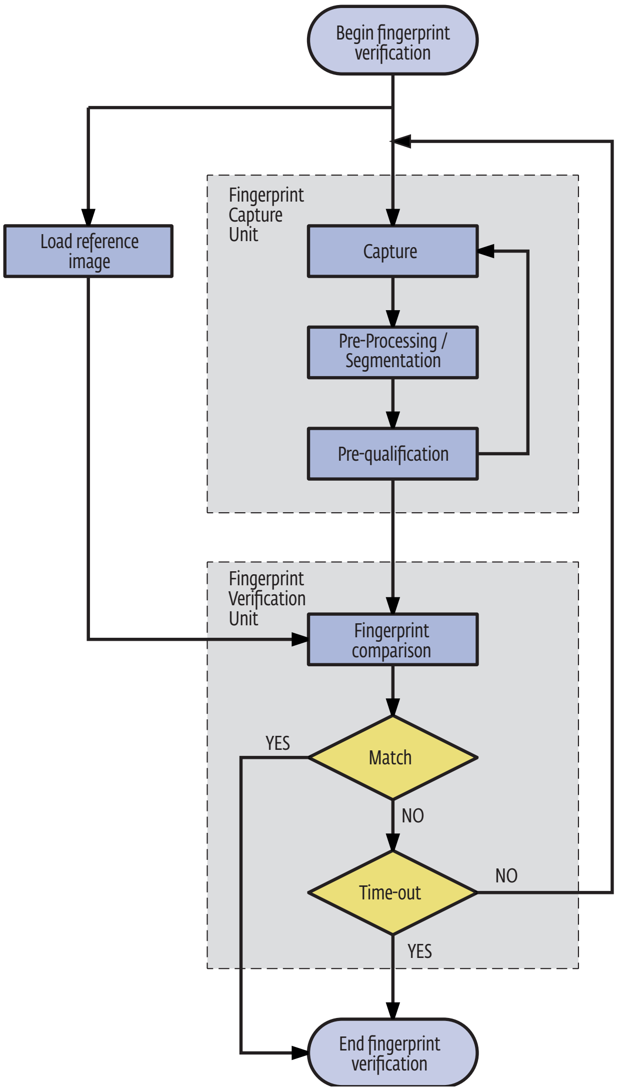
If the fingerprint image acquisition and/or the fingerprint verification are not successful, the process SHALL stop after a time-out. The time-out SHOULD be configurable.

The process and the e-Gate design SHALL guide the traveller directly to the capture unit. While the live fingerprint images are captured, other actions by the traveller SHOULD NOT be necessary and **no** eye-catchers apart from the feedback modules SHOULD distract the traveller's attention. The feedback modules (display, LEDs, etc.) SHOULD be installed very close to the fingerprint sensor device.

The result of the fingerprint verification process SHALL be provided to a monitoring and control station. At least the overall verification result SHALL be displayed in the summary view on the monitoring screen. It is RECOMMENDED that further details regarding the fingerprint verification process be shown upon request by the operator of the ABC system, e.g. the image data (DG3 images and live image used for the verification).

The process SHOULD provide a fake detection (or liveness detection respectively) to detect fake attacks or improper use. Therefore, the biometric components MAY provide technical features for fake detection like dedicated sensors or software-based mechanisms. Respective Common Criteria protection profiles PP0062 or PP0063 MAY be considered. A high-level illustration of the RECOMMENDED fingerprint capture and verification process for ABC systems is shown in **Figure 7**.

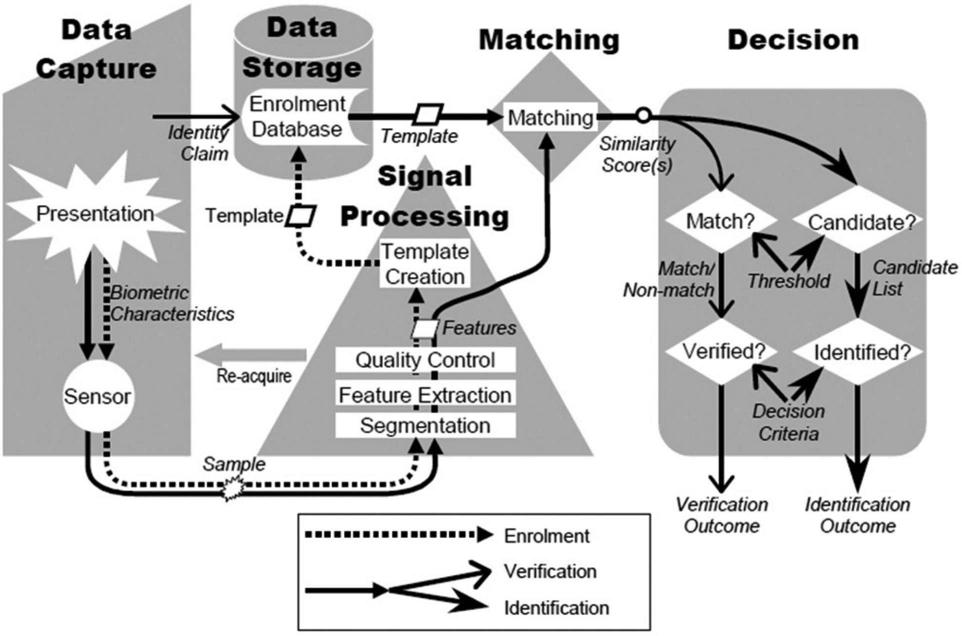
Figure 7: **Fingerprint capture and verification process**


Begin fingerprint verification
Load reference image
Fingerprint Capture Unit
Capture
Pre-Processing / Segmentation
Pre-qualification
Fingerprint Verification Unit
Fingerprint comparison
YES
Match
NO
NO
Time-out
YES
End fingerprint verification

5.3. Multi-biometrics

The general diagram of the biometric system decision process presented in **Figure 8** defines the process of biometric verification in ABC (in this case, 'data storage' is provided by e-MRTDs).

Figure 8: **General diagram of the biometric system decision process. The reproduction of this figure has been authorised by ISO.**



Multi-biometric systems take input from one or more sensors to capture one or several different types of biometric characteristics. In order to enhance the performance of authentication subsystems, multi-biometrics allow for better results than a process based on a single biometric, reducing the risk of false positives and negatives. The use of two or more biometric modalities or other kinds of multi-biometrics MAY be incorporated in national implementations of ABC systems.

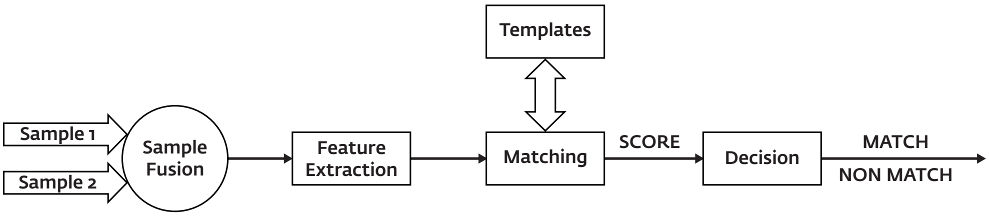
An overview of multi-biometrics is provided in ISO 24722. Several types of multi-biometrics can be applied directly to ABC systems in order to improve their performance and accuracy.

Sample level

The biometric process captures a collection of samples. The fusion process fuses these collections of samples into a single sample.

If this model is used in ABC systems it SHOULD be implemented in the biometric capture unit. A fused image of the biometric feature is then provided to the biometric verification process.

Figure 9: **Sample level fusion in multi-biometric systems (from ISO 24722). The reproduction of this figure has been authorised by ISO.**

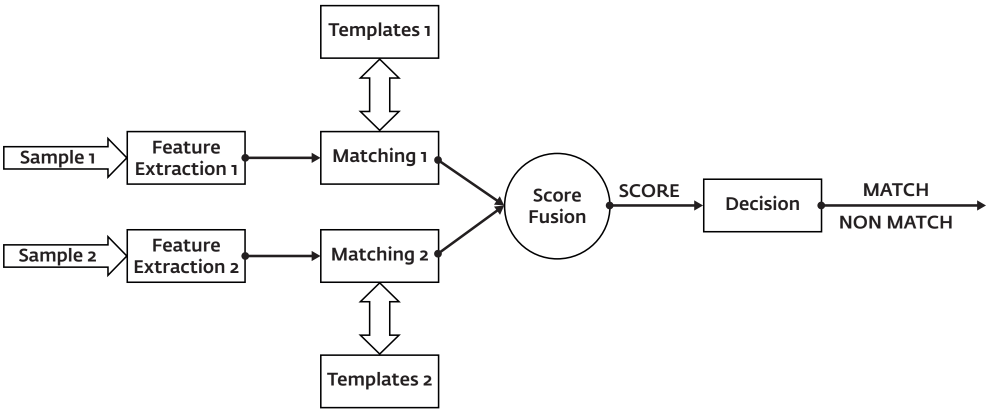


Score level

The biometric process performs several comparisons of samples with the reference image(s) resulting in multiple scores. The fusion process fuses these into a single score, which is then compared to the system acceptance threshold.

If this model is used in ABC systems to fuse different biometric modalities like face and fingerprints, it SHOULD be implemented in a specific verification unit that is able to process the input from several capture units.

Figure 10: **Score level fusion in multi-biometric systems (from ISO 24722). The reproduction of this figure has been authorised by ISO.**

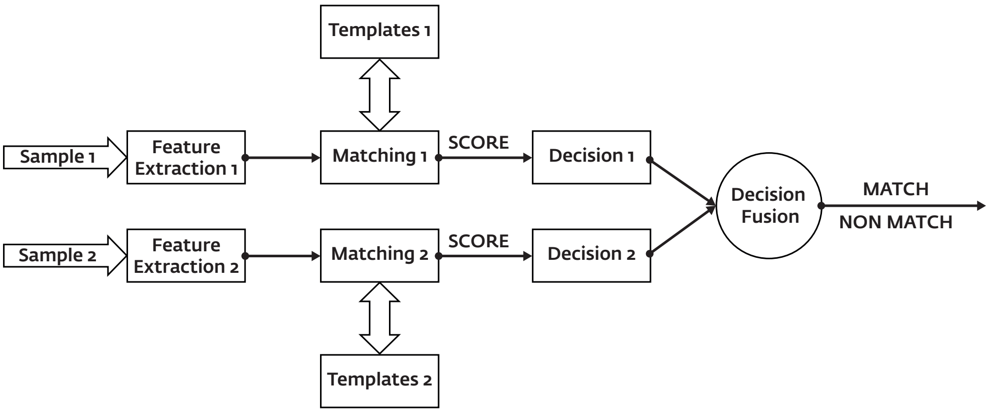


Decision level

Each individual biometric process outputs its own Boolean result. The fusion process fuses them together by a combination algorithm such as AND and OR, possibly taking further parameters such as sample quality scores, environmental conditions, etc. as input.

If this model is used in ABC systems to fuse different biometric modalities like face and fingerprints it SHOULD be implemented at the process level that is able to process the input from several verification units.

Figure 11: **Decision level fusion in multi-biometric systems (from ISO 24722). The reproduction of this figure has been authorised by ISO.**



6. Quality control and quality assurance

Quality control (QC) is the process whereby the quality of all factors involved in the operation and exploitation of the ABC system are measured. Quality assurance (QA) of an ABC service as such, in more practical terms, is the perception of the degree to which it meets the expectations of travellers and border management authorities.

Quality control is of importance when assessing the performance of a given ABC system and for identifying potential problems in its operation. Therefore, this section focuses on the minimum recommended anonymous operational data to be collected for QC/QA and the extraction of business statistics from ABC systems.

While QC/QA and statistical analysis are not part of the core functionality of an ABC system, it is nevertheless highly RECOMMENDED to implement them. This section should be read as a set of REQUIREMENTS and RECOMMENDATIONS for those cases where the system designer decides to provide data storage for QC/QA and statistical analysis.

Note that the following aspects are explicitly **out of the scope** of this document.

- Specific details on how to encode each data item to be stored.
- Specific tools for statistical analysis and performance indicator definition.

6.1. General recommendations

The following requirements and recommendations are broadly applicable when designing the dataset to be stored for QC/QA and statistics extraction.

Any set of operational data to be stored on a permanent basis in an ABC system MUST comply with the limitations imposed by national and EU Data Protection regulations[16]. Therefore personal data SHALL NOT be stored for the purposes of QC/QA and statistics extraction unless properly anonymised.

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

Anonymous operational data is stored in a centralised way at least at the ABC installation level (i.e. at the group of e-Gates and monitoring and control stations at a given airport/port hall). Detailed maintenance and SW debug traces MAY be stored at the local level (e.g. at a given e-Gate computer), since such data is unlikely to be of use when analysing operational performance.

It is RECOMMENDED that a clear interface for data extraction is offered, since providing built-in statistical analysis is out of the scope of the basic functionality of an ABC system.

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

[16] See in particular Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

at least the following types of transactions SHOULD be logged.

- Access attempts with documents not accepted by the system (e.g. non-electronic passports).
- Access attempts with non-eligible documents (e.g. third country nationals holding an e-Passport).
- Access attempts by an eligible traveller with a valid e-Passport but whose verification was not successful (e.g. 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. When a field within the transaction entry cannot be filled (e.g. unknown nationality or check not applicable for a document), a distinctive value MUST be used as placeholder, so that these gaps can be easily identified when processing the data.

The following sections add details concerning the sorts of data which are of interest when logging for QC/QA and performance analysis.

6.2. Access data

In all cases, the data entry MUST be time-stamped to allow for detailed performance and trend analysis.

In all cases, a data entry MUST include a specific field summarising the final outcome of the verification process, that is, whether the traveller was granted permission to cross the border without further manual action by the officers monitoring the BCP. In its simplest form this can be a Boolean value, or MAY include other information regarding the type(s) of failure of the verification process. Although, as depicted in the following sections, such details SHOULD be stored separately, so that changes in access logic (the decision tree in charge of granting or denying authorisation for border crossing to a traveller) affecting the outcome of the ABC verification process do not hide the result of each sub-process.

It is RECOMMENDED that the following traveller information is part of a data entry:

- nationality of the document issuer;
- age (or alternatively age bands, e.g. 21–25, 26–35…);
- gender.

It is RECOMMENDED that the timing information shown below is included in a data entry.

- Total verification time: defined as the time needed to fully verify an eligible traveller, regardless of the outcome of each particular check (document authentication, biometric verification, background checks, etc.).
- Total access time: defined as the total time spent in the process by an eligible traveller since the first interaction with the system (i.e. presentation of the travel document in an integrated two-step process ABC system, entry in the mantrap space in a one-step process ABC system, first interaction with the verification modules in a single e-Gate or segregated two-step process solution). The exact definition and estimate of this time will ultimately depend on the architecture of the system (e.g. when the full verification process takes place within a mantrap, this time measurement will always be greater than the verification time).

6.3. ABC installation data

It is RECOMMENDED that each ABC installation is uniquely identified within a national ABC deployment. It is RECOMMENDED that the identifier shows:

- a clear identification of the BCP (e.g. airport moniker);
- detailed information regarding the location within the BCP (e.g. terminal number, floor, arrival/departure hall number);
- information regarding the type of BCP: entries or exits.

It is RECOMMENDED that every component of an ABC installation is uniquely identified. This identification SHOULD be done at least at the verification and access module level, although a finer granularity MAY be used for maintenance logging purposes. It is RECOMMENDED that the identifier includes the details shown below.

- Module type (e.g. verification, access, monitoring).
- Module number. When numbering modules within a given ABC installation, designers SHOULD find the adequate criteria for numbering consistency in a given installation and across all the ABC system locations (e.g. the lower numbers are given to modules closest to the actual exit of the installation).

6.4. Document authentication data

It is RECOMMENDED to include a subsystem for the logging of statistical and technical data regarding the document authentication process, for the purpose of having continuous quality control, the extraction of business statistics and the improvement of the ABC system.

It is RECOMMENDED that the following details on the document inserted are included in each data entry:

- issuing country and date of expiry of the e-Passport (if allowed by the applicable national data protection regulations);
- date of issue (if extracted from the VIZ);
- e-Passport type (e.g. first or second generation e-Passport).

It is RECOMMENDED that the following details of a document electronic and optical authentication processes shown below are part of a data entry.

- Time period dedicated to the document authentication process as a whole (i.e. from the beginning of optical image capturing until the provision of the final document authentication result).
- Time period dedicated to the optical document checks.
- Time period dedicated to the RF chip reading process.
- Time period dedicated to the verification of the e-Passport data.
- Outcome of each of the authentication checks actually performed in the document, depending on the type of document and the authentication algorithm used. At least a Boolean value for each of the checks SHOULD be included, although the designer MAY choose to include more details on each field (e.g. indicating that a given check is/is not supported by the document being read).
- Result of the optical document check and results of each optical sub-step (B900 ink, UV-Brightness, MRZ consistency, etc.).
- Result of the e-Passport data authentication process and results of each authentication sub-step (EF.SOD verification, DS certificate signature verification, certificate validity period, etc.).
- Dump of the DS certificate used for the EF.SOD verification.
- Error messages from the particular process steps and document reader unit.

6.5. Biometric verification data

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 continuous quality control, the extraction of business statistics and the introduction of improvement to the ABC system. 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.

- Total time of the biometric verification process (i.e. from the beginning of the image capture until the provision of the final verification result).
- 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.
- Best quality score of all successfully captured facial images.
- The threshold against which the verification scores were compared.

For any other biometric verification which might be part of the system, it is RECOMMENDED that at least the following data is part of an entry.

- Time effort for the biometric verification process (i.e. from the beginning of the live sample capturing until the provision of the final verification result).
- Overall result of the verification process or, alternatively, the verification score and comparison threshold.
- Quality indicator of the best live sample (e.g. NIST NFIQ score for a fingerprint).
- Quality indicator of the reference image, if available (e.g. NIST NFIQ score for the fingerprint stored in DG3).

6.6. Other Data Sets

Depending on the exact features of the border control process, an ABC system MAY run other background checks in parallel with the document authentication and biometric verification checks. It is assumed that these background checks are performed by accessing systems external to the ABC (such as a query to a Lost & Stolen Document Database). For these background checks, it is RECOMMENDED that at least the following data is included within an entry:

- total connection (round-trip) time;
- overall result of the check.

For segregated two-step process systems in which access tokens are used, the data shown below SHOULD be part of an entry.

- If a physical token is issued, its serial number or any other identifier the token may carry.
- If a biometric token is used, the quality of the ‘enrolment sample’ captured at the verification module (e.g. NIST NFIQ score for a fingerprint).
- Total time invested in token generation or capture at the verification module.
- For successful verifications and token generation/capture, delays between the completion of the verification process and the crossing of one of the access modules. If the delay is too great or the crossing process is discarded by the border guard officer, this SHOULD be clearly indicated as a process abandoned or aborted by the officer.
- If a biometric token is used, the quality of the live sample captured at the access module (e.g. NIST NFIQ score for a fingerprint).
- Total time invested in token reading/capture and authentication/verification at the access module.
- Overall result of token reading/capture and authentication/verification at the access module.

Annex 1: References

Bradner, Scott. Key Words for Use in RFCs to Indicate Requirement Levels. BCP 14, RFC 2119, March 1997.

Bretschneider, Stuart, Frederick J. Marc-Aurele, and Jiannan Wu. 'Best practices' research: a methodological guide for the perplexed. *Journal of Public Administration Research and Theory* 15.2 (2005), pp. 307–323.

Council of Europe. European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos 11 and 14. 4 November 1950, ETS 5.Council of the European Union. EU Schengen Catalogue: External borders control, Return and readmission- Recommendations and best practices, Council document No 7864/09, 19 March 2009, p.6.

European Commission. 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.

European Commission. Communication of 13 February 2008 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Preparing the next steps in border management in the European Union, COM(2008) 69 final, 13.2.2008.

European Commission. Memo. 'Smart Borders': for an open and secure Europe, 28 February 2013.

European Council. The Stockholm Programme – An open and secure Europe serving and protecting citizens, OJ C 115, 4 May 2010, pp. 1–38.

European Migration Network. *Glossary* [last accessed: 30 June 2015].

European Union. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995, pp. 31–50.

European Union. 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, OJ L 385, 29 December 2004, pp. 1–6.

European Union. Regulation (EC) No 444/2009 of 28 May 2009 amending 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, OJ L 142, 6 June 2009, pp. 1–4.

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).

Eurostat. *Glossary* [last accessed: 30 June 2015].

Federal Office for Information Security (BSI). *Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP)*, Version 1.7, 2010 [PP0062].

Federal Office for Information Security (BSI). *Fingerprint Spoof Detection Protection Profile (FSDPP)*, Version 1.8, 2010 [PP0063].

Federal Office for Information Security (BSI). *Technical Guideline TR-03110 – Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token*, Parts 1, 2, 3 and 4, Version 2.20, 2015 [BSI03110].

Federal Office for Information Security (BSI). *Technical Guideline TR-03121 – Biometrics for Public Sector Applications*, Parts 1, 2 and 3, Version 3.0, 2013 [BSI03121].

Federal Office for Information Security (BSI). *Technical Guideline TR-03129 – PKIs for Machine Readable Travel Documents*, Part 1 and 2, Version 1.10, 2014 [BSI03129].

Federal Office for Information Security (BSI). *Technical Guideline TR-03135 – Machine Authentication of MRTDs for Public Sector Applications*, Version 2.0, 2014 [BSI03135].

Frontex. *Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Crossing Systems*, Version 1.1 March 2011.

Frontex. *Best Practice Operational Guidelines for Automated Border Control (ABC) Systems*, Version 2.1. June 2015.

Frontex. *Discussion paper on Public Key Infrastructure (PKI) and operational challenges of certificate exchange/management at the borders*, 14 June 2012.

Frontex. *Operational and Technical security of Electronic Passports*, July 2011.

ICAO. *A Primer on the ICAO Public Key Directory – White Paper*, Version 1.5, 20 May 2009.

ICAO. *Doc9303 – Machine Readable Travel Documents*, Part 1 Vol. 2 (second edition, 2006) and Part 3 Vol. 2 (third edition, 2008) [ICAO9303].

ICAO. *MRTD Glossary* [last accessed: 30 June 2015].

ICAO. *Supplemental Access Control for Machine Readable Travel Documents*, Version 1.1, 15 April 2014 [ICAOSAC].

ISO/IEC 14443, *Identification cards – Contactless integrated circuit cards – Proximity cards*, Parts 1–4 [ISO 14443].

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

ISO/IEC 19794-2:2011, *Information technology – Biometric data interchange formats*, Part 2: Finger minutia data [ISO 19794-2].

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

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

ISO/IEC 2382-37:2012, *Information technology – Vocabulary – Part 37: Harmonized biometric vocabulary* [ISO 2382-37].

ISO/IEC 7816-11:2004, *Identification cards – Integrated circuit cards*, Part 11: Personal verification through biometric methods [ISO 7816-11].

ISO/IEC TR 24722:2007, *Information technology – Biometrics – Multimodal and other multibiometric fusion* [ISO 24722].

ISO/IEC TR 24741:2007, *Information technology – Biometrics Tutorial* [ISO 24741].

Oxford University Press. *Oxford Dictionaries* [last accessed June 2015].

Ongaro, Edoardo. *A protocol for the extrapolation of 'Best' Practices: How to draw lessons from one experience to improve public management in another situation.* European Public Sector Award 2009, Final Symposium and Ceremony, Maastricht, 2009 [last accessed: 30 June 2015].

RFC 3369, *Cryptographic Message Syntax (CMS)*, August 2002 [RFC3369].

Veselý, Arnošt. Theory and Methodology of Best Practice Research: A Critical Review of the Current State, *Central European Journal of Public Policy*, Vol. 5, No 2, December 2011, pp. 98–117.

Annex 2: Additional reading

Biometrics

This section lists additional, publicly available references on biometrics for ABC systems.

Software Architecture An example of detailed requirements on the software architecture can be found in BSI 03121-1 and BSI 03121-2.

Process of Biometric Verification An example of detailed requirements on the process of biometric verification based on live captured face images can be found in BSI 03121-3, sections 'Verification of e-Passport and Identity Card using facial biometrics' and 'P-PH-VID'.

Face Capture Unit An example of detailed requirements on the functionality of the face capture unit can be found in [BSI03121-3], sections 'BIP-PH-VID', 'QA-PH-VID', and 'COM-PH-VID'.

Operational Issues An example of detailed requirements on the operational issues and can be found in [BSI03121-3], section 'O-PH-VID'.

User Interface An example of detailed requirements on the user interfaces can be found in [BSI03121-3], section 'UI-PH-VID'.

Evaluation of Error Rates An example workflow and architecture for obtaining impostor and genuine comparison scores for calculating FAR and FRR is described in [BSI03121-3], section 'P-PH-VID'.

Quality Control and Business Statistics An example of a detailed logging scheme can be found in [BSI03121-3], sections 'COD-PH-VID', and 'LOG-PH-VID'.

Document readers and document authentication

This section lists additional, publicly available references on document readers and document authentication processes for ABC systems.

Document Reader Requirements An example of detailed technical requirements and performance capabilities on document readers can be found in BSI 03135, section 3.

Authentication of MRTDs An example of detailed requirements on the process of document authentication and a comprehensive description of the procedures that compose a full featured MRTD inspection can be found in BSI03135, section 4.

In order to verify the compliance of e-MRTD authentication subsystems (e.g. electronic document reader hardware and software) to the relevant ISO and ICAO standards (especially ISO 14443, ISO 7816 and ICAO 9303), it is common to rely on established evaluation and certification schemes. Examples of independent or official evaluation and certification schemes are:

- Federal Office for Information Security: Technical Guideline TR-03105 – Conformity Tests for Official Electronic ID Documents, Part 4: Test plan for ICAO compliant Proximity Coupling Device (PCD) on Layer 2–4 BSI 03105-4.
- Federal Office for Information Security: Technical Guideline TR-03105 – Conformity Tests for Official Electronic ID Documents, Part 5.1: Test plan for ICAO compliant Inspection Systems with EACv1 BSI 03105-51.

Annex 3: Overview of ABC systems in the EU / Schengen Area

1 Selected TCNs eligible for ABC processing:
DE – RTP for citizens of the US and Hong Kong
FI – Japanese, South Korean, US, Canadian and New Zealand nationals who hold an e-Passport
FR – TCNs who are family members of EU citizens
NL – US citizens who register with a dedicated RTP programme
PT – RTP for Angolan citizens
UK – RTP for citizens of the US, Australia, New Zealand, Canada and Japan

2 The system is being implemented within the frames of the FP7 by the Project Consortium.

3 At the time of writing Belgian ABC system is expected to be operational in June 2015.

4 The fingerprint verification functionality is a part of the system, however, at the time of writing, it is not operational.

5 At the time of writing Danish ABC system is expected to be operational on 1 December 2015.

6 Spain has implemented both 1-step and 2-step segregated solutions; in case of the 1-step solution there are 12 e-Gates, while in case of the 2-step segregated solution there are 19 kiosks and 4 e-Gates.

7 Eligible travellers who do not hold an e-Passport can register in a dedicated database.

8 The ABC system in Norway has been originally envisaged to cater for all EU/EEA/CH citizens of the age of 18 and older who are holders of an e-passport; however, due to unavailability of verified certificates from other MSs, currently, only NO/SE/UK/FI/DK/IS citizens are eligible to use the system.

9 The fingerprint verification functionality is a part of the system, however, at the time of writing, it is not operational.

MS	Status			Eligible pax			Eligible document		Biometrics		Configuration			Owner			Operator			System provider(s)	Number of:	
	Operational	Pilot	Planned	Age	Nationality	Selected TCN1	ePassport	National eID	Face	Finger	1-step	2-step integrated	2-step segregated	Border/State Authority	Airport Authority	System provider	Border Authority	Airport Authority	System provider	System provider	Kiosks	E-gates
AT		■		≥18	EU/EEA/CH		■		■			■			■[2]		■			Project Consortium		1
BE			■[3]				■		■		■									Vision Box		6
BG	■			≥18	EU/EEA/CH		■	■	■	■[4]		■		■			■			Atos Bulgaria, Vision Box		16
CZ	■			≥15	EU/EEA/CH		■		■			■		■			■			L-1 Ident ity Solutions, Magnetic Autocontrol, Vitkovice Solution, Secunet		3
DE	■			≥18	EU/EEA/CH	■	■	■	■			■		■			■			Bundesdruckerei GmbH and Secunet Security Networks AG		117
DK			■[5]		EU/EEA/CH		■		■			■		■			■			Vision Box		9
EE	■			≥15	EU/EEA/CH		■		■	■			■	■			■			Vision Box	6	2
ES	■			≥18	EU/EEA/CH		■	■	■	■	■		■	■			■			Indra, Gunnebo, Neurotechnology	19	166
FI	■			≥18	EU/EEA/CH	■	■		■			■		■			■			Vision-Box		38
FR	■			≥18	EU/EEA/CH	■	■[7]		■	■		■		■			■			Morpho		41
HU	■			≥18	EU/EEA/CH		■	■	■	■			■	■			■			ARH Zrt.	4	1
IE		■		≥18	EU/EEA/CH		■		■			■		■			■			SITA, Accenture		4
IS			■				■															
IT	■			≥18	EU/EEA/CH		■		■	■	■	■		■			■			SITA		8
LV			■		EU/EEA/CH		■		■		■											2
NL	■			≥18	EU/EEA/CH	■	■		■							■	■			Accenture, Vision Box		36
NO	■			≥18	NO/SE/UK/ FI/DK/IS		■		■			■		■			■			Gemalto, Vision-Box		4
PT	■			≥18	EU/EEA/CH	■	■		■	■[9]		■		■			■			Vision-Box		81
RO			■				■		■		■			■			■	■				2
UK	■			≥18	EU/EEA/CH	■	■		■		■	■		■			■			Fujitsu, Vision Box, Accenture		111

FRONTEX

European Agency for the Management
of Operational Cooperation
at the External Borders of the Member
States of the European Union

Plac Europejski 6
00-844 Warsaw, Poland

T +48 22 205 95 00
F +48 22 205 95 01

frontex@frontex.europa.eu
www.frontex.europa.eu

Print version:
TT-02-16-152-EN-C
ISBN 978-92-95205-51-2
DOI 10.2819/86138

Online version:
TT-02-16-152-EN-N
ISBN 978-92-95205-50-5
DOI 10.2819/39041